

# DOCUMENTA MATHEMATICA

Extra Volume

## PROCEEDINGS OF THE INTERNATIONAL CONGRESS OF MATHEMATICIANS

Berlin 1998, August 18 - 27

### **Volume I : Plenary Lectures and Ceremonies** (662 pages)

- [Ceremonies](#) (p. 11-98)
- [The Work of the Fields Medalists and the Rolf Nevanlinna Prize Winner](#) (p. 99-142)
- [Invited One-Hour Plenary Lectures](#) (p. 143-606)
- [Lectures by the Fields Medalists and the Rolf Nevanlinna Prize Winner](#) (p. 607-632)
- [Appendix](#) (p. 633-658)  
(Three Invited Forty-Five Minute Lectures not included in Volumes II and III)
- Author Index for Volumes I, II, III: (p. 659-662)

### **Volume II : Invited Lectures** (881 pages)

Invited Forty-Five Minute Lectures at the Section Meetings, Sections 1 - 9

- [1. Logic](#) (p. 11-54), see also [Appendix Vol. I](#)
- [2. Algebra](#) (p. 55-140)
- [3. Number Theory and Arithmetic Algebraic Geometry](#) (p. 141-228)
- [4. Algebraic Geometry](#) (p. 229-288)
- [5. Differential Geometry and Global Analysis](#) (p. 289-422)
- [6. Topology](#) (p. 423-506)
- [7. Lie Groups and Lie Algebras](#) (p. 507-616)
- [8. Analysis](#) (p. 617-764)
- [9. Ordinary Differential Equations and Dynamical Systems](#) (p. 765-878)
- Author Index for Volumes II, III: (p. 879-881)

### **Volume III : Invited Lectures** (825 pages)

Invited Forty-Five Minute Lectures at the Section Meetings, Sections 10 - 19

- [10. Partial Differential Equations](#) (p. 11-98), see also [Appendix Vol. I](#)
- [11. Mathematical Physics](#) (p. 99-204)
- [12. Probability and Statistics](#) (p. 205-332)
- [13. Combinatorics](#) (p. 333-422)
- [14. Mathematical Aspects of Computer Science](#) (p. 421-480)
- [15. Numerical Analysis and Scientific Computing](#) (p. 481-544)
- [16. Applications](#), see also [Appendix Vol. I](#) (p. 545-644)
- [17. Control Theory and Optimization](#) (p. 645-719)
- [18. Teaching and Popularization of Mathematics](#) (p. 719-788)
- [19. History of Mathematics](#) (p. 789-822)
- Author Index for Volumes II, III: (p. 823-825)

ICM 1998  
CONTENTS OF VOLUMES I, II, AND III

Preface .....	I	11
Past Congresses .....	I	12
Past Fields Medalists and Rolf Nevanlinna Prize Winners .....	I	13
MARTIN GRÖTSCHEL: Organization of the Congress .....	I	15
The Committees of the Congress .....	I	19
List of Donors .....	I	21
Opening Ceremony .....	I	23
YURI I. MANIN: Presentation of the Fields Medals and a Special Tribute .....	I	45
DAVID MUMFORD: Presentation of the Rolf Nevanlinna Prize .....	I	49
Fax to the Federal President and to the Governing Mayor .....	I	50
Closing Ceremony .....	I	53
List of Participants .....	I	61
Participants by Country .....	I	96

THE WORK OF THE FIELDS MEDALISTS  
AND OF THE ROLF NEVANLINNA PRIZE WINNER

PETER GODDARD: The Work of Richard Ewen Borcherds .....	I	99
BÉLA BOLLOBÁS: The Work of William Timothy Gowers .....	I	109
CLIFFORD HENRY TAUBES: The Work of Maxim Kontsevich .....	I	119
STEVE SMALE: The Work of Curtis T. McMullen .....	I	127
RONALD GRAHAM: The Work of Peter W. Shor .....	I	133

INVITED ONE-HOUR PLENARY LECTURES

JEAN-MICHEL BISMUT: Local Index Theory and Higher Analytic Torsion .....	I	143
CHRISTOPHER DENINGER: Some Analogies Between Number Theory and Dynamical Systems on Foliated Spaces .....	I	163
PERSI DIACONIS: From Shuffling Cards to Walking Around the Building: An Introduction to Modern Markov Chain Theory .....	I	187
GIOVANNI GALLAVOTTI: Chaotic Hypothesis and Universal Large Deviations Properties .....	I	205
WOLFGANG HACKBUSCH: From Classical Numerical Mathematics to Scientific Computing .....	I	235
HELMUT H. W. HOFER: Dynamics, Topology, and Holomorphic Curves .....	I	255
EHUD HRUSHOVSKI: Geometric Model Theory .....	I	281
I. G. MACDONALD: Constant Term Identities, Orthogonal Polynomials, and Affine Hecke Algebras .....	I	303
STÉPHANE MALLAT: Applied Mathematics Meets Signal Processing ..	I	319
DUSA MCDUFF: Fibrations in Symplectic Topology .....	I	339

TETSUJI MIWA: Solvable Lattice Models and Representation Theory of Quantum Affine Algebras .....	I	359
JÜRGEN MOSER: Dynamical Systems – Past and Present .....	I	381
GEORGE PAPANICOLAOU: Mathematical Problems in Geophysical Wave Propagation .....	I	403
GILLES PISIER: Operator Spaces and Similarity Problems .....	I	429
PETER SARNAK: L-Functions .....	I	453
PETER W. SHOR: Quantum Computing .....	I	467
KARL SIGMUND: The Population Dynamics of Conflict and Cooperation .....	I	487
MICHEL TALAGRAND: Huge Random Structures and Mean Field Models for Spin Glasses .....	I	507
CUMRUN VAFA: Geometric Physics .....	I	537
MARCELO VIANA: Dynamics: A Probabilistic and Geometric Perspective .....	I	557
VLADIMIR VOEVODSKY: $\mathbf{A}^1$ -Homotopy Theory .....	I	579

LECTURES BY THE FIELDS MEDALISTS  
AND BY THE ROLF NEVANLINNA PRIZE WINNER

RICHARD E. BORCHERDS: What is Moonshine? .....	I	607
W. T. GOWERS: Fourier Analysis and Szemerédi's Theorem .....	I	617
CURTIS T. McMULLEN: Rigidity and Inflexibility in Conformal Dynamics .....	II	841
see also: .....	I	630
PETER W. SHOR: Quantum Computing .....	I	467

APPENDIX: INVITED FORTY-FIVE MINUTE LECTURES  
AT THE SECTION MEETINGS

This appendix contains three manuscripts of Invited Speakers  
which are not included in Volume II or III

SECTION 1. LOGIC:		
A. J. WILKIE: O-Minimality .....	I	633
SECTION 10. PARTIAL DIFFERENTIAL EQUATIONS:		
MIKHAIL SAFONOV: Estimates Near the Boundary for Solutions of Second Order Parabolic Equations .....	I	637
SECTION 12. PROBABILITY AND STATISTICS:		
F. GÖTZE: Errata: Lattice Point Problems .....	I	648
SECTION 16. APPLICATIONS:		
SERAFIM BATZOGLOU, BONNIE BERGER, DANIEL J. KLEITMAN, ERIC S. LANDER, AND LIOR PACHTER: Recent Developments in Computational Gene Recognition .....	I	649
AUTHOR INDEX FOR VOLUMES I, II, AND III .....	I	659

INVITED FORTY-FIVE MINUTE LECTURES  
AT THE SECTION MEETINGS  
CONTENTS OF VOLUMES II AND III

In case of several authors, Invited Speakers are marked with a \*.  
The author index is at the end of each of these two volumes.

SECTION 1. LOGIC

MATTHEW FOREMAN: Generic Large Cardinals: New Axioms for Mathematics? .....	II	11
GREG HJORTH: When is an Equivalence Relation Classifiable? .....	II	23
LUDOMIR NEWELSKI: Meager Forking and m-Independence .....	II	33
STEVO TODORCEVIC: Basis Problems in Combinatorial Set Theory ..	II	43

SECTION 2. ALGEBRA

ERIC M. FRIEDLANDER: Geometry of Infinitesimal Group Schemes ..	II	55
SERGEI V. IVANOV: On the Burnside Problem for Groups of Even Exponent .....	II	67
WILLIAM M. KANTOR: Simple Groups in Computational Group Theory .....	II	77
GUNTER MALLE: Spetses .....	II	87
ALEKSANDR V. PUKHLIKOV: Birational Automorphisms of Higher-Dimensional Algebraic Varieties .....	II	97
IDUN REITEN: Tilting Theory and Quasitilted Algebras .....	II	109
JEREMY RICKARD: The Abelian Defect Group Conjecture .....	II	121
ANER SHALEV: Simple Groups, Permutation Groups, and Probability	II	129

SECTION 3. NUMBER THEORY AND ARITHMETIC ALGEBRAIC GEOMETRY

VLADIMIR G. BERKOVICH: p-Adic Analytic Spaces .....	II	141
PIERRE COLMEZ: Représentations p-Adiques d'un Corps Local .....	II	153
W. DUKE: Bounds for Arithmetic Multiplicities .....	II	163
FRANÇOIS GRAMAIN: Quelques Résultats d'Indépendance Algébrique	II	173
LOÏC MEREL: Points Rationnels et Séries de Dirichlet .....	II	183
SHINICHI MOCHIZUKI: The Intrinsic Hodge Theory of p-Adic Hyperbolic Curves .....	II	187
HANS PETER SCHLICKWEI: The Subspace Theorem and Applications	II	197
TAKESHI TSUJI: p-Adic Hodge Theory in the Semi-Stable Reduction Case .....	II	207
SHOU-WU ZHANG: Small Points and Arakelov Theory .....	II	217

SECTION 4. ALGEBRAIC GEOMETRY

PAUL S. ASPINWALL: String Theory and Duality .....	II	229
VICTOR V. BATYREV: Mirror Symmetry and Toric Geometry .....	II	239
MAURIZIO CORNALBA: Cohomology of Moduli Spaces of Stable Curves	II	249

A. J. DE JONG: Barsotti-Tate Groups and Crystals .....	II	259
MARK L. GREEN: Higher Abel-Jacobi Maps .....	II	267
M. KAPRANOV: Operads and Algebraic Geometry .....	II	277

#### SECTION 5. DIFFERENTIAL GEOMETRY AND GLOBAL ANALYSIS

DMITRI BURAGO: Hard Balls Gas and Alexandrov Spaces of Curvature Bounded Above .....	II	289
TOBIAS H. COLDING: Spaces with Ricci Curvature Bounds .....	II	299
S. K. DONALDSON: Lefschetz Fibrations in Symplectic Geometry ....	II	309
BORIS DUBROVIN: Geometry and Analytic Theory of Frobenius Manifolds .....	II	315
YAKOV ELIASHBERG: Invariants in Contact Topology .....	II	327
S. GALLOT: Curvature-Decreasing Maps are Volume-Decreasing .....	II	339
GERHARD HUISKEN: Evolution of Hypersurfaces by Their Curvature in Riemannian Manifolds .....	II	349
DOMINIC JOYCE: Compact Manifolds with Exceptional Holonomy ....	II	361
FRANÇOIS LABOURIE: Large Groups Actions on Manifolds .....	II	371
JOACHIM LOHKAMP: Curvature Contents of Geometric Spaces .....	II	381
FRANZ PEDIT AND ULRICH PINKAL*: Quaternionic Analysis on Riemann Surfaces and Differential Geometry .....	II	389
LEONID POLTEROVICH: Geometry on the Group of Hamiltonian Diffeomorphisms .....	II	401
YONGBIN RUAN: Quantum Cohomology and its Application .....	II	411

#### SECTION 6. TOPOLOGY

A. N. DRANISHNIKOV: Dimension Theory and Large Riemannian Manifolds .....	II	423
W. G. DWYER: Lie Groups and p-Compact Groups .....	II	433
RONALD FINTUSHEL* AND RONALD J. STERN*: Constructions of Smooth 4-Manifolds .....	II	443
MICHAEL H. FREEDMAN: Topological Views on Computational Complexity .....	II	453
MARK MAHOWALD: Toward a Global Understanding of $\pi_*(S^n)$ .....	II	465
TOMOTADA OHTSUKI: A Filtration of the Set of Integral Homology 3-Spheres .....	II	473
BOB OLIVER: Vector Bundles over Classifying Spaces .....	II	483
CLIFFORD HENRY TAUBES: The Geometry of the Seiberg-Witten Invariants .....	II	493

#### SECTION 7. LIE GROUPS AND LIE ALGEBRAS

JAMES ARTHUR: Towards a Stable Trace Formula .....	II	507
JOSEPH BERNSTEIN: Analytic Structures on Representation Spaces of Reductive Groups .....	II	519
IVAN CHEREDNIK: From Double Hecke Algebra to Analysis .....	II	527
ALEX ESKIN: Counting Problems and Semisimple Groups .....	II	539

ROBERT E. KOTTWITZ: Harmonic Analysis on Semisimple p-Adic Lie Algebras .....	II	553
L. LAFFORGUE: Chtoucas de Drinfeld et Applications .....	II	563
SHAHAR MOZES: Products of Trees, Lattices and Simple Groups .....	II	571
VERA SERGANOVA: Characters of Irreducible Representations of Simple Lie Superalgebras .....	II	583
KARI VILONEN: Topological Methods in Representation Theory .....	II	595
MINORU WAKIMOTO: Representation Theory of Affine Superalgebras at the Critical Level .....	II	605

## SECTION 8. ANALYSIS

KARI ASTALA: Analytic Aspects of Quasiconformality .....	II	617
MICHAEL CHRIST: Singularity and Regularity — Local and Global ...	II	627
NIGEL HIGSON: The Baum-Connes Conjecture .....	II	637
MICHAEL T. LACEY: On the Bilinear Hilbert Transform .....	II	647
PERTTI MATTILA: Rectifiability, Analytic Capacity, and Singular Integrals .....	II	657
VITALI MILMAN: Randomness and Pattern in Convex Geometric Analysis .....	II	665
DETLEF MÜLLER: Functional Calculus on Lie Groups and Wave Propagation .....	II	679
STEFAN MÜLLER* AND VLADIMIR ŠVERÁK: Unexpected Solutions of First and Second Order Partial Differential Equations .....	II	691
KLAS DIEDERICH AND SERGEY PINCHUK*: Reflection Principle in Higher Dimensions .....	II	703
KRISTIAN SEIP: Developments from Nonharmonic Fourier Series .....	II	713
HART F. SMITH: Wave Equations with Low Regularity Coefficients ..	II	723
NICOLE TOMCZAK-JAEGERMANN: From Finite- to Infinite-Dimensional Phenomena in Geometric Functional Analysis on Local and Asymptotic Levels .....	II	731
STEPHEN WAINGER: Discrete Analogues of Singular and Maximal Radon Transforms .....	II	743
THOMAS WOLFF: Maximal Averages and Packing of One Dimensional Sets .....	II	755

## SECTION 9. ORDINARY DIFFERENTIAL EQUATIONS AND DYNAMICAL SYSTEMS

W. DE MELO: Rigidity and Renormalization in One Dimensional Dynamical Systems .....	II	765
L. H. ELIASSEN: Reducibility and Point Spectrum for Linear Quasi-Periodic Skew-Products .....	II	779
SHUHEI HAYASHI: Hyperbolicity, Stability, and the Creation of Homoclinic Points .....	II	789
MICHAEL HERMAN: Some Open Problems in Dynamical Systems ....	II	797
YURI KIFER: Random Dynamics and its Applications .....	II	809

SERGEI B. KUKSIN: Elements of a Qualitative Theory of Hamiltonian PDEs .....	II	819
KRYSZYNA KUPERBERG: Counterexamples to the Seifert Conjecture .	II	831
CURTIS T. MCMULLEN: Rigidity and Inflexibility in Conformal Dynamics .....	II	841
GRZEGORZ ŚWIĄTEK: Induced Hyperbolicity for One-Dimensional Maps .....	II	857
ZHIHONG XIA: Arnold Diffusion: A Variational Construction .....	II	867
SECTION 10. PARTIAL DIFFERENTIAL EQUATIONS		
FABRICE BETHUEL: Vortices in Ginzburg-Landau Equations .....	III	11
FRÉDÉRIC HÉLEIN: Phenomena of Compensation and Estimates for Partial Differential Equations .....	III	21
ROBERT R. JENSEN: Viscosity Solutions of Elliptic Partial Differential Equations .....	III	31
HANS LINDBLAD: Minimal Regularity Solutions of Nonlinear Wave Equations .....	III	39
M. MACHEDON: Fourier Analysis of Null Forms and Non-linear Wave Equations .....	III	49
FRANK MERLE: Blow-up Phenomena for Critical Nonlinear Schrödinger and Zakharov Equations .....	III	57
GUSTAVO PONCE: On Nonlinear Dispersive Equations .....	III	67
GUNTHER UHLMANN: Inverse Boundary Value Problems for Partial Differential Equations .....	III	77
D. YAFAEV: Scattering Theory: Some Old and New Problems .....	III	87
SECTION 11. MATHEMATICAL PHYSICS		
EUGENE BOGOMOLNY: Spectral Statistics .....	III	99
DETLEV BUCHHOLZ: Scaling Algebras in Local Relativistic Quantum Physics .....	III	109
J. T. CHAYES: Finite-Size Scaling in Percolation .....	III	113
P. COLLET: Extended Dynamical Systems .....	III	123
ROBERT DIJKGRAAF: The Mathematics of Fivebranes .....	III	133
ANTONIO GIORGILLI: On the Problem of Stability for Near to Integrable Hamiltonian Systems .....	III	143
GIAN MICHELE GRAF: Stability of Matter in Classical and Quantized Fields .....	III	153
ALEXANDER BERKOVICH AND BARRY M. MCCOY*: Rogers-Ramanujan Identities: A Century of Progress from Mathematics to Physics .....	III	163
ROBERTO H. SCHONMANN: Metastability and the Ising Model .....	III	173
FEODOR A. SMIRNOV: Space of Local Fields in Integrable Field Theory and Deformed Abelian Differentials .....	III	183
HORNG-TZER YAU: Scaling Limit of Particle Systems, Incompressible Navier-Stokes Equation and Boltzmann Equation .....	III	193

## SECTION 12. PROBABILITY AND STATISTICS

DAVID J. ALDOUS: Stochastic Coalescence .....	III	205
MAURY BRAMSON: State Space Collapse for Queueing Networks .....	III	213
MARK I. FREIDLIN: Random and Deterministic Perturbations of Nonlinear Oscillators .....	III	223
JAYANTA K. GHOSH: Bayesian Density Estimation .....	III	237
F. GÖTZE: Lattice Point Problems and the Central Limit Theorem in Euclidean Spaces .....	III	245
PETER HALL* AND BRETT PRESNELL: Applications of Intentionally Biased Bootstrap Methods .....	III	257
IAIN M. JOHNSTONE: Oracle Inequalities and Nonparametric Function Estimation .....	III	267
JEAN-FRANÇOIS LE GALL: Branching Processes, Random Trees and Superprocesses .....	III	279
DAVID SIEGMUND: Genetic Linkage Analysis: an Irregular Statistical Problem .....	III	291
ALAIN-SOL SZNITMAN: Brownian Motion and Random Obstacles ....	III	301
BORIS TSIRELSON: Within and Beyond the Reach of Brownian Innovation .....	III	311
R. J. WILLIAMS: Reflecting Diffusions and Queueing Networks .....	III	321

## SECTION 13. COMBINATORICS

BÉLA BOLLOBÁS: Hereditary Properties of Graphs: Asymptotic Enumeration, Global Structure, and Colouring .....	III	333
ANDRÁS FRANK: Applications of Relaxed Submodularity .....	III	343
ALAIN LASCoux: Ordonner le Groupe Symétrique: Pourquoi Utiliser l'Algèbre de Iwahori-Hecke ? .....	III	355
JIŘÍ MATOUŠEK: Mathematical Snapshots from the Computational Geometry Landscape .....	III	365
HARALD NIEDERREITER: Nets, $(t, s)$ -Sequences, and Algebraic Curves over Finite Fields with Many Rational Points .....	III	377
N. J. A. SLOANE: The Sphere Packing Problem .....	III	387
JOSEPH A. THAS: Finite Geometries, Varieties and Codes .....	III	397
ANDREI ZELEVINSKY: Multisegment Duality, Canonical Bases and Total Positivity .....	III	409

## SECTION 14. MATHEMATICAL ASPECTS OF COMPUTER SCIENCE

MIKLÓS AJTAI: Worst-Case Complexity, Average-Case Complexity and Lattice Problems .....	III	421
JOAN FEIGENBAUM: Games, Complexity Classes, and Approximation Algorithms .....	III	429
JOHAN HÅSTAD: On Approximating NP-Hard Optimization Problems	III	441
TONIANN PITASSI: Unsolvable Systems of Equations and Proof Complexity .....	III	451
MADHU SUDAN: Probabilistic Verification of Proofs .....	III	461



ARTUR ANDRZEJAK AND EMO WELZL*: Halving Point Sets .....	III	471
SECTION 15. NUMERICAL ANALYSIS AND SCIENTIFIC COMPUTING		
GREGORY BEYLKIN: On Multiresolution Methods in Numerical Analysis .....	III	481
P. DEIFT*, T. KRIECHERBAUER, K. T-R McLAUGHLIN, S. VENAKIDES AND X. ZHOU: Uniform Asymptotics for Orthogonal Polynomials .....	III	491
BJORN ENGQUIST: Wavelet Based Numerical Homogenization .....	III	503
HISASHI OKAMOTO: A Study of Bifurcation of Kolmogorov Flows with an Emphasis on the Singular Limit .....	III	513
JAN-OLOV STRÖMBERG: Computation with Wavelets in Higher Dimensions .....	III	523
LLOYD N. TREFETHEN* AND TOBIN A. DRISCOLL: Schwarz–Christoffel Mapping in the Computer Era .....	III	533
SECTION 16. APPLICATIONS		
MARCO AVELLANEDA: The Minimum-Entropy Algorithm and Related Methods for Calibrating Asset-Pricing Models .....	III	545
ANDREAS DRESS*, WERNER TERHALLE: The Tree of Life and Other Affine Buildings .....	III	565
LESLIE GREENGARD* AND XIAOBAI SUN: A New Version of the Fast Gauss Transform .....	III	575
ULF GRENANDER: Strategies for Seeing .....	III	585
FRANK HOPPENSTEADT* AND EUGENE IZHIKEVICH: Canonical Models in Mathematical Neuroscience .....	III	593
THOMAS YIZHAO HOU: Numerical Study of Free Interface Problems Using Boundary Integral Methods .....	III	601
GÉRARD IOOSS: Travelling Water-Waves, as a Paradigm for Bifurcations in Reversible Infinite Dimensional “Dynamical” Systems .....	III	611
YURY GRABOVSKY AND GRAEME W. MILTON*: Exact Relations for Composites: Towards a Complete Solution .....	III	623
CHARLES S. PESKIN: Optimal Dynamic Instability of Microtubules ..	III	633
SECTION 17. CONTROL THEORY AND OPTIMIZATION		
DAVID APPEGATE, ROBERT BIXBY, VAŠEK CHV’ATAL AND WILLIAM COOK*: On the Solution of Traveling Salesman Problems	III	645
MICHEL X. GOEMANS: Semidefinite Programming and Combinatorial Optimization .....	III	657
RICHARD H. BYRD AND JORGE NOCEDAL*: Active Set and Interior Methods for Nonlinear Optimization .....	III	667
RANGA ANBIL, JOHN J. FORREST AND WILLIAM R. PULLEYBLANK*: Column Generation and the Airline Crew Pairing Problem .....	III	677

ALEXANDER SCHRIJVER: Routing and Timetabling by Topological Search .....	III	687
JAN C. WILLEMS: Open Dynamical Systems and their Control .....	III	697
MICHAL KOČVARA AND JOCHEM ZOWE*: Free Material Optimization	III	707
<b>SECTION 18. TEACHING AND POPULARIZATION OF MATHEMATICS</b>		
GEORGE E. ANDREWS: Mathematics Education: Reform or Renewal?	III	719
MICHÈLE ARTIGUE: De la Compréhension des Processus d'Apprentissage a la Conception de Processus d'Enseignement .....	III	723
MARIA G. BARTOLINI BUSSI: Drawing Instruments: Theories and Practices from History to Didactics .....	III	735
MIGUEL DE GUZMÁN*, BERNARD R. HODGSON*, ALINE ROBERT* AND VINICIO VILLANI*: Difficulties in the Passage from Secondary to Tertiary Education .....	III	747
D. J. LEWIS: Mathematics Instruction in the Twenty-first Century ..	III	763
MOGENS NISS: Aspects of the Nature and State of Research in Mathematics Education .....	III	767
DAVID A. SMITH: Renewal in Collegiate Mathematics Education .....	III	777
<b>SECTION 19. HISTORY OF MATHEMATICS</b>		
KARINE CHEMLA: History of Mathematics in China: A Factor in World History and a Source for New Questions .....	III	789
JOSEPH W. DAUBEN: Marx, Mao and Mathematics: The Politics of Infinitesimals .....	III	799
JEREMY J GRAY: The Riemann-Roch Theorem and Geometry, 1854-1914 .....	III	811



## PREFACE

The Proceedings of the International Congress of Mathematicians 1998, held in Berlin, are published – electronically and in print – in three volumes. Volume I contains information on the organization of the Congress including the list of participants, reports on the opening and closing ceremonies, the Laudationes on the Fields Medalists and the Nevanlinna Prize Winner, and the Plenary Lectures. Volumes II and III contain the Invited Lectures.

For the first time, the Proceedings of an ICM have been produced completely electronically – without any commercial assistance. Using the facilities of DOCUMENTA MATHEMATICA, the contents of the Plenary and Invited Lectures were made available without charge on the Internet, already before the Congress started, at <http://www.mathematik.uni-bielefeld.de/documenta/>.

The printed versions of Volumes II and III were distributed to the participants at the beginning of the Congress. Volume I, containing material which had to be gathered during the Congress, was printed about three months after the Congress.

We want to thank all the speakers and organizers for their cooperation which made such fast publication possible.

October 1998

Gerd Fischer  
Ulf Rehmann

## PAST CONGRESSES

1897	Zürich	1954	Amsterdam
1900	Paris	1958	Edinburgh
1904	Heidelberg	1962	Stockholm
1908	Roma	1966	Moskva
1912	Cambridge, UK	1970	Nice
1920	Strasbourg	1974	Vancouver
1924	Toronto	1978	Helsinki
1928	Bologna	1982	Warszawa (held in 1983)
1932	Zürich	1986	Berkeley
1936	Oslo	1990	Kyoto
1950	Cambridge, USA	1994	Zürich

*1998 Berlin*

PAST FIELDS MEDALISTS  
AND ROLF NEVANLINNA PRIZE WINNERS

RECIPIENTS OF FIELDS MEDALS

1936	Lars V. Ahlfors Jesse Douglas	1978	Pierre R. Deligne Charles F. Fefferman Grigorii A. Margulis Daniel G. Quillen
1950	Laurent Schwartz Atle Selberg		
1954	Kunihiko Kodaira Jean-Pierre Serre	1982	Alain Connes William P. Thurston Shing-Tung Yau
1958	Klaus F. Roth René Thom		
1962	Lars Hörmander John W. Milnor	1986	Simon K. Donaldson Gerd Faltings Michael H. Freedman
1966	Michael F. Atiyah Paul J. Cohen Alexander Grothendieck Steve Smale	1990	Vladimir G. Drinfeld Vaughan F. R. Jones Shigefumi Mori Edward Witten
1970	Alan Baker Heisuke Hironaka Sergei P. Novikov John G. Thompson	1994	Jean Bourgain Pierre-Louis Lions Jean-Christophe Yoccoz Efim Zelmanov
1974	Enrico Bombieri David B. Mumford		

ROLF NEVANLINNA PRIZE WINNERS

1982	Robert E. Tarjan	1990	Alexander A. Razborov
1986	Leslie G. Valiant	1994	Avi Wigderson



## ORGANIZATION OF THE CONGRESS

MARTIN GRÖTSCHEL  
President of the ICM'98

In 1992 the German Mathematical Society (DMV) invited the International Mathematical Union (IMU) to hold the 1998 International Congress of Mathematicians in Berlin. The invitation was accepted by the 1994 General Assembly of the IMU in Luzern, the decision announced at the 1994 Congress in Zürich.

In January 1995 the Council (Präsidium) of the DMV and the representatives of the mathematical institutions in Berlin appointed the Board of Directors of the ICM'98 Organizing Committee (Martin Grötschel (TU and ZIB Berlin), President; Friedrich Hirzebruch (MPI Bonn), Honorary President; Martin Aigner (FU Berlin), Vice President; Jürgen Sprekels (HU and WIAS Berlin), Treasurer; Jörg Winkler (TU Berlin), Secretary) and also founded the *Verein zur Durchführung des International Congress of Mathematicians 1998 in Berlin* (VICM) to form a legal umbrella for the organization. In the course of the preparations, the Board of Directors asked many colleagues to join the organizing team. A list of its members can be found on the next pages.

Initial financial support came from the *Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie* and from the *Senat von Berlin*. Without the substantial backing from these two institutions an application would have been impossible. Other public and academic bodies, private corporations and foundations, individuals and mathematical institutes supported the Congress significantly as well. A list of donors can be found in this volume. The registration fee was DM 450 for early and DM 600 for late registration, there was no fee for accompanying persons. The registration fees accounted for about one third of the total budget.

The scientific program of the Congress was in the hands of a Program Committee appointed by the IMU. Its members were Phillip Griffiths (Chairman), Luis Caffarelli, Ingrid Daubechies, Gerd Faltings, Hans Föllmer, Michio Jimbo, John Milnor, Sergei Novikov, and Jacques Tits. The committee divided the program of the Congress into 19 sections and appointed, for each section, a panel to nominate



speakers. In early summer of 1997 the Program Committee selected 21 mathematicians to give one-hour plenary addresses and 169 colleagues to present 45-minute invited lectures. Five invited lecturers cancelled their talks at short notice due to personal reasons. Two of them, however, submitted written versions of their lectures to these Proceedings.

The Fields Medal Committee consisted of Yuri Manin (Chairman), John Ball, John Coates, J. J. Duistermaat, Michael Freedman, Jürg Fröhlich, Robert MacPherson, Kyoji Saito, and Steve Smale. The members of the Nevanlinna Prize Committee were David Mumford (Chairman), Bjorn Engquist, Tom Leighton, and Alexander Razborov. Both committees arrived at their decisions in spring 1998.

The Organizing Committee was responsible for all other activities of the Congress. DER-CONGRESS handled accommodation, registration and related arrangements as the official travel agent of the Organizing Committee.

The first day of the Congress, including the opening ceremony, took place at the International Congress Center (ICC) of Berlin. During the opening ceremony, attended by about 3,000 persons, the Fields Medals and the Nevanlinna Prize were awarded. Moreover, Andrew Wiles received an IMU silver plaque in recognition of his proof of “Fermat’s Last Theorem”. The opening ceremony was transmitted worldwide in the Internet via MBone. In the afternoon of August 18, the work of the Fields Medalists and the Nevanlinna Prize winner was presented in five lectures. The manuscripts of these lectures can be found in this volume. Jürgen Moser concluded the first day with a plenary lecture.

All further sessions of the Congress took place on the campus of the Technische Universität Berlin. The plenary lectures were held in morning sessions in the Audimax of the TU Berlin. They were transmitted via closed-circuit television to another large lecture hall. The 45-minute invited lectures were given in six parallel sessions from 2 pm to 6 pm each afternoon, from August 19 to 26, except for Sunday, August 23, which was kept free for excursions etc. The last day of the Congress, August 27, consisted of four plenary addresses and the closing ceremony.

In addition to the invited and plenary lectures, 1,098 short 15-minute contributions and 236 poster presentations were given. Moreover, 235 ad-hoc talks of 15 minutes length were scheduled during the Congress. Thus, ICM’98 had a total of 1569 contributed presentations.

The organization of the Congress was, to a large extent, based on electronic communication. Already in 1994, a World Wide Web Server on the International Congress was set up at the Konrad-Zuse-Zentrum in Berlin. This server was continuously extended to contain up-to-date material so that every mathematician interested in ICM’98 could look up most recent information. In addition to this, circular letters were e-mailed to all those who preregistered for the Congress electronically. These circular letters complemented the printed First and Second Announcements that were mailed out in August 1997 and January 1998, respectively, to thousands of mathematicians worldwide.

The Organizing Committee also offered the possibility of electronic registration. Two thirds of the ICM’98 members took advantage of this facility; 95% of the abstracts of the invited and contributed presentations were submitted electronically. Moreover, all but one of the plenary and invited speakers submitted

their paper for the proceedings volume electronically. This made it possible to produce Volumes II and III before the Congress, to make them available in the Internet, and to deliver them to the participants in printed form at registration in Berlin.

In all, 3,346 mathematicians from 98 countries participated in the Congress together with an estimated number of 800 accompanying persons; 31 exhibitors were present.

The Organizing Committee made significant efforts, together with the International Mathematical Union, to give financial support for participants from developing countries and Eastern Europe. A fund of more than DM 900,000 made it possible to sponsor the attendance of approximately 450 mathematicians. About 510 colleagues were invited, around 60 were unfortunately unable to attend; 93 young and 37 mature colleagues from developing countries received grants from the IMU and the local organization, 305 persons from the support program of the local Organizing Committee for mathematicians from Eastern Europe. Special grants from mathematical institutions and other support programs complemented these efforts.

The social events included a buffet lunch after the opening ceremony, an opera performance of the *Magic Flute* in the Deutsche Oper on August 23, and an ICM party on August 26. To convey some of the many facets of Berlin to the ICM'98 participants, and in particular to accompanying persons, many Berlin mathematicians, their friends and spouses offered informal tours, so called footloose tours, to points of special interest in Berlin. About 1,200 ICM'98 members and accompanying persons participated in these tours.

In accordance with the Program Committee and the IMU, the Organizing Committee opened a Section of Special Activities to cover topics of mathematical relevance that would not fit elsewhere in the official scientific program. These special activities included an afternoon session on electronic publishing with three talks and a panel discussion on "The Future of Electronic Communication, Information, and Publishing"; presentations of mathematical software on three afternoons; several special activities related to women in mathematics including the Emmy Noether Lecture given by Cathleen Synge Morawetz, and a panel discussion "Events and Policies: Effects on Women in Mathematics"; an afternoon on "Berlin as Centre of Mathematical Activity" (this workshop was suggested by the International Commission on the History of Mathematics); a roundtable discussion on "International Comparison of Mathematical Studies, University Degrees, and Professional Perspectives".

The exhibition "Terror and Exile" honored the memory of 53 Berlin mathematicians who suffered under the Nazi terror; this topic was also addressed in a special session "Mathematics in the Third Reich and Racial and Political Persecution".

Other events enhanced the scope of the ICM'98 activities. The special evening lecture of Andrew Wiles on "Twenty Years of Number Theory" on August 19 attracted an audience of about 2,300. Olli Lehto's book on the International Mathematical Union was presented and an exhibition of mathematical cartoons was shown at the TU Mathematics Library.

A major attempt to reach out to the non-mathematical public during the Congress were the activities in the Urania, an institution with a long tradition in the popularization of science. These included 11 lectures on mathematics for a general audience, the VideoMath Festival in which the VideoMath Reel, a composition of selected short videos on mathematics, and several other mathematical films were shown. Exhibitions on “Hands-on Mathematics” (addressing high-school students and teachers in particular), “Mathematical Stone Sculptures”, “Mathematics and Ceramics”, and works by high-school students on “Mathematics and the Art” complemented the Urania activities. An additional exhibition featuring paintings and sculptures related to mathematical objects (Innovation<sup>3</sup>) was shown at the Ludwig-Erhard-Haus. More than 5,000 persons attended the Urania lectures and video performances, about 10,000 visited the exhibitions in the Urania.

## THE COMMITTEES OF THE CONGRESS

## PROGRAM COMMITTEE (APPOINTED BY THE IMU)

Phillip Griffiths, <i>Chairman</i>	Institute for Advanced Study, Princeton, USA;
Luis Caffarelli	University of Texas, Austin, USA
Ingrid Daubechies	Princeton University, Princeton, USA
Gerd Faltings	Max-Planck-Institut, Bonn, Germany
Hans Föllmer	Humboldt-Universität, Berlin, Germany
Michio Jimbo	Kyoto Universtity, Kyoto, Japan
John Milnor	SUNY at Stony Brook, Stony Brook, USA
Sergei Novikov	Landau Institute, Moscow, Russia, and University of Maryland, USA
Jacques Tits	Collège de France, Paris, France

The German Mathematical Society together with representatives of the mathematical institutions of Berlin appointed the President, Honorary President, Vice President, Treasurer and Secretary (Board of Directors) of the Local Organizing Committee, who in turn appointed the members of all further committees.

## ORGANIZING COMMITTEE

Martin Grötschel	<i>President</i>	ZIB and TU Berlin
Friedrich Hirzebruch	<i>Honorary President</i>	Bonn
Martin Aigner	<i>Vice President</i>	FU Berlin
Jürgen Sprekels	<i>Finances</i>	WIAS and HU Berlin
Jörg Winkler	<i>Secretary</i>	TU Berlin
Rolf Möhring	<i>Local Arrangements</i>	TU Berlin

Ehrhard Behrends	FU Berlin	Sabine Marcus	TU Berlin
Gerhard Berendt	FU Berlin	Sybille Mattrisch	ZIB Berlin
A. Beutelspacher	Giessen	Hans-Otfried Müller	Dresden
Jochen Brüning	HU Berlin	Winfried Neun	ZIB Berlin
Wolfgang Dalitz	ZIB Berlin	Volker Nollau	Dresden
Gerd Fischer	Düsseldorf	Konrad Polthier	TU Berlin
Gerd Frey	Essen	Elke Pose	TU Berlin
Ulrich Fuchs	FU Berlin	Ulf Rehmann	Bielefeld
Stephan Hartmann	TU Berlin	Werner Römisch	HU Berlin
Christian Hege	ZIB Berlin	Vasco Schmidt	FU Berlin
Christoph Helmberg	ZIB Berlin	Renate Schubert	TU Berlin
Karl-Heinz Hoffmann	TU München	Ralph-Hardo Schulz	FU Berlin
Bettina Kasse	ZIB Berlin	Margitta Teuchert	WIAS Berlin
Herbert Kurke	HU Berlin	Michael Walter	ZIB Berlin
Eberhard Letzner	FU Berlin	Christiane Weber	Dresden
Jutta Lohse	WIAS Berlin	Günter M. Ziegler	TU Berlin

## LOCAL SCIENTIFIC COMMITTEE

Michael E. Pohst, <i>Chairman</i>	TU Berlin	Ralf Kornhuber	FU Berlin
Günter Albinus	WIAS Berlin	Jürg Kramer	HU Berlin
Helmut Alt	FU Berlin	Herbert Kurke	HU Berlin
Klaus Dieter Bierstedt	Paderborn	Joachim Naumann	HU Berlin
Alexander Bobenko	TU Berlin	Michael Nussbaum	WIAS Berlin
Peter Deuffhard	ZIB and FU Berlin	Erich Ossa	Wuppertal
Jean-Dominique Deuschel	TU Berlin	Christian Pommerenke	TU Berlin
Frank Duzaar	HU Berlin	Hans-Jürgen Prömel	HU Berlin
Dirk Ferus	TU Berlin	Siegfried Prößdorf	WIAS Berlin
Bernold Fiedler	TU Berlin	Lutz Recke	HU Berlin
Karl-Heinz Förster	TU Berlin	Klaus R. Schneider	WIAS Berlin
Herbert Gajewski	WIAS Berlin	Rüdiger Schultz	Leipzig
Joachim Gräter	Potsdam	Wolfgang Schulz	HU Berlin
Jens Gustedt	TU Berlin	Bert-Wolfgang Schulze	Potsdam
Klaus Hulek	Hannover	Martin Schweizer	TU Berlin
Heinz Adolf Jung	TU Berlin	Rudolf Seiler	TU Berlin
Markus Klein	Potsdam	Wilhelm Singhof	Düsseldorf
Eberhard Knobloch	TU Berlin	Helmut Strade	Hamburg
Helmut Koch	HU Berlin	Gernot Stroth	Halle
Hermann König	Kiel	Fredi Tröltzsch	Chemnitz
Sabine Koppelberg	FU Berlin	Elmar Vogt	FU Berlin
		Robert Weismantel	Magdeburg
		Günter M. Ziegler	TU Berlin

*Registration of the participants*

## LIST OF DONORS

The Organizing Committee is greatly indebted to all those who have supported the congress either by monetary contributions or by donating goods and services. Without these generous donations it would have been impossible to launch ICM'98. We would like to thank the following sponsors cordially:

## PUBLIC AND ACADEMIC BODIES

Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie  
Senat von Berlin  
Deutsche Forschungsgemeinschaft  
Sächsisches Staatsministerium für Wissenschaft und Kunst  
Alexander von Humboldt-Stiftung  
Berlin-Brandenburgische Akademie der Wissenschaften

International Mathematical Union  
Deutsche Mathematiker-Vereinigung  
European Mathematical Society  
Deutsche Gesellschaft für Versicherungsmathematik  
Berliner Mathematische Gesellschaft

## PRIVATE CORPORATIONS AND FOUNDATIONS

Allianz Lebensversicherungs-AG  
Siemens AG  
Stemmler-Stiftung  
Möllgaard-Stiftung  
Silicon Graphics  
Deutsche Telekom  
Storage Tek  
Herlitz AG  
Deutsche Bank AG  
Springer-Verlag  
Nikkei Culture  
Walter und Eva Andrejewski-Stiftung  
Minolta  
Sender Freies Berlin  
SUN Microsystems  
Berliner Verkehrsbetriebe  
Daimler-Benz-Stiftung  
T-Mobil



## CLOSING CEREMONY

*The closing ceremony was held on Thursday, August 27, 1998, starting at 15.00 in the main lecture hall of the TU Berlin*

DAVID MUMFORD, *President of the International Mathematical Union, addressed the audience as follows:*

We have come to the end now of what I believe was a remarkable and very successful Congress. As President of the IMU, it is my very pleasant duty first to congratulate the local organizing committee for their role in this.

I would like to underline several aspects of the Congress which I felt were especially successful. Firstly, in the entire pre-congress stage, the organizers have used email most effectively, putting on virtually everyone's desk the current plans, events, speakers as soon as announced and the registration form. Moreover, their ability to produce two thirds of the Proceedings before the Congress and one third immediately after (held back only by those like me who didn't write their speeches beforehand) is a remarkable demonstration of the potential to publish a major book at minimal cost with no commercial assistance.

Another great success is the quality of the presentations. I want to congratulate the Program Committee for their selections, the speakers on the clarity of their talks and the Organizing Committee for their instructions and suggestions to the speakers (that I'm sure were listened to from my own conversations with many of the speakers).

Still another area in which the organizers have succeeded beyond all expectations is in public relations. Both with unprecedented press coverage and with a beautiful array of programs at Urania, they have reached major groups of Berliners, of Germans and of the World. (My wife reports reading of the Fields Medals in the Boston Globe.)

Finally, I'd like to say that the physical arrangements seem to me to have been near ideal: many large lecture rooms in close proximity, transport passes, etc. Underlying all this, invisible but obviously vital, is probably the largest sum of money ever raised for an ICM. Its use in helping hundreds attend the Congress will be detailed later.

For this great job, I want now to propose a round of applause for the Organizers. BUT, as in all human activities, an institution cannot rest on its laurels. The Congress is really for you and we want your feedback. Taking our clue from the Organizers, we would like everyone who wishes to send us electronically their comments, suggestions and proposals. You can reach the IMU at "imu@impa.br."

My second duty is to report to you on the General Assembly (G. A.) of the IMU that took place in Dresden over the weekend preceding the Congress. Many of you may be unaware of the institutional infrastructure that supports the stately procession of International Congresses, so let me quickly sketch this. The IMU is



an organization whose members are countries – about 60 of them – which are represented by ‘adhering organizations’, National Academies or Mathematical Societies. Each of them sends delegates to the G. A. which precedes each Congress and here the whole chain of committees starts and the control rests. The G. A. elects the President, Secretary and Executive Committee, which in turn appoints the Program Committee (which appoints panels in every subfield), Fields Medal and Nevanlinna Prize Committees and works with the Organizing Committee of the next Congress. The goal, I should add, is to spread decision making over as large and as representative a group as possible.

At this point, I want to report to you the decisions taken at the Dresden G. A. The first decision is that:

*ICM 2002 will be held in Beijing, China.*

The President of the Chinese Mathematical Society, Professor K. C. Chang, will give further information in a few minutes.

Secondly, the G. A. passed a resolution in support of diversity:

*Building on the resolutions adopted at the 1986 and 1990 General Assemblies, the IMU shall continue to endeavour to attract the participation of all mathematicians. Subfields of mathematics and traditionally underrepresented groups should not be overlooked in IMU activities.*

Thirdly, the G. A. adopted an ‘enabling resolution’ to form a Committee on Electronic Information and Communication. This resolution reads:

*1. In the last decade, the internet has been transforming our communication and commerce. In the world of science, the internet is radically changing the modes of information transfer at all levels. Communication on hand-written and printed paper, distribution via postal mail and libraries is a system which has been stable for many centuries. We cannot foresee clearly the new system which is evolving except that it will involve electronic media and it will radically alter the economics of communication. This transformation will certainly be global and will affect mathematical research on all continents.*

*2. We strongly believe that the IMU can play several important roles during this transition. Among these are:*

- i) it can provide a forum where all parties, i. e., all countries and all interest groups (individual researchers, professional societies, publishers, and libraries) can discuss the issues and it can publish proceedings to increase general understanding of all the issues involved,*
- ii) it can recommend and promote international standards on electronic communication among mathematicians, when needed,*
- iii) it can act as a liaison between regional, national and local groups, coordinating their initiatives and discussions.*

*3. We therefore propose that the GA establish a*

*Committee on Electronic Information and Communication (CEIC)*  
*to accomplish its objectives whose terms of reference and initial additional membership will be decided by the ad hoc committee consisting of John Ewing, Martin Grötschel, Peter Michor, David Mumford and Jacob Palis and sent by mail ballot to the adhering organizations for approval.*

I am happy to report that this Committee is nearly in place and that Peter Michor has agreed to be its chairman for the next four years.

Fourthly, the G. A. elected as the next President of the IMU Professor Jacob Palis and as Secretary Professor Phillip Griffiths and I wish to congratulate them and wish them great success. The following are the full slates which were elected for various Committees and Commissions of the Union:

IMU EXECUTIVE COMMITTEE

President:	J. Palis	Brazil
Vice-Presidents:	S. Donaldson	United Kingdom
	S. Mori	Japan
Secretary:	P. Griffiths	USA
Members:	V. Arnold	Russia
	J. M. Bismut	France
	B. Engquist	Sweden
	M. Grötschel	Germany
	M. Raghunathan	India
ex-officio:	D. Mumford, Past President	USA

INTERNATIONAL COMMISSION ON MATHEMATICAL INSTRUCTION (ICMI)

President:	Hyman Bass	USA
Vice-Presidents:	M. Artigue	France
	N. Aguilera	Argentina
Secretary:	B. Hodgson	Canada
Members:	G. Leder	Australia
	Y. Namikawa	Japan
	I. Scharygin	Russia
	J. P. Wang	China
ex-officio:	Miguel de Guzman, Past President	Spain
	President of IMU	
	Secretary of IMU	

COMMISSION ON DEVELOPMENT AND EXCHANGE (CDE)

Chairman:	Rolando Rebolledo	Chile
Secretary:	Herb Clemens	USA
Members:	A. A. Ashour	Egypt
	K. C. Chang	China
	P. Cordaro	Brazil
	J.-P. Gossez	Belgium
	O. Nakoulima	Guadeloupe
	T. Sumada	Japan
ex-officio:	M. S. Narasimhan, Past Chairman	India
	President of IMU	
	Secretary of IMU	

INTERNATIONAL COMMISSION OF THE HISTORY OF MATHEMATICS (ICHM)

Jan P. Hogendijk (Netherlands) and Karen Parshall (USA)

I would now like to call on Jacob Palis to say a few words.

JACOB PALIS, *President of the IMU for 1999–2002, addressed the audience as follows:*

Dear colleagues,  
ladies and gentlemen:

It's a great honor for me to become the next President of the International Mathematical Union, a fundamental institution for the development of mathematics in the world. To have good mathematics in all regions, in all countries, is precisely a main goal of the Union: we shall pursue and achieve it together.

The Executive Committee and the Commissions of the Union will be engaged in this major goal. As part of such an effort, IMU members, through their mathematical societies and research agencies, have been contributing to our Special Development Fund; especially the US, Brazil, UK, Japan and France. Through the Fund and Local Organizing Committee, we were able to finance the participation at the ICM of about 100 young and 40 senior mathematicians from the Developing World. Actually, the Local Organizing Committee did more: it also made possible the presence of more than 300 mathematicians from the former Soviet Union and Eastern Europe. To talk about this, I wish to call to the podium Prof. ANATOLY M. VERSHIK (President of St. Petersburg Mathematical Society, Head of the Laboratory of the Mathematical Institute of the Russian Academy of Sciences).

ANATOLY M. VERSHIK *addressed the audience as follows:*

Dear Colleagues:

More than three hundred participants of our congress have arrived from Russia and the former Soviet Union (fSU). Almost all of them have obtained the special grants or partial financial support from the Organization Committee or other funds which that Committee was able to use. These are the results of the efforts of the Committee and all of us thank the organizers of the congress and the International Mathematical Union for this support.

This Congress is the second International Congress of Mathematicians (of course except Moscow Congress in '66) with such a wide presence of mathematicians from Russia and the fSU. It was impossible to imagine such a big group from those countries at a congress even 10 years ago. Everybody understands how important it is, especially for young mathematicians, to have the possibility to take part in a meeting of such a high scientific level, to listen to the talks of prominent

scientists about recent studies, to present their own achievements, to obtain new information and to look for new problems.

Those over 40 perhaps remember how limited the attendance of Soviet mathematics at the international congresses in the sixties, seventies and eighties was. Even invited speakers could not obtain the permission from “very high scientific” organizations for going abroad, e. g., I was an invited speaker at the Congress '74 in Vancouver but approximately 15 other invited speakers from Russia could not visit that congress. It was common at that time to have a gap in the schedule instead of the lectures of Soviet mathematicians or to entrust the reading of the lecture to some of the foreign colleagues. Moreover, even Fields Medalists from Russia (Novikov – Nice '70, Margulis – Helsinki '78) did not visit these congresses and did not receive the medal during the ceremony because they had not obtained permission for that!

The international mathematical community tried to help our mathematics and mathematicians in those days many times but it was impossible and hopeless. Indeed, the reasons for such stupid behaviour of Soviet authority were political or something similar to that. The result of that policy was the separation between the remarkable mathematical schools which had developed in the Soviet Union and in the worldwide mathematical community.

Now fortunately we do not need any permissions of authorities and there are no obstacles for going abroad, for having contact with our colleagues, for collaboration with them and for visiting the conferences and congresses. But we face completely new problems which are more understandable – for all that we need financial support. For that matter the International Mathematical Community has shown very deep and clear understanding of our problems, in this situation they can help and they do help. There are many examples of such help and two excellent ones are our visit to the Congress in Berlin and the previous Congress in Zürich.

Thank you very much. Needless to say how important this help is for us! Especially nowadays when the sole existence of the mathematics in our countries is in such a danger.

In a rather solemn way I can say that our mathematics must survive and will survive and the international solidarity of mathematicians is a guarantee for that.

JACOB PALIS *continued his speech as follows:*

Also as part of our strategy to achieve the goal of having good mathematics throughout the world, we have proposed, and the General Assembly has approved unanimously, a change in our statutes, to have multinational mathematical societies and unions to be affiliated with IMU in order to facilitate joint actions in their respective region. The same applies to professional associations and in this respect emerges our second main objective: the unity of mathematics in its diversity of themes. We should have good mathematics, beyond being pure or applied and this should reflect in the ICMs, as in the present one.

Finally, I wish to ask the mathematicians of the world to participate in our multiple activities of the World Mathematical Year 2000.

Thank you.

Now I'm very pleased to invite K. C. Chang.

KUNG CHIN CHANG, *President of the Chinese Mathematical Society*, addressed the audience as follows:

Ladies and gentlemen:

It is a great pleasure and honor for me to invite all of you, on behalf of the Chinese Mathematical Society, to the next ICM at Beijing, a city interweaving historical tradition with modern fascination.

All the past congresses were held in developed countries. Now, the next congress, the first in the new century, will be held for the first time in a developing country. This will add a new chapter to Prof. Olli Lehto's book "Mathematics Without Borders."

We are grateful to the Executive Committee and the General Assembly of IMU for the decision on the site of Beijing. To host such an important congress is not only a great chance, but also a big challenge. However, the successful experience of the previous congresses, in particular, of the Berlin congress with such high levels of hospitality and efficiency, will be very useful for us.

In the past two decades, many mathematicians all over the world, and most of the members of the Executive Committee of IMU have visited China. Their suggestions and ideas in organizing the congress are warmly welcome. With the help of IMU and the cooperation of mathematicians throughout the world, the Chinese mathematicians, who are eager to make the congress a success, will do their best to make your attendance fruitful and enjoyable.

I am looking forward to seeing you all in Beijing in the year 2002.

*The last speaker was MARTIN GRÖTSCHEL, President of the ICM'98:*

At the first International Congresses it has been a tradition to commemorate the mathematicians who have deceased in the previous years. We would like to resume this tradition today. Following a German custom, I would like to ask you to stand up for a few moments and remain in silence while I read some words of remembrance.

It is impossible to list here all mathematicians who have died in the last four years, even if we restrict the list to the most prominent ones. I have chosen six colleagues who, I believe, represent all those who we will miss in the future:

HANSGEORG JEGGLE. Jeggle has been a professor at TU Berlin since 1971 and has been dean of the Faculty of Mathematics for many years. He was killed in a car crash on August 22, 1998.

FRANÇOIS JAEGER. Jaeger, an expert in combinatorics and combinatorial knot theory, had been selected by the ICM'98 Program Committee as an Invited Speaker in Section 13 "Combinatorics". He died on August 18, 1997 on the day when the ICM'98 invitation was mailed to him.

ANDRÉ WEIL, a towering figure of our field, whose name came up in many of the plenary and invited presentations of this Congress. Weil died on August 6, 1998.

PAUL ERDÖS. Erdős was among the most productive mathematicians of all time and probably the most highly connected individual of us all. He died at a conference in Warsaw on September 22, 1996.

Finally, I would like to mention that two Fields medalists have deceased within the last four years.

LARS AHLFORS, the first recipient of a Fields Medal in 1936, died on October 11, 1996.

KUNIHIKO KODAIRA, who received a Fields Medal in 1954, died on July 26, 1997. Thank you for paying respect to the deceased colleagues. Please sit down again.

Ladies and Gentlemen, dear Colleagues:

One of the last sentences of my Opening Speech was:

“We would like to make ICM’98 an exceptional event. Let us hope that our dreams come true.”

I think our dreams came true.

However, not everything went exactly as planned. For instance, last night’s ICM party was going to be staged as an open air party on the greens behind the Math Building. Bad weather made a rescue operation necessary. The available facilities were, unfortunately, not really optimal for good queue management. I apologize for these inconveniences and a few others that came up during the last 10 days. Some participants, in fact, told me that they were happy that misfortunes such as these occurred. In their opinion, they made the ICM organization look more human.

I consider this as a compliment and would like to thank again all my colleagues in the Organizing Committee, our students, secretaries, spouses, children, and friends who have helped to run ICM’98 smoothly.

I have received a lot of additional requests. Participants would like to buy videos of the Opening Ceremony, of some of the Plenary Presentations, etc. We will consider all these issues in the near future, and I will write to you another Circular Letter to let you know what we can do and offer. One offer will be made right after the end of this Ceremony. We will show in the lecture hall H 104 the ICM’98 Special produced by channel B1 of Sender Freies Berlin which was broadcast on TV last week.

The ICM’98 Proceedings will be sold and distributed after the Congress by DOCUMENTA MATHEMATICA and the American Mathematical Society.

This is the right occasion to thank the many mathematical societies around the world who have generously helped the ICM’98 Organizing Committee distribute information about ICM’98 and advertise the Congress. This has been a very promising sign of international cooperation. I also consider it very positive that the IMU has decided to integrate the regional mathematical unions, such as the European Mathematical Society or the currently forming Asian Mathematical Union, into its activities. And I believe that electronic information and communication, another topic taken up by the IMU, will considerably foster joint work of

mathematicians from around the world, so that we can also reach those groups and countries that seem somewhat isolated. Additional efforts, however, are necessary on all sides.

It was somewhat difficult for me to attend lectures. But I managed to participate in most of the Plenary Addresses. I am grateful to all speakers that they have made efforts, in some cases really remarkable efforts, to address a broad mathematical audience. These lectures certainly formed the scientific backbone of our Congress. I would also like to thank those who have presented posters or gave short presentations. That's where most of the communication and discussion took place.

Many words of thanks have been said. I believe that only one word of thanks is left. No congress, however well organized, can be successful without enthusiastic participants. That is what you all have been. When officials of this university noticed that on Saturday at 6 p.m. there were still 1500 persons attending lectures they were really convinced that this Congress is an unusual event. I think that the participants of this Congress found the right mixture between leisure, fun, and hard work, and that many of us go home with a lot of new ideas and new friends.

Thank you very much for coming to Berlin and participating in ICM'98.

I declare the 23rd International Congress of Mathematicians closed.

*Members of the organization teams:  
Grötschel, Behrends, Brüning, Sprekels, Hartmann, Winkler, Aigner,  
Mumford, Palis, Hirzebruch, Möhring, Rehmann, Teuchert*

## LIST OF PARTICIPANTS

- Aasma, Ants (Estonia)  
 Abd Al-Kader, Gamal M. (Egypt)  
 Abdel-Megied, Mohamed (Egypt)  
 Abdounur, Oscar Joao (Brazil)  
 Abe, Yoshihiro (Japan)  
 Abel, Mati (Estonia)  
 Abeles, Francine F. (USA)  
 Abels, Herbert (Germany)  
 Abert, Miklos (Hungary)  
 Abkar, Ali (Sweden)  
 Abramochkin, Eugeny G. (Russian Federation)  
 Abramov, Gueorgui V. (Germany)  
 Abramovich, Dan (USA)  
 Abreu, Miguel (Portugal)  
 A'Campo-Neuen, Annette (Germany)  
 Accascina, Giuseppe (Italy)  
 Adelman, Clemens (Germany)  
 Adelson-Velsky, George M. (Israel)  
 Agud, Lucia (Spain)  
 Ahlswede, Rudolf (Germany)  
 Ahluwalia, Daljit S. (USA)  
 Ahuja, Om Parkash (Singapore)  
 Aiena, Pietro (Italy)  
 Aigner, Martin (Germany)  
 Aigner, Mats (Sweden)  
 Aikawa, Takanori (Japan)  
 Aipanov, Shamsha A. (Kazakhstan)  
 Aisagaliev, Serikbai A. (Kazakhstan)  
 Ajtai, Miklos (USA)  
 Akbari, Sajeed (Iran)  
 Akinyele, Olusola (USA)  
 Alain-Roger, Nkamnang (Germany)  
 Alania, Levan A. (Russian Federation)  
 Alaoui, Larbi (Morocco)  
 Albers, Bettina (Germany)  
 Albrecht, Raphael (Germany)  
 Albu, Toma (USA)  
 Alcantara-Bode, Julio (Peru)  
 Aldous, David John (USA)  
 Aleksandrov, Aleksandr G. (Russian Federation)  
 Alesker, Semyon (Israel)  
 Alessandrini, Lucia (Italy)  
 Alestalo, Pekka (Finland)  
 Alexeyev, Alexander A. (Russian Federation)  
 Aliev, Baimurod (Tajikistan)  
 Allende Alonso, Sira Maria (Cuba)  
 Alli, Vahid (Iran)  
 Alonso-Tarrio, Leovigildo (Spain)  
 Alpay, Safak (Turkey)  
 Alpers, Burkhard (Germany)  
 Alpers, Karsten (Germany)  
 Alpert, Christian (Germany)  
 Al-Rashed, Abdallah M. (Kingdom of Saudi-Arabia)  
 Alt, Franz L. (USA)  
 Alt, Helmut (Germany)  
 Al-Thukair, Fawzi A. (Kingdom of Saudi-Arabia)  
 Altmann, Doris (Germany)  
 Altmann, Klaus (Germany)  
 Aluffi, Paolo (USA)  
 Alves, Gloria L. M. (Brazil)  
 Alves, Manuel J. (Mozambique)  
 Al-Zanaidi, Mansour Abdullah (Kuwait)  
 Amir, Dan (Israel)  
 Ammann, Bernd (Germany)  
 Amosov, Grigori (Russian Federation)  
 Ancona, Vincenzo (Italy)  
 Anders, Igor (Ukraine)  
 Anderson, Joel H. (USA)  
 Anderson, Laura M. (USA)  
 Ando, Kazutoshi (Germany)  
 Ando, Shiro (Japan)  
 Andreian Cazacu, Cabiria I. (Romania)  
 Andrews, George Eyre (USA)  
 Andrié, Manfred (Germany)  
 Anichini, Giuseppe (Italy)  
 Ansoerge, Rainer (Germany)  
 Antipin, Anatoly (Russian Federation)  
 Aoki, Shigeru (Japan)  
 Appell, Jürgen (Germany)



- Appolinaire, Nzali (Germany)  
 Araki, Huzihiro (Japan)  
 Arancibia, Jacqueline (Brazil)  
 Aravinda, Chalya S. (India)  
 Arbarello, Enrico (Italy)  
 Aripov, Mersaid (Uzbekistan)  
 Arkin, Vadim I. (Russian Federation)  
 Armas-Sanabria, Lorena (Mexico)  
 Arnold, Hans-Joachim (Germany)  
 Arnold, Ludwig (Germany)  
 Arnold, Vladimir Igorevich (Russian Federation)  
 Arnoux, Pierre (France)  
 Arredondo, Juan H. (Mexico)  
 Arslanov, Marat-M. (Russian Federation)  
 Artamonov, Vyacheslav A. (Russian Federation)  
 Artamonova, Irena I. (Russian Federation)  
 Artemiadis, Nicolas (Greece)  
 Arthur, James Greig (Canada)  
 Artigue, Michele (France)  
 Asada, Akira (Japan)  
 Asada, Teruko (Japan)  
 Asavanant, Jack (Thailand)  
 Ascheuer, Norbert (Germany)  
 Ash, J. Marshall (USA)  
 Ashna, Amir Hossein (Iran)  
 Ashour, Attia A. (Egypt)  
 Asiedu-Addo, Samuel K. (Ghana)  
 Askarkhani, Abdoreza (Iran)  
 Askin, Suat (Russian Federation)  
 Aslanyan, Arthur (Russian Federation)  
 Aslund, Jan (Sweden)  
 Asmuss, Svetlana (Latvia)  
 Aspinwall, Paul S. (USA)  
 Assiamoua, Kofi V. S. (Togo)  
 Astala, Kari (Finland)  
 Asymont, Inna M. (Russian Federation)  
 Atela, Pau (USA)  
 Aubert, Jean-Christophe (Switzerland)  
 Aubert, Pierre, F. (France)  
 Auer, Franz (Germany)  
 Auer, Roland (Germany)  
 Aulaskari, Rauno (Finland)  
 Aung, Min (Thailand)  
 Ausekle, Jelena (Estonia)  
 Avdispahic, Muharem (Bosnia and Herzegovina)  
 Avellaneda, Marco (USA)  
 Avritzer, Dan (Brazil)  
 Axt, Paul (USA)  
 Ayoub, Christine Williams (USA)  
 Ayoub, Raymond G. (USA)  
 Ayupov, Shavkat A. (Uzbekistan)  
 Azarpanah, Fariborz (Iran)  
 Azevedo, Alberto C. P. (Brazil)  
 Azimi, Parviz (Iran)  
 Baas, Nils A. (Norway)  
 Babbitt, Donald G. (USA)  
 Babenko, Vladyslav F. (Ukraine)  
 Bach, Volker (Germany)  
 Bachmann, Heidy (Germany)  
 Bacopoulos, Alexis (Greece)  
 Badiozzaman, Abdul J. (Iran)  
 Baidyk, Tatyana N. (Ukraine)  
 Baier, Georg (Germany)  
 Baier, Stephan (Germany)  
 Baillif, Mathieu (Switzerland)  
 Baker, Matthew H. (USA)  
 Bakonyi, Mihaly (USA)  
 Bakushinskii, Anatolii Borisovich (Russian Federation)  
 Balaji, Vikraman (India)  
 Balashevich, Nataliya V. (Belarus)  
 Balashova, Galina S. (Russian Federation)  
 Baldus, Frank (Germany)  
 Balke, Ludwig (Germany)  
 Ball, John M. (United Kingdom)  
 Balogh, Jozsef (Hungary)  
 Bamba, Siaka Kante (Ivory Coast)  
 Banaszak, Grzegorz M. (Poland)  
 Bancerek, Grzegorz (Poland)  
 Banchoff, Thomas F. (USA)  
 Bandelow, Christoph (Germany)  
 Bandt, Christoph (Germany)  
 Bangert, Victor (Germany)  
 Bangyan, Wen (P. R. China)  
 Bank, Bernd (Germany)  
 Bank, Peter (Germany)  
 Bantien, Alexander (Germany)  
 Bantsur, Nataliya (Ukraine)  
 Baouendi, Salah (USA)  
 Barannyk, Lyudmyla L. (Ukraine)  
 Baranov, Alexander (Belarus)  
 Barberis, María L. (Argentina)  
 Barbu, Anca Stefania (Romania)  
 Barchini, Leticia I. (USA)  
 Baribaud, Claire M. C. (Switzerland)  
 Barinka, Arne (Germany)

- Barner, Klaus (Germany)  
 Barrett, David E. (USA)  
 Barrow-Green, June E. (United Kingdom)  
 Bartels, Stephan (Germany)  
 Barthel, Gottfried (Germany)  
 Bartkiewicz, Monika (Poland)  
 Bartolini Bussi, Mariolina (Italy)  
 Bartosiewicz, Zbigniew J. (Poland)  
 Bartsch, Thomas (Germany)  
 Bass, Hyman (USA)  
 Batistela, Claudia Helena F. (Brazil)  
 Batyrev, Victor Vadimovich (Germany)  
 Baudisch, Andreas (Germany)  
 Bauer, Joachim (Germany)  
 Bauhardt, Wolfgang (Germany)  
 Baum, Helga (Germany)  
 Baumann, Astrid (Germany)  
 Bavula, Vladimir (United Kingdom)  
 Bayer, Tilman (Germany)  
 Bayoumi, Aboubakr (Kingdom of Saudi-Arabia)  
 Bazarov, Serguei (Russian Federation)  
 Becker, Hans-J. (Germany)  
 Becker, Paul-Georg (Germany)  
 Behforooz, Hossein (USA)  
 Behncke, Horst (Germany)  
 Behrend, Kai A. (Canada)  
 Behrends, Ehrhard (Germany)  
 Belabas, Karim (France)  
 Belinsky, Eduard (Zimbabwe)  
 Bellaiche, Andre (France)  
 Belousov, Evgeny G. (Russian Federation)  
 Ben Hariz, Samir (France)  
 Benjamin, Elliot (USA)  
 Ben Massaoud, Hedi (Tunisia)  
 Bensic, Mirta (Croatia)  
 Benyash-Krivetz, Valerii Vaclavovich (Belarus)  
 Ben-Zvi, David (USA)  
 Berenstein, Carlos A. (USA)  
 Berezovskaya, Faina S. (Russian Federation)  
 Berg, Christian (Denmark)  
 Berger, Bonnie (USA)  
 Bergmann, Wolfgang Reinhold (Italy)  
 Bergweiler, Walter (Germany)  
 Berkovich, Vladimir (Israel)  
 Berkovits, Juha (Finland)  
 Berninger, Heiko (Germany)  
 Bernstein, Joseph (Israel)  
 Beschler, Edwin (USA)  
 Bessenrodt, Christine (Germany)  
 Best, Christoph (Germany)  
 Bethuel, Fabrice (France)  
 Beutelspacher, Albrecht F. (Germany)  
 Beutelspacher, Christoph (Germany)  
 Bey, Christian (Germany)  
 Beylkin, Gregory (USA)  
 Bezuglyi, Sergey (Ukraine)  
 Bhat, B. V. Rajarama (India)  
 Bhattacharyya, Prodipeswar (India)  
 Bhosle, Ushadevi N. (India)  
 Bhupal, Mohan (Germany)  
 Bierstedt, Klaus D. (Germany)  
 Billard, Lynne (USA)  
 Biller, Harald (Germany)  
 Binder, Christa (Austria)  
 Binder, Ilia A. (USA)  
 Binder, Thomas S. (Germany)  
 Birnir, Bjorn (USA)  
 Bismut, Jean-Michel (France)  
 Bissantz, Nicolai (Germany)  
 Biswas, Indranil (India)  
 Biucchi, Gabriele (Italy)  
 Bjelica, Momcilo (Yugoslavia)  
 Blackwood, Carol-Ann (USA)  
 Blasius, Don (USA)  
 Blatter, Christian (Switzerland)  
 Blattner, Robert J. (USA)  
 Bless, Michael H. (Germany)  
 Bley, Andreas (Germany)  
 Blicke, Manuel (USA)  
 Blinov, Alexei V. (Russian Federation)  
 Bloch, Spencer J. (USA)  
 Blömker, Dirk (Germany)  
 Boalch, Philip P. (United Kingdom)  
 Bobenko, Alexander I. (Germany)  
 Boche, Holger (Germany)  
 Böcherer, Siegfried (Germany)  
 Bock, Hans (Germany)  
 Bock, Hans Georg (Germany)  
 Böckle, Gebhard (Germany)  
 Boden, Hans U. (USA)  
 Bodfish, Ed (USA)  
 Bödighheimer, Carl-Friedrich (Germany)  
 Bodnarescu, M. V. (Germany)  
 Boese, Fritz (Germany)  
 Böge, Sigrid (Germany)  
 Bognar, Gabriella (Hungary)  
 Bogomolny, Eugene (France)

- Bogovskii, Mikhail E. (Russian Federation)  
 Bohle, Christoph (Germany)  
 Bojarski, Bogdan (Poland)  
 Bolger, Robert E. (USA)  
 Bolibok, Krzysztof M. (Poland)  
 Bollobás, Béla (United Kingdom)  
 Bonckaert, Patrick (Belgium)  
 Bonet, Jose (Spain)  
 Bonk, Mario (Germany)  
 Bonnet, Philippe (France)  
 Boo, Per-Anders (Sweden)  
 Booß-Barnbek, Bernhelm (Denmark)  
 Borchardt, Juergen (Germany)  
 Borchers, Richard E. (United Kingdom)  
 Bordag, Ljudmila A. (Germany)  
 Börgens, Manfred (Germany)  
 Börger, Reinhard (Germany)  
 Borgs, Christian (USA)  
 Borisovich, Andrei Yu. (Poland)  
 Borisovich, Yuri G. (Russian Federation)  
 Borndörfer, Ralf (Germany)  
 Borodin, Andrei Nikolaevich (Russian Federation)  
 Bors, Dorota (Poland)  
 Borwein, David (Canada)  
 Boskamp, Tobias (Germany)  
 Bottazzini, Umberto (Italy)  
 Böttcher, Roger (Germany)  
 Boucherif, Abdelkader (Algeria)  
 Bouchiba, Samir (Morocco)  
 Bouetou, Thomas (Cameroon)  
 Bouguima, Sidi Mohammed (Algeria)  
 Boukricha, Abderrahman (Tunisia)  
 Bourguignon, Jean-Pierre (France)  
 Bourman, Iouri M. (Russian Federation)  
 Boutot, Jean-Francois (France)  
 Bovier, Anton (Germany)  
 Boyallian, Carina (Argentina)  
 Bozeman, James R. (USA)  
 Bozer, Mehmet (Cyprus)  
 Bozin, Vladimir (Yugoslavia)  
 Braendli, Emil R. (Switzerland)  
 Bramson, Maury D. (USA)  
 Brandao, Paulo (Brazil)  
 Brandenburg, Harald (Germany)  
 Brandt, Manfred (Germany)  
 Brandt, Stephan (Germany)  
 Branner, Bodil (Denmark)  
 Bratzler, Clemens (Germany)  
 Brauer, George (USA)  
 Braun, Rüdiger W. (Germany)  
 Braunß, Hans-Andreas (Germany)  
 Brecht, Gerhard (Germany)  
 Breckner, Wolfgang W. (Romania)  
 Bredimas, Antoine-A. P. (France)  
 Breger, Manfred (Germany)  
 Brehm, Ulrich (Germany)  
 Bremer, Ingo (Germany)  
 Breuning, Manuel (Germany)  
 Brezhnev, Yurii (Russian Federation)  
 Bridges, Douglas S. (New Zealand)  
 Brieden, Andreas (Germany)  
 Brieskorn, Egbert (Germany)  
 Brinzanescu, Vasile P. (Romania)  
 Brodsky, Mikhail (USA)  
 Brokate, Martin (Germany)  
 Brookfield, Gary J. (USA)  
 Broser, Britta (Germany)  
 Brothers, Malgorzata (USA)  
 Broughan, Kevin A. (New Zealand)  
 Browder, Felix E. (USA)  
 Brown, Aldric L. (India)  
 Brown, Leon (USA)  
 Brown, Tom C. (Canada)  
 Brück, Rainer (Germany)  
 Brucker, David (Israel)  
 Bruckner, Gottfried (Germany)  
 Brueckmann, Klaus Peter (Germany)  
 Brunaud, Marc (France)  
 Brüning, Jochen (Germany)  
 Brunner, Götz (Germany)  
 Brunotte, Horst (Germany)  
 Bruns, Annika (Germany)  
 Bruns, Peter (Germany)  
 Bruns, Winfried (Germany)  
 Brykalov, Sergei A. (Russian Federation)  
 Brzezinski, Juliusz (Sweden)  
 Bu, Charles (USA)  
 Buan, Aslak B. (Norway)  
 Bănulescu, C. Martha (Romania)  
 Bubner, Nikolaus (Germany)  
 Buchanan, Thomas (Germany)  
 Buchholz, Detlev (Germany)  
 Buchsteiner, Alexandra (Germany)  
 Buchsteiner-Kießling, Edeltraud (Germany)  
 Buckwar, Evelyn (Germany)  
 Buescu, Jorge C. (Portugal)  
 Bujalance, Emilio (Spain)

- Bujalance, Jose A. (Spain)  
 Bulboaca, Teodor (Romania)  
 Bulckens, Anne M. (Australia)  
 Bulinski, Alexander V. (Russian Federation)  
 Bulinskij, Andrej V. (Russian Federation)  
 Bumby, Richard T. (USA)  
 Bungartz, Paul (Germany)  
 Bunke, Olaf (Germany)  
 Bunke, Ulrich (Germany)  
 Burago, Dmitri (USA)  
 Burde, Dietrich (Germany)  
 Burger, Heinz H. (Germany)  
 Burger, Isabella C. (South Africa)  
 Burns, Daniel M. (USA)  
 Busneag, Dumitru (Romania)  
 Buswell, Stephen (United Kingdom)  
 Butkovic, Davor (Croatia)  
 Buttler, Michael (USA)  
 Button, Jack O. (United Kingdom)  
 Byrne, Catriona M. (Germany)  
 Bytsko, Andrei G. (Russian Federation)  
 Byunghan, Kim (USA)
- Cabana, Alejandra (Venezuela)  
 Cafarov, Dzhuma (Tajikistan)  
 Cagliero, Leandro R. (Argentina)  
 Cahen, Paul-Jean (France)  
 Calkin, Neil J. (USA)  
 Calvo, Jorge Albert (USA)  
 Campbell, Paul J. (USA)  
 Campillo, Antonio (Spain)  
 Can, Mehmet (Turkey)  
 Canales, Mónica del Pilar (Chile)  
 Canas da Silva, Ana (USA)  
 Cannon, Anne (Australia)  
 Cannon, John J. (Australia)  
 Cappel, Sylvan (USA)  
 Caps, Oliver (Germany)  
 Caraman, Petru (Romania)  
 Cardiner, Anthony (United Kingdom)  
 Cardona, Augusto Vieira (Brazil)  
 Carlson, Robert (USA)  
 Carmona, Angeles (Spain)  
 Carnal, Henri C. (Switzerland)  
 Caro, Jaime D. L. (Philippines)  
 Carr, Jack (United Kingdom)  
 Carroll, Robert W. (USA)  
 Carter, J. Scott (USA)  
 Casacuberta, Carles (Spain)  
 Casati, Paolo (Italy)
- Cascon, Ana (United Kingdom)  
 Case, Bettye A. (USA)  
 Cassaigne, Julien (France)  
 Castellet, Manuel (Spain)  
 Catalan, Raquel-Garcia (Spain)  
 Catanese, Fabrizio M. E. (Germany)  
 Catinas, Emil A. (Romania)  
 Cazaran, Jilyana (Australia)  
 Cercignani, Carlo (Italy)  
 Chadan, John (USA)  
 Chahal, Jasbir S. (USA)  
 Chaleyat-Maurel, Mireille (France)  
 Chan, Tony F. (USA)  
 Chang, Kun Soo (Korea)  
 Chari, Manoj (Germany)  
 Chatterji, Srishti (S. D.) (Switzerland)  
 Chatyrko, Vitali (Sweden)  
 Chayes, Jennifer T. (USA)  
 Chebanov, Dmitriy A. (Ukraine)  
 Chebotarev, Alexander M. (Russian Federation)  
 Chechkin, Gregory A. (Russian Federation)  
 Cheddadi, Abdelkhalek (Morocco)  
 Chemla, Karine (France)  
 Chen, Chin-Yun (Germany)  
 Chen, Jiecheng (P. R. China)  
 Chen, Wenxiong (USA)  
 Chen, Zhiming (P. R. China)  
 Cheng, Chong-Qing (P. R. China)  
 Cheng, Ningning (P. R. China)  
 Chentsov, Alexander G. (Russian Federation)  
 Cherednik, Ivan V. (USA)  
 Cherinda, Marcos (Mozambique)  
 Cherniha, Roman M. (Ukraine)  
 Chernousov, Vladimir (Belarus)  
 Cherry, William A. (Germany)  
 Chiang, Tzue-Shuh (Taiwan)  
 Chien, Mao-Ting (Taiwan)  
 Chikrii, Arkadii A. (Ukraine)  
 Chillag, David (Israel)  
 Chin, Angelina Y. M. C. (Malaysia)  
 Chinen, Koji (Japan)  
 Chiu, Sou-yung (Taiwan)  
 Cho, Yong S. (Korea)  
 Choban (Cioban), Mitrofan M. (Moldova)  
 Chowdhury, Munibur Rahman (Bangladesh)  
 Christ, Michael (USA)

- Christ, Ulrich (Germany)  
 Christiansen, Chr. Andreas (Norway)  
 Chua, Kok Seng (Singapore)  
 Chynkulyak, Nataliya Nikolaevna  
 (Ukraine)  
 Ciegis, Raimondas (Lithuania)  
 Ciesielski, Zbigniew (Poland)  
 Cieslik, Dietmar (Germany)  
 Cioranescu, Doina (France)  
 Cipu, Mihai I. (Romania)  
 Ciric, Miroslav D. (Yugoslavia)  
 Clarke, Francis W. (United Kingdom)  
 Coates, John H. (United Kingdom)  
 Cohen, Paula B. (France)  
 Cohn, Harvey (USA)  
 Colding, Tobias Holck (USA)  
 Collet, Pierre (France)  
 Colli, Eduardo (France)  
 Colliot-Théle, Jean-Louis (France)  
 Colmez, Pierre (France)  
 Colonius, Fritz (Germany)  
 Conduché, Daniel (France)  
 Conlon, Lawrence W. (USA)  
 Connett, William C. (USA)  
 Conrad, Marc (Germany)  
 Conrani, Katia (United Kingdom)  
 Conte, Alberto (Italy)  
 Cook, William J. (USA)  
 Cooke, Roger L. (USA)  
 Coonce, Harry B. (USA)  
 Coornaert, Michel (France)  
 Cordaro, Paulo (Brazil)  
 Cordes, Frank (Germany)  
 Cordes, Heinz O. (USA)  
 Cornalba, Maurizio (Italy)  
 Costa, Sueli I. R. (Brazil)  
 Cowles, Lauren (USA)  
 Crapo, Henry (France)  
 Craveiro de Carvalho, Francisco J.  
 (Portugal)  
 Crespo, Teresa (Spain)  
 Crespo Crespo, Cecilia R. (Argentina)  
 Cristea, Valentin Gabriel (Romania)  
 Croft, Hallard T. (United Kingdom)  
 Cromme, Ludwig (Germany)  
 Cullen, Helen F. (USA)  
 Cuntz, Joachim (Germany)  
 Czarnecki, Maciej A. (Poland)  
 Czichowski, Günter (Germany)  
 Dahan-Dalmedico, Amy (France)  
 Dais, Dimitrios I. (Germany)  
 Dale, Knut Th. (Norway)  
 Dalitz, Wolfgang (Germany)  
 Damanik, David (Germany)  
 Damlamian, Alain (France)  
 Danchev, Daniel Marinov (Bulgaria)  
 D'Ancona, Piero A. (Italy)  
 Danet, Nicolae (Romania)  
 Danet, Rodica Mihaela (Romania)  
 Danishevs'kyy, Vladyslav V. (Ukraine)  
 Darafsheh, Mohammad Reza (Iran)  
 Dark, Rex (Ireland)  
 Das, Laxminarayan (India)  
 Dascalescu, Sorin (Romania)  
 Dashkova, Ol'ga Yu. (Ukraine)  
 Dasic, Vucic (Yugoslavia)  
 Dauben, Joseph (USA)  
 Daverman, Robert (USA)  
 David, Herbert A. (USA)  
 Davis, Chandler (Canada)  
 Davis, James F. (USA)  
 Davis, Philip J. (USA)  
 Davydov, Alexei (Russian Federation)  
 Dawson, Donald (Canada)  
 Dawson, John W. (USA)  
 Daxlberger, Christian (Germany)  
 Debicka, Joanna (Poland)  
 Debicki, Krzysztof (Poland)  
 Debinska-Nagorska, Anna (Poland)  
 De Blasi, Francesco (Italy)  
 Debnath, Joyati (USA)  
 Debnath, Narayan C. (USA)  
 Dediu, Luminita Simona (New Zealand)  
 de Faria, Edson (Brazil)  
 de Guzman, Miguel (Germany)  
 Deift, Percy Alec (USA)  
 Deitmar, Anton (Germany)  
 de Jong, Aise J. (USA)  
 de Jong, Johan (Netherlands)  
 Del Angel R., Pedro L. (Mexico)  
 Deligne, Pierre (USA)  
 Dell' Antonio, Gianfausto (Italy)  
 de Longueville, Mark (Germany)  
 Del Riego, Lilia (Mexico)  
 de Melo, Wellington (Brazil)  
 Demidenko, Gennadii V. (Russian  
 Federation)  
 Demidov, Sergei S. (Russian Federation)  
 Demuth, Michael (Germany)  
 Deninger, Christopher (Germany)

- Dennis, R. Keith (USA)  
 Denzler, Jochen (Germany)  
 De Sousa-Dias, M. Esmeralda (Portugal)  
 Desquith, Etienne (Ivory Coast)  
 Dessai, Anand (Germany)  
 Deszcz, Ryszard (Poland)  
 Deuber, Walter (Germany)  
 Deuffhard, Peter (Germany)  
 Deuschel, Jean-Dominique (Germany)  
 Diaconis, Persi W. (USA)  
 Diaconu, Calin A. (USA)  
 Didenko, Victor D. (Ukraine)  
 Diener, Karl-Heinz (Germany)  
 Diep, Do Ngoc (Vietnam)  
 Dieulefait, Luis V. (Spain)  
 Dijkgraaf, Robbert (Netherlands)  
 Dikoussar, Vassili (Russian Federation)  
 Dillen, Franki (Belgium)  
 Dimitric, Ivko M. (USA)  
 Dinar, Nathan (Israel)  
 Ding, Weiyue (P. R. China)  
 Dinges, Hermann (Germany)  
 Di Piazza, Luisa (Italy)  
 Dittrich, Bianca (Germany)  
 Djokovic, Dragomir (Canada)  
 Dold, Albrecht (Germany)  
 Dolzmann, Andreas (Germany)  
 Domanski, Pawel (Poland)  
 Domingo-Vecchioni, Miguel (Germany)  
 Domokos, Matyas (Hungary)  
 Donaldson, Simon K. (USA)  
 Donig, Jörg (Germany)  
 Dorn, Andreas (Germany)  
 Dorninger, Dietmar (Austria)  
 Dorschfeldt, Christoph (Germany)  
 Doser, Jürgen (Germany)  
 Dosiyevev, Adigezal (Cyprus)  
 Doslic, Tomislav (Croatia)  
 Dotti, Isabel G. (Argentina)  
 Doty, Stephen R. (USA)  
 Douady, Adrien (France)  
 Douady, Regine (France)  
 Douglas, Lloyd (USA)  
 Douglas, Robert J. (USA)  
 Döweling, Sebastian (Germany)  
 Downey, Jessica (USA)  
 Doyen, Jean V. (Belgium)  
 Drabant, Bernhard (United Kingdom)  
 Draexler, Peter (Germany)  
 Dragovic, Vladimir (Yugoslavia)  
 Dranishnikov, Alexander N. (USA)  
 Draper, Cristina (Spain)  
 Dress, Andreas W. M. (Germany)  
 Dreyer, Wolfgang (Germany)  
 Driver, Kathy A. (South Africa)  
 Droescher, Christian (Germany)  
 Druetta, Maria Josefina (Argentina)  
 Drygas, Hilmar (Germany)  
 Dryuma, Valery (Moldova)  
 Duan, Jinqiao (USA)  
 Dubickas, Arturas (Lithuania)  
 Dubinsky, Andrej Yu. (Russian Federation)  
 Dubischar, Daniel (Germany)  
 Dubrovin, Boris (Italy)  
 Dudley, Richard M. (USA)  
 Dudnikova, Tatjana (Russian Federation)  
 Duduchava, Roland (Georgia)  
 Duistermaat, Johannes J. (Netherlands)  
 Duke, William (USA)  
 Dümmel, Fritz (Germany)  
 Dumortier, Freddy (Belgium)  
 Dunne, Edward G. (USA)  
 Duplij, Steven (Ukraine)  
 Duren, Peter (USA)  
 Durfee, Alan H. (USA)  
 Dusembaev, Anuar (Kazakhstan)  
 Duzaar, Frank (Germany)  
 Dvoretzky, Aryeh (Israel)  
 Dvornicich, Roberto (Italy)  
 Dvorsky, Alexander (USA)  
 Dwyer, William Gerard (USA)  
 Dymara, Jan (Poland)  
 Dynkin, Evsei M. (Israel)  
 Dzhumadil'daev, Askar (Kazakhstan)  
 Dzhuraev, Abduhamid (Tajikistan)  
 Dziri, Raja (Tunisia)  
 Dziubanski, Jacek (Poland)  
 Eberhard, Walter (Germany)  
 Eberlein, Dominik (Germany)  
 Eberlein, Ernst W. (Germany)  
 Ebihara, Madoka (Japan)  
 Ebmeyer, Carsten (Germany)  
 Eckner, Stephan (Germany)  
 Eckstein, Frank (Germany)  
 Edwards, Elisabeth J. (United Kingdom)  
 Edwards, Robert D. (USA)  
 Eglewski, Dennis W. (USA)  
 Egorov, Alexandre A. (Russian Federation)

- Eguchi, Kazuo (Japan)  
 Ehret, Marietta (Germany)  
 Ehrig, Hartmut (Germany)  
 Ehrig, Rainald (Germany)  
 Eibeck, Andreas (Germany)  
 Eida, Atsuhiko (Japan)  
 Eilertsen, Stefan (Sweden)  
 Eisenblätter, Andreas (Germany)  
 Eisenbrand, Friedrich (Germany)  
 Eisenbud, David (USA)  
 Eisentraeger, Kirsten (USA)  
 Eisermann, Volker (Germany)  
 Ekama Sossa Mben, Andre Sam (Germany)  
 Ekeland, Ivar (France)  
 Ekhaguere, Godwin (Nigeria)  
 Ekong, Samuel (France)  
 Elbaz-Vincent, Philippe (France)  
 Eliashberg, Yakov (USA)  
 Eliasson, Håkan (Sweden)  
 El Kinani, El Hassan (Morocco)  
 Elliott, George A. (Canada)  
 Elschner, Johannes (Germany)  
 Elstrodt, Jürgen (Germany)  
 El Yacoubi, Nouzha (Morocco)  
 Emerson, Annette (USA)  
 Emmer, Michele (Italy)  
 Encinas, Andres, M. (Spain)  
 Engel, Konrad (Germany)  
 Engell, Sebastian (Germany)  
 Engler, Hans (USA)  
 Engquist, Bjorn Erik (Sweden)  
 Enkhbat, Rentsen (Mongolia)  
 Enock, Michel (France)  
 Enomoto, Kazuyuki (Japan)  
 Enß, Volker (Germany)  
 Epstein, Mordechai (Israel)  
 Erbay, Hüsnü Ata (Turkey)  
 Erbay, Saadet (Turkey)  
 Erdmann, Bodo (Germany)  
 Erdogan, Hakki Ismail (Turkey)  
 Eriksson, Folke S. (Sweden)  
 Erle, Dieter (Germany)  
 Eschenbach, Christina (Germany)  
 Eschenburg, Rolf (Germany)  
 Eskin, Alexander (USA)  
 Esser, Angelika E. (Germany)  
 Esteves, Eduardo S. (Brazil)  
 Estevez, José Luis (Spain)  
 Estevez Schwarz, Diana (Germany)
- Eto, Kazufumi (Japan)  
 Eudave-Munoz, Mario (Mexico)  
 Evans, David E. (United Kingdom)  
 Ewing, John H. (USA)  
 Eyles, Joseph W. (USA)  
 Ezquerro, Jose A. (Spain)
- Faatz, Vanessa (Germany)  
 Faber, Carel (USA)  
 Fabian, Benjamin (Germany)  
 Faddeev, Ludvig D. (Russian Federation)  
 Fahl, Michael (Germany)  
 Fahsi, Abdelhak (Morocco)  
 Faltings, Gerd (Germany)  
 Faminskii, Andrei V. (Russian Federation)  
 Fandom Noubiap, Roger (Germany)  
 Farge, Marie (France)  
 Farr, Graham E. (Australia)  
 Farsi, Carla E. (USA)  
 Fasso Velenik, Agnese (Germany)  
 Fathi, Albert (France)  
 Fayad, Bassam (France)  
 Faybusovich, Leonid (USA)  
 Fedosov, Boris (Germany)  
 Fedotov, Igor (South Africa)  
 Fedotov, Sergei (United Kingdom)  
 Fedynyak, Stepan (Ukraine)  
 Feehan, Paul M. N. (USA)  
 Feher, Franziska (Germany)  
 Feichtner, Eva Maria (Germany)  
 Feigenbaum, Joan (USA)  
 Feith, Michael (Germany)  
 Feix, Birte (United Kingdom)  
 Feldhusen, Dirk (Germany)  
 Fels, Marten (Germany)  
 Fel'shtyn, Alexander (Germany)  
 Felsner, Stefan (Germany)  
 Fernandes, Cristina G. (Brazil)  
 Fernandes, Rui L. (Portugal)  
 Fernandez, Arturo (Spain)  
 Feroe, John A. (USA)  
 Ferreira, Fernando Flavio (Portugal)  
 Ferreira, J. A. (Portugal)  
 Ferus, Dirk (Germany)  
 Fialowski, Alice (Hungary)  
 Fiedler, Bernold (Germany)  
 Fieker, Claus (Germany)  
 Fieseler, Martin (Germany)  
 Figiel, Tadeusz (Poland)  
 Filip, Anja (Germany)  
 Filipsson, Lars (Sweden)

- Fillmore, Peter A. (Canada)  
 Fimmel, Torsten (Germany)  
 Fintushel, Ronald A. (USA)  
 Fischer, Alexander (Germany)  
 Fischer, Andreas (Germany)  
 Fischer, Arthur E. (USA)  
 Fischer, Gerd (Germany)  
 Fishel, Susanna D. (Germany)  
 Fittler, Robert (Germany)  
 Fjelstad, Paul (USA)  
 Flach, Matthias (USA)  
 Flato, Moshé (France)  
 Fleischmann, Klaus (Germany)  
 Fleischmann, Peter (Germany)  
 Flor, Peter (Austria)  
 Flores-Bazan, Fabian (Chile)  
 Florit, Luis A. (Brazil)  
 Flytzanis, Elias (Greece)  
 Folland, Gerald B. (USA)  
 Föllmer, Hans (Germany)  
 Fontana, Marco (Italy)  
 Foreman, Matthew (USA)  
 Forger, Michael (Brazil)  
 Förster, Christian (Germany)  
 Förster, Karl-Heinz (Germany)  
 Forti, Marco (Italy)  
 Fossi Talom, Leopold (Germany)  
 Fossum, Robert M. (USA)  
 Fotheringham, Gerhard (Germany)  
 Fourie, Jan H. (South Africa)  
 Francis, George (USA)  
 Frank, András (Hungary)  
 Frank, Michael (USA)  
 Franke, Dirk (Germany)  
 Frankl, Astrid (Germany)  
 Franz, Matthias (Germany)  
 Freedman, Michael Hartley (USA)  
 Fregier, Yael (France)  
 Freidlin, Mark (USA)  
 Frese, Hans-Hermann (Germany)  
 Frey, Christian (Germany)  
 Friedland, Lew (USA)  
 Friedlander, Eric Mark (USA)  
 Friedlander, Susan (USA)  
 Friedman, Eduardo C. (Chile)  
 Friedrich, Axel (Germany)  
 Friedrichs, Carsten (Germany)  
 Friese, Nicolas (Germany)  
 Friese, Stephan (Germany)  
 Fring, Andreas (Germany)  
 Fritsch, F. Rudolf (Germany)  
 Fritzlar, Torsten (Germany)  
 Frolovitchev, Sergey (Russian Federation)  
 Fry, Robb C. (Canada)  
 Frydrych, Mariusz (Poland)  
 Fuchs, Ulrich (Germany)  
 Fuhrmann, Jürgen (Germany)  
 Fujii, Akio (Japan)  
 Fujii, Nobuo (Japan)  
 Fujita, Keiko (Japan)  
 Fukushima, Masatoshi (Japan)  
 Fukushima, Nobuhisa (Japan)  
 Furihata, Daisuke (Japan)  
 Furutani, Kenro (Japan)  
 Gaál, István (Hungary)  
 Gaertner, Klaus (Germany)  
 Gaiko, Valery A. (Belarus)  
 Gajda, Wojciech J. (Poland)  
 Gajewski, Herbert (Germany)  
 Galewski, Marek (Poland)  
 Gallavotti, Giovanni (Italy)  
 Gallot, Sylvestre (France)  
 Gamba, Irene M. (USA)  
 Gamst, Jens (Germany)  
 Gan, Shaobo (P. R. China)  
 Gangl, Herbert (Germany)  
 Ganief, M. Shahiem (South Africa)  
 Gao, Xuhong (USA)  
 Garimella, Venkatalakshmi Gayatri  
 (India)  
 Garling, David J. H. (United Kingdom)  
 Garrido Bullon, Angel L. (Spain)  
 Gärtner, Bernd (Switzerland)  
 Gärtner, Jürgen (Germany)  
 Gatermann, Karin (Germany)  
 Gattazzo, Remo (Italy)  
 Gatto, A. Eduardo (USA)  
 Gawrilow, Ewgenij (Germany)  
 Gay, David M. (USA)  
 Gebauer, Susanna (Germany)  
 Gebel, Michael (Germany)  
 Geddes, Keith O. (Canada)  
 Gehring, Frederick W. (USA)  
 Geiger, Jochen (Germany)  
 Geisser, Thomas H. (Germany)  
 Geissler, Katharina (Germany)  
 Gelfand, Sergei (USA)  
 Geller, Daryl N. (USA)  
 Geluk, Jaap (United Arab Emirates)  
 Georgescu, Adelina (Romania)



- Georgii, Hans-Otto (Germany)  
 Gérard, Olivier P. (France)  
 Gerisch, Magnus (Germany)  
 Gerlach, Eberhard (USA)  
 Gerstner, Manfred (Germany)  
 Geyler, Vladimir A. (Russian Federation)  
 Ghanaat, Patrick (Germany)  
 Ghate, Eknath P. (India)  
 Ghazel, Moncef (Tunisia)  
 Ghorpade, Sudhir R. (India)  
 Ghosh, Jayanta Kumar (India)  
 Ghoussoub, Nassif (Canada)  
 Giaquinto, Anthony (USA)  
 Gidea, Marian (USA)  
 Giesen, Joachim (Switzerland)  
 Gietl, Thomas (Germany)  
 Gigena, Salvador D. R. (Argentina)  
 Gil, Juan B. (Germany)  
 Gilanyi, Attila (Hungary)  
 Gilliard, Elizabeth (United Kingdom)  
 Gillman, Leonard (USA)  
 Gillot, Antonio E. (Guatemala)  
 Gil-Medrano, Olga (Spain)  
 Giordano, Anna (Italy)  
 Giorgilli, Antonio (Italy)  
 Giudici, Reinaldo (Venezuela)  
 Gjone, Gunnar (Norway)  
 Glass, Thomas (Germany)  
 Glazman, Mary (Mexico)  
 Gleska, Alina (Poland)  
 Glimm, Ekkehard (Germany)  
 Glitzky, Annegret (Germany)  
 Glöckner, Helge (Germany)  
 Gloden, Raoul R. F. G. (Luxembourg)  
 Glutsuk, Alexei A. (Russian Federation)  
 Göbel, Dietmar (Germany)  
 Göbel, Silke (Germany)  
 Goddard, Peter (United Kingdom)  
 Goemans, Michel X. (Belgium)  
 Goette, Sebastian (Germany)  
 Goetz, Abraham (USA)  
 Goldblatt, Robert (New Zealand)  
 Goldstern, Martin (Austria)  
 Gollek, Hubert (Germany)  
 Golodets, Valentyn Ja. (Ukraine)  
 Golomb, Michael (USA)  
 Golubeva, Valentina (Russian Federation)  
 Golovanov, Anton A. (Russian Federation)  
 Golovanova, Nina F. (Russian Federation)  
 Gomenyuk, Sergey (Ukraine)  
 Gomez Bermudez, Carlos (Spain)  
 Gomez Bofill, Walter (Germany)  
 Gomez-Mont, Xavier (Mexico)  
 Gomez Pardo, José L. (Spain)  
 Gonchar, Andrei A. (Russian Federation)  
 González, Cesareo (Spain)  
 Goodman, Gerald S. (Italy)  
 Goodman, Jacob E. (USA)  
 Gorenflo, Rudolf (Germany)  
 Goresky, R. Mark (USA)  
 Goritsky, Andrey Yu. (Russian Federation)  
 Gorodski, Claudio (Brazil)  
 Gottlieb, Daniel H. (USA)  
 Gottschalk, Harald (Germany)  
 Götze, Friedrich (Germany)  
 Gowers, W. Timothy (United Kingdom)  
 Grabitz, Martin (Germany)  
 Graeff, Robert (Germany)  
 Graf, Gian Michele (Switzerland)  
 Graf, Klaus-D. (Germany)  
 Graham, Ronald L. (USA)  
 Gramain, François (France)  
 Gramsch, Bernhard F. (Germany)  
 Granovsky, Boris L. (Israel)  
 Grase, Saida (Germany)  
 Grassi, Michele (Italy)  
 Grassmann, Hubert (Germany)  
 Gräter, Joachim (Germany)  
 Grattan-Guinness, Ivor (United Kingdom)  
 Gray, Jeremy John (United Kingdom)  
 Grayson, Daniel R. (USA)  
 Green, Mark L. (USA)  
 Greengard, Leslie Frederick (USA)  
 Greenspoon, Arthur (USA)  
 Greil, Anton (Germany)  
 Greither, Cornelius (Canada)  
 Grell, Juliana (Germany)  
 Grenander, Ulf (USA)  
 Greuel, Bernd (Germany)  
 Greuel, Gert-Martin W. (Germany)  
 Grieser, Daniel (Germany)  
 Griffiths, Peter L. (United Kingdom)  
 Grinberg, Natalia I. (Germany)  
 Grinnell, Raymond J. (Barbados)  
 Gritzmann, Peter (Germany)  
 Grkovska, Slavica (Macedonia)  
 Grobler, Jacobus J. (South Africa)  
 Grobstich, Peter (Germany)

- Gröwe-Kuska, Nicole (Germany)  
 Grof, Jozsef (Hungary)  
 Gröger, Konrad (Germany)  
 Grözl, Wolfgang (Germany)  
 Gromov, Nikolai (Russian Federation)  
 Gronau, Hans-Dietrich O. F. (Germany)  
 Gröpl, Clemens (Germany)  
 Gropp, Harald (Germany)  
 Grosse-Erdmann, Karl-Goswin (Germany)  
 Grotowski, Joseph F. (Germany)  
 Grötschel, Martin (Germany)  
 Gruber, Michael J. (Germany)  
 Grund, Friedrich (Germany)  
 Grundhöfer, Theo (Germany)  
 Grünvogel, Stefan Michael (Germany)  
 Grüter, Michael (Germany)  
 Grzanna, Jürgen (Germany)  
 Grzaslewicz, Ryszard (Poland)  
 Grzymkowski, Radoslaw (Poland)  
 Gu, Weiqing (USA)  
 Guccione, Linda (USA)  
 Guddat, Jürgen (Germany)  
 Guillaume, Anne (United Kingdom)  
 Guillopé, Laurent (France)  
 Gunawan, Hendra (Indonesia)  
 Gundlach, Karl-Bernhard (Germany)  
 Gunson, Jack (United Kingdom)  
 Günzler, Hans (Germany)  
 Guo, Jin Yun (P. R. China)  
 Guo, Shirong (United Kingdom)  
 Gurak, Stanley J. (USA)  
 Gursky, Matthew J. (USA)  
 Gusein-Zade, Sabir M. (Russian Federation)  
 Gusevskii, Nikolai (Brazil)  
 Gusinde, Ellinor (Germany)  
 Gustedt, Jens (Germany)  
 Guthschmidt, Norman (Germany)  
 Gutiérrez, José M. (Spain)  
 Guyard, Frederic (Germany)  
 Haase, Christian (Germany)  
 Haase, Markus (Germany)  
 Habetha, Klaus (Germany)  
 Haccou, Maryene (Netherlands)  
 Hachimori, Masahiro (Japan)  
 Hackbusch, Wolfgang (Germany)  
 Hafner, Paul R. (New Zealand)  
 Hag, Kari (Norway)  
 Hag, Per (Norway)  
 Haida, Minoru (Japan)  
 Haidar, Mahmoud (Kuwait)  
 Haines, Thomas J. (Germany)  
 Hajdu, Lajos (Hungary)  
 Hajduk, Boguslaw (Poland)  
 Hajnal, Peter (Hungary)  
 Hajto, Zbigniew (Spain)  
 Hakim, Jeffrey L. (USA)  
 Hakulinen, Ville (Finland)  
 Hales, Thomas C. (USA)  
 Hall, Peter Gavin (Australia)  
 Hall, Richard L. (Canada)  
 Haller, Rainis (Estonia)  
 Halperin, Benjamin D. (USA)  
 Halupczok, Karin (Germany)  
 Hamana, Yuji (Japan)  
 Hämarik, Uno (Estonia)  
 Han, Chong-Kyu (Korea)  
 Han, Zheng-Chao (USA)  
 Handa, Kenji (Japan)  
 Handrock-Meyer, Sybille (Germany)  
 Hanke, Bernhard (Germany)  
 Hanke, Timo (Germany)  
 Hannappel, Susanne (Germany)  
 Hansen, Sönke (Germany)  
 Hansen, Vagn L. (Denmark)  
 Hansen, Wolfhard (Germany)  
 Hantschmann, Andreas (Germany)  
 Happel, Dieter (Germany)  
 Harbater, David (USA)  
 Harmand, Peter (Germany)  
 Harms, Jan (Germany)  
 Haroutunian, Samvel (Armenia)  
 Harris, Michael H. (France)  
 Härterich, Jörg (Germany)  
 Härterich, Martin (Germany)  
 Hartl, Urs T. (Germany)  
 Hartmann, Stephan (Germany)  
 Hartmann, Sven (Germany)  
 Hartz, David (USA)  
 Harutjunjan, Gohar (Germany)  
 Harzheim, Egbert R. (Germany)  
 Hasegawa, Keizo (Japan)  
 Hasegawa, Kenji (Japan)  
 Hasenjaeger, Gisbert F. R. (Germany)  
 Hashagen, Ulf (Germany)  
 Hashiguchi, Hideko (Japan)  
 Hashiguchi, Norikazu (Japan)  
 Hashimoto, Hideya (Japan)  
 Hass, Joel (USA)  
 Hassler, Uwe (Germany)

- Håstad, Johan (Sweden)  
 Hatori, Asako (Japan)  
 Hattori, Akio (Japan)  
 Haus, Utz-Uwe (Germany)  
 Hausen, Jürgen (Germany)  
 Hauser, Nico (Germany)  
 Hausmann, Jean-Claude R. (Switzerland)  
 Haverhals, John S. (USA)  
 Hayashi, Shuhei (Japan)  
 Hayes, Brian T. (USA)  
 Hazewinkel, Michiel (Netherlands)  
 He, Xinyu (United Kingdom)  
 Hebermehl, Georg (Germany)  
 Hebert, Michel (Egypt)  
 Hedberg, Lars Inge (Sweden)  
 Hedenmalm, Haakan P. (Sweden)  
 Hege, Hans-Christian (Germany)  
 Heiermann, Volker J. (Germany)  
 Heiming, Helmut (Germany)  
 Hein, Georg (Germany)  
 Heinig, Hans P. (Canada)  
 Heintze, Ernst (Germany)  
 Heinz, Alois (Germany)  
 Heinze, Joachim (Germany)  
 Heiss, Stefan (Germany)  
 Hejzman, Jan (Czech Republic)  
 Helder mann, Norbert (Germany)  
 Hélein, Frédéric (France)  
 Helemskii, Alexander Ya. (Russian Federation)  
 Hell, Stephan (Germany)  
 Helmberg, Christoph (Germany)  
 Helmberg, Gilbert (Austria)  
 Helmbold, Matthias (Germany)  
 Helversen-Pasotto, Anna (France)  
 Hemkemeier, Boris (Germany)  
 Henk, Martin (Germany)  
 Hennig, Franziska (Germany)  
 Hennig, Steffen (Germany)  
 Henrion, René (Germany)  
 Heringlehner, Josef (Germany)  
 Herman, Michael (France)  
 Hermann, Frieder (Germany)  
 Herrmann, Burghard F. G. (Germany)  
 Herrmann, Eva (Germany)  
 Herrmann, Oliver J. (Germany)  
 Herrmann, Siegfried (Germany)  
 Hertling, Claus (Germany)  
 Hertrich-Jeromin, Udo J. (Germany)  
 Heß, Florian (Germany)  
 Heuer, Gerald A. (USA)  
 Heyer, Herbert K. W. (Germany)  
 Hidaka, Fumio (Japan)  
 Hidalgo, Ruben A. (Chile)  
 Higson, Nigel David (USA)  
 Hildebrand, Roland (Germany)  
 Hille, Lutz (Germany)  
 Hillman, Jonathan A. (Australia)  
 Hilsberg, Isabel (Germany)  
 Himonas, Alexandrou A. (USA)  
 Hinrichs, Aicke (Germany)  
 Hintermann, Thomas (Switzerland)  
 Hinz, Andreas M. (Germany)  
 Hinze, Annika (Germany)  
 Hinze, Michael (Germany)  
 Hirayama, Hiroshi (Japan)  
 Hironaka, Eriko (USA)  
 Hirzebruch, Friedrich E. P. (Germany)  
 Hjorth, Gregory (USA)  
 Hoang, Viet Ha (United Kingdom)  
 Höbel, Willi (Germany)  
 Hodgson, Bernard R. (Germany)  
 Hofer, Helmut H. W. (Switzerland)  
 Hoffmann, Detlev W. (France)  
 Hoffmann, Karl-Heinz (Germany)  
 Hoffmann, Sigrid (Germany)  
 Hoffmann, Tim (Germany)  
 Hoffmann, Werner (USA)  
 Hofmann, Karl-Heinrich (Germany)  
 Hofmann, Wolf (Germany)  
 Hohberger, Horst H. (Germany)  
 Hohmuth, Lars (USA)  
 Höhn, Gerald (Germany)  
 Holm, Thorsten (Germany)  
 Holmann, Harald R. A. (Switzerland)  
 Holme, Audun (Norway)  
 Holopainen, Ilkka (Finland)  
 Holst, Stefan (Germany)  
 Holt, Fred B. (USA)  
 Holte, John M. (USA)  
 Holtkamp, Ralf (Germany)  
 Holtmanns, Silke (Germany)  
 Holz, Martin (Germany)  
 Holzapfel, Rolf-Peter (Germany)  
 Hömberg, Dietmar (Germany)  
 Homburg, Ale Jan (Germany)  
 Hooke, Nigel (Australia)  
 Hoppensteadt, Frank (USA)  
 Hora, Akihito (Japan)  
 Horiuchi, Kiyomitsu (Japan)

- Horiuchi, Ryutaro (Japan)  
 Horiuchi, Toshio (Japan)  
 Horn, Dietmar (Germany)  
 Hornbostel, Jens (France)  
 Hornor, William E. (USA)  
 Horst, Ulrich (Germany)  
 Horstmann, Dirk (Germany)  
 Hotje, Herbert (Germany)  
 Hou, Thomas Yizhao (USA)  
 Hou, Zhanyuan (United Kingdom)  
 Houh, Chorng Shi (USA)  
 Houssni, Mohamed (Morocco)  
 Hovhannisyan, Gro (Armenia)  
 Hric, Roman (Slovakia)  
 Hrushovski, Ehud (Israel)  
 Hryniv, Ostap (Germany)  
 Hu, Po (USA)  
 Huang, Jing-Song (P. R. China)  
 Huber, Arla M. (USA)  
 Huebner, Friedrich-Karl  
     (Germany)  
 Huebner, Marianne (USA)  
 Hughes, Kenneth R. (South Africa)  
 Huisinga, Wilhelm (Germany)  
 Huisken, Barbara (Germany)  
 Huisken, Gerhard (Germany)  
 Huisman, Johannes (France)  
 Hulek, Klaus W. (Germany)  
 Hullet, Eduardo G. (Germany)  
 Hünlich, Rolf (Germany)  
 Hunt, John H. V. (South Africa)  
 Hürlimann, Werner S. (Switzerland)  
 Hurri-Syrjanen, Ritva (Finland)  
 Hurtubise, Jacques (Canada)  
 Husemoller, Dale (France)  
 Hussain, Mansour G. (Kuwait)  
 Hüseinov, Farhad V. (Turkey)  
 Hutchins, Carol (USA)  
 Hutchinson, Kevin (Ireland)  
 Hutchison, Jeanne S. (USA)  
 Huth, Reinhardt (Germany)  
 Hwang, Tea-Yuan (Taiwan)
- Ibisch, Horst (France)  
 Idczak, Dariusz (Poland)  
 Igarashi, Masayuki (Japan)  
 Ihara, Yasutaka (Japan)  
 Il'ichev, Vitaly G. (Russian Federation)  
 Ilolov, Mamadsho (Tajikistan)  
 Imamoglu, Özlem (Switzerland)  
 Im Hof, Hans-Christoph (Switzerland)
- Imhof, Jean-Pierre (Switzerland)  
 Imkeller, Peter (Germany)  
 Inassaridze, Hvedri (Georgia)  
 Ioffe, Dmitry (Germany)  
 Ion, Patrick D. F. (USA)  
 Ionescu, Cristodor P. (Romania)  
 Iooss, Gerard M. (France)  
 Iosifescu, Marius V. (Romania)  
 Iranmanesh, Ali (Iran)  
 Iricanin, Bratislav (Yugoslavia)  
 Isbell, John (USA)  
 Ischebeck, Friedrich (Germany)  
 Ishigami, Yoshiyasu (Japan)  
 Ishikawa, Takeshi (Japan)  
 Ishiwata, Emiko (Japan)  
 Ishizaki, Katsuya (Japan)  
 Israel, Giorgio (Italy)  
 Ito, Hiroyuki (USA)  
 Ito, Ryuichi (Japan)  
 Ito, Yukari (Japan)  
 Itoh, Jin-ichi (Japan)  
 Itoh, Tatsuo (Japan)  
 Iturriaga, Renato (Mexico)  
 Ivanov, Alexandr O. (Russian Federation)  
 Ivanov, Sergei (USA)  
 Ivansic, Ivan (Croatia)  
 Ivarsson, Björn (Sweden)  
 Iwasaki, Katsunori (Japan)  
 Iwasaki, Yoshimitsu (Japan)  
 Izadi, Elham (USA)
- Jackson, Allyn (USA)  
 Jacob, Niels (Germany)  
 Jaeger, Arno (Germany)  
 Jaehnisch, Michael (Germany)  
 Jaffe, Arthur M. (USA)  
 Jäger, Willi (Germany)  
 Jagers, Albertus A. (Netherlands)  
 Jahanshahi, Mohammad (Iran)  
 Jahn, Olaf (Germany)  
 Jahnke, Thomas (Germany)  
 Jaiani, George (Georgia)  
 Jakobsson, Stefan B. A. (Sweden)  
 James, Donald G. (USA)  
 James, Kevin (USA)  
 Jang, Sophia R.-J. (USA)  
 Janno, Jaan (Estonia)  
 Jannsen, Uwe (Germany)  
 Jansen, Karl-Heinz (Germany)  
 Januszkiewicz, L. Tadeusz (Poland)  
 Janz, Raimund (Switzerland)

- Jarnik, Jiri (Czech Republic)  
 Jarvis, Tyler J. (USA)  
 Jean, Roger V. (Canada)  
 Jeltsch, Rolf (Switzerland)  
 Jensen, Christian U. (Denmark)  
 Jensen, Robert R. (USA)  
 Jensen, Ronald B. (Germany)  
 Jeremias-Lopez, Ana (Spain)  
 Jeschke, Sabina (Germany)  
 Jewett, Rumara (USA)  
 Ji, Lizhen (USA)  
 Jiang, Renfang (USA)  
 Jiang, Song (P. R. China)  
 Jimenez, Miguel A. (Mexico)  
 Jing, Nailuan (USA)  
 Jochmann, Frank (Germany)  
 Johansson, Bo I. (Sweden)  
 John, Daniel (Germany)  
 Johnson, Harold H. (USA)  
 Johnson, Roy A. (USA)  
 Johnson, William B. (USA)  
 Johnston, Elizabeth A. (United Kingdom)  
 Johnstone, Iain Murray (USA)  
 Jones, Mark C. W. (United Kingdom)  
 Jones, Vaughan (USA)  
 Jorge, Maria H. (USA)  
 Jorgensen, Palle E. T. (USA)  
 Joseph, Benjamin S. (USA)  
 Jost, Michael (Germany)  
 Joswig, Michael (Germany)  
 Jovanovic, Bosko (Yugoslavia)  
 Joyce, Dominic (United Kingdom)  
 Józefiak, Tadeusz (USA)  
 Juhnke, Friedrich (Germany)  
 Jun, Sungtae (Korea)  
 Junek, Heinz (Germany)  
 Jung, Heinz Adolf, H. A. (Germany)  
 Jünger, Michael (Germany)  
 Jungnickel, Dieter (Germany)  
 Jurkschat, Henrik (Germany)  
 Just, Andrzej (Poland)  
 Jutila, Matti (Finland)
- Kabanov, Alexandre (USA)  
 Kaczor, Wiesława J. (Poland)  
 Kade, Wolfgang R. (Germany)  
 Kadeishvili, Tornike (Georgia)  
 Kadelburg, Zoran (Yugoslavia)  
 Kadets, Volodymyr M. (Ukraine)  
 Kadison, Richard V. (USA)  
 Kaenders, Rainer H. (Germany)
- Kahle, Reinhard (Germany)  
 Kahn, Bruno (France)  
 Kahn, Donald (USA)  
 Kaibel, Volker (Germany)  
 Kairies, Hans-Heinrich (Germany)  
 Kaiser, Hans-Christoph (Germany)  
 Kajikiya, Ryuji (Japan)  
 Kakiuchi, Nabuhiko (Japan)  
 Kalita, Evgeni A. (Ukraine)  
 Kallel, Sadok (Canada)  
 Kallies, Jürgen (Germany)  
 Kaluch I., Yuriy (Ukraine)  
 Kalus, Norbert (Germany)  
 Kamal, Ahmed A. M. (Egypt)  
 Kambayashi, Tatsuji (Japan)  
 Kamont, Anna (Poland)  
 Kamps, Klaus Heiner (Germany)  
 Kamvissis, Spyridon (France)  
 Kaneko, Makoto (Japan)  
 Kang, Ming-Chang (Taiwan)  
 Kangro, Raul (Estonia)  
 Kangro, Urve (Estonia)  
 Kantor, William M. (USA)  
 Kanzaki, Teruo T. K. (Japan)  
 Kappler, Fritz Otto (Germany)  
 Kappos, Efthimios (United Kingdom)  
 Kapranov, Mikhail M. (USA)  
 Kapur, Aruna (India)  
 Karamzadeh, Omid-Ali (Iran)  
 Karbe, Manfred (Germany)  
 Karcher, Hermann (Germany)  
 Karlof, John K. (USA)  
 Karolinsky, Eugene A. (Ukraine)  
 Karoubi, Max (France)  
 Karoui, Abderrazek (Tunisia)  
 Kasaev, Anzor D. (Russian Federation)  
 Kascelan, Vidosava (Yugoslavia)  
 Kashani, S. M. B. (Iran)  
 Kashiwada, Toyoko (Japan)  
 Kasse, Bettina (Germany)  
 Kassel, Christian (France)  
 Kasyanov, Victor (Russian Federation)  
 Katayama, Soichiro (Japan)  
 Katona, Gyula O. H. (Hungary)  
 Katre, Shashikant (India)  
 Kats, Isaak Yakovlevich (Russian Federation)  
 Katsnelson, Victor, E. (Israel)  
 Katz, Sheldon H. (USA)  
 Kauffmann, Andreas (Germany)

- Kauffmann, Louis H. (USA)  
Kaufmann, Ralph (France)  
Kaup, Burchard (Switzerland)  
Kaup, Ludger (Germany)  
Kausz, Ivan (Germany)  
Kawamata, Yujiro (Japan)  
Kawamura, Kiko (Japan)  
Kawano, Nichiro (Japan)  
Kawohl, Bernd (Germany)  
Kayll, Mark (USA)  
Kayumov, Ilgiz G. (Russian Federation)  
Kazantsev, Ivan G. (Russian Federation)  
Kazunori, Kikuchi (Japan)  
Kearton, Cherry (United Kingdom)  
Kecs, Wilhelm (Romania)  
Keedwell, A. Donald (United Kingdom)  
Keener, Lee L. (Canada)  
Kegel, Otto H. (Germany)  
Kellendonk, Johannes (Germany)  
Keller, Gerhard (Germany)  
Kemperman, Johannes H. (USA)  
Kenmotsu, Katsuei (Japan)  
Kerkour, Ahmed (Morocco)  
Kern, Uwe (Germany)  
Kersten, Ina (Germany)  
Ketelhut, Gunnar (Germany)  
Khalil, Zohel S. (Canada)  
Khan, Nazir M. (Pakistan)  
Khare, Chandrashekhar B. (India)  
Khelladi, Abdelkader (Algeria)  
Khilchenko, Lyudmila Y. (USA)  
Khimshiashvili, George N. (Poland)  
Khitrik, Mikhail (Sweden)  
Khokhlov, Vladimir (Russian Federation)  
Khorrampanahi, Mehrdad (USA)  
Khosrovshahi, Gholamreza B. (Iran)  
Khots, Boris S. (USA)  
Khrennikov, Andrei (Sweden)  
Kiechle, Hubert (Germany)  
Kifer, Yuri (Israel)  
Kiguradze, Ivan (Georgia)  
Kiguradze, Tariel (Georgia)  
Kikuchi, Shigeki S. K. (Japan)  
Kikuchi, Shigetaka S. K. (Japan)  
Kilsch, Dieter (Germany)  
Kim, Dohan (Korea)  
Kim, Hoil (Korea)  
Kim, Sang Moon (Korea)  
Kimura, Noriaki (Japan)  
Kimura, Takashi (USA)  
Kinnmark, Ingemar (USA)  
Kirchberg, Eberhard (Germany)  
Kirchgässner, Klaus (Germany)  
Kirchgraber, Urs (Switzerland)  
Kirchhoff, Dennis (Germany)  
Kirchner, Thomas (Germany)  
Kirrinnis, Peter (Germany)  
Kisaka, Masashi, M. K. (Japan)  
Kiselman, Christer O. (Sweden)  
Kisil, Vladimir V. (Ukraine)  
Kislyakov, Sergey (Russian Federation)  
Kissin, Edward (United Kingdom)  
Kister, James M. (USA)  
Kister, Jane E. (USA)  
Kitano, Teruaki (Japan)  
Kiyek, Karlheinz (Germany)  
Klassert, Steffen (Germany)  
Klazar, Martin (Czech Republic)  
Klein, Henning (Germany)  
Klein, Olaf (Germany)  
Kleshchev, Alexander S. (USA)  
Klesov, Oleg I. (Ukraine)  
Klimek, Malgorzata (Poland)  
Klimenko, Stanislav V. (Germany)  
Klin, Mikhail H. (Israel)  
Klingenberg, Christian (Germany)  
Klopsch, Benjamin (United Kingdom)  
Klüners, Jürgen (Germany)  
Knauf, Andreas (Germany)  
Kneissler, Jan (Germany)  
Knight, Frank B. (USA)  
Knobloch, Eberhard H. (Germany)  
Knopov, Pavel S. (Ukraine)  
Knuetel, Claudia D. (Germany)  
Ko, Hyoung J. (Korea)  
Kobayashi, Keiko (Japan)  
Koch, Helmut (Germany)  
Koch, Herbert (Germany)  
Koch, Robert (Germany)  
Koch, Tino (Germany)  
Kochol, Martin (Slovakia)  
Kochubei, Anatoly N. (Ukraine)  
Koda, Takashi (Japan)  
Kodiyalam, Vijay (India)  
Koenig, Wolfgang D. (Germany)  
Koepke, Peter G. (Germany)  
Koerner, Friederike (Germany)  
Kogiso, Takeyoshi (Japan)  
Kohaupt, Ludwig (Germany)  
Kohayakawa, Yoshiharu (Brazil)

- Köhler, Ekkehard (Germany)  
 Köhne, Hartmut (Germany)  
 Köhnen, Walter (Germany)  
 Kohr, Gabriela (Romania)  
 Kohr, Mirela (Romania)  
 Kojok, Badrie (Ivory Coast)  
 Kokilashvili, Vakhtang M. (Georgia)  
 Kokubu, Hiroshi (Japan)  
 Kolk, Johan A. (Netherlands)  
 Kolodyazhnyi, Volodymyr M. (Ukraine)  
 Kolomiets, Yuriy V. (Ukraine)  
 Koltchinskii, Vladimir I. (USA)  
 Kolumban, Iosif (Romania)  
 Komatsu, Hikosaburo (Japan)  
 Kometch, Alexandre (Russian Federation)  
 Kondratiev, Anatolii S. (Russian Federation)  
 Kondratiev, Vladimir A. (Russian Federation)  
 König, Gerhard (Germany)  
 König, Hermann (Germany)  
 Konno, Hitoshi (Japan)  
 Konnov, Valery (Russian Federation)  
 Konrad, Alois (Germany)  
 Kontsevich, Maxim (France)  
 Koorwinder, Tom H. (Netherlands)  
 Kopanskii, Alexander Ya. (Moldova)  
 Koppelberg, Sabine (Germany)  
 Koprucki, Thomas (Germany)  
 Kopylov, Iaroslav A. (Russian Federation)  
 Koranyi, Adam (USA)  
 Kordyukov, Yuri A. (Russian Federation)  
 Korepanov, Igor (Russian Federation)  
 Korey, Michael B. (Germany)  
 Korneichuk, Nikolaj P. (Ukraine)  
 Kornhuber, Ralf (Germany)  
 Kortesi, Peter (Hungary)  
 Koschorke, Ulrich (Germany)  
 Koshevoy, Gleb A. (Russian Federation)  
 Koshi, Shozo (Japan)  
 Kosinski, Antoni A. (USA)  
 Koskela, Pekka J. (Finland)  
 Kosmodemyanskii, Alexander A. (Russian Federation)  
 Kostant, Ann (USA)  
 Kosugi, Masako (Japan)  
 Kosyak, Alexandr V. (Ukraine)  
 Kota, Osamu (Japan)  
 Kotlyarov, Volodymyr (Ukraine)  
 Kotschick, Dieter (Germany)  
 Kottwitz, Robert Edward (USA)  
 Koua, Konin (Ivory Coast)  
 Koumandos, Stamatias (Cyprus)  
 Kovács, Sándor J. (USA)  
 Kovalev, Alexander M. (Ukraine)  
 Kovalev, Alexei G. (United Kingdom)  
 Kowalski, Michael (Germany)  
 Kowalski, Piotr (Poland)  
 Kozlov, Vladimir (Sweden)  
 Kracht, Marcus A. (Germany)  
 Krainer, Thomas (Germany)  
 Kraljevic, Hrvoje (Croatia)  
 Krämer, Helmut L. (Germany)  
 Kramer, Jürg (Germany)  
 Kranz, Matthias (Germany)  
 Krasilnikov, Alexei N. (Russian Federation)  
 Krasnov, Yakov (Israel)  
 Krason, Piotr (Poland)  
 Krattenthaler, Christian (Austria)  
 Kratz, Werner (Germany)  
 Kraus, Anne (Germany)  
 Krause, Henning (Germany)  
 Krause, Matthias (Germany)  
 Krause, Ulrich (Germany)  
 Krebs, Hans-Joachim (Germany)  
 Krejci, Pavel (Germany)  
 Kreußler, Bernd (Germany)  
 Kreuzer, Martin (Germany)  
 Kriecherbauer, Thomas C. (Germany)  
 Krieg, Aloys (Germany)  
 Krikorian, Raphael R. (France)  
 Kriz, Igor (USA)  
 Krolak, Andrzej (Poland)  
 Krötz, Bernhard (Germany)  
 Kruger, Alexander Ya. (Belarus)  
 Kruglikov, Boris Serafimovich (Russian Federation)  
 Krumke, Sven O. (Germany)  
 Kruse, Hans-Peter (Germany)  
 Krutitskii, Pavel A. (Russian Federation)  
 Kryakin, Yuri (Ukraine)  
 Krzyz, Jan G. (Poland)  
 Kuberek, Monika (Germany)  
 Kubo, Akisato (Japan)  
 Küchler, Uwe (Germany)  
 Kugelmann, Bernd (Germany)  
 Kühn, Ulf (Germany)  
 Kühnel, Arnold (Germany)  
 Kühnel, Wolfgang (Germany)

- Kühnlein, Stefan (Germany)  
 Kuksin, Sergei B. (Russian Federation)  
 Kuku, Aderemi O. (Italy)  
 Kulikov, Gennady Yu. (Russian Federation)  
 Kulikov, Viktor S. (Russian Federation)  
 Kumbhat, R. K. (India)  
 Kummer, Bernd (Germany)  
 Kummetz, Ralph (Germany)  
 Kündgen, André (USA)  
 Kunik, Matthias (Germany)  
 Kunz, Ernst (Germany)  
 Kuo, Tsang-Hai (Taiwan)  
 Kuperberg, Krystyna M. (USA)  
 Kupisch, Herbert (Germany)  
 Kurdachenko, Leonid A. (Ukraine)  
 Kuribayashi, Yukio (Japan)  
 Kurjo McNeill, Sabine U. (United Kingdom)  
 Kurke, Herbert (Germany)  
 Kürsten, Klaus-Detlef (Germany)  
 Kusch, Claudia (Germany)  
 Küssner, Thilo (France)  
 Kutev, Nicolay Draganov (Germany)  
 Kutz, Nadja (Germany)  
 Kwiecinski, Michal (Poland)  
 Labarca, Rafael (Chile)  
 Labourie, François (France)  
 Lacey, Michael T. (USA)  
 Lackschewitz, Christina B. (Germany)  
 Laffey, Thomas J. (Ireland)  
 Lafforgue, Laurent (France)  
 Lagarias, Jeffrey C. (USA)  
 Lahtinen, Aatos O. (Finland)  
 Lalonde, Francois (Canada)  
 Lamm, Christoph (Germany)  
 Lamprecht, Erich (Germany)  
 Lance, E. Christopher (United Kingdom)  
 Lanchon, Pierre (France)  
 Lang, Georg (Germany)  
 Lang, Jens (Germany)  
 Lang, Rainer (Germany)  
 Lange, Alexander (Germany)  
 Lange, Otfried (Germany)  
 Lange, Thomas (Germany)  
 Langenbruch, Michael (Germany)  
 Langer, Ottmar (Germany)  
 Langevin, Rémi N. (France)  
 Langmach, Hartmut (Germany)  
 Langmann, Hanns-Heinrich (Germany)  
 Lanza de Cristoforis, Massimo (Italy)  
 Lanzinger, Hartmut (Germany)  
 Lapidus, Michel L. (USA)  
 Lappan, Peter A. (USA)  
 Lara-Aparicio, Miguel (Mexico)  
 Laradji, Abdallah (Kingdom of Saudi-Arabia)  
 Lárússon, Finnur (Canada)  
 Lascoux, Alain (France)  
 Lastaria, Federico G. (Italy)  
 Laurenz, Henriette-Marie (Romania)  
 Laurincikas, Antanas (Lithuania)  
 Läuter, Henning (Germany)  
 Lauterbach, Reiner (Germany)  
 Lawrenz, Alexander (USA)  
 Lawton, Wayne M. (Singapore)  
 Lazinska, Anna (Poland)  
 Le, Thang T. Q. (USA)  
 Lebowitz, Joel (USA)  
 Lechner, Patrick O. (Germany)  
 Leck, Uwe (Germany)  
 Leck, Volker (Germany)  
 Leder, Judith (Germany)  
 Ledermann, Walter (United Kingdom)  
 Ledrappier, Francois (France)  
 Lee, Sa Ge (Korea)  
 Lee, Yuh-Jia (Taiwan)  
 Lefton, Lew E. (USA)  
 Le Gall, Jean-François (France)  
 Leger, George F. (USA)  
 Lehalle, Charles-Albert (France)  
 Lehmann, Detlef (Germany)  
 Lehmann, Ingmar (Germany)  
 Lehn, Jürgen (Germany)  
 Lehto, Olli (Finland)  
 Leichtweiß, Kurt (Germany)  
 Leiderman, Arkady (Israel)  
 Leindler, Laszlo (Hungary)  
 Leinert, Michael (Germany)  
 Leitao, Antonio C. (Brazil)  
 Leiterer, Günter Paul (Germany)  
 Leiterer, Jürgen (Germany)  
 Lemaire, Jean-Michel (France)  
 Lemaire-Body, Françoise (France)  
 Lemarié-Rieusset, Pierre Gilles (France)  
 Lempert, Laszlo (USA)  
 Lenard, Christopher T. (Australia)  
 Leng, W. S. (United Kingdom)  
 Lenski, Wolfgang (Germany)  
 Lenz, Daniel H. (Germany)



- Lenz, Hanfried (Germany)  
 Lenzing, Helmut (Germany)  
 Leonenko, Nikolai (Ukraine)  
 Leprevost, Franck (France)  
 Leruste, Christian P. (France)  
 Lesch, Matthias (Germany)  
 Leschke, Katrin (Germany)  
 Lescot, Paul E. (France)  
 Leseberg, Dieter (Germany)  
 Lessard, Sabin (Canada)  
 Leti, Guiseppe (Italy)  
 Letzner, Eberhard (Germany)  
 Leutbecher, Armin (Germany)  
 Leviatan, Dany (Israel)  
 Leviatan, Talma O. (Israel)  
 Levin, Alexander (USA)  
 Levin, Norman P. (USA)  
 Levy, Jason (Canada)  
 Levy, Stuart A. (USA)  
 Lewis, Donald J. (USA)  
 Lewis, Wayne (USA)  
 Li, An-Min (P. R. China)  
 Li, Cai-Heng (Australia)  
 Li, Congming (USA)  
 Li, Da-Qian (Ta-Tsien) (P. R. China)  
 Li, Gui-Song (P. R. China)  
 Li, Jiayu (P. R. China)  
 Li, Wei-Ping (P. R. China)  
 Li, Wenlin (P. R. China)  
 Li, Xing (P. R. China)  
 Li, Zhongkai (P. R. China)  
 Liandrat, Jacques (France)  
 Liang, Hua (P. R. China)  
 Liberati, Jose I. (USA)  
 Liberzon, Mark R. (Russian Federation)  
 Lica, Dionis (Romania)  
 Lichtenberg, Heiner (Germany)  
 Lickorish, W. B. Raymond (United Kingdom)  
 Liebscher, Stefan (Germany)  
 Liemant, Alfred (Germany)  
 Liesen, Jörg (Germany)  
 Lih, Ko-Wei (Taiwan)  
 Lim, Richard (United Kingdom)  
 Lima, Suely dos Santos (Brazil)  
 Lima de Sa, Eduardo (Venezuela)  
 Lin, Zongzhu (USA)  
 Lindblad, Hans (USA)  
 Lindemann, Ina (USA)  
 Lindenstrauss, Joram (Israel)  
 Lindner, Thomas (Germany)  
 Ling, San (Singapore)  
 Linton, Fred E. J. (USA)  
 Linton, Stephen A. (United Kingdom)  
 Lipkovski, Aleksandar T. (Yugoslavia)  
 Lipponen, Marjo R. (Finland)  
 Liss, Shari (USA)  
 List, Christoph (Ireland)  
 List, Tobias (Germany)  
 Litvinchuk, Gueorgui S. (Portugal)  
 Litwin, Oleq (Ukraine)  
 Liu, Feng (P. R. China)  
 Liu, Fon-Che (Taiwan)  
 Liu, Zheng (P. R. China)  
 Lizama, Carlos (Chile)  
 Lledó, Fernando (Germany)  
 Löbel, Andreas (Germany)  
 Loday, Jean-Louis (France)  
 Lodder, Gerald M. (USA)  
 Loeffelmann, Jochen (Germany)  
 Loewe, Benedikt (USA)  
 Loewy, Raphael (Israel)  
 Logachev, Dmitry (Russian Federation)  
 Loginov, Boris V. (Russian Federation)  
 Logofet, Dmitrii O. (Russian Federation)  
 Lohkamp, Joachim (Germany)  
 Lommatzsch, Klaus (Germany)  
 Lopes-Pinto, Antonio Jorge Brandao (Portugal)  
 Lorbeer, Boris (Germany)  
 Lorentz, Rudolph A. (Germany)  
 Loskutov, Alexander (Russian Federation)  
 Losonczi, Attila (Hungary)  
 Lott, John (USA)  
 Lotto, Benjamin A. (USA)  
 Louhivaara, Ilppo Simo (Germany)  
 Love, Eric R. (Australia)  
 Lu, Guozhen (USA)  
 Lu, Sylvia Chin-Pi (USA)  
 Luca, Florian G. (Germany)  
 Luchko, Yuri (Germany)  
 Ludwig, Garry (Canada)  
 Luedecke, Marcus (Germany)  
 Lügger, Joachim (Germany)  
 Luma, Charity (Philippines)  
 Lundmark, Hans (Sweden)  
 Lusala, Tsasa (Germany)  
 Lütkebohmert, Werner (Germany)  
 Lutsenka, Michael (Russian Federation)  
 Lutz, Frank H. (Germany)

- Luukkainen, Jouni (Finland)  
 Lyashenko, Elena I. (Ukraine)  
 Lyashenko, Igor N. (Ukraine)  
 Lyons, Jeremiah J. (USA)  
 Lyons, Terry J. (United Kingdom)  
 Lyubeznik, Gennady (USA)  
 Ma, Li (P. R. China)  
 Ma, Xiaonan (France)  
 Maalouf, Ramez N. (Lebanon)  
 Maass, Peter (Germany)  
 Macdivitt, Arthur (United Kingdom)  
 Macdonald, I. G. (United Kingdom)  
 Macedonska, Olga (Poland)  
 Machedon, Matei (USA)  
 Macintyre, Angus J. (United Kingdom)  
 MacPherson, Robert D. (USA)  
 Maddocks, John H. (Switzerland)  
 Madsen, Dag (Norway)  
 Maeda, Hironobu (Japan)  
 Maehara, Kazuhisa (Japan)  
 Mänz, Oleg (Germany)  
 Magden, Abdullah (Turkey)  
 Magenes, Enrico (Italy)  
 Magid, Andy R. (USA)  
 Magnus, Robert (Iceland)  
 Mahassen, Nadim (United Kingdom)  
 Mahdavi, Kazem (USA)  
 Mahdavi-Hezavehi, Mohammad (Iran)  
 Mahmoodian, Ebadollah S. (Iran)  
 Mahnke, Heidi (Germany)  
 Mahowald, Mark (USA)  
 Maier, Volker (Germany)  
 Mailybaev, Alexei A. (Russian Federation)  
 Makagon, Andrzej (USA)  
 Makarenko, Natalia Yur'evna (Russian Federation)  
 Makay, Géza (Hungary)  
 Mäkeläinen, Tuulikki (Finland)  
 Makhnev, Alexandre A. (Russian Federation)  
 Makinde, Oluwole Daniel (Zimbabwe)  
 Malamud, Mark M. (Ukraine)  
 Malik, Grit (Germany)  
 Malik, Surender K. (India)  
 Malinin, Dmitri (Belarus)  
 Mallat, Stéphane (France)  
 Malle, Gunter (Germany)  
 Malliavin, Paul (France)  
 Mallol Gurgui, Josep (Spain)  
 Maltsiniotis, Georges (France)  
 Mamadaliyev, Nazirdjan Kamildjanovich (Uzbekistan)  
 Mammitzsch, Volker (Germany)  
 Mampassi, Benjamin (Senegal)  
 Manders, Kenneth (USA)  
 Manin, Yuri (Germany)  
 Maniscalco, Caterina (Italy)  
 Manturov, Vasily Olegovich (Russian Federation)  
 Manuilov, Vladimir (Russian Federation)  
 Marathe, Kishore B. (USA)  
 Marchisio, Marina R. (Italy)  
 Marcolli, Matilde (USA)  
 Marcus, Andrei (Romania)  
 Mardesic, Sibe (Croatia)  
 Marichev, Oleg (USA)  
 Marin, Ivan F. (France)  
 Marinoschi, Gabriela G. (Romania)  
 Marioli, Carlo (Italy)  
 Markarian, Roberto (Uruguay)  
 Markgraf, Norman (Germany)  
 Markina, Irina (Russian Federation)  
 Maroscia, Paolo (Italy)  
 Marrero, Osvaldo (USA)  
 Marshall, Donald E. (USA)  
 Marsico, Tiziana (Italy)  
 Martchenko, Boris G. (Ukraine)  
 Martin, Alexander (Germany)  
 Martin, Benjamin M. (Australia)  
 Martin, Bernd (Germany)  
 Martin-Deschamps, Mireille R. (France)  
 Martinez, Raquel R. (Spain)  
 Martio, Olli T. (Finland)  
 Maruyama, Fumitsuna (Japan)  
 März, Roswitha (Germany)  
 Masanja, Verdiana Grace (Tanzania)  
 Masaya, Mochizuki (Japan)  
 Mascari, Giovanni Francesco (Italy)  
 Maseberg, Sönke (Germany)  
 Maslyuchenko, Volodymyr K. (Ukraine)  
 Massart, Daniel (Germany)  
 Massold, Heinrich (Germany)  
 Materov, Evgeni Nikolaevich (Russian Federation)  
 Matet, Pierre (France)  
 Mathé, Peter (Germany)  
 Mathieu, Martin (Ireland)  
 Mathieu, Oliver (France)  
 Mathieu, Pierre (Canada)  
 Matoušek, Jiri (Czech Republic)

- Matsumoto, Shigeki (Japan)  
 Matsumoto, Shigenori (Japan)  
 Matsumoto, Waichiro (Japan)  
 Matsumura, Toru (Japan)  
 Matsuyama, Yoshio (Japan)  
 Matsuzaki, Nagi (Japan)  
 Matthies, Karsten (Germany)  
 Mattila, Pertti (Finland)  
 Mattner, Lutz (Germany)  
 Mattrisch, Sybille (Germany)  
 Matuszewski, Roman (Poland)  
 Matveev, Oleg V. (Russian Federation)  
 Matveev, Vladimir S. (Russian Federation)  
 Maude, Ronald (United Kingdom)  
 Maumary, Serge (Switzerland)  
 Maxwell, James W. (USA)  
 Mayer, John C. (USA)  
 Mayer, Karl Heinz (Germany)  
 Mbakop, Guy Merlin (Germany)  
 Mbunga, Paulo (Germany)  
 McCoy, Barry (USA)  
 McCune, Catherine (Germany)  
 McDuff, Dusa (USA)  
 McMullen, Curtis Tracy (USA)  
 Mc Nulty, Jennifer (USA)  
 Mdzinarishvili, Leonard (Georgia)  
 Medghalchi, Alireza (Iran)  
 Mednykh, Alexander D. (Russian Federation)  
 Megginson, Robert E. (USA)  
 Mehri, Bahman (Iran)  
 Mehta, Ghanshyam B. (Australia)  
 Meier, David (Switzerland)  
 Meintrup, David (Germany)  
 Meissner, Nils (Germany)  
 Meltzer, Hagen (Germany)  
 Melville, Duncan J. (USA)  
 Mendes, Diana E. Aldea (Portugal)  
 Mendez, Jose (Germany)  
 Mendoza, Ramon (Brazil)  
 Mennicken, Reinhard (Germany)  
 Mercier, Armel (Canada)  
 Merel, Loic (France)  
 Merklen, Héctor (Brazil)  
 Merle, Frank Eric (France)  
 Mertins, Ulrich (Germany)  
 Merzon, Anatoli (Russian Federation)  
 Meskhi, Alexander N. (Georgia)  
 Mestrovic, Romeo (Yugoslavia)  
 Metsänkylä, Tauno (Finland)  
 Metzger, Roger J. (Brazil)  
 Meusers, Claudia (Germany)  
 Meyer, Gottfried Peter (Germany)  
 Meyer, Johannes H. (South Africa)  
 Meyer, Karoline (Germany)  
 Miana, Pedro J. (Spain)  
 Miatello, Roberto J. (Argentina)  
 Michaelis, Walter J. (USA)  
 Michailov, Leonid Grigorevich (Tajikistan)  
 Micheel, Jan (Germany)  
 Michel, Alexis P. (France)  
 Michel, Volker (Germany)  
 Michelucci, Maria Letizia (Italy)  
 Michev, Iordan P. (Japan)  
 Michor, Peter W. (Austria)  
 Micula, George (Romania)  
 Mielke, Hans F. (Germany)  
 Migda, Malgorzata (Poland)  
 Mignanego, Fausto (Italy)  
 Migorski, Stanislaw (Poland)  
 Mihalache, George (Germany)  
 Mihalache, Nicolae S. (Romania)  
 Mihalyko, Csaba (Hungary)  
 Mikaelian, Vahagn H. (Armenia)  
 Mikhalev, Alexander A. (Russian Federation)  
 Mikhalev, Alexandre V. (Russian Federation)  
 Mikhalkin, Grigory (USA)  
 Milka, Anatoly D. (Ukraine)  
 Miller, Stephen D. (USA)  
 Millett, Kenneth C. (USA)  
 Millionshikov, Dmitri V. (Russian Federation)  
 Milman, Vitali (Israel)  
 Milnes, Paul (Canada)  
 Milnor, John W. (USA)  
 Milstein, Grigori (Germany)  
 Milton, Graeme Walter (USA)  
 Minda, C. David (USA)  
 Minian, Elias G. (Germany)  
 Mio, Washington (USA)  
 Mirengi, Elvira (Italy)  
 Misaki, Norihiro (Japan)  
 Mishchenko, Alexander S. (Russian Federation)  
 Mishura, Yuliya Stepanovna (Ukraine)  
 Misiewicz, Jolanta K. (Poland)  
 Misiolek, Gerard (USA)

- Misra, Kailash C. (USA)  
 Missarov, Moukadas (Russian Federation)  
 Mititelu, Stefan M. (Romania)  
 Mitran, Ilie (Romania)  
 Mitschi, Claude (France)  
 Mitsumatsu, Yoshihiko (Japan)  
 Mittenhuber, Dirk (Germany)  
 Miwa, Tetsuji (Japan)  
 Miyajima, Kimio (Japan)  
 Mizutani, Tadayoshi (Japan)  
 Mlynarska, Elzbieta (Poland)  
 Mochizuki, Shinichi (Japan)  
 Moffatt, Keith (United Kingdom)  
 Mogk, Georg (Germany)  
 Mohammadzadeh, Mohsen (Iran)  
 Mohammed, Alip (Germany)  
 Mohn, Karl-Heinz (Germany)  
 Mohnke, Klaus (Germany)  
 Möhring, Rolf H. (Germany)  
 Moklyachuk, Mikhaïl (Ukraine)  
 Moldavskaya, Elina M. (Ukraine)  
 Möller, Andris (Germany)  
 Möller, Herbert (Germany)  
 Monastyrsky, Michael (Russian Federation)  
 Monod, Nicolas (Switzerland)  
 Montans, Fernando J. (Uruguay)  
 Montgomery, M. Susan (USA)  
 Moore, Charles N. (Ireland)  
 Moore, John D. (USA)  
 Morales Figueroa, Bernardo (Guatemala)  
 Morawetz, Cathleen Synge (USA)  
 Moree, Pieter (Germany)  
 Moreira, Carlos C. (Brazil)  
 Moreira, Carlos Gustavo T. de A. (Brazil)  
 Morgenthal, Klaus (Germany)  
 Morgulis, Andrey B. (Russian Federation)  
 Mori, Masao (Japan)  
 Morimoto, Hiroko (Japan)  
 Morimoto, Mitsuo (Japan)  
 Moritoh, Shinya (Japan)  
 Morley, Mary E. (USA)  
 Moroianu, Andrei, M. (France)  
 Morrell, Robert (United Kingdom)  
 Morris, Alun O. (United Kingdom)  
 Mörters, Peter (Germany)  
 Moser, Jürgen (Switzerland)  
 Moshnikova, Julia M. (Russian Federation)  
 Motohashi, Tomoe (Japan)  
 Motornaya, Oxana V. (Ukraine)  
 Mourrain, Bernard (France)  
 Moussa, Gonoko (France)  
 Moussavi, Ahmad (Iran)  
 Mouton, Sonja (South Africa)  
 Movisyan, Moevses (Armenia)  
 Mozes, Shahar (Israel)  
 Mucha, Hans-Joachim (Germany)  
 Mueller, Peter (Germany)  
 Mueller-Roehlck, Karin (Germany)  
 Müger, Michael (Italy)  
 Mulholland, Lawrence S. (United Kingdom)  
 Müller, Detlef H. (Germany)  
 Müller, Eva Nuria (Germany)  
 Müller, Franz (Switzerland)  
 Müller, Stefan (Germany)  
 Müller-Hannemann, Matthias (Germany)  
 Mumford, David (USA)  
 Mündlein, Heidrun (Germany)  
 Munembe, Joao S. P. (Mozambique)  
 Munkholm, Hans J. (Denmark)  
 Murakami, Hitoshi (Japan)  
 Murali, Venkat (South Africa)  
 Muranov, Yuri V. (Russian Federation)  
 Murasugi, Kunio (Canada)  
 Muscalu, Florin C. (USA)  
 Mushtari, Daniar H. (Russian Federation)  
 Mustonen, Vesa (Finland)  
 Myshkis, Anatoli (Russian Federation)  
 Näättänen, Marjatta (Finland)  
 Nagaev, Sergei (Russian Federation)  
 Nagahara, Takashi (Japan)  
 Nagaoka, Shoyu (Japan)  
 Nagasaka, Kenji (Japan)  
 Nagasawa, Takeyuki (Japan)  
 Nagel, Uwe (Germany)  
 Nagy, Gábor P. (Hungary)  
 Näher, Holger D. (Germany)  
 Nair, Sunil (United Kingdom)  
 Naito, Hirotada (Japan)  
 Nakagawa, Jin (Japan)  
 Nakai, Eiichi (Japan)  
 Nakamura, Iku (Japan)  
 Nakamura, Kirio K. (Japan)  
 Nakano, Daniel K. (USA)  
 Nakano, Minoru (Japan)  
 Nakayashiki, Atsushi, An (France)  
 Nakazawa, Hideaki (Japan)  
 Nanbu, Tokumori (Japan)

- Narasimhan, Mudumbai Seshachalu (Italy)  
 Narayanaswami, Pallasena P. (Canada)  
 Nassau, Christian (Germany)  
 Nassopoulos, Georgios F. (Greece)  
 Nastold, Hans-Joachim (Germany)  
 Nasyrov, Samyon R. (Russian Federation)  
 Natanzon, Sergei (Russian Federation)  
 Natarajan, Raja (India)  
 Natroshvili, David (Georgia)  
 Natsume, Toshikazu (Japan)  
 Naude, Cornelia G. (South Africa)  
 Naumann, Joachim (Germany)  
 Naveira, Antonio M. (Spain)  
 Naydonova, Anna V. (Ukraine)  
 Nazarova, Ludmila Aleksandrovna (Ukraine)  
 Nazipov, Albert A. (Russian Federation)  
 Ndimubandi, Jean (Burundi)  
 Neeb, Karl-Hermann (Germany)  
 Nefedov, Nikolay N. (Russian Federation)  
 Neff, Patrizio (Germany)  
 Nejaddeghan, Yadollah (Iran)  
 Nelius, Christian-Frieder (Germany)  
 Nepotu, Gabriel-Lucian (Romania)  
 Nesetril, Jaroslav (Czech Republic)  
 Nesselmann, Dieter (Germany)  
 Neto, Orlando (Portugal)  
 Netsvetaev, Nikita Yu. (Russian Federation)  
 Neubauer, Mathias (Germany)  
 Neuberger, Barbara O. (USA)  
 Neuberger, John W. (USA)  
 Neumann, Bernhard H. (Australia)  
 Neumann, Heike (Germany)  
 Neumann, Olaf G. (Germany)  
 Neumann, Peter (Germany)  
 Neun, Winfried (Germany)  
 Neunhaeuserer, Joerg (Germany)  
 Neusel, Mara D. (Germany)  
 Newelski, Ludomir (Poland)  
 Nezit, Pierre (Ivory Coast)  
 Ngom, Papa (France)  
 Nguyen, Anh-Tuan (Germany)  
 Nguyen, Dinh Cong (Vietnam)  
 Nguyen, Dinh Tri (Vietnam)  
 Ngwa, Gideon A. (Cameroon)  
 Nicodeme, Pierre (Germany)  
 Nicolae, Florin (Romania)  
 Nicolas, Anne-Marie (France)  
 Nicolas, Jean-Louis (France)  
 Niebsch, Jenny (Germany)  
 Niederhauser, Beat M. (Germany)  
 Niederkorn, Philippe (Belgium)  
 Niederreiter, Harald (Austria)  
 Nierhoff, Till (Germany)  
 Nieto, Isidro P. (Mexico)  
 Nietzsche, Josef (Germany)  
 Niezgodna, Marek (Poland)  
 Nikcevic, Stana (Yugoslavia)  
 Nikitin, Igor N. (Germany)  
 Nikolova, Ivanka P. (USA)  
 Nikoltjeva-Hedberg, Margarita (Sweden)  
 Nikonov, Oleg I. (Russian Federation)  
 Nill, Benjamin (Germany)  
 Nilsson, Marcus L. G. (Sweden)  
 Ninnemann, Olaf (Germany)  
 Ninomiya, Yasushi (Japan)  
 Nishimura, Jun-ichi (Japan)  
 Nishimura, Shigeto (Japan)  
 Niss, Mogens (Denmark)  
 Noaghi, Sorin (Romania)  
 Nocedal, Jorge (USA)  
 Nolan, Clifford J. (USA)  
 Nollau, Volker (Germany)  
 Nomura, Yasutoshi (Japan)  
 Nongxa, Loyiso (South Africa)  
 Nörenberg, Rainer (Germany)  
 Norkin, Vladimir (Ukraine)  
 Nörtemann, Stefan (Germany)  
 Nourani, Cyrus F. (USA)  
 Novikov, Igor Ya. (Russian Federation)  
 Nowack, Dieter (Germany)  
 Nowak, Ivo (Germany)  
 Nowak, Maria T. (Poland)  
 Nowak, Ulrich (Germany)  
 Nummelin, Esa (Finland)  
 Nürnberg, Reiner (Germany)  
 Nüsken, Michael (Germany)  
 Nussbaum, Michael (Germany)  
 Nusser, Harald (Germany)  
 Oakes, Susan M. (United Kingdom)  
 Oberschelp, Arnold (Germany)  
 Obukhovskii, Valeri V. (Russian Federation)  
 Odai, Yoshitaka (Japan)  
 Odell, Edward (USA)  
 Oevel, Walter (Germany)  
 Oeverdieck, Lars (Germany)  
 Ogata, Hayao (Japan)

- Ogata, Shoetsu (Japan)  
 Ohba, Kiyoshi (Japan)  
 Ohmiya, Mayumi, EM. (Japan)  
 Ohno, Hiloshi (Japan)  
 Ohno, Masahiro (Japan)  
 Ohno, Shuichi (Japan)  
 Ohta, Minolu (Japan)  
 Ohtsuki, Tomotada (Japan)  
 Oja, Eve (Estonia)  
 Oja, Peeter (Estonia)  
 Oka, Hiro-e (Japan)  
 Okada, Tatsuya (Japan)  
 Okamoto, Hisashi (Japan)  
 Okayasu, Takashi (Japan)  
 Okikiolu, Kate (USA)  
 Okoya, Samuel S. (Nigeria)  
 Olbrich, Martin (Germany)  
 Oleinik, Vladimir L. (Russian Federation)  
 Olenko, Andrew Ya. (Ukraine)  
 Oliver, Robert A. (France)  
 Olshanskii, Maxim A. (Russian Federation)  
 Olsson, Jorn B. (Denmark)  
 Omarjee, Moubinoöl (France)  
 O'Neill, Bruce (Egypt)  
 Onishi, Yoshihiro (Japan)  
 Ono, Kaoru (Japan)  
 Ono, Ken (USA)  
 Ontaneda, Pedro (Brazil)  
 Opfer, Gerhard (Germany)  
 Opozda, Barbara (Poland)  
 Orazov, Mered (Turkmenistan)  
 Orman, Gabriel V. (Romania)  
 O'Shea, Donal B. (USA)  
 Osilike, Micah O. (Nigeria)  
 Osipenko, George (Russian Federation)  
 Ostermann, Alexander (Austria)  
 Osthus, Deryk (Germany)  
 Otachel, Zdzislaw (Poland)  
 Otsuka, Kayo (Japan)  
 Otsuka, Kenichi (Japan)  
 Ovchinnikov, Vladimir I. (Russian Federation)  
 Oversteegen, Lex G. (USA)  
 Owa, Shigeyoshi (Japan)  
 Özlük, Ali E. (USA)  
 Paatz, Andrea (Germany)  
 Paccagnan, Diego (Italy)  
 Pacheco Esteban, Juan Pablo (Spain)  
 Padial, Juan Francisco (Spain)  
 Paditz, Ludwig (Germany)  
 Paetsch, Olaf (Germany)  
 Paffenroth, Randy (Switzerland)  
 Pahlig, Hans-Christian (Germany)  
 Palais, Richard, S. (Germany)  
 Palamodov, Victor P. (Germany)  
 Palencia, Cesar (Spain)  
 Palis, Jacob (Brazil)  
 Palka, Bruce P. (USA)  
 Panazzolo, Daniel C. (Brazil)  
 Pandey, Jagdish N. (Canada)  
 Panov, Evgeniy Yur'evich (Russian Federation)  
 Pantelidis, Georgios (Greece)  
 Papanicolaou, George C. (USA)  
 Papaschinopoulos, Garyfalos (Greece)  
 Pappas, Christian E. (USA)  
 Parkhomenko, Victoria (Ukraine)  
 Parmenter, Michael M. (Canada)  
 Parring, Aivo (Estonia)  
 Parthasaraty, Kalyanapuram Rangachari (India)  
 Paseman, Gerhard R. (USA)  
 Passaquindici, Maria (Italy)  
 Passare, Mikael (Sweden)  
 Patetta, Nicolás D. (Argentina)  
 Pauen, Raimund (Germany)  
 Pauly, Marc (Belgium)  
 Pavcevic, Mario-Osvin (Croatia)  
 Pavel, Monique L. (France)  
 Pavicevic, Zarko (Yugoslavia)  
 Pawalowski, Krzysztof M. (Poland)  
 Pawlowsky-Glahn, Vera (Spain)  
 Paxia, Giuseppe (Italy)  
 Paycha, Sylvie (France)  
 Pecher, Hartmut (Germany)  
 Pedas, Arvet (Estonia)  
 Pedit, Franz (Germany)  
 Pein, Jan (Germany)  
 Pekonen, Osmo (Finland)  
 Pelczar, Andrzej (Poland)  
 Peller, Vladimir V. (USA)  
 Peltonen, Kirsi (Finland)  
 Penssel, Christian (Germany)  
 Perepelitsa, Vitaly A. (Russian Federation)  
 Peretyat'kin, Mikhail (Kazakhstan)  
 Pereverziev, Sergii (Ukraine)  
 Perez, Javier (Spain)  
 Perez Riera, Mario (Spain)

- Peric, Veselin S. (Yugoslavia)  
 Perisic, Vesna (Germany)  
 Perov, Anatolii Ivanovich (Russian Federation)  
 Perovic, Miodrag (Yugoslavia)  
 Persson, Lars-Erik (Sweden)  
 Pesch, Hans Josef (Germany)  
 Pete, Gabor (Hungary)  
 Petean, Jimmy (Germany)  
 Peters, Klaus (USA)  
 Peters, Meinhard H. (Germany)  
 Petersen, Carsten Lunde (Denmark)  
 Petersson, Henrik (Sweden)  
 Petrogradsky, Victor M. (Russian Federation)  
 Petrosjan, Leon A. (Russian Federation)  
 Petti, Richard J. (USA)  
 Petukhov, Alexander P. (Russian Federation)  
 Petzoldt, Martin (Germany)  
 Peyre, Emmanuel (France)  
 Pfeiffer, Helmut (Germany)  
 Pfeiffer, Ruth (USA)  
 Pfender, Michael (Germany)  
 Pfetsch, Marc E. (Germany)  
 Pfister, Albrecht (Germany)  
 Pfister, Gerhard (Germany)  
 Pflaum, Christoph (Germany)  
 Pflaum, Markus J. (Germany)  
 Pflueger, Klaus (Germany)  
 Philip, Peter (Germany)  
 Philippin, Gerard A. (Canada)  
 Phillips, Keith L. (USA)  
 Phillips, N. Christopher (USA)  
 Phung, Ho (Vietnam)  
 Pickrell, Douglas M. (USA)  
 Piefke, Frank (Germany)  
 Piene, Ragni (Norway)  
 Pier, Jean-Paul (Luxembourg)  
 Pilipovic, Stevan (Yugoslavia)  
 Pillay, Anand (USA)  
 Pilyugin, Sergei Yu. (Russian Federation)  
 Pilz, Alexander (Germany)  
 Pinchuk, Sergey Ivanovich (Russian Federation)  
 Pinheiro, Vilton (Brazil)  
 Pink, Richard (Germany)  
 Pinkall, Ulrich (Germany)  
 Pinto, Alberto Adrego (Portugal)  
 Piovan, Luis A. (Argentina)  
 Pisier, Gilles (France)  
 Pitassi, Toniann (USA)  
 Pittet, Christophe (Germany)  
 Pizzo, Aldo Bruno (Argentina)  
 Plato, Robert (Germany)  
 Platonov, Sergei S. (Russian Federation)  
 Platzek, Maria I. (Argentina)  
 Plaza, Sergio (Chile)  
 Plewe, Klaus J. (Germany)  
 Plümer, Judith (Germany)  
 Poensgen, Diana A. I. (Germany)  
 Pöhle, Bärbel (Germany)  
 Pöhle, Uwe (Germany)  
 Pohozaev, Stanislav I. (Russian Federation)  
 Pohst, Michael E. (Germany)  
 Poldvere, Märt (Estonia)  
 Polterovich, Leonid (Israel)  
 Polthier, Konrad (Germany)  
 Polyakova, Katerina (Russian Federation)  
 Polzehl, Jörg (Germany)  
 Pomazanov, Michael V. (Russian Federation)  
 Ponce, Gustavo Alberto (USA)  
 Ponge, Raphael S. (France)  
 Ponomarenko, Andrej (Germany)  
 Ponomarev, Paul (USA)  
 Popa, Anca (Romania)  
 Popescu, Dorin-Mihail (Romania)  
 Popov, Igor Yu. (Russian Federation)  
 Popova, Elena V. (Russian Federation)  
 Porteous, Hugh L. (United Kingdom)  
 Poschadel, Norbert (Germany)  
 Pöschel, Reinhard (Germany)  
 Post, Katharina D. E. (Germany)  
 Postelnicu, Tiberiu V. (Romania)  
 Postnikov, Mihkail M. (Russian Federation)  
 Potapov, Vadim D. (Russian Federation)  
 Potthast, John (USA)  
 Potthast, Roland (Germany)  
 Pourkazemi, Mohammad H. (Iran)  
 Pragarauskas, Henrikas (Lithuania)  
 Präve, Alexandra (Germany)  
 Preissler, Gabi (Germany)  
 Presman, Ernst L. (Russian Federation)  
 Prestin, Jürgen (Germany)  
 Preston, Gordon B. (Australia)  
 Preunkert, Marc (Germany)  
 Preuß, Gerhard (Germany)

- Pribitkin, Wladimir de Azevedo (Germany)  
 Priebe, Volker (Germany)  
 Prieto, Carlos (Mexico)  
 Pripplata, Christine (Germany)  
 Prishlyak, Alexander (Ukraine)  
 Prokhorov, Yuri (Russian Federation)  
 Prömel, Hans J. (Germany)  
 Prüfer, Friedbert (Germany)  
 Pruschke, Thilo (Germany)  
 Prytula, Yaroslav Ya. (Ukraine)  
 Ptak, Marek (Poland)  
 Puchta, Jan-Christoph (Hungary)  
 Pujals, Enrique Ramiro E. R. P. (Brazil)  
 Pukhlikov, Aleksandr (Russian Federation)  
 Pulkina, Ludmila S. (Russian Federation)  
 Pulleyblank, William R. (USA)  
 Puppe, Dieter (Germany)  
 Puppe, Volker (Germany)  
 Pustynnikov, Lev L. D. (Russian Federation)  
  
 Quast, Peter (Germany)  
 Quian, Minping (P. R. China)  
 Quine, John R. (USA)  
 Quinn, Frank (USA)  
  
 Rabindranathan, Malayattil (USA)  
 Rabinovich, Vladimir S. (Russian Federation)  
 Rachele, Lizabeth V. (USA)  
 Rack, Heinz-Joachim (Germany)  
 Racke, Reinhard (Germany)  
 Rackwitz, Hans-Georg (Germany)  
 Raczynski, Andrzej (Poland)  
 Rademacher, Hans-Bert (Germany)  
 Rademacher, Jens (Germany)  
 Radic, Mirko V. (Sweden)  
 Radtke, Achim (Germany)  
 Radu, Mircea (Romania)  
 Radyno, Alexander Yakovlevich (Belarus)  
 Radyno, Nikolai Ya. (Belarus)  
 Raghavan, K. N. (India)  
 Raghavendra, Nyshadham (India)  
 Ragusa, Alfio (Italy)  
 Raikov, George D. (Bulgaria)  
 Raitums, Uldis (Latvia)  
 Rajabov, Nusrat (Tajikistan)  
 Rakhimov, Abdugafaz (Uzbekistan)  
  
 Rakic, Zoran (Yugoslavia)  
 Rakosník, Jirí (Czech Republic)  
 Ramachandran, Niranjan (USA)  
 Rambau, Jörg (Germany)  
 Ramirez, Alejandro F. (Switzerland)  
 Ramirez-De-Arellano, Enrique (Mexico)  
 Ramollo, Motlatsi Pius (Lesotho)  
 Randow von, Thomas (Germany)  
 Rangarajan, Govindan (India)  
 Rapoport, Michael (Germany)  
 Rappoport, Juri M. (Russian Federation)  
 Rassias, Themistocles M. (Greece)  
 Rasskazov, Alexey (Russian Federation)  
 Rathsfeld, Andreas (Germany)  
 Ratnakumar, Peetta Kandy (India)  
 Rawat, Rama (Israel)  
 Rayskin, Victoria (USA)  
 Rebelo, Julio Cesar (Brazil)  
 Rebholz, Joachim (United Kingdom)  
 Rebiai, Salah-Eddine (Algeria)  
 Rebolledo, Rolando (Chile)  
 Recke, Lutz (Germany)  
 Reddy, B. Daya (South Africa)  
 Reemtsen, Rembert (Germany)  
 Rees, S. Mary (United Kingdom)  
 Rego, F. Alfredo (Guatemala)  
 Rehberg, Joachim (Germany)  
 Rehmann, Ulf (Germany)  
 Reichel, Hans-Christian (Austria)  
 Reichert-Hahn, Marianne (Germany)  
 Reigle, Dennis J. (USA)  
 Reiher, Gesine (Germany)  
 Reimann, Hans Martin (Switzerland)  
 Reinelt, Gerhard (Germany)  
 Reinhardt, Gerd (Germany)  
 Reiris i Thurralde, Martin (Uruguay)  
 Reiss, Markus (Germany)  
 Reiten, Idun (Norway)  
 Reitz, Stefan (Germany)  
 Rempala, Grzegorz A. (USA)  
 Ren, Nanheng (P. R. China)  
 Rendall, Alan D. (Germany)  
 Renteria-Marquez, Carlos (Mexico)  
 Rentner, Wolf-Dietrich (Germany)  
 Rentschler, Rudolf (France)  
 Repovs, Dusan (Slovenia)  
 Rerikh, Konstantin V. (Russian Federation)  
 Ressel, Paul (Germany)  
 Revalski, Julian P. (Bulgaria)



- Reyes Rodríguez, Armando (Mexico)  
 Riahi, Hasna (Tunisia)  
 Ribe, Martin G. (Sweden)  
 Ricci, Fulvio (Italy)  
 Richter, Thomas (Germany)  
 Rickard, Jeremy C. (United Kingdom)  
 Rickmann, Seppo U. (Finland)  
 Riede, Adolf J. I. (Germany)  
 Rieder, Andreas (Germany)  
 Rieder, Ulrich (Germany)  
 Riedl, Johannes (Germany)  
 Rieger, Marc Oliver (Germany)  
 Riemenschneider, Oswald W. (Germany)  
 Riesel, Hans (Sweden)  
 Rieutord, Michel L. E. (France)  
 Rindler, Harald (Austria)  
 Ringel, Claus Michael (Germany)  
 Riordan, Oliver M. (United Kingdom)  
 Ritter, Günter (Germany)  
 Rizvi, Syed Tariq (USA)  
 Robbiani, Marcello L. (Switzerland)  
 Robbiano, Lorenzo (Italy)  
 Robert, Aline (France)  
 Roberts, Brooks K. (Canada)  
 Robertson, Ian (USA)  
 Robinson, Bencion (Israel)  
 Robinson, Margaret M. (USA)  
 Rocsoareanu, Carmen (Romania)  
 Roczen, Marko (Germany)  
 Rodkina, Alexandra E. (Russian Federation)  
 Rodrigues, Jose Francisco (Portugal)  
 Rodriguez del Rio, Roberto (Spain)  
 Rodriguez Santiesteban, Antonio Ramon (Germany)  
 Rodriguez Trueba, Maria Isabel (Spain)  
 Roegner, Katherine S. (Germany)  
 Roendigs, Oliver (Germany)  
 Røgen, Peter (Denmark)  
 Rogmann, Sascha A. (Germany)  
 Rogowski, Andrzej (Poland)  
 Roitzsch, Rainer (Germany)  
 Rolles, Silke W. (Germany)  
 Roman, Olena (Ukraine)  
 Römisch, Werner (Germany)  
 Ronconi, Maria Cristina (Italy)  
 Ronto, Miklos (Hungary)  
 Roos, Jan-Erik I. (Sweden)  
 Roque, Tatiana (France)  
 Rosa, Renata (Brazil)  
 Rosado, Fernando (Portugal)  
 Rosemeier, Frank J. (Germany)  
 Rosenbaum, Kurt (Germany)  
 Rosenbaum, Wolfram (Germany)  
 Rosenberger, Gerhard (Germany)  
 Rosenknop, John (Germany)  
 Rosenthal, Haskell P. (USA)  
 Rösler, Margit (Germany)  
 Rosset, Shmuel (Israel)  
 Rossetti, Juan Pablo (Argentina)  
 Rossi, Louis F. (USA)  
 Rothschild, Linda P. (USA)  
 Roubicek, Tomas (Czech Republic)  
 Rouillier, Fabrice F. R. (France)  
 Roushon, Sayed Khaled Mr. (Germany)  
 Rowe, David E. (Germany)  
 Rowley, Christopher (United Kingdom)  
 Royter, Andriy (Ukraine)  
 Rozanova, Olga S. (Russian Federation)  
 Rozanski, Roman (Poland)  
 Ru, Min (USA)  
 Ruan, Yongbin (USA)  
 Rubin, Boris (Israel)  
 Ruckmann, Jan-J. (Germany)  
 Rudolf, Ingeborg (Germany)  
 Rudyak, Yuli B. (Germany)  
 Ruffing, Andreas (Germany)  
 Ruh, Ernst A. (Switzerland)  
 Runge, Bernhard (Germany)  
 Runge, Daniel (Germany)  
 Rusch, Beate (Germany)  
 Rüssmann, Helmut (Germany)  
 Ruzicka, Michael (Germany)  
 Ryska, Norbert (Germany)  
 Ryushi, Goto (Japan)  
 Sabitova, Mary Nailevna (Russian Federation)  
 Sablatnig, Jan-H. (Germany)  
 Sadyrbaev, Felix (Latvia)  
 Safonov, Mikhail Vasilevich (USA)  
 Sahab, Salem A. (Kingdom of Saudi-Arabia)  
 Saintloup, Bernard (France)  
 Saitoh, Hitoshi (Japan)  
 Sakakibara, Nobuhisa (Japan)  
 Sakata, Hiroshi (Japan)  
 Saktikov, Evgueni (Russian Federation)  
 Salberger, Per (Sweden)  
 Saldanha, Nicolau (Brazil)  
 Salinas, Norberto (USA)

- Salinger, David L. (United Kingdom)  
 Salmhofer, Manfred (Switzerland)  
 Sambarino Ottino, Martin Javier  
 (Uruguay)  
 Samoilenko, Anatolij M. (Ukraine)  
 Sanatani, Sunoy (Canada)  
 Sanchez Ruiz, Luis M. (Spain)  
 Sancho, Fernando (Spain)  
 Sand, Guido (Germany)  
 Sandler, Hanna M. (USA)  
 Saneblidze, Samson (Georgia)  
 Sangare, Daouda (France)  
 San Martín, Bernardo A. (Chile)  
 Sanni, Sikiru A. (Nigeria)  
 Sano, Kimiro (Japan)  
 Santos, Francisco (Spain)  
 Sanz-Solé, Marta (Spain)  
 Sarhan, Ammar (Egypt)  
 Sarnak, Peter (USA)  
 Sasao, Seiya (Japan)  
 Sastry, Seemanapalli V. (Brazil)  
 Satake, Ichiro (Japan)  
 Sato, Atsushi (Brazil)  
 Sato, Ken-iti (Japan)  
 Sato, Yumiko (Japan)  
 Sauermann, Markus (Germany)  
 Savas, Ekrem (Turkey)  
 Saveliev, Nikolai (USA)  
 Sawada, Ken (Japan)  
 Sawae, Ryuichi (Japan)  
 Sawon, Justin (United Kingdom)  
 Sawyer, Patrice (Canada)  
 Sax, Ulrich K. (Germany)  
 Sbordone, Carlo (Italy)  
 Scardua, Bruno (Brazil)  
 Scepanovic, Radoje (Yugoslavia)  
 Schachermayer, Walter (Austria)  
 Schäl, Manfred (Germany)  
 Scharlach, Christine (Germany)  
 Scharlau, Rudolf M. E. (Germany)  
 Scharlau, Winfried (Germany)  
 Scharlemann, Martin (USA)  
 Schauenburg, Peter (Germany)  
 Schechtman, Gideon (Israel)  
 Scheel, Arnd (Germany)  
 Scheerer, Hans (Germany)  
 Scheiderer, Claus (Germany)  
 Schein, Boris M. (USA)  
 Schendel, Udo (Germany)  
 Schenzel, Peter (Germany)  
 Schermuly, Carola M. (Germany)  
 Scheutzow, Michael K. R. (Germany)  
 Schied, Alexander (Germany)  
 Schiffels, Gerhard (Germany)  
 Schilling, Susan (USA)  
 Schilling, Tanja (Germany)  
 Schimmerling, Ernest (USA)  
 Schimming, Rainer (Germany)  
 Schinas, Christos J. (Greece)  
 Schinas, John (Greece)  
 Schleicher, Dierk (Germany)  
 Schlesinger, Karl-Georg (Germany)  
 Schlichting, Günter H. (Germany)  
 Schlichting, Marco (France)  
 Schlickewei, Hans Peter (Germany)  
 Schlippe, Johannes (Germany)  
 Schlomiuk, Dana (Canada)  
 Schlosser, Hartmut (Germany)  
 Schlundt, Rainer (Germany)  
 Schmalz, Gerd (Germany)  
 Schmeelk, John (USA)  
 Schmehr, Dirk R. W. (Germany)  
 Schmeling, Joerg (Germany)  
 Schmelzer, Ilja (Germany)  
 Schmickler-Hirzebruch, Ulrike (Germany)  
 Schmid, Wilfried (USA)  
 Schmidt, Alexander (Germany)  
 Schmidt, Andreas U. (Germany)  
 Schmidt, Frank (Germany)  
 Schmidt, Gunther (Germany)  
 Schmidt, Marco (Germany)  
 Schmidt, Rita Maria (Germany)  
 Schmidt, Siegbert (Germany)  
 Schmidt, Stefan E. (USA)  
 Schmidt, Werner (Germany)  
 Schmidt-Ehrenberg, Johannes (Germany)  
 Schmidtmann, Olaf (Germany)  
 Schmieta, Stefan H. (USA)  
 Schmitt, Burkhard J. (Germany)  
 Schmitt, Nikolaus (Germany)  
 Schmitt, Peter (Austria)  
 Schmüdgen, Konrad (Germany)  
 Schneider, Kai (Germany)  
 Schneider, Klaus R. (Germany)  
 Schnürer, Oliver C. (Germany)  
 Schock, Eberhard (Germany)  
 Schoenwaelder, Ulrich F. K. (Germany)  
 Scholz, Hartmut (Germany)  
 Scholz, Reinhard (Germany)  
 Schönhage, Arnold (Germany)

- Schonmann, Roberto (USA)  
 Schoppmeier, Ulrich (Germany)  
 Schork, Matthias (Germany)  
 Schrader, Rainer (Germany)  
 Schrader, Robert (Germany)  
 Schramm, Ruben (Israel)  
 Schreyer, Frank (Germany)  
 Schrijver, Alexander (Netherlands)  
 Schrohe, Elmar (Germany)  
 Schubert, Roman (Germany)  
 Schult, Jörg (Germany)  
 Schulte, Udo (Germany)  
 Schultz, Rüdiger (Germany)  
 Schultz, Reinhard E. (USA)  
 Schulz, Andreas S. (Germany)  
 Schulz, Bernd (Germany)  
 Schulz, Christian (Germany)  
 Schulz, Dirk (Germany)  
 Schulz, Ralph-Hardo (Germany)  
 Schulz, Ursula (Germany)  
 Schulz, Wolfgang (Germany)  
 Schulz-Baldes, Hermann (Germany)  
 Schulze, Bert-Wolfgang (Germany)  
 Schulze, Felix (Germany)  
 Schulze, Volker (Germany)  
 Schulze-Pillot, Rainer (Germany)  
 Schurath, Ronald (Germany)  
 Schurr, Ingo (Germany)  
 Schurz, Henri U. (Colombia)  
 Schuster, Peter Michael (Germany)  
 Schwachhöfer, Lorenz (Germany)  
 Schwartz, Alan L. (USA)  
 Schwartz, Alexander (Germany)  
 Schwartz, Thomas (Germany)  
 Schwarz, Ernst (Germany)  
 Schwarz, Wolfgang K. (Germany)  
 Schweigert, Dietmar (Germany)  
 Schweizer, Jürgen (Germany)  
 Schweizer, Martin (Germany)  
 Schwenk, Angela (Germany)  
 Schwertfeger, Karl-Heinz (Germany)  
 Schwichtenberg, Helmut (Germany)  
 Schwitzer, Felix (Austria)  
 Scott, Richard (USA)  
 Sczech, Robert (USA)  
 Sedykh, Vyacheslav D. (Russian Federation)  
 Seeländer, Jörg (Germany)  
 Seidel, Jacob (Netherlands)  
 Seifoullaev, Roustam K. (Azerbaijan)  
 Seiler, Joerg (Germany)  
 Seiler, Ruedi (Germany)  
 Seiler, Wolfgang K. (Germany)  
 Seip, Kristian (Norway)  
 Sekiguchi, Takeshi (Japan)  
 Sekita, Eitaro (Japan)  
 Selder, Erich (Germany)  
 Selfridge, John L. (USA)  
 Seligman, George B. (USA)  
 Selivanova, Elena Nikolaevna (Russian Federation)  
 Selwat, Karol (Poland)  
 Semeria, Severine (France)  
 Semmler, Beate (Germany)  
 Semmler, Klaus-Dieter (Switzerland)  
 Senf, Peter (Germany)  
 Serbetcioglu, Aglaia Marissa (Germany)  
 Serganova, Vera (USA)  
 Sergeev, Armen (Russian Federation)  
 Series, Caroline (United Kingdom)  
 Sevenster, Arjen (Netherlands)  
 Seydel, Detlef (Germany)  
 Sezinando, Helena (Portugal)  
 Shabozov, Mirgand (Tajikistan)  
 Shadman, Darinsh (Iran)  
 Shadwick, William F. (United Kingdom)  
 Shah, Nimish A. (India)  
 Shah, Riddhi (India)  
 Shahvarani-Semnani, Ahmad (Iran)  
 Shaidurov, Vladimir V. (Russian Federation)  
 Shaikhet, Leonid E. (Ukraine)  
 Shakunle, Lere O. (Germany)  
 Shalev, Aner (Israel)  
 Shaneson, Julius L. (USA)  
 Sharipbaev, Altynbek (Kazakhstan)  
 Sharma, B. K. (India)  
 Shatz, Stephen S. (USA)  
 Shaw, Sen-Yen (P. R. China)  
 Shchepanika, Elena (Russian Federation)  
 Shchepanuk, Gennady (Ukraine)  
 Shen, Yu (USA)  
 Shepelsky, Dmitry (Ukraine)  
 Sheshko, Michal (Poland)  
 Sheth, Dilip (D. N.) (India)  
 Shevchenko, Yurii (Russian Federation)  
 Shevelev, Vladimir S. (Russian Federation)  
 Shi, Niandong (USA)  
 Shi, Wujie (P. R. China)

- Shiba, Hironori (Japan)  
 Shibano, Hiroki (Japan)  
 Shibata, Tetsutaro T. (Japan)  
 Shima, Kazuhisa (Japan)  
 Shimomura, Katsunori (Japan)  
 Shimura, Tatsuya (Japan)  
 Shintani, Toshitada (Japan)  
 Shiraiwa, Kenichi K. S. (Japan)  
 Shiratani, Katsumi (Japan)  
 Shirikyan, Armen (Russian Federation)  
 Shishikura, Mitsuhiro (Japan)  
 Shiu, Christine (United Kingdom)  
 Shiu, Peter (United Kingdom)  
 Shmygowskyi, Mykola (Ukraine)  
 Shoji, Mayumi (Japan)  
 Shomron, Noam (USA)  
 Shor, Naum Zuselevich (Ukraine)  
 Shor, Peter W. (USA)  
 Shtern, Alexander I. (Russian Federation)  
 Shtykel, Tatyana (Germany)  
 Shu, Chi-Wang (USA)  
 Shubin, Mikhail (USA)  
 Shubladze, Mamuka (Georgia)  
 Siddo, Carol (United Kingdom)  
 Siebeneicher, Christian (Germany)  
 Siebenmann, Laurent C. (France)  
 Sieber, Jan (Germany)  
 Siegfanz, Monika (Germany)  
 Siegmund, David Oliver (USA)  
 Siegmund, Stefan (Germany)  
 Siegmund-Schultze, Rainer (Germany)  
 Siegmund-Schultze, Reinhard (Germany)  
 Siemon, Helmut (Germany)  
 Sieveking, Malte (Germany)  
 Sigmund, Karl (Austria)  
 Sigrist, Francois (Switzerland)  
 Sigurdsson, Ragnar (Sweden)  
 Silva, Jorge-Nuno O. (Portugal)  
 Simeliene, Nijole (Lithuania)  
 Simic, Slavko (Yugoslavia)  
 Simic, Slobodan (USA)  
 Simic, Slobodan K. (Yugoslavia)  
 Simms, David J. (Ireland)  
 Simon, Jacques C. H. (France)  
 Simon, Udo H. (Germany)  
 Simons, Gordon E. (Canada)  
 Sims, Charles C. (USA)  
 Singer, Ivan (Romania)  
 Singh, Ajit Iqbal (India)  
 Singh, Anand Prakash (India)  
 Singh, Shobh N. (South Africa)  
 Sireteanu, Tudor (Romania)  
 Siu, Man-Keung (P. R. China)  
 Sjögren, Peter (Sweden)  
 Skill, Thomas (Germany)  
 Skopenkov, Arkady (Russian Federation)  
 Skrypnik, Igor I. (Ukraine)  
 Skutella, Martin (Germany)  
 Slateff, Andreas (Austria)  
 Slattery, Suzanne (USA)  
 Slawig, Thomas (Germany)  
 Slembek, Silke (France)  
 Sloane, Neil J. A. (USA)  
 Slovak, Jan (Czech Republic)  
 Slungård, Inger Heidi (Norway)  
 Smale, Steve (P. R. China)  
 Smirnov, Fedor (France)  
 Smirnov, Georgi V. (Portugal)  
 Smirnov, Stanislav (Germany)  
 Smital, Jaroslav (Czech Republic)  
 Smith, David Alexander (USA)  
 Smith, Hart F. (USA)  
 Smith, Perry B. (USA)  
 Smith, Stuart P. (USA)  
 Smoluk, Antoni (Poland)  
 Soares, Marcio G. (Brazil)  
 Sobolev, Vladimir (Russian Federation)  
 Soboleva, Eugenia S. (Russian Federation)  
 Socolowsky, Jürgen (Germany)  
 Soergel, Wolfgang (Germany)  
 Sofronidis, Nikolas Efstathiou (USA)  
 Soibelman, Yan (USA)  
 Sokolowski, Jan (France)  
 Solano, Cesar (Germany)  
 Solberg, Oyvind (Norway)  
 Söllner, Hildegard (Germany)  
 Solodkyy, Sergiy Georgievich (Ukraine)  
 Sologuren, Santiago (Bolivia)  
 Sommerhäuser, Yorck (Germany)  
 Sonin, Constatin I. (Russian Federation)  
 Sonntag, Rolf (Germany)  
 Sormani, Christina (USA)  
 Sos, Vera T. (Hungary)  
 Sostak, Alexander (Latvia)  
 Soto-Andrade, Jorge (Chile)  
 Soulé, Christophe (France)  
 Spandaw, Jeroen G. (Germany)  
 Sparla, Eric (Germany)  
 Speck, Frank-Olme (Portugal)  
 Speh, Birgit E. M. (USA)

- Speicher, Roland (Germany)  
 Speier, Joseph D. (USA)  
 Spengler, Andreas (Germany)  
 Sperber, Wolfram (Germany)  
 Spichtinger, Peter (Germany)  
 Spielberg, Holger (France)  
 Spitkovsky, Ilya M. (USA)  
 Spitzweck, Markus (Germany)  
 Sprekels, Jürgen (Germany)  
 Spresser, Diane M. (USA)  
 Springborn, Boris A. (Germany)  
 Srinivas, Vasudevan (India)  
 Srinivasan, Bhama (USA)  
 Stadje, Wolfgang (Germany)  
 Stafford, Richard M. (USA)  
 Stagnaro, Ezio (Italy)  
 Stagnii, Valerii (Ukraine)  
 Stahlke, Colin (Germany)  
 Stallmann, Friedemann W. (USA)  
 Stamm, Roland (Germany)  
 Stangler, Sieghart S. (Germany)  
 Stanley, Donald (Germany)  
 Stanley, Richard P. (USA)  
 Stark, Harold M. (USA)  
 Staude, Ulrich (Germany)  
 Stawicki, Michael (Germany)  
 Stefánsson, Jón R. (Iceland)  
 Steger, Tim J. (Italy)  
 Stein, Elias M. (USA)  
 Stein, Michael R. (USA)  
 Stein, Oliver (Germany)  
 Stein, Ralf (Germany)  
 Steinbach, Marc C. (Germany)  
 Steinbart, Enid M. (USA)  
 Steiner, Hans-Georg (Germany)  
 Steiner, Richard J. (United Kingdom)  
 Steinhorn, Charles I. (USA)  
 Stelter, Andreas (Germany)  
 Stempien, Zdzislaw (Poland)  
 Stephan, Holger (Germany)  
 Stephanidis, Nikolaus K. (Greece)  
 Stern, Eugene (USA)  
 Stern, Ronald J. (USA)  
 Sternheimer, Daniel H. (France)  
 Steuding, Jörn (Germany)  
 St. Mary, Donald F. (USA)  
 Stock, Josef K. (Germany)  
 Stocke, A. Britt-Marie (Sweden)  
 Stocks, Douglas R. (USA)  
 Stoer, Josef (Germany)  
 Stolle, Hermann (Germany)  
 Stoppel, Hannes (Germany)  
 Stork, Frederik (Germany)  
 Storvick, David A. (USA)  
 Stoyan, Yuri Grigoriyevich (Ukraine)  
 Strade, Helmut (Germany)  
 Strano, Rosario (Italy)  
 Strassen, Volker (Germany)  
 Stratigos, Panagiotis D. (USA)  
 Strauch, Matthias (Germany)  
 Strauss, Vladimir (Venezuela)  
 Stray, Arne (Norway)  
 Strazdins, Indulis (Latvia)  
 Streit, Manfred F. G. (Germany)  
 Strey, Gerhard (Germany)  
 Strömberg, Jan-Olov (Norway)  
 Strooker, Jan R. (Netherlands)  
 Stroth, Gernot (Germany)  
 Strugar, Igor (Yugoslavia)  
 Strunkov, Sergey P. (Russian Federation)  
 Struwe, Michael (Switzerland)  
 Strzelecki, Pawel (Poland)  
 Stüben, Hinnerk (Germany)  
 Stühler, Andrea (Germany)  
 Subbotin, Igor Ya. (USA)  
 Suchlandt, Hans E. (Germany)  
 Suciu, Ioan (Romania)  
 Suda, Hiroshi (Japan)  
 Sudan, Madhu (USA)  
 Sugawa, Toshiyuki (Japan)  
 Sugawara, Kazuko (Japan)  
 Suger Cofino, Eduardo (Guatemala)  
 Sujatha, R. (Germany)  
 Sullivan, John M. (USA)  
 Sultangazin, Umirzak (Kazakhstan)  
 Sumi, Hiroki (Japan)  
 Sun, Jialin (P. R. China)  
 Sundberg, Carl (USA)  
 Sunder, V. S. (India)  
 Suresh, Venapally (India)  
 Surkova, Anna (Ukraine)  
 Sustar Rossetti, Ana M. (Argentina)  
 Svendsen, John A. (Norway)  
 Swallow, John (USA)  
 Swanson, Irena (USA)  
 Swart, Henda (South Africa)  
 Swiatek, Grzegorz (USA)  
 Swiatkowski, Jacek (Poland)  
 Sy, Polly W. (Philippines)  
 Symeonidis, Eleutherius E. (Germany)

- Symington, Margaret F. (USA)  
 Sytchev, Mikhail A. (Germany)  
 Sytova, Svetlana N. (Belarus)  
 Szabo, Zoltan Istvan (Hungary)  
 Szegedy, Balazs (Hungary)  
 Szemberg, Tomasz (Poland)  
 Sznitman, Alain-Sol (Switzerland)  
 Szolnoki, Dietmar (Germany)  
 Tachikawa, Atsushi (Japan)  
 Taffin, Erik (France)  
 Taft, Earl J. (USA)  
 Taghavi, Mohsen (Iran)  
 Tai, Yung-sheng (USA)  
 Takahashi, Satoshi (Japan)  
 Takahashi, Sechiko S. (Japan)  
 Takakura, Tatsuru (Japan)  
 Takashima, Keizo (Japan)  
 Takenaka, Shigeo (Japan)  
 Takenouchi, Osamu (Japan)  
 Takeuchi, Kiyoshi (Japan)  
 Talagrand, Michel (France)  
 Taljaard, Monica (South Africa)  
 Tamamura, Akie (Japan)  
 Tamanoi, Hirotaka (USA)  
 Tambieva, Jannet A. (Russian Federation)  
 Tamrazov, Promarz M. (Ukraine)  
 Tanaka, Hisao (Japan)  
 Tanaka, Minoru M. T. (Japan)  
 Tang, Shanjian (P. R. China)  
 Tang, Zizhou (P. R. China)  
 Taniguchi, Yoshiharu (Japan)  
 Tankeev, Serguei G. (Russian Federation)  
 Tao, Terence C. (USA)  
 Tapiz, Chiney (Philippines)  
 Taqqu, Murad S. (USA)  
 Tarasov, Vitaly (Russian Federation)  
 Taraz, Anusch (Germany)  
 Tarkhanov, Nikolai (Germany)  
 Tasaki, Hiroyuki (Japan)  
 Taubes, Clifford Henry (USA)  
 Tavgen, Oleg I. (Belarus)  
 Tchourkin, Andrey V. (Russian Federation)  
 Tedorov, Kaltscho (Bulgaria)  
 Teicher, Mina (Israel)  
 Terakawa, Hiroyuki (Japan)  
 Terng, Chuu-Lian (USA)  
 Terras, Audrey A. (USA)  
 Teschke, Lothar (Germany)  
 Teschke, Olaf (Germany)  
 Teuchert, Margitta (Germany)  
 Thalhammer, Mechthild (Austria)  
 Thao, Vo Dang (Vietnam)  
 Thas, Joseph Adolphe François (Belgium)  
 Thomas, Charles B. (United Kingdom)  
 Thomason, Andrew G. (United Kingdom)  
 Thomassen, Carsten (Denmark)  
 Thomsen, Andreas (Germany)  
 Tiba, Dan (Romania)  
 Tienari, Matti (Finland)  
 Tietz, Horst (Germany)  
 Tietze, Walter (Germany)  
 Tijun, Xiao (P. R. China)  
 Tillmann, Heinz-Günther (Germany)  
 Tilouine, Jacques (France)  
 Timmreck, Dagmar (Germany)  
 Timofeeva, Galina A. (Russian Federation)  
 Timoney, Richard M. (Ireland)  
 Tirado, Eleazar (Venezuela)  
 Tita, Nicolae (Romania)  
 Titzhoff, Frank (Germany)  
 Tkachenko, Natalia Valeryevna (Ukraine)  
 Tkachenko, Vadim A. (Israel)  
 Tkachenko, Viktor Ivanovich (Ukraine)  
 Tkachev, Vladimir G. (Russian Federation)  
 Tobies, Renate (Germany)  
 Toda, Masahito (Japan)  
 Todorcevic, Stevo B. (Canada)  
 Toffalori, Carlo (Italy)  
 Togari, Yoshio (Japan)  
 Tohge, Kazuya (Japan)  
 Tokizawa, Masamichi (Japan)  
 Tolev, Doytchin (Bulgaria)  
 Toll, Charles H. (USA)  
 Tolok, Alexey (Ukraine)  
 Tolokonnikov, Vadim (Germany)  
 Tomczak-Jaegermann, Nicole (Canada)  
 Tomida, Masamichi (Japan)  
 Tominaga, Yasuo (Japan)  
 Tondeur, Philippe (USA)  
 Ton-That, Tuong (USA)  
 Topalov, Peter (Bulgaria)  
 Törner, Günter (Germany)  
 Totaro, Burt (USA)  
 Totok, Alexander A. (Russian Federation)  
 Toyoshiba, Hiroyoshi (Japan)  
 Tralle, Aleksy (Poland)  
 Trautmann, Günther (Germany)

- Trefethen, Lloyd N. (United Kingdom)  
 Trenogin, Vladilen A. (Russian Federation)  
 Trittler, Matthias (Germany)  
 Trivedi, Vijaylaxmi (India)  
 Troitsky, Evgenij V. (Russian Federation)  
 Tröltzsch, Fredi (Germany)  
 Tronel, Gérard H. (France)  
 Trotman, David J. A. (France)  
 Trott, Michael (USA)  
 Trunk, Carsten (Germany)  
 Tsarkov, Yevgeny (Latvia)  
 Tschinkel, Yuri (USA)  
 Tsevendorj, Ider (Mongolia)  
 Tsirelson, Boris (Israel)  
 Tsou, Sheung Tsun (United Kingdom)  
 Tsuboi, Takashi (Japan)  
 Tsuji, Takeshi (Japan)  
 Tsukui, Yasuyuki (Japan)  
 Tumulka, Roderich A. (Germany)  
 Tuneke, Hilmar R. (Germany)  
 Tung, Chia-Chi (USA)  
 Turaev, Dmitry (Germany)  
 Turo, Jan (Poland)  
 Tuschmann, Wilderich (Germany)  
 Tuzhilin, Alexei A. (Russian Federation)  
 Twardowska, Krystyna (Poland)  
 Tylli, Hans-Olav I. (Finland)  
 Tzafriri, Lior (Israel)  
 Uetake, Yoichi (Poland)  
 Uetz, Marc (Germany)  
 Uhle, Manfred (Germany)  
 Uhlmann, Gunther A. (USA)  
 Ukon, Michihisa (Japan)  
 Ulecia, Teresa (Spain)  
 Ullrich, Peter (Germany)  
 Unger, Luise (Germany)  
 Uraltseva, Nina N. (Russian Federation)  
 Urbach, Paul (Netherlands)  
 Urbonas, Alsimanjas Pranas (Lithuania)  
 Usmanov, Shukhrat (Uzbekistan)  
 Vaccaro, Michelangelo (Italy)  
 Vafa, Cumrun (USA)  
 Väisälä, Jussi (Finland)  
 Valadier, Michel (France)  
 Valla, Giuseppe (Italy)  
 Valtr, Pavel (Czech Republic)  
 van der Geer, Gerard (Netherlands)  
 van der Hoeven, Joris (France)  
 van der Kallen, Wilberd L. (Netherlands)  
 van der Poorten, Alfred J. (Australia)  
 Vanecek, Antonin (Czech Republic)  
 van Gelderen, J. A. (Netherlands)  
 van Lint, Jacobus H. (Netherlands)  
 Vanoli, Marie (France)  
 van Rienen, Ursula (Germany)  
 Varilly, Joseph C. (Costa Rica)  
 Varona, Juan L. (Spain)  
 Varvak, Mark (USA)  
 Vasco, Carlos E. (Colombia)  
 Vasilchuk, Vladimir (Ukraine)  
 Vasil'ev, Alexander Jur'evich (Colombia)  
 Vasiliev, Mikhail (Russian Federation)  
 Vasiliev, Oleg (Russian Federation)  
 Vasilieva, Ekaterina A. (Belarus)  
 Vasilieva, Olga O. (Colombia)  
 Vasilyeva, Tatiana Anatolyevna (Russian Federation)  
 Veeramani, Palanichamy (India)  
 Velenik, Yvan (Germany)  
 Veloso, Jose Miguel (Brazil)  
 Vêlu, Jacques (France)  
 Vemuri, Murali K. (USA)  
 Venema, Gerard A. (USA)  
 Vera Valenzuela, Jaime A. (Chile)  
 Verbitsky, Misha S. (France)  
 Vergara Caffarelli, Giorgio (Italy)  
 Vergne, Michele F. (France)  
 Verrill, Helena A. (Germany)  
 Vershik, Anatoly (Russian Federation)  
 Vershinin, Vladimir V. (Russian Federation)  
 Vesnin, Andrei Yu. (Russian Federation)  
 Vetter, Udo (Germany)  
 Veys, Willem (Belgium)  
 Viana, Marcelo (Brazil)  
 Vielhaber, Michael J. (Germany)  
 Vignoli, Alfonso (Italy)  
 Viharos, László (Hungary)  
 Villani, Vinicio (Germany)  
 Villella, José A. (Argentina)  
 Vilonen, Kari (USA)  
 Vinberg, Ernest B. (Germany)  
 Vinogradova, Natalya V. (Russian Federation)  
 Viola, Carlo (Italy)  
 Virag, Balint (USA)  
 Vlad, Carmen D. (USA)  
 Vladimir, Samovol (Russian Federation)  
 Vladimirescu, Mihai M. (Canada)

- Vladimirov, V. S. (Russian Federation)  
 Vodop'yanov, Serguei (Russian Federation)  
 Voevodsky, Vladimir (USA)  
 Vogel, Hans-Jürgen (Germany)  
 Vogelsang, Rudolf (Germany)  
 Vogt, Dietmar (Germany)  
 Vogt, Elmar (Germany)  
 Vogt, Rainer (Germany)  
 Voit, Michael P. (Germany)  
 Volcheck, Emil J. (USA)  
 Volcic, Aljosa (Italy)  
 Volk, Wolfgang (Germany)  
 Vollrath, Hans-Joachim (Germany)  
 Volz, Dietmar (Germany)  
 von Mouche, Pierre (Netherlands)  
 von Schroeders, Nicolai (Germany)  
 von Törne, Christian (Germany)  
 Vortisch, Wilhelm (Germany)  
 Voskresenskii, Valentin E. (Russian Federation)  
 Voss, Leonard (Germany)  
 Vukovic, Mirjana (Bosnia and Herzegovina)  
 Waadeland, Haakon S. (Norway)  
 Wacker, Markus (Germany)  
 Wada, Hidekazu (Japan)  
 Wagler, Annegret (Germany)  
 Wagner, Jacques (France)  
 Wagner, Ulrich (Germany)  
 Wagner, Wolfgang (Germany)  
 Wahl, Jonathan M. (USA)  
 Wainger, Stephen (USA)  
 Wakabayashi, Yoshiko (Brazil)  
 Wakimoto, Minoru (Japan)  
 Wakolbinger, Anton (Germany)  
 Walczak, Pawel (Poland)  
 Walczak, Zofia (Poland)  
 Walden, Rainer (Germany)  
 Waldhausen, Maja (Germany)  
 Waldschmidt, Michel (France)  
 Wallace, David A. R. (United Kingdom)  
 Walter, Michael (Germany)  
 Walters, Samuel G. (Canada)  
 Wan, Zhe-Xian (Sweden)  
 Wang, Bai-Ling (Australia)  
 Wang, Feng-Yu (P. R. China)  
 Wang, Hwai-Chiuan (Taiwan)  
 Wang, Lan (USA)  
 Wang, Ya-Guang (P. R. China)  
 Wang, Zeke (P. R. China)  
 Wändefors, Magnus (Sweden)  
 Wanger, Anke (Germany)  
 Wanka, Gert (Germany)  
 Warmuth, Elke (Germany)  
 Warmuth, Walter (Germany)  
 Wassermann, Gordon (Germany)  
 Watanabe, Hisao (Japan)  
 Watanabe, Shuji (Japan)  
 Watanabe, Toshiro (Japan)  
 Watson, Bill (USA)  
 Watson, Richard O. (Ireland)  
 Waugh, Jason M. (USA)  
 Webber, David (United Kingdom)  
 Weber, Georg (Germany)  
 Wegert, Elias (Germany)  
 Wegmann, Helmut (Germany)  
 Wegner, Bernd (Germany)  
 Wei, Guofang (USA)  
 Weibel, Charles A. (USA)  
 Weigl, Thomas (Germany)  
 Weihmann, Nadja Ilka (Germany)  
 Weikard, Rudi (USA)  
 Weill, Georges G. (USA)  
 Weimann, Lutz (Germany)  
 Weimar-Woods, Evelyn (Germany)  
 Weintraub, Steven H. (USA)  
 Weiser, Martin (Germany)  
 Weisfeld, Morris (USA)  
 Weispfenning, Volker (Germany)  
 Weiss, Jürgen (Germany)  
 Weizsäcker, Heinrich (Germany)  
 Welch, Philip D. (Japan)  
 Welker, Volkmar (Germany)  
 Wellin, Paul R. (USA)  
 Welzl, Emo (USA)  
 Wenk, Carola (Germany)  
 Wenzel, Jörg (Germany)  
 Werbowski, Jaroslaw (Poland)  
 Werner, Dirk (Germany)  
 Werner, Wend (Germany)  
 Wessäly, Roland (Germany)  
 Westerhoff, Natascha (Germany)  
 Westphal, Ursula (Germany)  
 Wiczorek, Tina (Germany)  
 Wiedorn, Corinna (Germany)  
 Wiegand, Sylvia M. (USA)  
 Wiegmann, Klaus Werner (Germany)  
 Wiehe, Martin (Germany)  
 Wieners, Christian (Germany)



- Wihstutz, Volker (USA)  
 Wildenhain, Günther (Germany)  
 Wiles, Andrew J. (USA)  
 Wilhelm, Hannes (Germany)  
 Wilke, Marc (Germany)  
 Wilkens, Bettina (Germany)  
 Wilkens, David L. (United Kingdom)  
 Wilkie, Alex James (United Kingdom)  
 Wilkins, David R. (Ireland)  
 Willems, Jan C. (Netherlands)  
 Willerton, Simon (France)  
 Williams, Ruth J. (USA)  
 Wilmanski, Krzysztof (Germany)  
 Wilson, John S. (United Kingdom)  
 Wilson, Pelham M. H. (United Kingdom)  
 Winczewski, Vincent (Germany)  
 Winkelkemper, Horst E. (USA)  
 Winkler, Jörg (Germany)  
 Winkler, Renate C. (Germany)  
 Winterfeld, Ulrike (Germany)  
 Winterhof, Arne (Germany)  
 Winzer, Olga (Ukraine)  
 Witt, Ingo (Germany)  
 Witte, Dave (USA)  
 Witte, Jürgen (Germany)  
 Wittwer, Janine (USA)  
 Woit, Peter (USA)  
 Wojciechowky, Michal (Poland)  
 Woldar, Andrew J. (USA)  
 Wolf, Joerg (Germany)  
 Wolf, Joseph A. (USA)  
 Wolfart, Jürgen (Germany)  
 Wolfrum, Matthias (Germany)  
 Wong, Siman (USA)  
 Woodin, W. Hugh (USA)  
 Woods, E. James (Germany)  
 Wotzlaw, Lorenz (Germany)  
 Wright, Margaret H. (USA)  
 Wschebor, Mario (Uruguay)  
 Wu, Ching-Tang (Germany)  
 Wu, Jiahong (USA)  
 Wu, Pei Yuan (Taiwan)  
 Wu, Sijue S. (USA)  
 Wu, Siye (Australia)  
 Wu, Xinsheng (P. R. China)  
 Wulff, Claudia (Germany)  
 Wulfsohn, Aubrey (United Kingdom)  
 Wünsch, Volkmar (Germany)  
 Wüstner, Michael (Germany)  
 Wynands, Alexander (Germany)
- Xambó-Descamps, Sebastià (Spain)  
 Xia, Zhihong (USA)  
 Xie, Quanbo (Germany)  
 Ximin, Liu (P. R. China)  
 Xu, Fei (P. R. China)  
 Xu, Xiaoping (P. R. China)  
 Xu, Zhongling (P. R. China)
- Yadrenko, Mikhailo (Ukraine)  
 Yafaev, Dmitri (France)  
 Yagola, Anatoly G. (Russian Federation)  
 Yagunov, Serge A. (Russian Federation)  
 Yamanaka, Takeharu (Japan)  
 Yamanoshita, Tsuneyo (Japan)  
 Yamashima, Shigeho (Japan)  
 Yamashita, Hajime (Japan)  
 Yan, Min (P. R. China)  
 Yanchuk, Sergiy, V. (Ukraine)  
 Yang, Chung-Chun (P. R. China)  
 Yang, Jae-Hyun (Korea)  
 Yang, Lo (P. R. China)  
 Yang, Tonghai (USA)  
 Yang, Weiqi (P. R. China)  
 Yanusi, Mahmud Yusuf (Tajikistan)  
 Yaroshevsky, Vassily A. (Russian Federation)  
 Yasuda, Julia Y. (USA)  
 Yasuhiro, Asoo (Japan)  
 Yau, Horng-Tzer (USA)  
 Yebdri, Mustapha (Algeria)  
 Yemelyanova, Inna Sergeevna (Russian Federation)  
 Yengibarran, Norayi (Georgia)  
 Yevtouchik, Leonik (Russian Federation)  
 Ylinen, Kari E. (Finland)  
 Yoshida, Katsuaki (Japan)  
 Yoshida, Tomoyuki (Japan)  
 Yoshimoto, Akinori (Japan)  
 Yoshino, Masafumi (France)  
 Yost, David (Thailand)  
 Yu, Guoliang (USA)  
 Yu, Jie-Tai (P. R. China)  
 Yu, Joseph M. L. (Canada)  
 Yu, Kunrui (P. R. China)  
 Yu, Pei (Canada)  
 Yu, Rupert W. T. (France)  
 Yugai, Lev (Uzbekistan)  
 Yurko, Vjacheslav A. (Russian Federation)  
 Yushkevich, Alexander A. (USA)
- Zacharias, Klaus (Germany)

- Zacher, Giovanni G. (Italy)  
Zagier, Don, B. (Germany)  
Zaicev, Mikhail V. (Russian Federation)  
Zaitsev, Dmitri (Germany)  
Zaitsev, Iuri M. (Brazil)  
Zakharov, Victor V. (Russian Federation)  
Zand, Hossein (United Kingdom)  
Zapatrin, Roman (Russian Federation)  
Zarbaliev, Sakhatat Mail (Russian Federation)  
Zastrow, Andreas (Germany)  
Zavalishchin, Stanislav T. (Russian Federation)  
Zayed, Ahmed I. (USA)  
Zdravkovska, Smilka (USA)  
Zegarlini, Boguslaw (United Kingdom)  
Zeidler, Eberhard (Germany)  
Zelazko, Wieslaw (Poland)  
Zelevinsky, Andrei V. (USA)  
Zelikin, Mikhail (Russian Federation)  
Zelman, Mark (USA)  
Zeman, Martin (Germany)  
Zemanek, Jaroslav (Poland)  
Zepf, Günther (Germany)  
Zerouali, Elhassan (Morocco)  
Zgliczynski, Piotr (Poland)  
Zhang, Gong Qing (P. R. China)  
Zhang, Jian (USA)  
Zhang, Jinyu (P. R. China)  
Zhang, Meirong (P. R. China)  
Zhang, Pu (P. R. China)  
Zhang, Shou-Wu (USA)  
Zhang, Shunian (P. R. China)  
Zhao, Jennifer J. (USA)  
Zhao, Yiquiang Q. (Canada)  
Zhao, Yue (USA)  
Zharinov, Victor V. (Russian Federation)  
Zhdanov, Renat Z. (Ukraine)  
Zheng, Fangyang (USA)  
Zhu, Jianping (USA)  
Ziegenbalg, Jochen (Germany)  
Ziegler, Günter M. (Germany)  
Ziegler, Martin (Germany)  
Zielke, Roland J. (Germany)  
Zillmann, Désirée (Germany)  
Zimmer, Johannes (Germany)  
Zimmermann, Bernd (Germany)  
Zimmermann, Uwe T. (Germany)  
Zinchenko, Olga A. (Russian Federation)  
Zink, Wilhelm (Germany)  
Zipperer, Jörg (Germany)  
Zitzwitz, Gerhard (Germany)  
Ziza, Oxana A. (Russian Federation)  
Zizchenko, Alexei B. (Russian Federation)  
Zoch, Avery (USA)  
Zolotykh, Andrej A. (Russian Federation)  
Zorn, Erhard (Germany)  
Zouling, Zhou (P. R. China)  
Zowe, Jochem (Germany)  
Zschiedrich, Lin (Germany)  
Zschiegner, Marc (Germany)  
Zseby, Siegfried (Germany)  
Zubrilin, Konstantin A. (Russian Federation)  
Zuev, Sergey V. (Russian Federation)  
Zvyagin, Victor G. (Russian Federation)  
Zwahlen, Bruno (Switzerland)  
Zygmunt, Marcin J. (Poland)

## PARTICIPANTS BY COUNTRY

(according to their mailing address)

Algeria.....	5	Guatemala.....	4	Peru.....	1
Argentina.....	15	Hungary.....	25	Philippines.....	4
Armenia.....	4	Iceland.....	2	Poland.....	74
Australia.....	18	India.....	35	Portugal.....	18
Austria.....	17	Indonesia.....	1	Romania.....	43
Azerbaijan.....	1	Iran.....	24	Russian Federation....	202
Bangladesh.....	1	Ireland.....	10	Senegal.....	1
Barbados.....	1	Israel.....	36	Singapore.....	4
Belarus.....	12	Italy.....	65	Slovakia.....	2
Belgium.....	9	Ivory Coast.....	5	Slovenia.....	1
Bolivia.....	1	Japan.....	205	South Africa.....	17
Bosnia and Herzegovina .	2	Kazakhstan.....	7	Spain.....	44
Brazil.....	42	Kingdom of Saudi-Arabia	5	Sweden.....	37
Bulgaria.....	6	Korea.....	10	Switzerland.....	39
Burundi.....	1	Kuwait.....	3	Taiwan.....	11
Cameroon.....	2	Latvia.....	6	Tajikistan.....	8
Canada.....	45	Lebanon.....	1	Tanzania.....	1
Chile.....	11	Lesotho.....	1	Thailand.....	3
Colombia.....	4	Lithuania.....	6	Togo.....	1
Costa Rica.....	1	Luxembourg.....	2	Tunesia.....	6
Croatia.....	7	Macedonia.....	1	Turkey.....	8
Cuba.....	1	Malaysia.....	1	Turkmenistan.....	1
Cyprus.....	3	Mexico.....	15	USA.....	500
Czech Republic.....	11	Moldova.....	3	Ukraine.....	75
Denmark.....	11	Mongolia.....	2	United Arab Emirates...	1
Egypt.....	7	Morocco.....	9	United Kingdom.....	88
Estonia.....	13	Mozambique.....	3	Uruguay.....	5
Finland.....	27	Netherlands.....	19	Uzbekistan.....	6
France.....	138	New Zealand.....	5	Venezuela.....	5
Georgia.....	13	Nigeria.....	4	Vietnam.....	5
Germany.....	1087	Norway.....	18	Yugoslavia.....	21
Ghana.....	1	P. R. China.....	52	Zimbabwe.....	2
Greece.....	10	Pakistan.....	1		

## THE WORK OF RICHARD EWEN BORCHERDS

PETER GODDARD

## 1 INTRODUCTION

Richard Borcherds has used the study of certain exceptional and exotic algebraic structures to motivate the introduction of important new algebraic concepts: vertex algebras and generalized Kac-Moody algebras, and he has demonstrated their power by using them to prove the “moonshine conjectures” of Conway and Norton about the Monster Group and to find whole new families of automorphic forms.

A central thread in his research has been a particular Lie algebra, now known as the Fake Monster Lie algebra, which is, in a certain sense, the simplest known example of a generalized Kac-Moody algebra which is not finite-dimensional or affine (or a sum of such algebras). As the name might suggest, this algebra *appears* to have something to do with the Monster group, *i.e.* the largest sporadic finite simple group.

The story starts with the observation that the Leech lattice can be interpreted as the Dynkin diagram for a Kac-Moody algebra,  $\mathcal{L}_\infty$ . But  $\mathcal{L}_\infty$  is difficult to handle; its root multiplicities are not known explicitly. Borcherds showed how to enlarge it to obtain the more amenable Fake Monster Lie algebra. In order to construct this algebra, Borcherds introduced the concept of a vertex algebra, in the process establishing a comprehensive algebraic approach to (two-dimensional) conformal field theory, a subject of major importance in theoretical physics in the last thirty years.

To provide a general context for the Fake Monster Lie algebra, Borcherds has developed the theory of generalized Kac-Moody algebras, proving, in particular, generalizations of the Kac-Weyl character and denominator formulae. The denominator formula for the Fake Monster Lie algebra motivated Borcherds to construct a “real” Monster Lie algebra, which he used to prove the moonshine conjectures. The results for the Fake Monster Lie algebra also motivated Borcherds to explore the properties of the denominator formula for other generalized Kac-Moody algebras, obtaining remarkable product expressions for modular functions, results on the moduli spaces of certain complex surfaces and much else besides.

2 THE LEECH LATTICE AND THE KAC-MOODY ALGEBRA  $\mathcal{L}_\infty$ 

We start by recalling that a finite-dimensional simple complex Lie algebra,  $\mathcal{L}$ , can be expressed in terms of generators and relations as follows. There is a non-singular invariant bilinear form  $(,)$  on  $\mathcal{L}$  which induces such a form on the rank  $\mathcal{L}$  dimensional space spanned by the roots of  $\mathcal{L}$ . Suppose  $\{\alpha_i : 1 \leq i \leq \text{rank } \mathcal{L}\}$  is a

basis of simple roots for  $\mathcal{L}$ . Then the numbers  $a_{ij} = (\alpha_i, \alpha_j)$  have the following properties:

$$a_{ii} > 0, \quad (1)$$

$$a_{ij} = a_{ji}, \quad (2)$$

$$a_{ij} \leq 0 \quad \text{if } i \neq j, \quad (3)$$

$$2a_{ij}/a_{ii} \in \mathbb{Z}. \quad (4)$$

The symmetric matrix  $A = (a_{ij})$  obtained in this way is positive definite.

The algebra  $\mathcal{L}$  can be reconstructed from the matrix  $A$  by the system of generators and relations used to define  $\mathcal{L}_\infty$ ,

$$[e_i, f_i] = h_i, \quad [e_i, f_j] = 0 \quad \text{for } i \neq j, \quad (5)$$

$$[h_i, e_j] = a_{ij}e_j, \quad [h_i, f_j] = -a_{ij}f_j, \quad (6)$$

$$\text{Ad}(e_i)^{n_{ij}}(e_j) = \text{Ad}(f_i)^{n_{ij}}(f_j) = 0, \quad \text{for } n_{ij} = 1 - 2a_{ij}/a_{ii}. \quad (7)$$

These relations can be used to define a Lie algebra,  $\mathcal{L}_A$ , for any matrix  $A$  satisfying the conditions (1-4).  $\mathcal{L}_A$  is called a (symmetrizable) Kac-Moody algebra. If  $A$  is positive definite,  $\mathcal{L}_A$  is semi-simple and, if  $A$  is positive semi-definite,  $\mathcal{L}_A$  is a sum of affine and finite-dimensional algebras.

Although Kac and Moody only explicitly considered the situation in which the number of simple roots was finite, the theory of Kac-Moody algebras applies to algebras which have an infinite number of simple roots. Borcherds and others [1] showed how to construct such an algebra with simple roots labelled by the points of the Leech lattice,  $\Lambda_L$ . We can conveniently describe  $\Lambda_L$  as a subset of the unique even self-dual lattice,  $\text{II}_{25,1}$ , in 26-dimensional Lorentzian space,  $\mathbb{R}^{25,1}$ .  $\text{II}_{25,1}$  is the set of points whose coordinates are all either integers or half odd integers which have integral inner product with the vector  $(\frac{1}{2}, \dots, \frac{1}{2}, \frac{1}{2}) \in \mathbb{R}^{25,1}$ , where the norm of  $x = (x_1, x_2, \dots, x_{25}; x_0)$  is  $x^2 = x_1^2 + x_2^2 + \dots + x_{25}^2 - x_0^2$ .

The vector  $\rho = (0, 1, 2, \dots, 24; 70) \in \text{II}_{25,1}$  has zero norm,  $\rho^2 = 0$ ; the Leech lattice can be shown to be isomorphic to the set  $\{x \in \text{II}_{25,1} : x \cdot \rho = -1\}$  modulo displacements by  $\rho$ . We can take the representative points for the Leech lattice to have norm 2 and so obtain an isometric correspondence between  $\Lambda_L$  and

$$\{r \in \text{II}_{25,1} : r \cdot \rho = -1, r^2 = 2\}. \quad (8)$$

Then, with each point  $r$  of the Leech lattice, we can associate a reflection  $x \mapsto \sigma_r(x) = x - (r \cdot x)r$  which is an automorphism of  $\text{II}_{25,1}$ . Indeed these reflections  $\sigma_r$  generate a Weyl group,  $W$ , and the whole automorphism group of  $\text{II}_{25,1}$  is the semi-direct product of  $W$  and the automorphism group of the affine Leech lattice, which is the Dynkin/Coxeter diagram of the Weyl group  $W$ . To this Dynkin diagram can be associated an infinite-dimensional Kac-Moody algebra,  $\mathcal{L}_\infty$ , generated by elements  $\{e_r, f_r, h_r : r \in \Lambda_L\}$  subject to the relations (5-7). Dividing by the linear combinations of the  $h_r$  which are in the centre reduces its rank to 26.

The point about Kac-Moody algebras is that they share many of the properties enjoyed by semi-simple Lie algebras. In particular, we can define a Weyl group,

$W$ , and for suitable (*i.e.* lowest weight) representations, there is a straightforward generalization of the Weyl character formula. For a representation with lowest weight  $\lambda$ , this generalization, the Weyl-Kac character formula, states

$$\chi_\lambda = \sum_{w \in W} \det(w) w(e^{\rho+\lambda}) \Big/ e^\rho \prod_{\alpha > 0} (1 - e^\alpha)^{m_\alpha}, \quad (9)$$

where  $\rho$  is the Weyl vector, with  $\rho \cdot r = -r^2/2$  for all simple roots  $r$ ,  $m_\alpha$  is the multiplicity of the root  $\alpha$ , the sum is over the elements  $w$  of the Weyl group  $W$ , and the product is over positive roots  $\alpha$ , that is roots which can be expressed as the sum of a subset of the simple roots with positive integral coefficients.

Considering even just the trivial representation, for which  $\lambda = 0$  and  $\chi_0 = 1$ , yields a potentially interesting relation from (9),

$$\sum_{w \in W} \det(w) w(e^\rho) = e^\rho \prod_{\alpha > 0} (1 - e^\alpha)^{m_\alpha}. \quad (10)$$

Kac showed that this denominator identity produces the Macdonald identities in the affine case. Kac-Moody algebras, other than the finite-dimensional and affine ones, would seem to offer the prospect of new identities generalizing these but the problem is that in other cases of Kac-Moody algebras, although the simple roots are known (as for  $\mathcal{L}_\infty$ ), which effectively enables the sum over the Weyl group to be evaluated, the root multiplicities,  $m_\alpha$ , are not known, so that the product over positive roots cannot be evaluated.

No general simple explicit formula is known for the root multiplicities of  $\mathcal{L}_\infty$  but, using the “no-ghost” theorem of string theory, I. Frenkel established the bound

$$m_\alpha \leq p_{24}(1 - \frac{1}{2}\alpha^2), \quad (11)$$

where  $p_k(n)$  is the number of partitions of  $n$  using  $k$  colours. This bound is saturated for some of the roots of  $\mathcal{L}_\infty$  and, where it is not, there is the impression that that is because something is missing. What seems to be missing are some simple roots of zero or negative norm. In Kac-Moody algebras all the simple roots are specified by (1) to be of positive norm, even though some of the other roots they generate may not be.

### 3 VERTEX ALGEBRAS

Motivated by Frenkel’s work, Borchers introduced in [3] the definition of a vertex algebra, which could in turn be used to define Lie algebras with root multiplicities which are explicitly calculable. A vertex algebra is a graded complex vector space,  $V = \bigoplus_{n \in \mathbb{Z}} V_n$ , together with a “vertex operator”,  $a(z)$ , for each  $a \in V$ , which is a formal power series in the complex variable  $z$ ,

$$a(z) = \sum_{m \in \mathbb{Z}} a_m z^{-m-n}, \quad \text{for } a \in V_n, \quad (12)$$

where the operators  $a_m$  map  $V_n \rightarrow V_{n-m}$  and satisfy the following properties:

1.  $a_n b = 0$  for  $n > N$  for some integer  $N$  dependent on  $a$  and  $b$ ;
2. there is an operator (derivation)  $D : V \rightarrow V$  such that  $[D, a(z)] = \frac{d}{dz} a(z)$ ;
3. there is a vector  $\mathbf{1} \in V_0$  such that  $\mathbf{1}(z) = 1$ ,  $D\mathbf{1} = 0$ ;
4.  $a(0)\mathbf{1} = a$ ;
5.  $(z - \zeta)^N (a(z)b(\zeta) - b(\zeta)a(z)) = 0$  for some integer  $N$  dependent on  $a$  and  $b$ .

[We may define vertex operators over other fields or over the integers with more effort if we wish but the essential features are brought out in the complex case.]

The motivation for these axioms comes from string theory, where the vertex operators describe the interactions of “strings” (which are to be interpreted as models for elementary particles). Condition (5) states that  $a(z)$  and  $b(\zeta)$  commute apart from a possible pole at  $z = \zeta$ , *i.e.* they are local fields in the sense of quantum field theory. A key result is that, in an appropriate sense,

$$(a(z - \zeta)b)(\zeta) = a(z)b(\zeta) = b(\zeta)a(z). \quad (13)$$

More precisely

$$\int_0 d\zeta \int_{\zeta} dz (a(z - \zeta)b)(\zeta)f = \int_0 dz \int_0 d\zeta a(z)b(\zeta)f - \int_0 d\zeta \int_0 dz b(\zeta)a(z)f. \quad (14)$$

where  $f$  is a polynomial in  $z$ ,  $\zeta$ ,  $z - \zeta$  and their inverses, and the integral over  $z$  is a circle about  $\zeta$  in the first integral, one about  $\zeta$  and the origin in the second integral and a circle about the origin excluding the  $\zeta$  in the third integral. The axioms originally proposed by Borchers [2] were somewhat more complicated in form and follow from those given here from the conditions generated by (14).

We can associate a vertex algebra to any even lattice  $\Lambda$ , the space  $V$  then having the structure of the tensor product of the complex group ring  $\mathbb{C}(\Lambda)$  with the symmetric algebra of a sum  $\bigoplus_{n>0} \Lambda_n$  of copies  $\Lambda_n$ ,  $n \in \mathbb{Z}$ , of  $\Lambda$ . In terms of string theory, this is the Fock space describing the (chiral) states of a string moving in a space-time compactified into a torus by imposing periodicity under displacements by the lattice  $\Lambda$ .

The first triumph of vertex algebras was to provide a natural setting for the Monster group,  $M$ .  $M$  acts on a graded infinite-dimensional space  $V^{\natural}$ , constructed by Frenkel, Lepowsky and Meurman, where  $V^{\natural} = \bigoplus_{n \geq -1} V_n^{\natural}$ , and the dimensions of  $\dim V_n^{\natural}$  is the coefficient,  $c(n)$  of  $q^n$  in the elliptic modular function,

$$j(\tau) - 744 = \sum_{n=-1}^{\infty} c(n)q^n = q^{-1} + 196884q + 21493760q^2 + \dots, \quad q = e^{2\pi i\tau}. \quad (15)$$

A first thought might have been that the Monster group should be related to the space  $V_{\Lambda_L}$ , the vertex algebra directly associated with the Leech lattice, but  $V_{\Lambda_L}$  has a grade 0 piece of dimension 24 and the lowest non-trivial representation of the Monster is of dimension 196883.  $V^{\natural}$  is related to  $V_{\Lambda_L}$  but is a sort of twisted version of it; in string theory terms it corresponds to the string moving on an orbifold rather than a torus.

The Monster group is precisely the group of automorphisms of the vertex algebra  $V^{\natural}$ ,

$$ga(z)g^{-1} = (ga)(z), \quad g \in M. \quad (16)$$

This characterizes  $M$  in a way similar to the way that two other sporadic simple finite groups, Conway's group  $Co_1$  and the Mathieu group  $M_{24}$ , can be characterized as the automorphism groups of the Leech lattice (modulo  $-1$ ) and the Golay Code, respectively.

#### 4 GENERALIZED KAC-MOODY ALGEBRAS

In their famous moonshine conjectures, Conway and Norton went far beyond the existence of the graded representation  $V^{\natural}$  with dimension given by  $j$ . Their main conjecture was that, for each element  $g \in M$ , the Thompson series

$$T_g(q) = \sum_{n=-1}^{\infty} \text{Trace}(g|V_n^{\natural})q^n \quad (17)$$

is a Hauptmodul for some genus zero subgroup,  $G$ , of  $SL_2(\mathbb{R})$ , *i.e.*, if

$$H = \{\tau : \text{Im}(\tau) > 0\} \quad (18)$$

denotes the upper half complex plane,  $G$  is such that the closure of  $H/G$  is a compact Riemann surface,  $\overline{H/G}$ , of genus zero with a finite number of points removed and  $T_g(q)$  defines an isomorphism of  $\overline{H/G}$  onto the Riemann sphere.

To attack the moonshine conjectures it is necessary to introduce some Lie algebraic structure. For any vertex algebra,  $V$ , we can introduce [2, 4] a Lie algebra of operators

$$L(a) = \frac{1}{2\pi i} \oint a(z)dz = a_{-h+1}, \quad a \in V_h. \quad (19)$$

Closure  $[L(a), L(b)] = L(L(a)b)$  follows from (14), but this does not define a Lie algebra structure directly on  $V$  because  $L(a)b$  is not itself antisymmetric in  $a$  and  $b$ . However,  $DV$  is in the kernel of the map  $a \mapsto L(a)$  and  $L(a)b = -L(b)a$  in  $V/DV$ , so it does define a Lie algebra  $\mathcal{L}^0(V)$  on this quotient [2], but this is not the most interesting Lie algebra associated with  $V$ .

Vertex algebras of interest come with an additional structure, an action of the Virasoro algebra, a central extension of the Lie algebra of polynomial vector fields on the circle, spanned by  $L_n, n \in \mathbb{Z}$  and 1,

$$[L_m, L_n] = (m-n)L_{m+n} + \frac{c}{12}m(m^2-1)\delta_{m,-n}, \quad [L_n, c] = 0, \quad (20)$$

with  $L_{-1} = D$  and  $L_0a = ha$  for  $a \in V_h$ . For  $V_{\Lambda}$ ,  $c = \dim \Lambda$ , and for  $V^{\natural}$ ,  $c = 24$ . The Virasoro algebra plays a central role in string theory. The space of "physical states" of the string is defined by the Virasoro conditions: let

$$P^k(V) = \{a \in V : L_0a = ka; L_na = 0, n > 0\}, \quad (21)$$



the space of physical states is  $P^1(V)$ . The space  $P^1(V)/L_{-1}P^0(V)$  has a Lie algebra structure defined on it (because  $L_{-1}V \cap P^1(V) \subset L_{-1}P^0(V)$ ). This can be reduced in size further using a contravariant form (which it possesses naturally for lattice theories). The “no-ghost” theorem states that the space of physical states  $P^1(V)$  has lots of null states and is positive semi-definite for  $V_\Lambda$ , where  $\Lambda$  is a Lorentzian lattice with  $\dim \Lambda \leq 26$ . So we can quotient  $P^1(V)/L_{-1}P^0(V)$  further by its null space with the respect to the contravariant form to obtain a Lie algebra  $\mathcal{L}(V)$ .

The results of factoring by the null space are most dramatic when  $c = 26$ . The vertex algebra  $V_L$  has a natural grading by the lattice  $L$  and the “no-ghost” theorem states that the dimension of the subspace of  $\mathcal{L}(V)$  of non-zero grade  $\alpha$  is  $p_{24}(1 - \frac{1}{2}\alpha^2)$  if  $\Lambda$  is a Lorentzian lattice of dimension 26 but  $p_{k-1}(1 - \alpha^2/2) - p_{k-1}(\alpha^2/2)$  if  $\dim \Lambda = k \neq 26$ ,  $k > 2$ . Thus the algebra  $\mathcal{L}'_M = \mathcal{L}(V_{II_{25,1}})$  saturates Frenkel’s bound, and Borcherds initially named it the “Monster Lie algebra” because it appeared to be directly connected to the Monster; it is now known as the “Fake Monster Lie algebra.”

Borcherds [4] had the great insight not only to construct the Fake Monster Lie algebra, but also to see how to generalize the definition of a Kac-Moody algebra effectively in order to bring  $\mathcal{L}'_M$  within the fold. What was required was to relax the condition (1), requiring roots to have positive norm, and to allow them to be either zero or negative norm. The condition (4) then needs modification to apply only in the space-like case  $a_{ii} > 0$  and the same applies to the condition (7) on the generators. The only condition which needs to be added is that

$$[e_i, e_j] = [f_i, f_j] = 0 \quad \text{if } a_{ij} = 0. \quad (22)$$

The closeness of these conditions to those for Kac-Moody algebras means that most of the important structural results carry over; in particular there is a generalization of the Weyl-Kac character formula for representations with highest weight  $\lambda$ ,

$$\chi_\lambda = \sum_{w \in W} \det(w)w \left( e^\rho \sum_{\mu} \epsilon_\lambda(\mu) e^{\mu+\lambda} \right) / e^\rho \prod_{\alpha > 0} (1 - e^\alpha)^{m_\alpha}, \quad (23)$$

where the second sum in the numerator is over vectors  $\mu$  and  $\epsilon_\lambda(\mu) = (-1)^n$  if  $\mu$  can be expressed as the sum of  $n$  pairwise orthogonal simple roots with non-positive norm, all orthogonal to  $\lambda$ , and 0 otherwise. Of course, putting  $\lambda = 0$  and  $\chi_\lambda = 1$  again gives a denominator formula.

The description of generalized Kac-Moody algebras in terms of generators and relations enables the theory to be taken over rather simply from that of Kac-Moody algebras but it is not so convenient as a method of recognising them in practice, *e.g.* from amongst the algebras  $\mathcal{L}(V)$  previously constructed by Borcherds. But Borcherds [3] gave an alternative characterization of them as graded algebras with an “almost positive definite” contravariant bilinear form. More precisely, he showed that a graded Lie algebra,  $\mathcal{L} = \bigoplus_{n \in \mathbb{Z}} \mathcal{L}_n$ , is a generalized Kac-Moody algebra if the following conditions are satisfied:

1.  $\mathcal{L}_0$  is abelian and  $\dim \mathcal{L}_n$  is finite if  $n \neq 0$ ;
2.  $\mathcal{L}$  possesses an invariant bilinear form such that  $(\mathcal{L}_m, \mathcal{L}_n) = 0$  if  $m \neq n$ ;
3.  $\mathcal{L}$  possesses an involution  $\omega$  which is  $-1$  on  $\mathcal{L}_0$  and such that  $\omega(\mathcal{L}_m) \subset \mathcal{L}_{-m}$ ;
4. the contravariant bilinear form  $\langle L, M \rangle = -(L, \omega(M))$  is positive definite on  $\mathcal{L}_m$  for  $m \neq 0$ ;
5.  $\mathcal{L}_0 \subset [\mathcal{L}, \mathcal{L}]$ .

This characterization shows that the Fake Monster Lie algebra,  $\mathcal{L}'_M$ , is a generalised Kac-Moody algebra, and its root multiplicities are known to be given by  $p_{24}(1 - \frac{1}{2}\alpha^2)$ , but Borchers' theorem establishing the equivalence of his two definitions does not give a constructive method of finding the simple roots. As we remarked in the context of Kac-Moody algebras, if we knew both the root multiplicities and the simple roots, the denominator formula

$$\sum_{w \in W} \det(w)w \left( e^\rho \sum_{\mu} \epsilon_{\mu}(\alpha) e^{\mu} \right) = e^\rho \prod_{\alpha > 0} (1 - e^\alpha)^{m_\alpha} \quad (24)$$

might provide an interesting identity. Borchers solved [4] the problem of finding the simple roots, or rather proving that the obvious ones were all that there were, by inverting this argument. The positive norm simple roots can be identified with the Leech lattice as for  $\mathcal{L}_\infty$ . Writing  $\Pi_{25,1} = \Lambda_L \oplus \Pi_{1,1}$ , which follows by uniqueness or the earlier comments, the 'real' or space-like simple roots are  $\{(\lambda, 1, \frac{1}{2}\lambda^2 - 1) : \lambda \in \Lambda_L\}$ . (Here we are using we are writing  $\Pi_{1,1} = \{(m, n) : m, n \in \mathbb{Z}\}$  with  $(m, n)$  having norm  $-2mn$ .) Light-like simple roots are quite easily seen to be  $n\rho$ , where  $n$  is a positive integer and  $\rho = (0, 0, 1)$ . The denominator identity is then used to prove that there are no other light-like and that there are no time-like simple roots.

The denominator identity provides a remarkable relation between modular functions (apparently already known to some of the experts in the subject) which is the precursor of other even more remarkable identities. If we restrict attention to vectors  $(0, \sigma, \tau) \in \Pi_{25,1} \otimes \mathbb{C}$ , with  $\text{Im}(\sigma) > 0$ ,  $\text{Im}(\tau) > 0$ , it reads

$$p^{-1} \prod_{m>0, n \in \mathbb{Z}} (1 - p^m q^n)^{c'(mn)} = \Delta(\sigma)\Delta(\tau)(j(\sigma) - j(\tau)) \quad (25)$$

where  $c'(0) = 24$ ,  $c'(n) = c(n)$  if  $n \neq 0$ ,  $p = e^{2\pi i\sigma}$ ,  $q = e^{2\pi i\tau}$ , and

$$\Delta(\tau)^{-1} = q^{-1} \prod_{n>1} (1 - q^n)^{-24} = \sum_{n \geq 0} p_{24}(n) q^{n-1}. \quad (26)$$

## 5 MOONSHINE, THE MONSTER LIE ALGEBRA AND AUTOMORPHIC FORMS

The presence of  $j(\sigma)$  in (25) suggests a relationship to the moonshine conjectures and Borchers used [5, 6] this as motivation to construct the "real" Monster Lie Algebra,  $\mathcal{L}_M$  as one with denominator identity obtained by multiplying each side of (25) by  $\Delta(\sigma)\Delta(\tau)$ , to obtain the simpler formula

$$p^{-1} \prod_{m>0, n \in \mathbb{Z}} (1 - p^m q^n)^{c(mn)} = j(\sigma) - j(\tau). \quad (27)$$

This looks like the denominator formula for a generalised Kac-Moody algebra which is graded by  $\Pi_{1,1}$  and is such that the dimension of the subspace of grade  $(m, n) \neq (0, 0)$  is  $c(mn)$ , the dimension of  $V_{mn}^{\natural}$ . It is not difficult to see that this can be constructed by using the vertex algebra which is the tensor product  $V^{\natural} \otimes V_{\Pi_{1,1}}$  and defining  $\mathcal{L}_M$  to be the generalised Lie algebra,  $\mathcal{L}(V^{\natural} \otimes V_{\Pi_{1,1}})$ , constructed from the physical states.

Borcherds used [5, 6] twisted forms of the denominator identity for  $\mathcal{L}_M$  to prove the moonshine conjectures. The action of  $M$  on  $V^{\natural}$  provides an action on  $V = V^{\natural} \otimes V_{\Pi_{1,1}}$  induces an action on the physical state space  $P^1(V)$  and on its quotient,  $\mathcal{L}_M = \mathcal{L}(V)$ , by its null space. The ‘‘no-ghost’’ theorem implies that the part of  $\mathcal{L}_M$  of grade  $(m, n)$ ,  $(\mathcal{L}_M)_{(m,n)}$ , is isomorphic to  $V_{mn}^{\natural}$  as an  $M$  module. Borcherds adapted the argument he used to establish the denominator identity to prove the twisted relation

$$\begin{aligned} p^{-1} \exp \left( - \sum_{N>0} \sum_{m>0, n \in \mathbb{Z}} \text{Tr}(g^N | V_{mn}^{\natural}) p^{mN} q^{nN} / N \right) \\ = \sum_{m \in \mathbb{Z}} \text{Tr}(g | V_m^{\natural}) p^m - \sum_{n \in \mathbb{Z}} \text{Tr}(g | V_n^{\natural}) q^n. \end{aligned} \quad (28)$$

These relations on the Thompson series are sufficient to determine them from their first few terms and to establish that they are modular functions of genus 0.

Returning to the Fake Monster Lie Algebra, the denominator formula given in (25) was restricted to vectors of the form  $v = (0, \sigma, \tau)$  but we consider it for more general  $v \in \Pi_{25,1} \otimes \mathbb{C}$ , giving the denominator function

$$\Phi(v) = \sum_{w \in W} \det(w) e^{2\pi i(w(\rho), v)} \prod_{n>0} \left( 1 - e^{2\pi i n(w(\rho), v)} \right)^{24}. \quad (29)$$

This expression converges for  $\text{Im}(v)$  inside a certain cone (the positive light cone). Using the explicit form for  $\Phi(v)$  when  $v = (0, \sigma, \tau)$ , the known properties of  $j$  and  $\Delta$  and the fact that  $\Phi(v)$  manifestly satisfies the wave equation, Borcherds [6, 7, 9] establishes that  $\Phi(v)$  satisfies the functional equation

$$\Phi(2v/(v, v)) = -((v, v)/2)^{12} \Phi(v). \quad (30)$$

It also has the properties that

$$\Phi(v + \lambda) = \Phi(v) \quad \text{for } \lambda \in \Pi_{25,1} \quad (31)$$

and

$$\Phi(w(v)) = \det(w) \Phi(v) \quad \text{for } w \in \text{Aut}(\Pi_{25,1})^+, \quad (32)$$

the group of automorphisms of the lattice  $\Pi_{25,1}$  which preserve the time direction. These transformations generate a discrete subgroup of the group of conformal transformations on  $\mathbb{R}^{25,1}$ , which is itself isomorphic to  $O_{26,2}(\mathbb{R})$ ; in fact the discrete group is isomorphic to  $\text{Aut}(\Pi_{26,2})^+$ . The denominator function for the Fake Monster Lie algebra defines in this way an automorphic form of weight 12 for the discrete subgroup  $\text{Aut}(\Pi_{26,2})^+$  of  $O_{26,2}(\mathbb{R})^+$ . This result once obtained is seen not

to depend essentially on the dimension 26 and Borchers has developed this approach of obtaining representations of modular functions as infinite products from denominator formulae for generalized Kac-Moody algebras to obtain a plethora of beautiful formulae [7, 9, 11], *e.g.*

$$j(\tau) = q^{-1} \prod_{n>0} (1 - q^n)^{c_0(n^2)} = q^{-1} (1 - q)^{-744} (1 - q^2)^{80256} (1 - q^3)^{-12288744} \dots, \quad (33)$$

where  $f_0(\tau) = \sum_n c_0(n)q^n$  is the unique modular form of weight  $\frac{1}{2}$  for the group  $\Gamma_0(4)$  which is such that  $f_0(\tau) = 3q^{-3} + \mathcal{O}(q)$  at  $q = 0$  and  $c_0(n) = 0$  if  $n \equiv 2$  or  $3 \pmod{4}$ . He has also used these denominator functions to establish results about the moduli spaces of Enriques surfaces and families of K3 surfaces [8, 10].

Displaying penetrating insight, formidable technique and brilliant originality, Richard Borchers has used the beautiful properties of some exceptional structures to motivate new algebraic theories of great power with profound connections with other areas of mathematics and physics. He has used them to establish outstanding conjectures and to find new deep results in classical areas of mathematics. This is surely just the beginning of what we have to learn from what he has created.

#### REFERENCES

- [1] *A monster Lie algebra?* (with J. H. Conway, L. Queen and N. J. A. Sloane) Adv. Math. 53 (1984) 75-79.
- [2] *Vertex algebras, Kac-Moody algebras and the monster*, Proc. Nat. Acad. Sci. U.S.A. 83 (1986) 3068-3071.
- [3] *Generalized Kac-Moody algebras*, J. Alg. 115 (1988) 501-512.
- [4] *The monster Lie algebra*, Adv. Math. 83 (1990) 30-47.
- [5] *Monstrous moonshine and monstrous Lie algebras*, Invent. Math. 109 (1992) 405-444.
- [6] *Sporadic groups and string theory*, in *Proceedings of the First European Congress of Mathematics, Paris July 1992*, ed. A. Joseph *et al.*, Vol. 1, Birkhauser (1994) pp. 411-421.
- [7] *Automorphic forms on  $O_{s+2,2}(\mathbb{R})$  and infinite products*, Invent. Math. 120 (1995) 161-213.
- [8] *The moduli space of Enriques surfaces and the fake monster Lie superalgebra*, Topology 35 (1996) 699-710.
- [9] *Automorphic forms and Lie algebras*, in *Current developments in mathematics*, International Press (1996).
- [10] *Families of K3 surfaces*, (with L. Katzarkov, T. Pantev, N. I. Shepherd-Barron) J. Algebraic Geometry 7 (1998) 183-193.
- [11] *Automorphic forms with singularities on Grassmannians*, Invent. Math. 132 (1998) 491-562.

Peter Goddard  
St John's College  
Cambridge CB2 1TP

## RICHARD EWEN BORCHERDS

Department of Mathematics & Mathematical Statistics  
Cambridge University, Cambridge, England

Born: November 29, 1959, Cape Town, South Africa  
Nationality: British  
Marital Status: married

1978–1981 Undergraduate at Cambridge  
1981–1983 Ph.D. at Cambridge under J. H. Conway  
1983–1987 Research Fellow of Trinity College, Cambridge  
1987–1988 Morrey Assistant Professor at University of California,  
Berkeley  
1988–1992 Royal Society University Research Fellow, Cambridge  
1992–1993 Lecturer at D.P.M.M.S., Cambridge University  
1993–1996 Professor at the University of California, Berkeley  
1996 Royal Society Research Professor at D.P.M.M.S.,  
Cambridge University

Fields of Interest: Algebra and Number Theory

*Richard Ewen Borchers and Peter Goddard*

## THE WORK OF WILLIAM TIMOTHY GOWERS

BÉLA BOLLOBÁS

It gives me great pleasure to report on the beautiful mathematics of William Timothy Gowers that earned him a Fields Medal at ICM'98.

Gowers has made spectacular contributions to the theory of Banach spaces, pure combinatorics, and combinatorial number theory. His hallmark is his exceptional ability to attack difficult and fundamental problems the *right* way: a way that with hindsight is very natural but a priori is novel and extremely daring.

In functional analysis Gowers has solved many of the best-known and most important problems, several of which originated with Banach in the early 1930s. The shock-waves from these results will reverberate for many years to come, and will dramatically change the theory of Banach spaces. The great success of Gowers is due to his exceptional talent for combining techniques of analysis with involved and ingenious combinatorial arguments.

In combinatorics, Gowers has made fundamental contributions to the study of randomness: his tower type lower bound for Szemerédi's lemma is a tour de force. In combinatorial number theory, he has worked on the notoriously difficult problem of finding arithmetic progressions in sparse sets of integers. The ultimate aim is to prove Szemerédi's theorem with the optimal bound on the density that suffices to ensure long arithmetic progressions. Gowers proved a deep result for progressions of length four, thereby hugely improving the previous bound. The difficult and beautiful proof, which greatly extends Roth's argument, and makes clever use of Freiman's theorem, amply demonstrates Gowers' amazing mathematical power.

## 1 BANACH SPACES

A major aim of functional analysis is to understand the connection between the geometry of a Banach space  $X$  and the algebra  $\mathcal{L}(X)$  of bounded linear operators from the space  $X$  into itself. In particular, what conditions imply that a space  $X$  contains 'nice' subspaces, and that  $\mathcal{L}(X)$  has a rich structure?

In order to start this global project, over the past sixty years numerous major concrete questions had to be answered. As Hilbert said almost one hundred years ago, "Wie überhaupt jedes menschliche Unternehmen Ziele verfolgt, so braucht die mathematische Forschung Probleme. Durch die Lösung von Problemen stählt sich die Kraft des Forschers; er findet neue Methoden und Ausblicke, er gewinnt einen weiteren und freieren Horizont."

In this spirit, the theory of Banach spaces has been driven by a handful of fundamental problems, like the basis problem, the unconditional basic sequence problem, Banach's hyperplane problem, the invariant subspace problem, the distortion problem, and the Schröder-Bernstein problem. For over half a century,

progress with these major problems had been very slow: it is due to Gowers more than to anybody else that a few years ago the floodgates opened, and with the solutions of many of these problems the subject now has a ‘spacious, free horizon’.

If a space (infinite-dimensional separable Banach space)  $X$  can be represented as a sequence space then an operator  $T \in \mathcal{L}(X)$  is simply given by an infinite matrix, so it is desirable to find a basis of the space. A *Schauder basis* or simply *basis* of a space  $X$  is a sequence  $(e_n)_{n=1}^\infty \subset X$  such that every vector  $x \in X$  has a *unique* representation as a norm-convergent sum  $x = \sum_{n=1}^\infty a_n e_n$ . In 1973, solving a forty year old problem, Enflo [4] proved that not every separable Banach space has a basis, so our operators cannot always be given in this simple way. On the other hand, it is almost trivial that every Banach space contains a *basic sequence*: a sequence  $(x_n)_{n=1}^\infty$  that is a basis of its closed linear span.

The relationship between an operator  $T \in \mathcal{L}(X)$  and closed subspaces of  $X$  can also be very involved. In the 1980s Enflo [5] and Read [22] solved in the negative the invariant subspace problem for Banach spaces, and a little later Read [23] showed that this phenomenon can arise on a ‘nice’ space as well: he constructed a bounded linear operator on  $\ell_1$  that has only trivial invariant subspaces.

Although a basis  $(e_n)_{n=1}^\infty$  of a space  $X$  leads to a representation of the operators on  $X$  as matrices, it does not guarantee that  $\mathcal{L}(X)$  has a rich structure. For example, it does not guarantee that  $\mathcal{L}(X)$  contains many non-trivial projections. Thus, if  $x = \sum_{n=1}^\infty a_n e_n$  and  $\epsilon_n = 0, 1$ , then  $\sum_{n=1}^\infty \epsilon_n a_n e_n$  need not even converge. Similarly, a permutation of a basis need not be a basis, and if  $\sum_{n=1}^\infty a_n e_n$  is convergent and  $\pi : \mathbb{N} \rightarrow \mathbb{N}$  is a permutation then  $\sum_{n=1}^\infty a_{\pi(n)} e_{\pi(n)}$  need not converge. A basis is said to be *unconditional* if it *does* have these very pleasant properties; equivalently, a basis  $(e_n)_{n=1}^\infty$  is unconditional if there is a constant  $C > 0$  such that, if  $(a_n)_{n=1}^m$  and  $(\lambda_n)_{n=1}^m$  are scalar sequences with  $|\lambda_n| \leq 1$  for all  $n$ , then

$$\left\| \sum_{n=1}^m \lambda_n a_n e_n \right\| \leq C \left\| \sum_{n=1}^m a_n e_n \right\|.$$

Also, a sequence  $(x_n)_{n=1}^\infty$  is an *unconditional basic sequence* if it is an unconditional basis of its closed linear span. The standard bases of  $c_0$  and  $\ell_p$ ,  $1 \leq p < \infty$ , are all unconditional (and symmetric).

An unconditional basis guarantees much more structure than a basis, so it is not surprising that even classical spaces like  $C([0, 1])$  and  $L_1$  fail to have unconditional bases. However, the fundamental question of whether every space has a subspace with an unconditional basis (or, equivalently, whether every space contains an unconditional basic sequence) was open for many years, even after Enflo’s result.

The search for a subspace with an unconditional basis is closely related to the search for other ‘nice’ subspaces. For example, it is trivial that not every space contains a Hilbert space, but it is far from clear whether every space contains  $c_0$  or  $\ell_p$  for some  $1 \leq p < \infty$ . Indeed, this question was answered only in 1974, when Tsirelson [28] constructed a counterexample by a clever inductive procedure. This development greatly enhanced the prominence of the unconditional basic sequence problem.

The breakthrough came in the summer of 1991, when Gowers and Maurey [17] independently constructed spaces without unconditional basic sequences. As the constructions and proofs were almost identical, they joined forces to simplify the proofs and to exploit the consequences of the result. The Gowers-Maurey space  $X_{GM}$  is based on a construction of Schlumprecht [25] that eventually enabled Odell and Schlumprecht [21] to solve the famous *distortion problem*. Odell and Schlumprecht constructed a space isomorphic to  $\ell_2$  that contains no subspace almost isometric to  $\ell_2$ . The main difficulty Gowers and Maurey had to overcome in order to make use of Schlumprecht's space  $X_S$  was that  $X_S$  itself had an unconditional basis.

Johnson observed that the proofs could be modified to show that the Gowers-Maurey space not only has no unconditional basic sequence, but it does not even have a *decomposable subspace* either: no subspace of  $X_{GM}$  can be written as a topological direct sum of two (infinite-dimensional) subspaces. Thus the space  $X_{GM}$  is not only the first example of a *non-decomposable* infinite-dimensional space, but it is also *hereditarily indecomposable*. Equivalently, every closed subspace  $Y$  of  $X_{GM}$  is such that every projection in  $\mathcal{L}(Y)$  is essentially trivial: either its rank or its corank is finite. To appreciate how exotic a hereditarily indecomposable space is, note that a space  $X$  is hereditarily indecomposable if and only if the distance between the unit spheres of any two infinite-dimensional subspaces is 0: if  $Y$  and  $Z$  are infinite-dimensional subspaces then

$$\inf\{\|y - z\| : y \in Y, z \in Z, \|y\| = \|z\| = 1\} = 0.$$

In fact, Gowers and Maurey [16] showed that if  $X$  is a complex hereditarily indecomposable space then the algebra  $\mathcal{L}(X)$  is rather small. An operator  $S \in \mathcal{L}(X)$  is said to be *strictly singular* if there is no subspace  $Y \subset X$  such that the restriction of  $S$  to  $Y$  is an isomorphism. Equivalently,  $S \in \mathcal{L}(X)$  is strictly singular if for every (infinite-dimensional) subspace  $Y \subset X$  and every  $\epsilon > 0$  there is a vector  $y \in Y$  with  $\|Sy\| < \epsilon\|y\|$ .

**THEOREM.** *Let  $X$  be a complex hereditarily indecomposable space. Then every operator  $T \in \mathcal{L}(X)$  is a linear combination of the identity and a strictly singular operator.*

Gowers [9] was the first to solve *Banach's hyperplane problem* when he constructed a space with an unconditional basis that is not isomorphic to any of its hyperplanes or even proper subspaces. The theorem above implies that every complex hereditarily indecomposable space answers Banach's hyperplane problem since it is not isomorphic to *any* of its proper subspaces. In fact, Ferenczi [7] showed that a complex Banach space  $X$  is hereditarily indecomposable if and only if for every subspace  $Y \subset X$ , every bounded linear operator from  $Y$  into  $X$  is a linear combination of the inclusion map and a strictly singular operator. Recently, Argyros and Felouzis [1] showed that every Banach space contains either  $\ell_1$  or a subspace that is a quotient of a hereditarily indecomposable space.

It was not by chance that in order to construct a space without an unconditional basis, Gowers and Maurey constructed a hereditarily indecomposable space.



As shown by the following stunning *dichotomy theorem* of Gowers [12], having an unconditional basis or being hereditarily indecomposable are the only two ‘pure states’ for a space.

**THEOREM.** *Every infinite-dimensional Banach space contains an infinite-dimensional subspace that either has an unconditional basis or is hereditarily indecomposable.*

Gowers based his proof of the dichotomy theorem on a combinatorial game played on sequences and subspaces. In order to describe this game, we need some definitions. Given a space  $X$  with a basis  $(e_n)_{n=1}^\infty$ , the *support* of a vector  $a = \sum_{n=1}^\infty a_n e_n \in X$  is  $\text{supp}(a) = \{n : a_n \neq 0\}$ . A vector  $a = \sum_{n=1}^\infty a_n e_n$  *precedes* a vector  $b = \sum_{n=1}^\infty b_n e_n$  if  $n < m$  for all  $n \in \text{supp}(a)$  and  $m \in \text{supp}(b)$ . A *block basis* is a sequence  $x_1 < x_2 < \dots$  of non-zero vectors, and a *block subspace* is the closed linear span of a block basis. For a subspace  $Y \subset X$ , write  $\sum(Y)$  for the set of all sequences  $(x_i)_1^n$  of non-zero vectors of norm at most 1 in  $Y$  with  $x_1 < \dots < x_n$ . Call a set  $\sigma \subset \sum(X)$  *large* if  $\sigma \cap \sum(Y) \neq \emptyset$  for every (infinite-dimensional) block subspace  $Y$ . For a set  $\sigma \subset \sum(X)$  and a sequence  $\Delta = (\delta_i)_{i=1}^\infty$  of positive reals, the *enlargement of  $\sigma$  by  $\Delta$*  is

$$\sigma_\Delta = \{(x_i)_1^n \in \sum(X) : \|x_i - y_i\| < \delta_i, 1 \leq i \leq n, \text{ for some } (y_i)_1^n \in \sigma\}.$$

And now for the two-player game  $(\sigma, Y)$  defined by a set  $\sigma \subset \sum(X)$  and a block subspace  $Y \subset X$ . The first player, *Hider*, chooses a block subspace  $Y_1 \subset Y$ ; the second player, *Seeker*, replies by picking a finitely supported vector  $y_1 \in Y_1$ . Then Hider chooses a block subspace  $Y_2 \subset Y$ , and Seeker picks a finitely supported vector  $y_2 \in Y_2$ . Proceeding in this way, Seeker wins the  $(\sigma, Y)$ -game if, at any stage, the sequence  $(y_i)_1^n$  is in  $\sigma$ . Hider wins if he manages to make the game go on for ever. Clearly, Seeker has a winning strategy for the  $(\sigma, Y)$  game if  $\sigma$  is big when measured by  $Y$ .

The combinatorial foundation of Gowers’ dichotomy theorem is then the following result [12].

**THEOREM.** *Let  $X$  be a Banach space with a basis and let  $\sigma \subset \sum(X)$  be large. Then for every positive sequence  $\Delta$  there is a block subspace  $Y \subset X$  such that Seeker has a winning strategy for the  $(\sigma_\Delta, Y)$ -game.*

The beautiful proof of this result bears some resemblance to arguments of Galvin and Prikrý [8] and Ellentuck [3] concerning Ramsey-type results for sequences.

Gowers’ dichotomy theorem has been the starting point of much new research on Banach spaces. For example, it can be used to tackle the still open problem of classifying minimal Banach spaces. A Banach space is *minimal* if it embeds into all of its infinite-dimensional subspaces. Casazza et al [2] used the dichotomy theorem to show that every minimal Banach space embeds into a minimal Banach space with an unconditional basis. Hence, a minimal space is either reflexive or embeds into  $c_0$  or  $\ell_1$ .

The *Schröder-Bernstein problem* asks whether two Banach spaces are necessarily isomorphic if each is a complemented subspace of the other. In [13] Gowers gave the first counterexample, and later with Maurey [16] constructed the following further examples with even stronger paradoxical properties.

**THEOREM.** *For every  $n \geq 1$  there is a Banach space  $X_n$  such that two finite-codimensional subspaces of  $X_n$  are isomorphic if and only if they have the same codimension modulo  $n$ . Also, there is a Banach space  $Z_n$  such that two product spaces  $Z_n^r$  and  $Z_n^s$  are isomorphic if and only if  $r$  and  $s$  are equal modulo  $n$ .*

For  $n \geq 2$ , the space  $Z_n$  can be used to solve the Schröder-Bernstein problem; even more, with  $X = Z_3$  and  $Y = Z_3 \oplus Z_3$  we have  $Y \oplus Y = Z_3^4 \cong Z_3 = X$ . Thus not only are  $X$  and  $Y$  complemented subspaces of each other, but  $X \cong Y \oplus Y$  and  $Y \cong X \oplus X$ . However,  $X = Z_3$  and  $Y = Z_3^2$  are not isomorphic.

The last result we shall discuss here is Gowers' solution of Banach's homogeneous spaces problem. A space is *homogeneous* if it is isomorphic to all of its subspaces. Banach asked whether there were any examples other than  $\ell_2$ . Gowers proved the striking result that homogeneity, in fact, characterizes Hilbert space [12].

**THEOREM.** *The Hilbert space  $\ell_2$  is the only homogeneous space.*

To prove this, Gowers could make use of results of Szankowski [25], and Komorowski and Tomczak-Jaegermann [19] that imply that a homogeneous space with an unconditional basis is isomorphic to  $\ell_2$ . What happens if  $X$  is homogeneous but does not have an unconditional basis? By the dichotomy theorem,  $X$  has a subspace  $Y$  that either has an unconditional basis or is hereditarily indecomposable. Since  $X \cong Y$  and  $X$  does not have an unconditional basis,  $Y$  is hereditarily indecomposable. But this is impossible, since a hereditarily indecomposable space is not isomorphic to any of its proper subspaces, let alone all of them!

## 2 ARITHMETIC PROGRESSIONS

In 1936 Erdős and Turán [6] conjectured that, for every positive integer  $k$  and  $\delta > 0$ , there is an integer  $N$  such that every subset of  $\{1, \dots, N\}$  of size at least  $\delta N$  numbers contains an arithmetic progression of length  $k$ . In 1953 Roth [24] used exponential sums to prove the conjecture in the special case  $k = 3$ : this was one of the results Davenport highlighted in 1958 when Roth was awarded a Fields Medal. In 1969 Szemerédi found an entirely combinatorial proof for the case  $k = 4$ , and six years later he proved the full Erdős-Turán conjecture. Szemerédi's theorem trivially implies van der Waerden's theorem.

In 1977 Fürstenberg [7] used techniques of ergodic theory to prove not only the full theorem of Szemerédi, but also a number of substantial extensions of it. This proof revolutionized ergodic theory.

In spite of these beautiful results, there is still much work to be done on the Erdős-Turán problem. Write  $f(k, \delta)$  for the minimal value of  $N$  that will do in

Szemerédi's theorem. The proofs of Szemerédi and Fürstenberg give extremely weak bounds for  $f(k, \delta)$ , even in the case  $k = 4$ . In order to improve these bounds, and to make it possible to attack some considerable extensions of Szemerédi's theorem, it would be desirable to use exponential sums to prove the general case.

Recently, Gowers [15] set out to do exactly this. He introduced a new notion of *pseudorandomness*, called *quadratic uniformity* and, using techniques of harmonic analysis, showed that a quadratically uniform set contains about the expected number of arithmetic progressions of length four. In order to find arithmetic progressions in a set that is not quadratically uniform, Gowers avoided the use of Szemerédi's uniformity lemma or van der Waerden's theorem, and instead made use of Weyl's inequality and, more importantly, Freiman's theorem. This theorem states that if for some finite set  $A \subset \mathbb{Z}$  the sum  $A + A = \{a + b : a, b \in A\}$  is not much larger than  $A$  then  $A$  is not far from a generalized arithmetic progression. By ingenious and involved arguments Gowers proved the following result [14].

**THEOREM.** *There is an absolute constant  $C$  such that*

$$f(4, \delta) \leq \exp \exp \exp((1/\delta)^C).$$

*In other words, if  $A \subset \{1, \dots, N\}$  has size at least  $|A| = \delta N > 0$  and  $N \geq \exp \exp \exp((1/\delta)^C)$ , then  $A$  contains an arithmetic progression of length 4.*

The bound in this theorem is incomparably better than the previous best bounds.

The entirely new approach of Gowers raises the hope that one could prove the full theorem of Szemerédi with good bounds on  $f(k, \delta)$ . In fact, there is even hope that Gowers' method could lead to a proof of the Erdős conjecture that if  $A \subset \mathbb{N}$  is such that  $\sum_{a \in A} 1/a = \infty$  then  $A$  contains arbitrarily long arithmetic progressions. The most famous special case of this conjecture is that the primes contain arbitrarily long arithmetic progressions.

### 3 COMBINATORICS

The basis of Szemerédi's original proof of his theorem on arithmetic progressions was a deep lemma that has become an extremely important tool in the study of the structure of graphs. This result, *Szemerédi's uniformity lemma*, states that the vertex set of every graph can be partitioned into boundedly many pieces  $V_1, \dots, V_k$  such that 'most' pairs  $(V_i, V_j)$  are 'uniform'. In order to state this lemma precisely, recall that, for a graph  $G = (V, E)$ , and sets  $U, W \subset V$ , the *density*  $d(U, W)$  is the proportion of the elements  $(u, w)$  of  $U \times W$  such that  $uw$  is an edge of  $G$ . For  $\epsilon, \delta > 0$  a pair  $(U, W)$  is called  $(\epsilon, \delta)$ -*uniform* if for any  $U' \subset U$  and  $W' \subset W$  with  $|U'| \geq \delta|U|$  and  $|W'| \geq \delta|W|$ , the densities  $d(U', W')$  and  $d(U, W)$  differ by at most  $\epsilon/2$ .

Szemerédi's uniformity lemma [27] claims that for all  $\epsilon, \delta, \eta > 0$  there is a  $K = K(\epsilon, \delta, \eta)$  such that the vertex set of any graph  $G$  can be partitioned into at most  $K$  sets  $U_1, \dots, U_k$  of sizes differing by at most 1, such that at least  $(1 - \eta)k^2$  of the pairs  $(U_i, U_j)$  are  $(\epsilon, \delta)$ -uniform.

Loosely speaking, a ‘Szemerédi partition’  $V(G) = \bigcup_{i=1}^k U_i$  is one such that for most pairs  $(U_i, U_j)$  there are constants  $\alpha_{ij}$  such that if  $U'_i \subset U_i$  and  $U'_j \subset U_j$  are not too small then  $G$  contains about  $\alpha_{ij}|U'_i||U'_j|$  edges from  $U'_i$  to  $U'_j$ . In some sense, Szemerédi’s uniformity lemma gives a classification of all graphs. The main drawback of the lemma is that the bound  $K(\epsilon, \delta, \eta)$  is extremely large: in the case  $\epsilon = \delta = \eta$ , all we know about  $K(\epsilon, \epsilon, \epsilon)$  is that it is at most a tower of  $2s$  of height proportional to  $\epsilon^{-5}$ . This is an enormous bound, and in many applications a smaller bound, say of the type  $e^{\epsilon^{-100}}$  would be significantly more useful. As the lemma is rather easy to prove, it was not unreasonable to expect a bound like this.

It was a great surprise when Gowers [14] proved the deep result that  $K(\epsilon, \delta, \eta)$  is of tower type in  $1/\delta$ , even if  $\epsilon$  and  $\eta$  are kept large.

**THEOREM.** *There are constants  $c_0, \delta_0 > 0$  such that for  $0 < \delta < \delta_0$  there is a graph  $G$  that does not have a  $(1/2, \delta, 1/2)$ -uniform partition into  $K$  sets, where  $K$  is a tower of  $2s$  of height at most  $c_0\delta^{-1/16}$ .*

It is well known that even exponential lower bounds are hard to come by, let alone tower type lower bounds, so this is a stunning result indeed! The proof, which makes use of clever random choices to construct graphs whose small sets of vertices do *not* behave like subsets of random graphs, goes some way towards clarifying the nature of randomness. It also indicates that any proof of an upper bound for  $K(\epsilon, \delta, \eta)$  must involve a long sequence of refinements of partitions, each exponentially larger than the previous one.

This sketch has been all too brief, and a deeper study of Gowers’ work would be needed to properly appreciate his clarity of thought and mastery of elaborate structures. However, I hope that enough has been said to give some taste of his remarkable mathematical achievements. In the theory of Banach spaces, not only has he solved many of *the* main classical problems of the century, but he has also opened up exciting new directions. In combinatorics, too, he has tackled some of the most notorious questions, bringing about their solution with the same exceptional blend of combinatorial power and technical skill. Hilbert would surely agree that Gowers has given us wider and freer horizons.

#### REFERENCES

- [1] S.A. Argyros and V. Felouzis, Interpolating H.I. Banach spaces, to appear
- [2] P.G. Casazza, N.J. Kalton, D. Kutzarova and M. Mastyło, Complex interpolation and complementably minimal spaces, in *Interaction between Functional Analysis, Harmonic Analysis, and Probability*, Lecture Notes in Pure and Applied Math., Dekker, N.Y., 1996, pp. 135–143.
- [3] E. Ellentuck, A new proof that analytic sets are Ramsey, *J. Symbolic Logic* 39 (1974), 163–165.
- [4] P. Enflo, A counterexample to the approximation property in Banach spaces, *Acta Math.* 130 (1973), 309–317.

- [5] P. Enflo, On the invariant-subspace problem in Banach spaces, *Acta Math.* 158 (1987), 213–313.
- [6] P. Erdős and P. Turán, On some sequences of integers, *J. London Math. Soc.* 11 (1936), 261–264.
- [7] V. Ferenczi, Operators on subspaces of hereditarily indecomposable Banach spaces, *Bull. London Math. Soc.* 29 (1997), 338–344.
- [8] F. Galvin and K. Prikry, Borel sets and Ramsey’s theorem, *J. Symbolic Logic* 38 (1973), 193–198.
- [9] W.T. Gowers, A solution to Banach’s hyperplane problem, *Bull. London math. Soc.* 26 (1994), 523–530.
- [10] W.T. Gowers, A Banach space not containing  $c_0$ ,  $\ell_1$  or a reflexive subspace, *Trans. Amer. Math. Soc.* 344 (1994), 407–420.
- [11] W.T. Gowers, A hereditarily indecomposable space with an asymptotic unconditional basis, *Oper. Theory: Adv. Appl.* 77, (1995), 111–120.
- [12] W.T. Gowers, A new dichotomy for Banach spaces, *Geom. Funct. Anal.* 6 (1996), 1083–1093.
- [13] W.T. Gowers, A solution to the Schroeder-Bernstein problem for Banach spaces, *Bull. London Math. Soc.* 28 (1996), 297–304.
- [14] W.T. Gowers, Lower bounds of tower type for Szemerédi’s uniformity lemma, *Geom. Funct. Anal.* 7 (1997), 322–337.
- [15] W.T. Gowers, A new proof of Szemerédi’s theorem for arithmetic progressions of length four, *Geom. Funct. Anal.* bf 8 (1998), 529–551.
- [16] W.T. Gowers and B. Maurey, The unconditional basis sequence problem, *J. Amer. Math. Soc.* 6 (1993), 851–874.
- [17] W.T. Gowers and B. Maurey, Banach spaces with small spaces of operators, *Math. Ann.* 307 (1997), 543–568.
- [18] R.C. James, Bases and reflexivity of Banach spaces, *Ann. of Math.* (2) 52 (1950), 518–527.
- [19] R. Komorowski and N. Tomczak-Jaegermann, Banach spaces without local unconditional structure, *Israel J. Math.* 89 (1995), 205–226.
- [20] J. Lindenstrauss and L. Tzafriri, Classical Banach Spaces I: Sequence Spaces, Springer-Verlag, Berlin and New York 1977.
- [21] E. Odell and T. Schlumprecht, The distortion problem, *Acta. Math.* 173 (1994), 259–281.
- [22] C.J. Read, A solution to the Invariant Subspace Problem, *Bull. London Math. Soc.* 16 (1984), 337–401.

- [23] C.J. Read, A solution to the Invariant Subspace Problem on the space  $\ell_1$ , *Bull. London Math. Soc.* 17 (1985), 305–317.
- [24] K.F. Roth, On certain sets of integers, *J. London Math. Soc.* 28 (1953) 245–252.
- [25] T. Schlumprecht, An arbitrarily distortable Banach space, *Israel J. Math.* 76 (1991), 81–95.
- [26] E. Szemerédi, On sets of integers containing no  $k$  elements in arithmetic progression, *Acta Arith.* 27 (1975), 199–245.
- [27] E. Szemerédi, Regular partitions of graphs, in “Proc. Colloque Inter. CNRS” (J.C. Bermond, J.-C. Fournier, M. Las Vergnas, D. Sotteau, eds.), 1978, pp.399-401.
- [28] B.S. Tsirelson, Not every Banach space contains  $\ell_p$  or  $c_0$ , *Functional Anal. Appl.* 8 (1974), 139–141.

Béla Bollobás  
Trinity College  
University of Cambridge  
Cambridge CB2 1SB  
England  
and  
Dept. of Math. Sciences  
University of Memphis  
Memphis TN 38152, USA

## WILLIAM TIMOTHY GOWERS

Department of Pure Mathematics & Mathematical Statistics,  
Cambridge University, Cambridge, England

Born: November 20, 1963, Marlborough, England  
Nationality: British  
Marital Status: married, three children

1982–1985 Undergraduate at Cambridge  
1985–1986 Postgraduate at Cambridge  
1986–1990 Ph.D. at Cambridge under B. Bollobás  
1989–1993 Research Fellow at Trinity College, Cambridge  
1991–1994 Lecturer in Mathematics at University College London  
1994–1995 Reader in Mathematics at University College London  
1995 Lecturer at D.P.M.M.S., University of Cambridge, and  
Teaching Fellow at Trinity College

Fields of Interest: Analysis and Combinatorics

*Béla Bollobás and William Timothy Gowers*

## THE WORK OF MAXIM KONTSEVICH

CLIFFORD HENRY TAUBES

Maxim Kontsevich is known principally for his work on four major problems in geometry. In each case, it is fair to say that Kontsevich's work and his view of the issues has been tremendously influential to subsequent developments. These four problems are:

- Kontsevich presented a proof of a conjecture of Witten to the effect that a certain, natural formal power series whose coefficients are intersection numbers of moduli spaces of complex curves satisfies the Korteweg-de Vries hierarchy of ordinary, differential equations.
- Kontsevich gave a construction for the universal Vassiliev invariant for knots in 3-space, and generalized this construction to give a definition of perturbative Chern-Simons invariants for three dimensional manifolds. In so doing, he introduced the notion of Graph Cohomology which succinctly summarizes the algebraic side of the invariants. His constructions also vastly simplified the analytic aspects of the definitions.
- Kontsevich used the notion of stable maps of complex curves with marked points to compute the number of rational, algebraic curves of a given degree in various complex projective varieties. Moreover, Kontsevich's techniques here have greatly affected this branch of algebraic geometry. Kontsevich's formulation with Manin of the related Mirror Conjecture about Calabi-Yau 3-folds has also proved to be highly influential.
- Kontsevich proved that every Poisson structure can be formally quantized by exhibiting an explicit formula for the quantization.

What follows is a brief introduction for the non-expert to these four areas of Kontsevich's work. Here, I focus almost solely on the contributions of Kontsevich to the essential exclusion of many others; and I ask to be pardoned for my many and glaring omissions.

## 1 INTERSECTION THEORY ON THE MODULI SPACE OF CURVES AND THE MATRIX AIRY FUNCTION [1]

To start the story, fix integers  $g \geq 0$  and  $n > 0$  which are constrained so  $2g + n \geq 2$ . That is, the compact surface of genus  $g$  with  $n$  punctures has negative Euler characteristic. Introduce the moduli space  $M_{g,n}$  of smooth, compact, complex curves of genus  $g$  with  $n$  distinct marked points. This is to say that a



point in  $M_{g,n}$  consists of an equivalence class of tuple consisting of a complex structure  $j$  on a compact surface  $C$  of genus  $g$ , together with an ordered set  $\Lambda \equiv \{x_1, \dots, x_n\} \subset C$  of  $n$  points. The equivalence is under the action of the diffeomorphism group of the surface. This  $M_{g,n}$  has a natural compactification (known as the Deligne-Mumford compactification) which will not be notationally distinguished. Suffice it to say that the compactification has a natural fundamental class, as well as an  $n$ -tuple of distinguished, complex line bundles. Here, the  $i$ 'th such line bundle,  $L_i$ , at the point  $(j, \Lambda) \in M_{g,n}$  is the holomorphic cotangent space at  $x_i \in \Lambda$ .

With the preceding understood, note that when  $\{d_1, \dots, d_n\}$  are non-negative integers which sum to the dimension of  $M_{g,n}$  (which is  $3g - 3 + n$ ). Then, a number is obtained by pairing the cohomology class

$$\prod_{1 \leq i \leq n} c_i(L_i)^{d_i}$$

with the afore-mentioned fundamental class of  $M_{g,n}$ . (Think of representing these Chern classes by closed 2-forms and then integrating the appropriate wedge product over the smooth part of  $M_{g,n}$ .) Using Poincaré duality, such numbers can be viewed as intersection numbers of varieties on  $M_{g,n}$  and hence the use of this term in the title of Kontsevich's article.

As  $g, n$  and the integers  $\{d_1, \dots, d_n\}$  vary, one obtains in this way a slew of intersection numbers from the set of spaces  $\{M_{g,n}\}$ . In this regard, it proved convenient to keep track of all these numbers with a generating functional. The latter is a formal power series in indeterminants  $t_0, t_1, \dots$  which is written schematically as

$$F(t_0, t_1, \dots) = \sum_{(k)} \langle \tau_0^{k_0} \tau_1^{k_1} \dots \rangle \prod_{i \geq 0} \frac{t_i^{k_i}}{k_i!}, \quad (1)$$

where,  $(k)$  signifies the multi-index  $(k_0, k_1, \dots)$  consisting of non-negative integers where only finitely many are non-zero. Here, the expression  $\langle \tau_0^{k_0} \tau_1^{k_1} \dots \rangle$  is the number which is obtained as follows: Let

$$n = k_1 + k_2 + \dots, \quad \text{and} \quad g = \frac{1}{3}(2(k_1 + 2k_2 + 3k_3 + \dots) - n) + 1.$$

If  $g$  is not a positive integer, set  $\langle \tau_0^{k_0} \tau_1^{k_1} \dots \rangle = 0$ . If  $g$  is a positive integer, construct on  $M_{g,n}$  the product of  $c_1(L_j)$  for  $1 \leq j \leq k_1$  times the product of  $c_1(L_j)^2$  for  $k_1 + 1 \leq j \leq k_1 + k_2$  times  $\dots$  etc.; and thus construct a form whose dimension is  $3g - 3 + n$ , which is that of  $M_{g,n}$ . Finally, pair this class on the fundamental class of  $M_{g,n}$  to obtain  $\langle \tau_0^{k_0} \tau_1^{k_1} \dots \rangle$ .

By comparing formal properties of two hypothetical quantum field theories, E. Witten was led to conjecture that the formal series  $U \equiv \partial^2 F / \partial t_0^2$  obeys the classical KdV equation,

$$\frac{\partial U}{\partial t_1} = U \frac{\partial U}{\partial t_0} + \frac{1}{12} \frac{\partial^3 U}{\partial t_0^3}. \quad (2)$$

(As  $U$  is a formal power series, this last formula can be viewed as a conjectural set of relations among the intersection numbers which appear in the definition of  $F$  in (1).)

Kontsevich gave the proof that  $U$  obeys this KdV equation. His proof of Equation (2) is remarkable if nothing else then for the fact that he gives what is essentially an explicit calculation of the intersection numbers  $\{\langle \tau_0^{k_0} \tau_1^{k_1} \dots \rangle\}$ . To this end, Kontsevich first introduces a model for  $M_{g,n}$  based on what he calls ribbon graphs with metrics. (A ribbon graph is obtained from a 3-valent graph by more or less thickening the edges to bands. They are related to Riemann surfaces through the classical theory of quadratic differentials.) With an explicit, almost combinatorial model for  $M_{g,n}$  in hand, Kontsevich proceeds to identify the classes  $c_1(L_j)$  directly in terms of his model. Moreover, this identification is sufficiently direct to allow for the explicit computation of the integrals for  $\{\langle \tau_0^{k_0} \tau_1^{k_1} \dots \rangle\}$ . It should be stressed here that this last step involves some extremely high powered combinatorics. Indeed, many of the steps in this proof exhibit Kontsevich's unique talent for combinatorial calculations. In any event, once the coefficients of  $U$  are obtained, the proof ends with an identification of the expression for  $U$  with a novel expansion for certain functions which arises in the KdV story. (These are the matrix Airy functions referred to at the very start of this section.)

## 2 FEYNMAN DIAGRAMS AND LOW DIMENSIONAL TOPOLOGY [2]

From formal quantum field theory arguments, E. Witten suggested that there should exist a family of knot invariants and three manifolds invariants which can be computed via multiple integrals over configuration spaces. Kontsevich gave an essentially complete mathematical definition of these invariants, and his ideas have profoundly affected subsequent developments.

In order to explain, it proves useful to first digress to introduce some basic terminology. First of all, the three dimensional manifolds here will be all taken to be smooth, compact and oriented, or else Euclidean space. A knot in a three manifold is a connected, 1-dimensional submanifold, which is to say, the embedded image of the circle. A link is a finite, disjoint collection of knots. A knot or link invariant is an assignment of some algebraic data to each knot or link (for example, a real number), where the assignments to a pair of knots (or links) agree when one member of the pair is the image of the other under a diffeomorphism of the ambient manifold. (One might also restrict to diffeomorphisms which can be connected by a path of diffeomorphisms to the identity map.)

A simple example is provided by the Gauss linking number an invariant of links with two components which can be computed as follows: Label the components as  $K_1$  and  $K_2$ . A point in  $K_1$  together with one in  $K_2$  provides the directed vector from the former to the latter, and thus a point in the 2-sphere. Since both  $K_1$  and  $K_2$  are copies of the circle, this construction provides a map from the 2-torus (the product of two circles) to the 2-sphere. The Gauss linking number is the degree of this map. (The invariance of the degree under homotopies implies that this number is an invariant of the link.) Alternately, one can introduce the standard, oriented volume form  $\omega$  on the 2-sphere, and then the Gauss linking

number is the integral over the  $K_1 \times K_2$  of the pull-back of the form  $\omega$ .

Witten conjectured the existence of a vast number of knot, link and 3-manifold invariants of a form which generalizes this last formula for the Gauss linking number. Independently of Kontsevich, significant work towards constructing these invariants for knots and links had been carried out by Bar-Natan, Birman, Garoufalidis, Lin, and Guadagnini-Martinelli-Mintchev. Meanwhile, Axelrod and Singer had developed a formulation of the three-manifold invariants.

In any event, what follows is a three step sketch of Kontsevich's formulation for an invariant of a three-manifold  $M$  with vanishing first Betti number.

*Step 1:* The invariants in question will land in a certain graded, abelian group which is constructed from graphs. Kontsevich calls these groups "graph cohomology groups." To describe the groups, introduce the set  $G_0$  of pairs consisting of a compact graph  $\Gamma$  with only three-valent vertices and a certain kind of orientation  $o$  for  $\Gamma$ . To be precise,  $o$  is an orientation for

$$\left( \bigoplus_{\text{edges}(\Gamma)} \mathbb{R} \right) \otimes H^1(\Gamma).$$

Note that isomorphisms between such graphs pull back the given  $o$ . Thus, one can think of  $G_0$  as a set of isomorphism classes. Next, think of the elements of  $G_0$  as defining a basis for a vector space over  $\mathbb{Z}$  where consistency forces the identification of  $(\Gamma, -o)$  with  $-(\Gamma, o)$ .

One can make a similar definition for graphs where all vertices are three valent save for one four valent vertex. The resulting  $\mathbb{Z}$ -module is called  $G_1$ . In fact, for each  $n \geq 0$  there is a  $\mathbb{Z}$ -module  $G_n$  which is constructed from graphs with all vertices being at least 3-valent, and with the sum over the vertices of (valence  $-3$ ) equal to  $n$ .

With the set  $\{G_n\}_{n \geq 0}$  more or less understood, remark that there are natural homomorphisms  $\partial: G_n \rightarrow G_{n+1}$  which obey  $\partial^2 = 0$ . Indeed,  $\partial$  is defined schematically as follows:

$$\partial(\Gamma, o) = \sum_{e \in \text{edges}(\Gamma)} (\Gamma/e, \text{induced orientation from } o).$$

Here,  $\Gamma/e$  is the graph which is obtained from  $\Gamma$  by contracting  $e$  to a point. The induced orientation is quite natural and left to the reader to work out. In any event, with  $\partial$  in hand, the modules  $\{G_n\}$  define a differential complex, whose cohomology groups are

$$GC_* \equiv \text{kernel}(\partial: G_* \rightarrow G_{*+1}) / \text{Image}(\partial: G_{*-1} \rightarrow G_*). \quad (3)$$

This is 'graph cohomology'. For the purpose of defining 3-manifold invariants, only  $GC_0$  is required.

*Step 2:* Fix a point  $p \in M$  and introduce in  $M \times M$  the subvariety

$$\Sigma = (p \times M) \cup (M \times p) \cup \Delta,$$

where  $\Delta$  denotes the diagonal. A simple Meyer-Vietoris argument finds closed 2-forms on  $M \times M - \Sigma$  which integrate to 1 on any linking 2-sphere of any of

the three components of  $\Sigma$ . Moreover, there is such a form  $\omega$  with  $\omega \wedge \omega = 0$  near  $\Sigma$ . In fact, near  $\Sigma$ , this  $\omega$  can be specified almost canonically with the choice of a framing for the tangent bundle of  $M$ . (The tangent bundle of an oriented 3-manifold can always be framed. Furthermore, Atiyah essentially determined a canonical frame for  $TM$ .) Away from  $\Sigma$ , the precise details of  $\omega$  are immaterial. In any event, fix  $\omega$  using the canonical framing for  $TM$ .

With  $\omega$  chosen, consider a pair  $(\Gamma, o)$  from  $G_0$ . Associate to each vertex of  $\Gamma$  a copy of  $M$ , and to each oriented edge  $e$  of  $\Gamma$ , the copy of  $M \times M$  where the first factor of  $M$  is labeled by the starting vertex of  $e$ , and the second factor by the ending vertex. Associate to this copy of  $M \times M$  the form  $\omega$ , and in this way, the edge  $e$  labels a (singular) 2-form  $\omega_e$  on  $\times_{\text{vertices}(\Gamma)} M$ .

*Step 3:* At least away from all versions of the subvariety  $\Sigma$ , the forms  $\{\omega_e\}_{e \in \text{edges}(\Gamma)}$  can be wedged together to give a top dimensional form  $\prod_{e \in \text{edges}(\Gamma)} \omega_e$ , on  $\times_{v \in \text{vertices}(\Gamma)} M$ . It is a non-trivial task to prove that this form is integrable. In any event, the assignment of this integral to the pair  $(\Gamma, o)$  gives a  $\mathbb{Z}$ -linear map from  $G_0$  to  $\mathbb{R}$ . The latter map does not define an invariant of  $M$  from the pair  $(\Gamma, o)$  as there are choices involved in the definition of  $\omega$ , and these choices effect the value of the integral. However, Kontsevich found a Stokes theorem argument which shows that this map from  $G_0$  to  $\mathbb{R}$  descends to the kernel of  $\partial$  as an invariant of  $M$ . That is, these graph-parameterized integrals define a 3-manifold invariant with values in the dual space  $(GC_0)^*$ . (A recent paper by Bott and Cattaneo has an exceptionally elegant discussion of these points.)

Kontsevich's construction of 3-manifold invariants completely separates the analytic issues from the algebraic ones. Indeed, the module  $GC_0$  encapsulates all of the algebra; while the analysis, as it were, is confined to issues which surround the integrals over products of  $M$ . In particular, much is known about  $GC_0$ ; for example, it is known to be highly non-trivial.

Kontsevich has a similar story for knots which involves integrals over configuration spaces that consist of points on the knot and points in the ambient space. Here, there is a somewhat more complicated analog of graph cohomology. In the case of knots in 3-sphere, Kontsevich's construction is now known to give all Vassiliev invariant of knots.

In closing this section, it should be said that Kontsevich has a deep understanding of these and related graph cohomology in terms of certain infinite dimensional algebras [3].

### 3 ENUMERATION OF RATIONAL CURVES VIA TORUS ACTIONS [4]

The general problem here is as follows: Suppose  $X$  is a compact, complex algebraic variety in some complex projective space. Fix a 2-dimensional homology class on  $X$  and 'count' the number of holomorphic maps from the projective line  $\mathbb{P}^1$  into  $X$  which represent the given homology class. To make this a well posed problem, maps should be identified when they have the same image in  $X$ . The use of quotes around the word count signifies that further restrictions are typically necessary in order to make the problem well posed. For example, a common additional restriction fixes some finite number of points in  $X$  and requires the

maps in question to hit the given points.

These algebro-geometric enumeration problems were considered very difficult. Indeed, for the case where  $X = \mathbb{P}^2$ , the answer was well understood prior to Kontsevich's work only for the lowest multiples of the generator of  $H_2(\mathbb{P}^2; \mathbb{Z})$ . Kontsevich synthesized an approach to this counting problem which has been quickly adopted by algebraic geometers as the method of choice. Of particular interest are the counts made by Kontsevich for the simplest case of  $X = \mathbb{P}^2$  and for the case where  $X$  is the zero locus in  $\mathbb{P}^4$  of a homogeneous, degree 5 polynomial. (The latter has trivial canonical class which is the characterization of a Calabi-Yau manifold.)

There are two parts to Kontsevich's approach to the counting problem. The first is fairly general and is roughly as follows: Let  $V$  be a compact, algebraic variety and let  $\beta$  denote a 2-dimensional homology class on  $V$ . Kontsevich introduces a certain space  $M$  of triples  $(C, x, f)$  where  $C$  is a connected, compact, reduced complex curve, while  $x = (x_1, \dots, x_k)$  is a  $k$ -tuple of pairwise distinct points on  $C$  and  $f: C \rightarrow V$  is a holomorphic map which sends the fundamental class of  $C$  to  $\beta$ . Moreover, the associated automorphism group of  $f$  is suitably constrained. (Here,  $k$  could be zero.) This space  $M$  is designed so that its compactification is a reasonable, complex algebraic space with a well defined fundamental class. (This compactification covers, in a sense, the oft used Deligne-Mumford compactification of the space of complex curves with marked points.) The utilization of this space  $M$  with its compactification is one key to Kontsevich's approach. In particular, suppose  $X \subset V$  is an algebraic subvariety. Under certain circumstances, the problem of counting holomorphic maps from  $C$  into  $X$  can be computed by translating the latter problem into that of evaluating the pairing of  $M$ 's fundamental class with certain products of Chern classes on  $M$ . The point here is that the condition that a map  $f: C \rightarrow V$  lie in  $X$  can be reinterpreted as the condition that the corresponding points in  $M$  lie in the zero locus of a certain section of a certain bundle over  $M$ .

With these last points understood, Part 2 of Kontsevich's approach exploits the observation that  $V = \mathbb{P}^n$  has a non-trivial torus action. Such an action induces one on  $M$  and its compactification. Then, in the manner of Ellingsrud and Stromme, Kontsevich uses one of Bott's fixed point formulas to obtain a formula for the appropriate Chern numbers in various interesting examples.

#### 4 DEFORMATION QUANTIZATION OF POISSON MANIFOLDS

This last subject comes from very recent work of Kontsevich, so the discussion here will necessarily be brief. A 'Poisson structure' on a manifold  $X$  can be thought of as a bilinear map

$$B_1: C^\infty(X) \otimes C^\infty(X) \rightarrow C^\infty(X)$$

which gives a Lie algebra structure to  $C^\infty(X)$ . In particular,  $B_1$  sends a pair  $(f, g)$  to  $\langle \alpha, df \wedge dg \rangle$  where  $\alpha$  is a non-degenerate section of  $\Lambda^2 TX$  which satisfies a certain quadratic differential constraint. The problem of quantizing such a Poisson structure can be phrased as follows: Let  $h$  be a formal parameter (think Planck's

constant). Find a set of bi-differential operators  $B_2, B_3, \dots$  so that

$$f * g \equiv fg + h \cdot B_1(f, g) + h^2 \cdot B_2(f, g) + \dots$$

defines an associative product taking pairs of functions on  $X$  and returning a formal power series with  $C^\infty(X)$  valued coefficients. (A bi-differential operator acts as a differential operator on each entry separately.) Kontsevich solves this problem by providing a formula for  $\{B_2, B_3, \dots\}$  in terms of  $B_1$ . The solution has the following remarkable form

$$f * g = \sum_{0 \leq n \leq \infty} h^n \sum_{\Gamma \in G[n]} \omega_\Gamma B_{\Gamma, \alpha}(f, g),$$

where

- $G[n]$  is a certain set of  $(n(n+1))^n$  labeled graphs with  $n+2$  vertices and  $n$  edges.
- $B_{\Gamma, \alpha}$  is a bi-differential operator whose coefficients are constructed from multiple order derivatives of the given  $\alpha$  by a rules which come from the graph  $\Gamma$ .
- $\omega_\Gamma$  is a number which is obtained from  $\Gamma$  by integrating a certain  $\Gamma$ -dependent differential form over the configuration space of  $n$  distinct points in the upper half plane.

The details can be found in [5].

#### REFERENCES TO PAPERS OF KONTSEVICH:

- [1] *Intersection theory on the moduli space of curves and the matrix Airy Function*. Commun. Math. Phys. 147 (1992) 1-23.
- [2] *Feynman diagrams and low-dimension topology*, in: First European Congress of Mathematics (Paris 1992), Vol. II, Progress in Mathematics 120, Birkhauser (1994) 97-121.
- [3] *Formal, (non)-commutative symplectic geometry*, in: Proceedings of the I. M. Gelfand Seminar, 1990-1992, edited by L. Corwin, I. Gelfand & J. Lepowsky, Birkhauser (1993), 173-188.
- [4] *Enumeration of rational curve via torus actions*, in: The Moduli Space of Curves, edited by R. Dijkgraaf, C. Faber & G. Van der Geer, Progress in Mathematics 129, Birkhauser (1995) 120-139.
- [5] *Deformation quantization of Poisson manifolds*, I, preprint 1997.

Clifford Henry Taubes  
Math. Dept.  
Harvard University  
Cambridge, MA 02138, USA

## MAXIM KONTSEVICH

Institut des Hautes Études Scientifiques, Bures-sur-Yvette, France

Born: August 25, 1964, Khimki, former U.S.S.R.  
Nationality: Russian  
Marital Status: married

1980–1985 Undergraduate at Moscow State University  
1985–1990 Junior Researcher at the Institute for Problems of  
Information Transmission, Moscow  
1992 Ph.D. at Bonn University  
1990–1995 Visiting positions at Harvard University  
Max-Planck-Institut für Mathematik, Bonn  
Institute for Advanced Study, Princeton  
1993–1996 Professor at University of California, Berkeley  
1995 Professor at I.H.E.S., Bures-sur-Yvette  
1995 Distinguished Visiting Professor at Rutgers University

Fields of Interest: Algebra, Geometry, Mathematical Physics

*Maxim Kontsevich and Clifford Henry Taubes*

## THE WORK OF CURTIS T. McMULLEN

STEVE SMALE

Curtis T. McMullen has been awarded the Fields Medal for his work in dynamics as well as for his contributions to the theory of computation, complex variables, geometry of three manifolds, and other areas of mathematics. I limit myself here to a brief discussion of some of his results.

The search for understanding of solutions of a polynomial equation has had a central and glorious place in the history of mathematics. Already the ancient Greek mathematicians had approximated the square root of two, i.e., the solution of  $x^2 = 2$  by what is now called Newton's Method. Providing a solution for equations such as  $x^2 + 1 = 0$  led to the introduction of complex numbers in mathematics. Group theory was introduced to understand which polynomial equations could be solved in terms of radicals. Earlier there had been such formulas for degrees 2 (the quadratic formula taught in high school), 3 and 4. For degrees greater than 4 there are no such formulae.

Instead of formulae, algorithms have been developed which produce (perhaps by complex routines) a sequence of better and better approximations to a solution of a general polynomial equation. In the most satisfactory case, iteration of a single map, Newton's Method, converges to a zero for almost all quadratic polynomials and initial points; it is a "generally convergent algorithm." But for degree 3 polynomials it converges too infrequently.

Thus I was led to raise the question as to whether there existed for each degree such a generally convergent algorithm which succeeds for all polynomial equations of that degree.

McMullen answers this question in his thesis, under Dennis Sullivan, where he shows that no such algorithm exists for polynomials of degree greater than 3, and for polynomials of degree 3 he produces a new algorithm which does converge to a solution for almost all polynomials and initial points.

Thus McMullen "finished the job" since this work answers, in degree 3, "yes," and degree greater than three, "no;" it is complete. This indicates his depth of understanding of the situation and is characteristic of his later work.

For the proof of his result McMullen establishes a rigidity theorem for full families of rational maps of  $\mathbb{C}$  into  $\mathbb{C}$  with no attracting cycles other than fixed points. Members of such families are conjugate by a linear fractional (Möbius) transformation. The attracting cycles condition is implied by the general convergence.

One obtains radicals by Newton's method applied to the polynomial

$$f(x) = x^d - a,$$



starting from any initial point. In this way solution by radicals can be seen as a special case of solution by generally convergent algorithms. This fact led Doyle and McMullen to extend Galois Theory for finding zeros of polynomials. This extension uses McMullen's thesis together with the composition of generally convergent algorithms (a "tower") and the introduction of finite Moebius groups.

They showed that the zeros of a polynomial could be found by a tower if and only if its Galois group is nearly solvable, extending the notion of solvable with the inclusion of the Moebius group  $A_5$  (the alternating group). As a consequence, for polynomials of degree bigger than 5 no tower will succeed.

For degree 5, Doyle and McMullen construct an algorithm following some ideas dating to Felix Klein's famous lectures on the quintic and the icosahedron, and using the classical theory of invariant polynomials. Thus the power of the tower of generally convergent algorithms is found. Quite beautiful!

T. Y. Li and Jim Yorke introduced the word "chaos" into dynamics in connection with the map of population biology,

$$L_r : [0, 1] \rightarrow [0, 1], \quad L_r(x) = rx(1 - x).$$

Bob May had been intrigued by this map because there was an infinite sequence of period doubling parameters  $r_i$  converging to  $s = 3.57\dots$

Soon thereafter, Mitch Feigenbaum's work (with similar results due to Couillet-Tresser) demonstrating the universality properties of this map, helped establish the acceptance by physicists of the new discipline of dynamical systems. The sequence  $(r_i - r_{i-1})/(r_{i+1} - r_i)$  has a limit, a number which is independent of the period doubling map! Key to Feigenbaum's work was the concept of renormalization and the convergence of the renormalizations of an iterate of the Feigenbaum map  $L_s$  to a fixed point  $F$  of the renormalization operator.

Let us see what renormalization means for the second iterate  $L^2$  of  $L = L_r$  for some  $2 < r < 4$ . So  $L([0, 1]) \subset [0, 1]$  as above, and  $L$  has a second fixed point  $q = (r - 1)/r$ . Define  $p$  by the conditions  $0 < p < q$  and  $L(p) = q$ . Thus  $L^2$  acts on  $[p, q]$  (with a sign reversal) something like  $L$  on  $[0, 1]$ . If  $L^2([p, q]) \subset [p, q]$  the conditions for renormalization are present. Let  $A$  be the map  $Ax = (x - q)/(p - q)$ , sending  $[p, q]$  onto  $[0, 1]$ . The renormalized  $L^2$  is given by  $RL(x) = AL^2A^{-1}(x)$ , where  $R$  is the renormalization operator acting on  $L$ .

For certain  $r$  one may be able to repeat this process. If one can do it indefinitely then  $L$  is called infinitely renormalizable. This is a very special situation but occurs for the Feigenbaum map  $L_s$  above.

Lanford found computer assisted proofs of the conjectures of Feigenbaum and subsequently Sullivan put them into a broader, detailed, conceptual framework, finding important relations between 1-dimensional dynamics and parts of classical function theory as Kleinian groups.

Yet the proof of fast (exponential) convergence of the renormalizations, a basic ingredient in this program, was missing until McMullen's beautiful work was published in the second of his two Annals of Math Studies in 1996. The fast convergence was necessary to yield the crucial rigidity of the theory (" $C^{1+\alpha}$  conjugacy").

With the notation as above, McMullen's result for the Feigenbaum map may be expressed by the estimate:

$$|R^k L_s(x) - F(x)| < c\beta^k, \quad \beta < 1.$$

Complex one dimensional dynamics is the study of the iterates of a polynomial map  $P : \mathbb{C} \rightarrow \mathbb{C}$ . This has become the most advanced and the most technical part of dynamics. Yet one simple problem may be singled out as giving some focus to this subject.

*Among polynomial maps of a given degree  $d$ , are the hyperbolic ones dense?*

A polynomial is called hyperbolic (sometimes axiom A), if the orbits of its critical points tend under time to an attracting cycle ("including infinity").

I naively gave this as a thesis problem in the 1960's. Today it is still unsolved even for  $d = 2$ , but there are a number of partial results.

Quadratic dynamics may be studied for polynomials in the normalized form

$$P_c(z) = z^2 + c$$

with parameter  $c \in \mathbb{C}$ . The unique critical point is zero and if it tends to  $\infty$  under iteration, the dynamics is well understood in terms of symbolic dynamics. The Mandelbrot set  $M$  is defined as the set of  $c \in \mathbb{C}$  for which this is not the case. This often pictured set can be thought of as a "tree with fruit," the fruit being the components of its interior. McMullen proves in the first of his *Annals of Math Studies*:

*If  $c$  is in a component of the interior of the Mandelbrot set which meets the real axis, then  $P_c$  is hyperbolic.*

As McMullen writes, "if one runs the real axis through  $M$ , then all the fruit which is skewered is good."

Earlier Yoccoz had done an important special case, and I am ignoring here much other earlier fundamental work in complex (and real) dynamics such as Fatou, Julia, Douady and Hubbard. I am also ignoring the later work of Lyubich and Graczyk-Swiatek.

Again the ideas of renormalization play a big role in the proof but now in the context of complex maps.

To describe more precisely these ideas, the idea of a quadratic-like map is useful. A quadratic polynomial map  $\mathbb{C} \rightarrow \mathbb{C}$  is a proper map of degree 2. A holomorphic proper map  $f : U \rightarrow V$  of degree 2, with the closure of  $U$  a compact subset of  $V$ , and having a critical point  $q$  in  $U$ , is called quadratic-like. Here  $U, V$  are supposed simply connected open sets of the complex numbers. For example, an iterate of a quadratic polynomial restricted to an appropriate neighborhood of its critical point is often quadratic like. If moreover, the critical point of  $f$  doesn't escape (all the iterates of  $q$  are well defined), then according to Douady-Hubbard, this map is topologically conjugate to a quadratic map of the form  $P_c(z) = z^2 + c$ , for some  $c$  in the Mandelbrot set  $M$ .

The map  $P_c(z) = z^2 + c$  with  $c \in M$  is said to be renormalizable if  $P_c^n$  is quadratic-like, the critical point  $0 \in U$  and  $0$  doesn't escape.  $P_c$  is called infinitely renormalizable if there are infinitely many values of such  $n$ . For the problem of

density of hyperbolic polynomials in degree two, the case of finitely renormalizable points had been dealt with earlier by Yoccoz. McMullen's work is on the problem of infinitely renormalizable points in  $M$ . It contains an intricate analysis of the dynamics of these maps.

Moreover in these two books McMullen establishes new results in complex function theory and the geometry of 3-manifolds.

Another important result of McMullen is his proof of Kra's "Theta conjecture." Let  $X$  be a compact Riemann surface with a finite number of points removed and its associated Riemannian curvature constant at  $-1$ , in other words a hyperbolic surface. Its universal covering,  $\Delta \rightarrow X$ , has as its group of covering transformation,  $G$ , the fundamental group of  $X$ . Let  $Q(\Delta)$  be the space of holomorphic quadratic differentials  $\phi$  with finite norm given by  $\|\phi\| = \int |\phi|$  and similarly define  $Q(X)$ . To  $\phi \in Q(\Delta)$  one may associate  $\Theta\phi \in Q(X)$  by the formula  $\Theta\phi = \sum g^*\phi$ , the sum being over the elements  $g$  of  $G$ . This is well defined since the sum is  $G$ -invariant. The sum is the Poincaré series.

It is easily shown that the norm of this operator  $\Theta$  is less than or equal to one. Kra's conjecture and McMullen's theorem asserts that in fact  $\|\Theta\|$  is strictly less than one. But McMullen proves much more. For a general class of coverings  $Y \rightarrow X$  of Riemann surfaces he characterizes those for which his conclusion is true (in terms of "amenable" covers).

Armed with this work on Kra's conjecture, he is able to make a substantial contribution to Thurston's program of introducing hyperbolic structures for a large class of 3-manifolds.

I have given a brief glimpse of what Curt McMullen has accomplished, but would like to emphasize that his work has encompassed a large realm of the kind of mathematics that lies at the cross-section of many paths of our rich culture. McMullen is not a dynamicist, not an analyst nor a geometer. He is a mathematician.

#### IMPORTANT PUBLICATIONS OF MCMULLEN

P. Doyle and C. McMullen. Solving the quintic by iteration. *Acta Math.* 163(1989), 151–180.

C. McMullen. Families of rational maps and iterative root-finding algorithms. *Annals of Math.* 125(1987), 467–493.

C. McMullen. Amenability, Poincaré series and quasiconformal maps. *Invent. math.* 97(1989), 95–127.

C. McMullen. Iteration on Teichmüller space. *Invent. math.* 99(1990), 425–454.

C. McMullen. Cusps are dense. *Annals of Math.* 133(1991), 217–247.

C. McMullen. Riemann surfaces and the geometrization of 3-manifolds. *Bull. Amer. Math. Soc.* 27(1992), 207–216.

C. McMullen. *Complex Dynamics and Renormalization*. Annals of Math Studies 135, Princeton University Press, 1994.

C. McMullen. Frontiers in complex dynamics. *Bull. Amer. Math. Soc.* 31(1994), 155–172.

C. McMullen. *Renormalization and 3-Manifolds with Fiber over the Circle*. Annals of Math Studies 142, Princeton University Press, 1996.

Steve Smale  
Department of Mathematics  
City University of Hong Kong  
Kowloon, Hong Kong

## CURTIS T. McMULLEN

Mathematics Department, Harvard University, Cambridge, MA, USA

Born: May 21, 1958, Berkeley, CA, USA

Nationality: US Citizen

1976–1980 B.A. at Williams College, Williamstown

1980–1981 Herchel Smith Fellow, Cambridge University

1981–1985 Ph.D. at Harvard University under Dennis P. Sullivan

1985–1986 Instructor at Massachusetts Institute of Technology

1987–1990 Assistant Professor at Princeton University

1990–1998 Professor at University of California, Berkeley

1998 Professor at Harvard University

Fields of Interest: Riemann Surfaces, Hyperbolic 3-Manifolds,  
Complex Dynamics

*Curtis T. McMullen*

*Steve Smale*

## THE WORK OF PETER W. SHOR

RONALD GRAHAM

Much of the work of Peter Shor has a strong geometrical flavor, typically coupled with deep ideas from probability, complexity theory or combinatorics, and always woven together with brilliance and insight of the first magnitude. Due to the space limitations of this note, I will restrict myself to brief descriptions of just four of his remarkable achievements, (unfortunately) omitting discussions of his seminal work [8] on randomized incremental algorithms (of fundamental importance in computational geometry) and his provocative results in computational biology on self-assembling virus shells.

## 1 TWO-DIMENSIONAL DISCREPANCY, MINIMAX GRID MATCHINGS AND ONLINE BIN PACKING

The minimax grid matching problem is a fundamental combinatorial problem arising in the average case analysis of algorithms. To state it, we consider a square  $S$  of area  $N$  in the plane, and a regularly spaced  $\sqrt{N} \times \sqrt{N}$  array  $G$  (=grid) of points in  $S$ . Let  $P$  be a set of  $N$  points selected independently and uniformly in  $S$ . By a perfect matching of  $P$  to  $G$  we mean a 1 - 1 map  $\lambda : P \rightarrow G$ . For each selection  $P$ , define  $L(P) = \min_{\lambda} \max_{p \in P} \mathbf{d}(p, \lambda(p))$ , where  $\lambda$  ranges over all perfect matchings of  $P$  to  $G$ , and  $\mathbf{d}$  denotes Euclidean distance.

THEOREM [Shor [24], Leighton/Shor [21]]

*With very high probability,*

$$\mathbf{E}(L(P)) = \Theta((\log N)^{3/4})$$

The proof is very intricate and ingenious, and contains a wealth in new ideas which have spawned a variety of extensions and generalizations, notably in the work of M. Talagrand [30] on majorizing measures and discrepancy.

A classical paradigm in the analysis of algorithms is the so-called bin packing problem [10], in which a list  $W = (w_1, w_2, \dots, w_n)$  of “weights” is given, and we are to required to pack all the  $w_i$  into “bins” with the constraint that no bin can contain a weight total of more than 1. Since it is NP-hard to determine the minimum number of bins which  $W$  requires for a successful packing (or even to decide if this minimum number is 2!), extensive efforts have been made for finding good approximation algorithms for producing near-optimal packings.

In the Best Fit algorithm, after the first  $i$  weights are packed, the next weight  $w_{i+1}$  is placed into the bin in which it fits best, i.e., so that the unused space

in that bin is less than it would be in any other bin. (This is actually an online algorithm). In his thesis [23], Shor proved the very surprising (and deep) result that when the  $w_i$  are chosen uniformly at random from  $[0, 1]$ , then with very high probability, the amount of wasted space has size  $\Theta(n^{1/2}(\log n)^{3/4})$ .

An “up-right” region  $R = R(f)$  of the square  $S$  is defined as the region in  $S$  lying above some continuous monotonically non-increasing function  $f$  (e.g.,  $S$  is itself up-right). If  $P$  is a set of  $N$  points chosen uniformly and independently at random in  $S$ , we can define the *discrepancy*  $\Delta(R) = ||R \cap P| - \text{area}(R)|$ . An old problem in mathematical statistics (from the 1950’s; see [5]) was the estimation of  $\sup_R \Delta(R)$  over all up-right regions of  $S$ . This was finally answered by Leighton and Shor in [24, 21], and it is now known that

$$\sup_R \Delta(R) = \Theta(N^{1/2}(\log N)^{3/4}).$$

The preceding results give just a hint of the numerous applications these fertile techniques have found to such diverse areas as pseudo-random number generation, dynamic storage allocation, wafer-scale integration and two-dimensional bin packing (see [9, 20, 17]).

## 2 DAVENPORT-SCHINZEL SEQUENCES

A Davenport-Schinzel sequence  $DS(n, s)$  is a sequence  $U = (u_1, u_2, \dots, u_m)$  composed of  $n$  distinct symbols such that  $u_i \neq u_{i+1}$  for all  $i$ , and such that  $U$  contains no alternating subsequence of length  $s + 2$ , i.e., there do not exist indices  $i_1 < i_2 < \dots < i_{s+2}$  such that  $u_{i_1} = u_{i_3} = u_{i_5} = \dots = a \neq b = u_{i_2} = u_{i_4} = \dots$ . We define

$$\lambda_s(n) = \max\{m : (u_1, \dots, u_m) \text{ is a } DS(n, s) \text{ - sequence}\}.$$

Davenport-Schinzel sequences have turned out to be of central importance in computational and combinatorial geometry, and have found many applications in such areas as motion planning, visibility, Voronoi diagrams and shortest path algorithms. It is known that  $DS(n, s)$ -sequences provide a combinatorial characterization of the lower envelope of  $n$  continuous univariate functions, each pair of which intersect in at most  $s$  points. Hence,  $\lambda_s(n)$  is just the maximum number of connected components of the graphs of such functions, and accurate estimates of  $\lambda_s(n)$  can often be translated into sharp bounds for algorithms which depend on function minimization. It is trivial to show that  $\lambda_1(n) = n$  and  $\lambda_2(n) = 2n - 1$ . The first surprise came when it was shown [15] that  $\lambda_3(n) = \Theta(n\alpha(n))$  where  $\alpha(n)$  is defined to be the functional inverse of the Ackermann function  $A(t)$ , i.e.,  $\alpha(n) := \min\{t : A(t) \geq n\}$ . Note that  $\alpha(n)$  is an extremely slowly growing function of  $n$  since  $A$  is defined as follows:

$$A_1(t) = 2t, \quad t \geq 1, \quad \text{and} \quad A_k(t) = A_{k-1}(A_k(t-1)), \quad k \geq 2, \quad t \geq 2.$$

Thus,  $A_2(t) = 2^t$ ,  $A_3(t)$  is an exponential tower of  $n$  2’s, and so on. Then  $A(t)$  is defined to be  $A_t(t)$ . The best bounds for  $\lambda_s(n)$ ,  $s > 3$  in [15] were rather

weak. This was remedied in [1] where Shor and his coauthors managed to show by extremely delicate and clever techniques that  $\lambda_4(n) = \Theta(n2^{\alpha(n)})$ . Thus,  $DS(n, 4)$ -sequences can be *much* longer than  $DS(n, 3)$ -sequences (but are still only *slightly* non-linear). In addition, they also obtained almost tight bounds on all other  $\lambda_s(n)$ ,  $s > 4$ .

### 3 TILING $\mathbb{R}^n$ WITH CUBES

In 1907, Minkowski made the conjecture (in connection with his work on extremal lattices) that in any *lattice* tiling of  $\mathbb{R}^n$  with unit  $n$ -cubes, there must be two cubes having a complete facet (=  $(n - 1)$ -face) in common. This was generalized by O. Keller [18] in 1930 to the conjecture that *any* tiling of  $\mathbb{R}^n$  by unit  $n$ -cubes must have this property. This was confirmed by Perron [22] in 1940 for  $n \leq 6$ , and shortly thereafter, Hajós [14] proved Minkowski's original conjecture for all  $n$ . However, in spite of repeated efforts, no further progress was made in proving Keller's conjecture for the next 50 years. Then in 1992, Shor struck. He showed (with his colleague J. Lagarias) that in fact Keller's conjecture is *false* for all dimensions  $n \geq 10$ . They managed to do this with an very ingenious argument showing that certain special graphs suggested by Corrádi and Szabó [11] of size  $4^n$ , must always have cliques of size  $2^n$  (contrary to the prevailing opinions then), from which it followed that Keller's conjecture must fail for  $\mathbb{R}^n$ . The reader is referred to [19] for the details of this combinatorial gem, and to [29] for a fascinating history of this problem. I might point out that this is another example of an old conjecture in geometry being shattered by a subtle combinatorial construction, an earlier one being the recent disproof of the Borsuk conjecture by Kahn and Kalai [16]. It is still not known what the truth for Keller's conjecture is when  $n = 7, 8$ , or  $9$ .

### 4 QUANTUM COMPUTATION

It has been generally believed that a digital computer (or more abstractly, a Turing machine) can simulate any physically realizable computational device. This, in fact is the thrust of the celebrated Church - Turing thesis. Moreover, it was also assumed that this could always be done in an efficient way, i.e., involving at most a polynomial expansion in the time required. However, it was first pointed out by Feynman [13] that certain quantum mechanical systems seemed to be extremely difficult (in fact, impossible) to simulate efficiently on a standard (von Neumann) computer. This led him to suggest that it might be possible to take advantage of the quantum mechanical behavior of nature itself in designing a computer which overcame these difficulties. In fact, in doing so, such a "quantum" computer might be able to solve some of the classical difficult problems much more efficiently as well. These ideas were pursued by Benioff [4], Deutsch [12], Bennett [2] and others, and slowly, a model of quantum computation began to evolve. However, the first bombshell in this embryonic field occurred when Peter Shor [25, 26] in 1994 announced the first *significant* algorithm for such a hypothetical quantum



computer, namely a method for factoring an arbitrary composite integer  $N$  in

$$c(\log N)^2 \log \log N \log \log \log N$$

steps. This should be contrasted with the best current algorithm on (classical) digital computers whose best running time estimates grow like

$$\exp(cN^{1/3}(\log N)^{2/3}).$$

Of course, no one has yet ruled out the possibility that a polynomial-time factoring algorithm exists for classical computers (cf. the infamous P vs. NP problem), but it is felt by most knowledgeable people that this is extremely unlikely. In the same paper, Shor also gives a polynomial-time algorithm for a quantum computer for computing discrete logarithms, another (apparently) intractable problem for classical computers.

There is not space here to describe these algorithms in any detail, but a few remarks may be in order. In a classical computer, information is represented by binary symbols 0 and 1 (bits). An  $n$ -bit memory can exist in any of  $2^n$  logical states. Such computers also manipulate this binary data using functions like the Boolean AND and NOT. By contrast, a quantum bit or “qubit” is typically a microscopic system such as an electron (with its spin) or a polarized photon. The Boolean states 0 and 1 are represented by (reliably) distinguishable states of the qubit, e.g.,  $|0\rangle \leftrightarrow \text{spin } \frac{1}{2}$  and  $|1\rangle \leftrightarrow \text{spin } -\frac{1}{2}$ . However, according to the laws of quantum mechanics, the qubit can also exist in a continuum of intermediate states, or “superpositions”,  $\alpha|0\rangle + \beta|1\rangle$  where  $\alpha$  and  $\beta$  are complex numbers satisfying  $|\alpha|^2 + |\beta|^2 = 1$ .

More generally, a string of  $n$  qubits can exist in any state of the form

$$\psi = \sum_{x=00\dots0}^{11\dots1} \psi_x |x\rangle$$

where the  $\psi_x$  are complex numbers such that  $\sum_x |\psi_x|^2 = 1$ . In other words, a quantum state of  $n$  qubits is represented by a unit vector in a  $2^n$ -dimensional complex Hilbert space, defined as the tensor product of the  $n$  copies of the 2-dimensional Hilbert space representing the state of a single qubit. It is the exponentially large dimensionality of this space which distinguishes quantum computers from classical computers. Whereas the state of a classical system can be completely described by separately specifying the state of each part, the overwhelming majority of states in a quantum computer are “entangled,” i.e., not representable as a direct product of the states of its individual qubits. As stated in [3], “the ability to preserve and manipulate entangled states is the distinguishing feature of quantum computers, responsible both for their power and for the difficulty in building them.”

The crux of Shor’s factoring algorithm (after reducing the problem of factoring  $N$  to that of determining for a random  $X$  coprime to  $N$ , the order of  $X$  (modulo  $N$ )), is a brilliant application of the discrete Fourier transform in such a way as to have all the incorrect candidate orders (quantum mechanically) cancel out, leaving only (multiples) of the correct order of  $X$  appearing (with high probability) when the

output is finally measured. I heartily recommend that the reader consult the paper of Shor in this Volume, or [26, 31] for more details.

Of course, complicated quantum systems are delicate creatures and any substantial interaction with the external environment can cause rapid “decoherence,” which then can result in the system collapsing to some classical state, thereby prematurely terminating the ongoing computation. This was the basis for the strong initial skepticism that any serious quantum computer could actually ever be built. However, Shor’s subsequent contributions changed this situation substantially. His paper [27] in 1995 announced the discovery of quantum error-correcting codes, cutting through some widely held misconceptions about quantum information, and showing that suitable measurements of a quantum system can acquire sufficient information for detecting and correcting errors *without* disturbing any of the encoded information. These ideas were further developed in [6, 7] to produce a new theory of quantum error-correcting codes for protection against multiple errors, using clever ideas from orthogonal geometry and properties of the recently discovered ordinary (as opposed to quantum) codes over  $GF(4)$ .

Finally, any quantum computer which is actually built will be composed of components which are not completely reliable. Thus, it will be essential to create algorithms which are “fault-tolerant” on such computers. In yet another path-breaking paper [28], Shor in 1996 showed how this indeed could be done.

Not only does Peter Shor’s work on quantum computation during the past four years represent scientific achievements of the first rank, but in my mind it holds out the first real promise that non-trivial quantum computers may actually exist in our lifetimes.

#### REFERENCES

- [1] P. K. Agarwal, M. Sharir and P. Shor, Sharp upper and lower bounds on the length of general Davenport-Schinzel sequences, *J. Comb. Theory (A)* 52 (1989), 228-274.
- [2] C. H. Bennett, Logical reversibility of computation, *IBM J. Res. Develop.* 17, (1973), 525-532.
- [3] C. H. Bennett and P. W. Shor, Quantum information theory, (*to appear*)
- [4] P. Benioff, Quantum mechanical models of Turing machines that dissipate no energy, *Phys. Rev. Letters* 48 (1982), 1581-1585.
- [5] J. Blum, On convergence of empirical distribution functions, *Ann. Math. Stat* 26 (1955), 527-529.
- [6] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, *Phys. Review A* 54 (1995), 1098-1106.
- [7] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over  $GF(4)$ , *IEEE Trans. Inf. Theory* 44 (1998), 1369-1387.

- [8] K. L. Clarkson and P. W. Shor, Applications of random sampling in computational geometry, II, *Discrete and Comput. Geom.* 4 (1989), 387-421.
- [9] E. G. Coffman, Jr. and F. T. Leighton, A provably efficient algorithm for dynamic storage allocation, *J. Comput. System Sci.* 38 (1989), 2-35.
- [10] E. G. Coffman, Jr., M. R. Garey, and D. S. Johnson, Approximation algorithms for bin-packing – an updated survey, *Algorithm design for computer system design*, CISM Courses and Lectures 284, Springer-Verlag, Vienna (1984), 49-106.
- [11] K. Corrádi and S. Szabó, A combinatorial approach for Keller’s conjecture, *Period. Math. Hungar.* 21 (1990), 91-100.
- [12] D. Deutsch, Quantum theory, the Church-Turing principle, and the universal quantum computer, *Proc. Royal Soc. London A*400 (1985), 97-117.
- [13] R. Feynman, Simulating physics with computers, *Internat. J. Theoret. Phys.* 21 (1982), 467-488.
- [14] G. Hajós, Über einfache und mehrfache Bedeckung des  $n$ -dimensionalen Raumes mit einem Würfelgitter, *Math. Z.* 47 (1942), 427-467.
- [15] S. Hart and M. Sharir, Nonlinearity of Davenport-Schinzel sequences and of generalized path compression schemes, *Combinatorica* 6 (1986), 151-177.
- [16] J. Kahn and G. Kalai, A counterexample to Borsuk’s conjecture, *Bull. Amer. Math. Soc. (New Series)* 29 (1993), 60-62.
- [17] R. M. Karp, M. Luby and A. Marchetti-Spaccamela, Probabilistic analysis of multi-dimensional bin packing problems, *Proceedings 25th ACM Symp. on Theory of Computing* (1984), 289-298.
- [18] O. H. Keller, Über einfache und mehrfache Bedeckung des  $n$ -dimensionalen Raumes mit einem Würfelgitter, *J. Reine Angew. Math.* 163 (1930), 231-248.
- [19] J. C. Lagarias and P. W. Shor, Keller’s cube-tiling conjecture is false in high dimensions, *Bull. Amer. Math. Soc. (New Series)* 27 (1992), 279-283.
- [20] F. T. Leighton and C. E. Leiserson, Wafer-scale integration of systolic arrays, *IEEE Trans. on Computers* C-34 (1985), 448-461.
- [21] T. Leighton and P. Shor, Tight bounds for minimax grid matching with applications to the average case analysis of algorithms, *Combinatorica* 9 (1989), 161-187.
- [22] O. Perron, Über lückenlose Ausfüllung des  $n$ -dimensionalen Raumes durch kongruente Würfel, I, II, *Math. Z.* 46 (1940), 1-26, 161-180.
- [23] P. W. Shor, *Random Planar Matching and Bin Packing*, Ph. D. Thesis, MIT Math. Dept., 1985.

- [24] P. W. Shor, The average-case analysis of some on-line algorithms for bin packing, *Combinatorica* 6 (1986), 179-200.
- [25] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, *Proc. 35th Symp. Foundations of Comp. Sci.*, IEEE Computer Society Press, (1994), 124-134.
- [26] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Computing* 26 (1997), 1484-1509.
- [27] P. W. Shor, Scheme for reducing decoherence in quantum computer memory, *Phys. Review A* 52 (1995), R2493-R2496.
- [28] P. W. Shor, Fault-tolerant quantum computation, *Proceedings 37th Symp. Foundations Comp. Science* IEEE Computer Society Press, Los Alamitos, CA (1996), 56-65.
- [29] S. Stein and S. Szabó, Algebra and Tiling, Carus Math. Monograph no. 25, Math. Assoc. America, Washington, 1994.
- [30] M. Talagrand, Matching theorems and empirical discrepancy computations using majorizing measures, *J. Amer. Math. Soc.* 7 (1994), 455-537.
- [31] C. Williams and S. Clearwater, *Explorations in Quantum Computing*, Springer-Verlag, Santa Clara, CA, 1998.

Ronald Graham  
AT&T Labs  
Florham Park, NJ  
and  
UCSD  
La Jolla, CA  
USA

## PETER W. SHOR

Information Sciences Center, AT&T Labs–Research, Florham Park, NJ, USA

Born: August 14, 1959, New York City, USA  
Nationality: US Citizen  
Marital Status: married, one daughter

1977–1981 Undergraduate at California Institute of Technology,  
Pasadena  
1981–1985 Ph.D. in Mathematics,  
Massachusetts Institute of Technology  
1985–1986 Postdoctoral Fellow at Mathematical Sciences  
Research Institute, Berkeley  
1986–1996 Member of Technical Staff, AT&T Bell Labs, Murray Hill  
1996 Principal Research Staff Member, AT&T Labs,  
Florham Park

Fields of Interest: Theoretical Computer Science, Combinatorics

*Ronald Graham and Peter W. Shor*

## LOCAL INDEX THEORY AND HIGHER ANALYTIC TORSION

JEAN-MICHEL BISMUT<sup>1</sup>

ABSTRACT. In this paper, we report on the construction of secondary invariants in connection with the Atiyah-Singer index theorem for families, and the theorem of Riemann-Roch-Grothendieck. The local families index theorem plays an important role in the construction.

In complex geometry, the corresponding objects are the analytic torsion forms and the analytic torsion currents. These objects exhibit natural functorial properties with respect to composition of maps. Gillet and Soulé have used these objects to prove a Riemann-Roch theorem in Arakelov geometry.

Also we state a Riemann-Roch theorem for flat vector bundles, and report on the construction of corresponding higher analytic torsion forms.

1991 Mathematics Subject Classification: 32L10,57R20,58G10

Keywords and Phrases: Sheaves and cohomology of sections of holomorphic vector bundles. Characteristic classes and numbers. Index theory and related fixed point theory.

The purpose of this paper is to report on the construction of certain secondary invariants which appear in connection with the families index theorem of Atiyah-Singer [4] and the Riemann-Roch-Grothendieck theorem [7]. These invariants are refinements of the  $\eta$  invariant of Atiyah-Patodi-Singer [2], and of the Ray-Singer analytic torsion for de Rham and Dolbeault complexes [50], [51], which are spectral invariants of the considered manifolds.

Progress in this area was made possible by the development of several related tools:

- The discovery by Quillen [48] of superconnections.
- A better understanding of local index theory (Getzler [31]) and the proof of a local families index theorem by the author [9], and of related results by Berline-Vergne [6], Berline-Getzler-Vergne [5].
- Progress on the theory of determinant bundles, by Quillen [49], Freed and the author [16], and Gillet, Soulé and the author [17].
- The development of adiabatic limit techniques to study the behaviour of certain spectral invariants (like the  $\eta$ -invariants of Atiyah-Patodi-Singer [2]) under degenerations, by Cheeger and the author [15], Mazzeo-Melrose [44], and Dai [29].

---

<sup>1</sup>Supported by the Institut Universitaire de France (I.U.F.) and by C.N.R.S., URA 1169.

Algebraic geometry gave an essential impetus to the above developments. Extending earlier work by Arakelov and Faltings, Gillet and Soulé [33],[34] developed an algebraic formalism which could use as an input results coming from analysis, and invented the adequate Riemann-Roch-Grothendieck theorem.

Our starting point is the local families index theorem [9], [5]. Let  $\pi : X \rightarrow S$  be a fibration with compact even dimensional oriented Riemannian spin fibre  $Z$ . Let  $E$  be a complex vector bundle on  $X$ . Let  $(D_s^Z)_{s \in S}$  be the associated family of Dirac operators [3] acting along the fibres  $Z$ . Let  $\text{Ind}(D_+^Z) \in K(S)$  be the corresponding index bundle. In [4], Atiyah and Singer proved the index theorem for families,

$$(0.1) \quad \text{ch}(\text{Ind}(D_+^Z)) = \pi_* \left[ \widehat{A}(TZ) \text{ch}(E) \right] \text{ in } H(S, \mathbf{Q}).$$

In [9], starting from natural geometric data, connections were introduced on the vector bundles appearing in (0.1), so that by Chern-Weil theory, we can represent the cohomology classes in (0.1) by differential forms. Using a special case of a Quillen superconnection [48], the Levi-Civita superconnection [9], a “natural” family of closed differential forms  $\alpha_t|_{t \in \mathbf{R}_+}$  on  $S$  was produced, which interpolates between the differential forms representing the right-hand side of (0.1) (for  $t \rightarrow 0$ ) and the left-hand side of (0.1) (for  $t \rightarrow +\infty$ , by [6], [5]). Moreover, following earlier work by Quillen [49], Freed and the author [16] proved a curvature theorem for smooth determinant bundles associated to a family of Dirac operators. Also extending earlier work in [16], [27], Cheeger and the author [15] constructed an odd form on  $S$ ,  $\tilde{\eta}$ , which transgresses equation (0.1) at the level of differential forms. These forms  $\tilde{\eta}$  were used to evaluate the “adiabatic” limit of  $\eta$ -invariants [16], [27], [15].

Let  $f : X \rightarrow S$  be a proper holomorphic map of complex quasiprojective manifolds, and let  $E$  be a holomorphic vector bundle on  $X$ . By Riemann-Roch-Grothendieck [7],

$$(0.2) \quad \text{Td}(TS) \text{ch}(f_*E) = f_*[\text{Td}(TX) \text{ch}(E)] \text{ in } H(S, \mathbf{Q}).$$

Assume that  $\pi : X \rightarrow S$  is a holomorphic fibration with compact fibre  $Z$ . Let  $E$  be a holomorphic vector bundle on  $X$ . Let  $(\Omega(Z, E|_Z), \bar{\partial}^Z)$  be the family of relative Dolbeault complexes along the fibres  $Z$ . Let  $\omega^X$  be a closed (1,1)-form on  $X$  restricting to a Kähler metric  $g^{TZ}$  along the fibres  $Z$ , and let  $g^E$  be a Hermitian metric on  $E$ . Recall that a holomorphic Hermitian vector bundle is naturally equipped with a unitary connection, which can be used to calculate Chern-Weil forms. Assume that  $R\pi_*E$  is locally free. Let  $g^{R\pi_*E}$  be the  $L_2$  metric on  $R\pi_*E$  one obtains via Hodge theory. In work by Gillet, Soulé and the author [17], and by Köhler and the author [20], a sum of real  $(p, p)$  forms on  $S$  was constructed, the analytic torsion forms  $T(\omega^X, g^E)$ , such that the following refinement of (0.2) holds,

$$(0.3) \quad \frac{\bar{\partial}\partial}{2i\pi} T(\omega^X, g^E) = \text{ch}(R\pi_*E, g^{R\pi_*E}) - \pi_* [\text{Td}(TZ, g^{TZ}) \text{ch}(E, g^E)].$$

The forms  $T(\omega^X, g^E)$  also refine the forms  $\tilde{\eta}$  of [15]. The component of degree 0 of  $T(\omega^X, g^E)$  is the fibrewise holomorphic Ray-Singer torsion [51] of the considered

Dolbeault complex, a spectral invariant of the Hodge Laplacians along the fibres. It was used by Quillen [49] to construct a metric on  $(\det(R\pi_*E))^{-1}$ , whose properties were studied by Quillen [49], and by Gillet, Soulé and the author [17].

At the same time, Gillet and Soulé were pursuing their effort to construct an intersection theory on arithmetic varieties, in order to formulate a Riemann-Roch-Grothendieck in Arakelov geometry. In [33], [34], they constructed refined Chow groups  $\widehat{CH}$ , and Hermitian K-theory groups  $\widehat{K}$ . They used the analytic torsion forms  $T(\omega^X, g^E)$  to define a direct image in  $\widehat{K}$ . From a computation with Zagier [35] of the analytic torsion of  $\mathbf{P}^N$  equipped with the Fubini-Study metric, they conjectured a Riemann-Roch-Grothendieck theorem in Arakelov geometry, where the additive genus associated to an exotic power series  $R(x)$  appears as a correction to the Todd genus  $\widehat{Td}$ .

In [11], a secondary characteristic class for short exact sequences of holomorphic vector bundles was constructed, which was evaluated in terms of the  $R$  class.

In [10], [18], the analogue of the above construction for submersions was carried out for immersions. Namely, let  $i : Y \rightarrow X$  be an embedding of complex manifolds, let  $F$  be a holomorphic vector bundle on  $Y$ , and let  $(E, v)$  be a resolution of  $i_*F$  by a complex of holomorphic vector bundles on  $X$ . Under natural compatibility assumptions on Hermitian metrics  $g^E, g^F, g^{N_{Y/X}}$ , analytic torsion currents  $T(E, g^E)$  were constructed on  $X$ , such that

$$(0.4) \quad \frac{\bar{\partial}\partial}{2i\pi}T(E, g^E) = \text{Td}^{-1}(N_{Y/X}, g^{N_{Y/X}})\text{ch}(F, g^F)\delta_Y - \text{ch}(E, g^E).$$

Again, (0.4) refines (0.2) at the level of currents. The functoriality of these constructions was established in work by Gillet, Soulé and the author [19].

In [21], using [11], Lebeau and the author calculated the behaviour of Quillen metrics under resolutions. Then Gillet and Soulé [36] gave a proof of their Riemann-Roch formula for the first Chern class. In [30], Faltings provided an alternative strategy to a proof of the Riemann-Roch theorem of Gillet-Soulé, by using deformation to the normal cone. In [13], the author extended his previous result with Lebeau [21]. Namely, in the case of the composition of an embedding and a submersion, a natural combination of analytic torsion forms is expressed in terms of analytic torsion currents. When combined with the arguments of Gillet and Soulé [36], this leads to a proof of the Riemann-Roch-Grothendieck theorem of Gillet and Soulé in the general case. A remaining mystery of the theory was the fact that the genus  $R$  seemed to appear twice in the theory: through the explicit spectral computations in [35] of the analytic torsion of  $\mathbf{P}_n$ , and also in the evaluation of certain characteristic classes in [11]. The mystery was solved by Bost [24] and Roessler [53]. They show in particular that the evaluation in [35] of the analytic torsion of  $\mathbf{P}_n$  can be obtained as a consequence of [11],[21].

In [22], Lott and the author extended the formalism of higher analytic torsion to de Rham theory. Assume that  $\pi : X \rightarrow S$  is a fibration of real manifolds with compact fibre  $Z$ . Let  $F$  be a complex flat vector bundle on  $X$ . Then  $R\pi_*F$  is a flat vector bundle on  $S$ . The differential characters of Cheeger-Simons [28] produce Chern classes of flat vector bundles on a manifold  $M$ , with values in  $H^{\text{odd}}(M, \mathbf{C}/\mathbf{Z})$ . In [22], a Riemann-Roch-Grothendieck formula was established



for the real part of these classes, and corresponding real higher analytic torsion forms were introduced, whose part of degree 0 is just the Ray-Singer torsion of [50]. From these torsion forms, one can produce certain even cohomology classes on  $S$ . In degree 0, the Ray-Singer conjecture, proved by Cheeger [26] and Müller [45], shows that, for unitarily flat vector bundles, the Ray-Singer torsion coincides with the Reidemeister torsion [52]. In positive degree, the evaluation of the higher analytic torsion forms of [22] is still mysterious, although some evidence suggests they might possibly be related to constructions by Igusa and Klein [39] using Borel regulators.

This paper is organized as follows. In Section 1, we state the local families index theorem. In Section 2, we introduce the higher analytic torsion forms. In Section 3, we describe the analytic torsion currents. In Section 4, we give a compatibility result between analytic torsion forms and analytic torsion currents, and we state the Riemann-Roch theorem of Gillet-Soulé. Finally, in Section 5, we state a Riemann-Roch theorem for flat vector bundles.

For a more detailed survey on the analytic aspects of this paper, we refer the reader to [14].

## 1. THE LOCAL FAMILIES INDEX THEOREM

1.1. THE LOCAL INDEX THEOREM. Let  $Z$  be a compact even dimensional oriented spin manifold. Let  $g^{TZ}$  be a Riemannian metric on  $TZ$ . Let  $S^{TZ} = S_+^{TZ} \oplus S_-^{TZ}$  be the  $\mathbf{Z}_2$ -graded hermitian vector bundle of  $(TZ, g^{TZ})$  spinors. Let  $\nabla^{TZ}$  be the Levi-Civita connection on  $(TZ, g^{TZ})$ . Let  $\nabla^{S^{TZ}} = \nabla^{S_+^{TZ}} \oplus \nabla^{S_-^{TZ}}$  be the corresponding unitary connection on  $S^{TZ} = S_+^{TZ} \oplus S_-^{TZ}$ . Let  $(E, g^E, \nabla^E)$  be a complex Hermitian vector bundle on  $Z$ , equipped with a unitary connection  $\nabla^E$ .

Let  $c(TZ)$  be the bundle of Clifford algebras of  $(TZ, g^{TZ})$ . Then  $S^{TZ} \otimes E$  is a Clifford module for the Clifford algebra  $c(TZ)$ . If  $X \in TZ$ , let  $c(X)$  denote the action of  $X \in c(TZ)$  on  $S^{TZ} \otimes E$ . Put

$$(1.1) \quad H = C^\infty(Z, S^{TZ} \otimes E), \quad H_\pm = C^\infty(Z, S_\pm^{TZ} \otimes E).$$

Let  $e_1, \dots, e_n$  be an orthonormal basis of  $TZ$ .

Let  $D^Z$  be the Dirac operator acting on  $H$ ,

$$(1.2) \quad D^Z = \sum_1^n c(e_i) \nabla_{e_i}^{S^{TZ} \otimes E}.$$

Let  $D_\pm^Z$  be the restriction of  $D^Z$  to  $H_\pm$ , so that

$$(1.3) \quad D^Z = \begin{bmatrix} 0 & D_-^Z \\ D_+^Z & 0 \end{bmatrix}.$$

The elliptic operator  $D_+^Z$  is Fredholm. Its index  $\text{Ind}(D_+^Z) \in \mathbf{Z}$  is given by

$$(1.4) \quad \text{Ind}(D_+^Z) = \dim(\ker D_+^Z) - \dim(\ker D_-^Z).$$

Let  $\widehat{A}$  be the multiplicative genus associated to the power series

$$(1.5) \quad \widehat{A}(x) = \frac{x/2}{\sinh(x/2)}.$$

The Atiyah-Singer index theorem [3] asserts that

$$(1.6) \quad \text{Ind}(D_+^Z) = \int_Z \widehat{A}(TZ) \text{ch}(E).$$

If  $F = F_+ \oplus F_-$  is a  $\mathbf{Z}_2$ -graded vector space, let  $\tau = \pm 1$  on  $F_\pm$  define the grading. If  $A \in \text{End}(F)$ , let  $\text{Tr}_s[A]$  be the supertrace of  $A$ , i.e.  $\text{Tr}_s[A] = \text{Tr}[\tau A]$ . Now we state the McKean-Singer formula [42].

PROPOSITION 1.1. *For any  $t > 0$ ,*

$$(1.7) \quad \text{Ind}(D_+^Z) = \text{Tr}_s[\exp(-tD^{Z,2})].$$

Let  $P_t(x, y)$  be the smooth kernel of  $\exp(-tD^{Z,2})$  with respect to the volume element  $dy$ , so that (1.7) can be written as

$$(1.8) \quad \text{Ind}(D_+^Z) = \int_Z \text{Tr}_s[P_t(x, x)] dx.$$

In Patodi [46], Gilkey [32], Atiyah-Bott-Patodi [1], it was proved that, as conjectured in [42], “fantastic cancellations” occur in the asymptotic expansion of  $\text{Tr}_s[P_t(x, x)]$ , so that as  $t \rightarrow 0$ ,

$$(1.9) \quad \text{Tr}_s[P_t(x, x)] \rightarrow \{\widehat{A}(TZ, \nabla^{TZ}) \text{ch}(E, \nabla^E)\}^{\max}.$$

Another proof of (1.9) by Getzler [31] has considerably improved our geometric understanding of the above cancellations. Equation (1.9) is known as a local index theorem. From (1.8), (1.9), one recovers the index formula (1.6).

1.2. QUILLEN’S SUPERCONNECTIONS. Here we follow Quillen [48]. Let  $E = E_+ \oplus E_-$  be a  $\mathbf{Z}_2$ -graded vector bundle on a manifold  $S$ .

DEFINITION 1.2. A superconnection is an odd first order differential operator  $A$  acting on  $C^\infty(S, \Lambda(T^*S) \widehat{\otimes} E)$  such that if  $\omega \in C^\infty(S, \Lambda(T^*S))$ ,  $s \in C^\infty(S, E)$ ,

$$(1.10) \quad A(\omega s) = d\omega s + (-1)^{\deg \omega} \omega A s.$$

By definition, the curvature of  $A$  is  $A^2 \in C^\infty(S, \Lambda(T^*S) \widehat{\otimes} \text{End}(E)^{\text{even}})$ . Let  $\varphi : \omega \in \Lambda(T^*S) \rightarrow \varphi \omega = (2i\pi)^{-\deg \omega / 2} \omega \in \Lambda(T^*S)$ .

DEFINITION 1.3. Let  $\text{ch}(E, A)$  be the even form on  $S$ ,

$$(1.11) \quad \text{ch}(E, A) = \varphi \text{Tr}_s[\exp(-A^2)].$$

THEOREM 1.4. *The even form  $\text{ch}(E, A)$  is closed, and its cohomology class  $[\text{ch}(E, A)]$  is given by*

$$(1.12) \quad [\text{ch}(E, A)] = \text{ch}(E_+) - \text{ch}(E_-).$$

Remark 1.5. Observe the striking algebraic similarity of the right-hand sides of (1.7) and (1.11) with the density  $\exp(-x^2)$  of the gaussian distribution on  $\mathbf{R}$ .

1.3. LOCAL FAMILIES INDEX THEOREM AND ADIABATIC LIMITS. Let  $\pi : X \rightarrow S$  be a submersion of smooth manifolds with even dimensional compact fibre  $Z$ . We assume that  $TZ$  is oriented and spin. Let  $g^{TZ}$  be a Riemannian metric on  $TZ$ . Let  $(E, g^E, \nabla^E)$  be a Hermitian vector bundle on  $X$  with unitary connection. Let  $(D_s^Z)_{s \in S}$  be the family of Dirac operators acting fibrewise along the fibres  $Z$  on  $H_s = H_{+s} \oplus H_{-s}$ . Then to the family of Fredholm operators  $(D_{+,s}^Z)_{s \in S}$ , there is an associated virtual vector bundle  $\text{Ind}(D_{+}^Z) \in K(S)$ . The families index theorem of Atiyah-Singer [4] asserts in particular that

$$(1.13) \quad \text{ch}(\text{Ind}(D_{+}^Z)) = \pi_*[\widehat{A}(TZ)\text{ch}(E)] \text{ in } H^{\text{even}}(S, \mathbf{Q}).$$

Assume temporarily that  $X$  and  $S$  are even dimensional oriented compact spin manifolds. Let  $g^{TX}, g^{TS}$  be Riemannian metrics on  $TX, TS$ . For  $\varepsilon > 0$ , put

$$(1.14) \quad g_\varepsilon^{TX} = g^{TX} + \frac{1}{\varepsilon} \pi^* g^{TS}.$$

Letting  $\varepsilon$  tend to 0 is often described as taking an adiabatic limit. Let  $D_\varepsilon^X$  be the Dirac operator associated to  $(g_\varepsilon^{TX}, \nabla^E)$ .

Let  $\nabla_\varepsilon^{TX}$  and  $\nabla^{TS}$  be the Levi-Civita connections on  $(TX, g_\varepsilon^{TX})$  and  $(TS, g^{TS})$ . Let  $T^H X$  be the orthogonal bundle to  $TZ$  in  $TX$  with respect to  $g^{TX}$ . If  $U \in TS$ , let  $U^H \in T^H X$  be the lift of  $U$  in  $T^H X$ . Let  $P^{TZ}$  be the projection  $TX = T^H X \oplus TZ \rightarrow TZ$ . Let  $\nabla^{TZ}$  be the connection on  $(TZ, g^{TZ})$ ,

$$(1.15) \quad \nabla^{TZ} = P^{TZ} \nabla_\varepsilon^{TX},$$

which does not depend on  $\varepsilon > 0$ . A trivial calculation shows that as  $\varepsilon \rightarrow 0$ ,

$$(1.16) \quad \widehat{A}(TX, \nabla_\varepsilon^{TX}) \rightarrow \pi^*[\widehat{A}(TS, \nabla^{TS})]\widehat{A}(TZ, \nabla^{TZ}).$$

Let  $P_t^\varepsilon(x, y)$  be the smooth kernel of  $\exp(-tD_\varepsilon^{X,2})$ . Then by (1.9),

$$(1.17) \quad \text{Tr}_s[P_t^\varepsilon(x, x)] \rightarrow \{\widehat{A}(TX, \nabla_\varepsilon^{TX})\text{ch}(E, \nabla)\}^{\text{max}}.$$

We change our notation slightly, and temporarily assume that  $g_\varepsilon^{TX}$  is given by  $g_\varepsilon^{TX} = \pi^* \frac{g^{TS}}{\varepsilon} \oplus g^{TZ}$ . If  $U, V \in TS$ , put

$$(1.18) \quad T(U, V) = -P^{TZ}[U^H, V^H].$$

If  $U \in TS$ , let  $\text{div}_Z(U^H)$  be the divergence of  $U^H$  with respect to the vertical volume form  $dv_Z$ . Let  $(e_1, \dots, e_n)$  and  $(f_1, \dots, f_m)$  be orthogonal bases of  $(TZ, g^{TZ})$  and  $(TS, g^{TS})$ . If  $S_\varepsilon^{TX}$  is the vector bundle of  $(TX, g_\varepsilon^{TX})$  spinors,

$$(1.19) \quad S_\varepsilon^{TX} = \pi^* S^{TS} \widehat{\otimes} S^{TZ}.$$

Put

$$(1.20) \quad D^H = \sum_1^m c(f_\alpha)(\nabla_{f_\alpha} \pi^* S^{TS} \widehat{\otimes} S^{TZ} \otimes E + \frac{1}{2} \text{div}_Z(f_\alpha^H)).$$

Then by [15],

$$(1.21) \quad D^{X,\varepsilon} = \sqrt{\varepsilon} D^H + D^Z - \frac{\varepsilon}{8} c(f_\alpha) c(f_\beta) c(T(f_\alpha, f_\beta)).$$

Put

$$(1.22) \quad H = C^\infty(Z, (S^{TZ} \otimes E)|_Z).$$

Then  $H = H_+ \oplus H_-$  is an infinite dimensional  $\mathbf{Z}_2$ -graded vector bundle on  $S$ , and  $C^\infty(M, \pi^* S^{TS} \otimes E) = C^\infty(S, S^{TS} \widehat{\otimes} H)$ .

DEFINITION 1.6. Let  $\nabla^H$  be the connection on  $H$ , such if  $U \in TS, s \in C^\infty(S, H)$ ,

$$(1.23) \quad \nabla_U^H s = \nabla_{U^H}^{S^{TZ} \otimes E} s + \frac{1}{2} \operatorname{div}_Z(U^H) s$$

Then  $D^H$  is the Dirac operator action on  $C^\infty(S, S^{TS} \widehat{\otimes} H)$  associated to  $(g^{TS}, \nabla^H)$ . Following [9], we formally replace  $c(f_\alpha)$  by  $f^\alpha \wedge \cdot$  in (1.21).

DEFINITION 1.7. For  $t > 0$ , put

$$(1.24) \quad A_t = \nabla^H + \sqrt{t} D^Z - \frac{1}{8\sqrt{t}} f^\alpha f^\beta c(T(f_\alpha, f_\beta)).$$

Then  $A_t$  is a superconnection on  $H$ , the Levi-Civita superconnection associated to  $(T^H X, g^{TZ}, \nabla^E)$ .

For  $t > 0$ , let  $\alpha_t$  be the even form on  $S$

$$(1.25) \quad \alpha_t = \varphi \operatorname{Tr}_s[\exp(-A_t^2)].$$

Now we state the local families index theorem [9], [6], [5].

THEOREM 1.8. *The form  $\alpha_t$  is real, even and closed. Moreover*

$$(1.26) \quad [\alpha_t] = \operatorname{ch}(\operatorname{Ind} D_+^Z) \in H^{\operatorname{even}}(B, \mathbf{Q}).$$

As  $t \rightarrow 0$ ,

$$(1.27) \quad \alpha_t = \pi_*[\widehat{A}(TZ, \nabla^{TZ}) \operatorname{ch}(E, \nabla^E)] + \mathcal{O}(t).$$

If  $\ker D^Z \subset H$  is a vector bundle, and  $\nabla^{\ker D^Z}$  is the orthogonal projection of  $\nabla^H$  on  $\ker D^Z$ , as  $t \rightarrow +\infty$ ,

$$(1.28) \quad \alpha_t = \operatorname{ch}(\ker D^Z, \nabla^{\ker D^Z}) + \mathcal{O}\left(\frac{1}{\sqrt{t}}\right).$$

Remark 1.9. Equations (1.26) and (1.27) were proved by the author in [9], and equation (1.28) by Berline-Vergne [6], Berline-Getzler-Vergne [5]. Equation (1.27) is known as the local families index theorem. It extends the local index formula given in (1.9).

## 2. COMPLEX GEOMETRY AND HIGHER ANALYTIC TORSION FORMS

2.1. THE ANALYTIC TORSION FORMS OF A HOLOMORPHIC COMPLEX. Here we follow [17]. Let  $S$  be a complex manifold, and let

$$(2.1) \quad (E, v) : 0 \rightarrow E_m \xrightarrow{v} E_{m-1} \dots \xrightarrow{v} E_0 \rightarrow 0$$

be a holomorphic complex of vector bundles on  $S$ . Put

$$(2.2) \quad E_+ = \bigoplus_{i \text{ even}} E_i, \quad E_- = \bigoplus_{i \text{ odd}} E_i.$$

Then  $E = E_+ \oplus E_-$  is  $\mathbf{Z}_2$ -graded. Let  $g^E = \bigoplus_{i=0}^m g^{E_i}$  be a Hermitian metric on  $E = \bigoplus_{i=0}^m E_i$ . Let  $\nabla^E = \bigoplus_{i=0}^m \nabla^{E_i}$  be the corresponding holomorphic Hermitian connection. Let  $v^*$  be the adjoint of  $v$ . Set

$$(2.3) \quad V = v + v^*.$$

For  $t > 0$ , set

$$(2.4) \quad \begin{aligned} C_t'' &= \nabla^{E''} + \sqrt{t}v, & C_t' &= \nabla^{E'} + \sqrt{t}v^*, \\ C_t &= C_t'' + C_t'. \end{aligned}$$

Let  $N$  be the number operator of  $E$ , which acts on  $E_k$  by multiplication by  $k$ .

PROPOSITION 2.1. *The following identities hold*

$$(2.5) \quad \begin{aligned} C_t''^2 &= 0, & C_t'^2 &= 0, \\ \frac{\partial C_t''}{\partial t} &= \frac{1}{2t}[C_t'', N], & \frac{\partial C_t'}{\partial t} &= -\frac{1}{2t}[C_t', N]. \end{aligned}$$

DEFINITION 2.2. Let  $P^S$  be the set of smooth real forms on  $S$ , which are sums of forms of type  $(p, p)$ . Let  $P^{S,0}$  be the set of  $\alpha \in P^S$  which can be written as  $\alpha = \bar{\partial}\beta + \partial\gamma$ , with  $\beta$  and  $\gamma$  smooth.

DEFINITION 2.3. For  $t > 0$ , put

$$(2.6) \quad \alpha_t = \varphi \text{Tr}_s[\exp(-C_t^2)], \quad \gamma_t = \varphi \text{Tr}_s[N \exp(-C_t^2)].$$

The following result is obtained in [17] as an easy consequence of Proposition 2.1.

PROPOSITION 2.4. *The forms  $\alpha_t$  and  $\gamma_t$  lie in  $P^S$ . Also*

$$(2.7) \quad \frac{\partial \alpha_t}{\partial t} = \frac{\bar{\partial}\partial}{2i\pi} \gamma_t.$$

Assume now that  $H(E, v)$  is of locally constant dimension. Then  $H(E, v)$  is a holomorphic  $\mathbf{Z}$ -graded vector bundle. By finite dimensional Hodge theory,  $H(E, v) \simeq \ker V$  inherits a Hermitian metric  $g^{H(E,v)}$ . Set

$$(2.8) \quad \text{ch}'(E, g^E) = \sum_{i=0}^m (-1)^i i \text{ch}(E, g^E).$$

By [6], [5], as  $t \rightarrow +\infty$ ,

$$(2.9) \quad \begin{aligned} \alpha_t &= \text{ch}(H(E, v), g^{H(E,v)}) + \mathcal{O}\left(\frac{1}{\sqrt{t}}\right), \\ \gamma_t &= \text{ch}'(H(E, v), g^{H(E,v)}) + \mathcal{O}\left(\frac{1}{\sqrt{t}}\right). \end{aligned}$$

DEFINITION 2.5. For  $s \in \mathbf{C}$ ,  $0 < \text{Re}(s) < 1/2$ , set

$$(2.10) \quad \begin{aligned} R(E, g^E)(s) &= \frac{1}{\Gamma(s)} \int_0^{+\infty} t^{s-1} (\gamma_t - \gamma_\infty) dt, \\ T(E, g^E) &= \frac{\partial}{\partial s} R(E, g^E)(0). \end{aligned}$$

As the notation suggests, by (2.9),  $R(E, g^E)(s)$  extends to a holomorphic function of  $s$  near  $s = 0$ , so that  $T(E, g^E)$  is well defined.

PROPOSITION 2.6. *The form  $T(E, g^E)$  lies in  $P^{S,0}$ , and*

$$(2.11) \quad \frac{\bar{\partial}\partial}{2i\pi} T(E, g^E) = \text{ch}(H(E, v), g^{H(E,v)}) - \text{ch}(E, g^E).$$

2.2. BOTT-CHERN CLASSES. Let  $E$  be a holomorphic vector bundle on a complex manifold  $S$ . Let  $g^E, g'^E$  be two Hermitian metrics on  $E$ . Then by Bott and Chern [25], and by [17], there is a uniquely defined class  $\tilde{\text{ch}}(E, g^E, g'^E) \in P^S/P^{S,0}$  such that

- If  $g^E = g'^E$ ,  $\tilde{\text{ch}}(E, g^E, g'^E) = 0$ .
- The class  $\tilde{\text{ch}}(E, g^E, g'^E)$  is functorial.
- The following equation holds

$$(2.12) \quad \frac{\bar{\partial}\partial}{2i\pi} \tilde{\text{ch}}(E, g^E, g'^E) = \text{ch}(E, g'^E) - \text{ch}(E, g^E).$$

The above classes are called Bott-Chern classes. The same construction applies to classes like  $\tilde{\text{Td}}(E, g^E, g'^E)$ . The class of forms  $T(E, g^E) \in P^S/P^{S,0}$  constructed in Definition 2.5 is also a Bott-Chern class.

2.3. THE HIGHER ANALYTIC TORSION FORMS ASSOCIATED TO A HOLOMORPHIC SUBMERSION. Following work by Gillet, Soulé and the author [17], we will extend the arguments of Section 2.1 to an infinite dimensional situation.

Let  $\pi : X \rightarrow S$  be a holomorphic submersion with compact fibre  $Z$ . Let  $E$  be a holomorphic vector bundle on  $X$ , and let  $R\pi_*E$  be the direct image of  $E$ . In the sequel  $TX, TZ = TX/S \dots$  denote the corresponding holomorphic tangent bundles. Let  $\omega^X$  be a real closed  $(1, 1)$  form on  $X$  which restricts to a fibrewise Kähler form on  $TZ = TX/S$ , so that if  $J^{T\mathbb{R}Z}$  is the complex structure of  $T_{\mathbb{R}}Z$ ,  $\omega(J^{T\mathbb{R}Z}, \cdot, \cdot)$  is a Hermitian product  $g^{TZ}$  on  $TZ$ . Let  $g^E$  be a Hermitian metric on  $E$ . Let  $T^H X$  be the orthogonal bundle to  $TZ$  in  $TX$  with respect to  $\omega^X$ . Let  $(\Omega(Z, E|_Z), \bar{\partial}^Z)$  be the family of relative Dolbeault complexes along the fibres  $Z$ . Then  $\Omega(Z, E|_Z)$  can be equipped with the  $L_2$  metric

$$(2.13) \quad \langle s, s' \rangle = \int_Z \langle s, s' \rangle_{\Lambda(T^{*(0,1)}Z) \otimes E} \frac{dv_Z}{(2\pi)^{\dim Z}}.$$

Let  $\bar{\partial}^{Z*}$  be the adjoint of  $\bar{\partial}^Z$ . Put

$$(2.14) \quad D^Z = \bar{\partial}^Z + \bar{\partial}^{Z*}.$$

DEFINITION 2.7. Let  $\nabla^{\Omega(Z, E|_Z)}$  be the connection on  $\Omega(Z, E|_Z)$ , such that if  $U \in T_{\mathbb{R}}S$ , if  $s$  is a smooth section of  $\Lambda(T^{*(0,1)}Z) \otimes E$ ,

$$(2.15) \quad \nabla_U^{\Omega(Z, E|_Z)} s = \nabla_{U^H}^{\Lambda(T^{*(0,1)}Z) \otimes E} s.$$

Let  $T$  be the tensor defined in (1.18) associated to  $(g^{TZ}, T^H X)$ . Then  $T$  is of type  $(1, 1)$ . Let  $N$  be the number operator of  $\Omega(Z, E|_Z)$ . Let  $\omega^{X,H}$  be the restriction of  $\omega^X$  to  $T_{\mathbb{R}}^H X$ . Then  $\omega^{X,H}$  is a smooth section of  $\pi^* \Lambda^{(1,1)}(T_{\mathbb{R}}^* S)$ . Finally recall that  $\Lambda(T^{*(0,1)}S) \otimes E$  is a Clifford module for the Clifford algebra of  $(T_{\mathbb{R}}Z, g^{T_{\mathbb{R}}Z})$ .

DEFINITION 2.8. For  $t > 0$ , put

$$\begin{aligned}
 (2.16) \quad B_t'' &= \sqrt{t} \bar{\partial}^Z + \nabla^{\Omega(Z, E|_Z)''} - \frac{c(T^{(1,0)})}{2\sqrt{2t}}, \\
 B_t' &= \sqrt{t} \bar{\partial}^{Z*} + \nabla^{\Omega(Z, E|_Z)'} - \frac{c(T^{(0,1)})}{2\sqrt{2t}}, \\
 B_t &= B_t'' + B_t', \quad N_t = N + i \frac{\omega^{X,H}}{t}.
 \end{aligned}$$

Then one can show that, in (2.16), the superconnection  $B_t$  is a form of the Levi-Civita superconnection  $A_{t/2}$  considered in (1.24). Also, by [17], an obvious analogue of Proposition 2.1 holds, with  $C_t'', C_t'$  replaced by  $B_t'', B_t'$ , and  $N$  replaced by  $N_t$ .

DEFINITION 2.9. For  $t > 0$ , set

$$(2.17) \quad \alpha_t = \varphi \text{Tr}_s[\exp(-B_t^2)], \quad \gamma_t = \varphi \text{Tr}_s[N_t \exp(-B_t^2)].$$

THEOREM 2.10. For  $t > 0$ , the form  $\alpha_t$  and  $\gamma_t$  lie in  $P^S$ , the form  $\alpha_t$  is closed and

$$\begin{aligned}
 (2.18) \quad [\alpha_t] &= \text{ch}(R\pi_* E) \text{ in } H^{\text{even}}(S, \mathbf{Q}), \\
 \frac{\partial \alpha_t}{\partial t} &= -\frac{\bar{\partial} \bar{\partial}}{2i\pi} \frac{\gamma_t}{t}.
 \end{aligned}$$

Furthermore, as  $t \rightarrow 0$ , there are forms  $C_{-1}, C_0 \in P^S$  such that

$$\begin{aligned}
 (2.19) \quad \alpha_t &= \pi_* [\text{Td}(TZ, g^{TZ}) \text{ch}(E, g^E)] + \mathcal{O}(t), \\
 \gamma_t &= \frac{C_{-1}}{t} + C_0 + \mathcal{O}(t).
 \end{aligned}$$

Observe that the first equation in (2.19) is a consequence of the local families index theorem of [9] stated in (1.27)

Assume that  $R\pi_* E$  is locally free. Then the holomorphic vector bundle  $R\pi_* E \simeq \ker D^Z$  inherits a metric  $g^{R\pi_* E}$ . By [5], as  $t \rightarrow +\infty$ ,

$$\begin{aligned}
 (2.20) \quad \alpha_t &= \text{ch}(R\pi_* E, g^{R\pi_* E}) + \mathcal{O}\left(\frac{1}{\sqrt{t}}\right), \\
 \gamma_t &= \text{ch}'(R\pi_* E, g^{R\pi_* E}) + \mathcal{O}\left(\frac{1}{\sqrt{t}}\right).
 \end{aligned}$$

DEFINITION 2.11. For  $s \in \mathbf{C}, 0 < \text{Re}(s) < 1/2$ , put

$$\begin{aligned}
 (2.21) \quad R(\omega^X, g^E)(s) &= -\frac{1}{\Gamma(s)} \int_0^{+\infty} t^{s-1} (\gamma_t - \gamma_\infty) dt, \\
 T(\omega^X, g^E) &= \frac{\partial}{\partial s} R(\omega^X, g^E)(0).
 \end{aligned}$$

In fact, by equations (2.19), (2.20),  $R(\omega^X, g^E)(s)$  extends to a holomorphic function of  $s$  near  $s = 0$ , so that  $T(\omega^X, g^E)$  is well-defined. The forms  $T(\omega^X, g^E)$  are called higher analytic torsion forms. The following result was established in work by Gillet-Soulé and the author [17], and Köhler and the author [20].

THEOREM 2.12. *The form  $T(\omega^X, g^E)$  lies in  $P^S$ . Moreover*

$$(2.22) \quad \frac{\bar{\partial}\partial}{2i\pi} T(\omega^X, g^E) = \text{ch}(R\pi_*E, g^{R\pi_*E}) - \pi_*[\text{Td}(TZ, g^{TZ})\text{ch}(E, g^E)].$$

*Remark 2.13.* Clearly (2.22) refines (0.2) at the level of differential forms. Köhler and the author [20] showed that  $T(\omega^X, g^E) \in P^S/P^{S,0}$  depends on  $\omega^X, g^E$  via Bott-Chern classes. This result was proved before in degree 0 in [17]. A consequence of [20] is that  $T(\omega^X, g^E) \in P^S/P^{S,0}$  depends on  $\omega^X$  only via  $g^{TZ}$ . Let  $P^{\ker D^Z}$  be the orthogonal projection of  $\Omega(Z, E|_Z)$  on  $\ker D^Z$ . Set  $P^{\ker D^Z, \perp} = 1 - P^{\ker D^Z}$ . For  $s \in \mathbf{C}, \text{Re}(s) \gg 0$ , put

$$(2.23) \quad \theta(s) = -\text{Tr}_s[N(D^{Z,2})^{-s} P^{\ker D^Z, \perp}]$$

Then

$$(2.24) \quad T(\omega^X, g^E)^{(0)} = \frac{\partial\theta}{\partial s}(0).$$

Also  $\exp(-\frac{1}{2} \frac{\partial\theta}{\partial s}(0))$  is called the Ray-Singer analytic torsion [51] of the complex  $\Omega(Z, E|_Z)$ . The Ray-Singer torsion is an alternate product of generalized determinants of Laplacians.

By [17], the odd form  $\tilde{\eta} = \frac{1}{4i\pi}(\bar{\partial} - \partial)T(\omega^X, g^E)$  coincides with the form constructed by Cheeger and the author in [15].

2.4. QUILLEN METRICS. Assume temporarily that  $S$  is a point. Put

$$(2.25) \quad \lambda = (\det H(Z, E|_Z))^{-1}.$$

Then  $\lambda$  is a complex line, the inverse of the determinant of the cohomology of  $E$ . Let  $|\cdot|_\lambda$  be the metric on  $\lambda$  induced by the fibrewise  $L_2$  metric on  $g^{H(Z, E|_Z)}$ , which we obtain by identifying  $H(Z, E|_Z)$  to the corresponding harmonic forms.

DEFINITION 2.14. The Quillen metric  $\|\cdot\|_\lambda$  on  $\lambda$  is defined by

$$(2.26) \quad \|\cdot\|_\lambda = |\cdot|_\lambda \exp(-\frac{1}{2} \frac{\partial\theta}{\partial s}(0)).$$

In the general case where  $S$  is not a point, we still assume the existence of a form  $\omega^X$  taken as in Section 2.3. Let  $g^{TZ}$  be an arbitrary fibrewise Kähler metric on  $TZ$ . Let  $g^E$  be a Hermitian metric on  $E$ . We no longer assume  $R\pi_*E$  to be locally free. Put

$$(2.27) \quad \lambda(E) = (\det R\pi_*E)^{-1}.$$

Then by Knudsen-Mumford [40],  $\lambda(E)$  is a holomorphic line bundle on  $S$ , and for any  $s \in S$ , there is a canonical isomorphism.

$$(2.28) \quad \lambda(E)_s \simeq (\det(H(Z_s, E|_{Z_s})))^{-1}.$$

By Definition 2.14, the fibres  $\lambda(E)_s$  are equipped with the Quillen metric  $\|\cdot\|_{\lambda(E)_s}$ . The following result was established by Quillen [49] in the case where the fibres  $Z$  are a fixed Riemann surface, and by Gillet, Soulé and the author [17], following earlier work by Freed and the author [16] on smooth determinant bundles.



THEOREM 2.15. *The Quillen metric is smooth on  $\lambda(E)$ . Moreover*

$$(2.29) \quad c_1(\lambda(E), \|\cdot\|_{\lambda(E)}) = -\pi_*[\text{Td}(TZ, g^{TZ})\text{ch}(E, g^E)]^{(2)}.$$

*Remark 2.16.* Theorem 2.15 is a consequence of (2.22), and also of anomaly formulas [17], describing the variation of Quillen metrics when  $g^{TZ}, g^E$  themselves vary. These anomaly formulas extend the Polyakov anomaly formulas for generalized determinants on Riemann surfaces [47].

2.5. FUNCTORIALITY OF THE ANALYTIC TORSION FORMS WITH RESPECT TO COMPOSITION OF SUBMERSIONS. Let

$$(2.30) \quad \begin{array}{ccc} Z & \longrightarrow & W \\ \pi_{Z/Y} \downarrow & \pi_{W/V} \downarrow & \searrow \pi_{W/S} \\ Y & \longrightarrow & V \xrightarrow{\pi_{V/S}} S \end{array}$$

be a diagram of submersions  $\pi_{W/S}, \pi_{V/S}, \pi_{W/V}$ , with compact fibres  $Z, Y, X$ . Let  $\omega^W, \omega^V$  be closed (1,1) forms on  $W, V$  as in Section 2.3 . Let  $(E, g^E)$  be a holomorphic Hermitian vector bundle on  $W$ , such that  $R\pi_{W/S}*E, R\pi_{W/V}*E, R\pi_{W/S}*R\pi_{W/V}*E$  are locally free. Let  $T_{W/V}(\omega^W, g^E), T_{W/S}(\omega^W, g^E), T_{V/S}(\omega^V, g^{R\pi_{W/V}*E})$  be the analytic torsion forms which are associated to the maps in the above diagram. Then in work by Berthomieu and the author [8] and by Ma [41], using the adiabatic limit techniques of Cheeger and the author [15], Mazzeo-Melrose [44] and Dai [29], these forms were shown to be naturally compatible, i.e. they verify a relation which refines the functoriality of Riemann-Roch with respect to the composition of submersions. Namely, let  $\widetilde{\text{Td}}(TZ, TY, g^{TZ}, g^{TY}) \in P^W/P^{W,0}$  be the Bott-Chern class such that

$$(2.31) \quad \frac{\bar{\partial}\partial}{2i\pi} \widetilde{\text{Td}}(TZ, TY, g^{TZ}, g^{TY}) = \text{Td}(TZ, g^{TZ}) - \pi_{W/V}^* [\text{Td}(TY, g^{TY})] \text{Td}(TX, g^{TX}).$$

Under suitable assumptions, Ma [41] has constructed a Bott-Chern class  $\alpha \in P^S/P^{S,0}$  such that

$$(2.32) \quad \begin{aligned} \frac{\bar{\partial}\partial}{2i\pi} \alpha &= \text{ch}(R\pi_{V/S}*R\pi_{W/V}*E, g^{R\pi_{V/S}*R\pi_{W/V}*E}) \\ &\quad - \text{ch}(R\pi_{W/S}*E, g^{R\pi_{W/S}*E}), \end{aligned}$$

for which the following result holds.

THEOREM 2.17. *The following identity holds*

$$(2.33) \quad \begin{aligned} T_{W/S}(\omega^W, g^E) &= T_{V/S}(\omega^V, g^{R\pi_{W/V}*E}) + \pi_{W/S}^*[\text{Td}(TY, g^{TY})T_{W/V}(\omega^W, g^E)] \\ &\quad + \alpha - \pi_{W/S}^*[\widetilde{\text{Td}}(TZ, TY, g^{TZ}, g^{TY})\text{ch}(E, g^E)] \text{ in } P^S/P^{S,0}. \end{aligned}$$

*Remark 2.18.* The case where  $S$  is a point was considered in [8].

3. THE ANALYTIC TORSION CURRENTS ASSOCIATED TO AN EMBEDDING

3.1. CONSTRUCTION OF THE ANALYTIC TORSION CURRENTS. Let  $i : Y \rightarrow X$  be an embedding of complex manifolds. Let  $N_{Y/X}$  be the normal bundle to  $Y$  in  $X$ . Let  $F$  be a holomorphic vector bundle on  $Y$ . Let

$$(3.1) \quad (E, v) : 0 \rightarrow E_m \xrightarrow{v} E_{m-1} \dots \xrightarrow{v} E_0 \rightarrow 0$$

be a holomorphic complex of vector bundles on  $X$ , which, together with a holomorphic restriction map:  $r : E_{0|Y} \rightarrow F$ , provides a resolution of the sheaf  $i_*\mathcal{O}_Y(F)$ . In particular  $(E, v)$  is acyclic on  $X \setminus Y$ . By [10],  $H(E, v)|_Y$  is a holomorphic vector bundle on  $Y$ . Move precisely, if  $U \in TX|_Y$ , let  $\partial_U v$  be the derivative of  $v$  in any holomorphic trivialization of  $(E, v)$  near  $Y$ . Then by  $\partial_U v$  only depends on the image  $z \in N_{Y/X}$  of  $U$ , and  $(\partial_z v)^2 = 0$ . Let  $\pi : N_{Y/X} \rightarrow Y$  be the canonical projection. Then there is a canonical isomorphism

$$(3.2) \quad (\pi^* H((E, v)|_Y), \partial_z v) \simeq (\pi^*(\Lambda(N_{Y/X}) \otimes F), \sqrt{-1}i_z).$$

Let  $g^E = \oplus_{i=0}^m g^{E_i}, g^{N_{Y/X}}, g^F$  be Hermitian metrics on  $E = \oplus_{i=0}^m E_i, N_{Y/X}, F$ . As in (2.3), put  $V = v + v^*$ . Then  $H(E, v)|_Y \simeq \ker V|_Y \subset E|_Y$ . Let  $g^{H(E,v)}$  be the corresponding metric on  $H(E, v)$ .

We will say that  $g^E$  verifies assumption (A) with respect to  $g^{N_{Y/X}}, g^F$  if (3.2) is an isometry. By [10], given  $g^{N_{Y/X}}, g^F$ , there exists  $g^E = \oplus_{i=0}^m g^{E_i}$  such that assumption (A) is verified. From now on, we assume that (A) holds. For  $t > 0$ , we define  $\alpha_t, \gamma_t \in P^X$  as in (2.6). Let  $\delta_Y$  be the current of integration on  $Y$ . The following result was proved in [10], using formulas of Mathai and Quillen [43].

THEOREM 3.1. *As  $t \rightarrow +\infty$ ,*

$$(3.3) \quad \alpha_t = \text{Td}^{-1}(N_{Y/X}, g^{N_{Y/X}}) \text{ch}(F, g^F) \delta_Y + \mathcal{O}\left(\frac{1}{\sqrt{t}}\right),$$

where  $\mathcal{O}\left(\frac{1}{\sqrt{t}}\right)$  is taken in the suitable Sobolev space.

Remark 3.2. Using (1.12), we find that (3.3) refines the theorem of Riemann-Roch-Grothendieck [7] stated in (0.2) at the level of currents.

By (3.3), one can construct a current  $T(E, g^E)$  on  $X$  as in (2.10). Let  $P_Y^X$  be the set of real currents which are sum of currents of type  $(p, p)$ , whose front set is included in  $N_{Y/X, \mathbf{R}}^*$ . We define  $P_Y^{X,0}$  as in Definition 2.2. The following result was proved in [18].

THEOREM 3.3. *The current  $T(E, g^E)$  lies in  $P_Y^X$ . Moreover*

$$(3.4) \quad \frac{\bar{\partial}\partial}{2i\pi} T(E, g^E) = \text{Td}^{-1}(N_{Y/X}, g^{N_{Y/X}}) \text{ch}(F, g^F) \delta_Y - \text{ch}(E, g^E).$$

Remark 3.4. Harvey and Lawson [38] have also constructed currents related to smooth versions of Riemann-Roch-Grothendieck for embeddings.

3.2. FUNCTORIALITY OF THE ANALYTIC TORSION CURRENTS WITH RESPECT TO THE COMPOSITION OF EMBEDDINGS. Let  $i': Y' \rightarrow X, F', (E', v')$  be another set of data similar to the above data. Assume that  $Y$  and  $Y'$  intersect transversally. Put  $Y'' = Y \cap Y'$ . Then  $(E \widehat{\otimes} E', v \widehat{\otimes} 1 + 1 \widehat{\otimes} v')$  is a resolution of  $(F|_{Y''} \widehat{\otimes} F'|_{Y''})$ .

Let  $(g^E, g^{N_{Y/X}}, g^F)$  and  $(g^{E'}, g^{N_{Y'/X}}, g^{F'})$  be metrics verifying (A). Recall that  $N_{Y''/X} = N_{Y/X|Y''} \oplus N_{Y'/X|Y''}$ . Then  $(g^E \widehat{\otimes} g^{E'}, g|_{Y''}^{N_{Y/X}} \oplus g|_{Y''}^{N_{Y'/X}}, (g^{F''} \widehat{\otimes} g^{F'}))$  also verify (A). Let  $P_{Y \cup Y'}^X, P_{Y \cup Y'}^{X,0}$  be the obvious analogues of  $P_Y^X, P_Y^{X,0}$ , when replacing  $Y$  by  $Y \cup Y'$ . The following result was proved by Gillet, Soulé and the author in [19].

THEOREM 3.5. *The following identity holds*

$$(3.5) \quad \begin{aligned} T(E \widehat{\otimes} E', g^{E \widehat{\otimes} E'}) &= T(E, g^E) \text{ch}(E', g^{E'}) + \\ \text{Td}^{-1}(N_{Y/X}, g^{N_{Y/X}}) \text{ch}(F, g^F) T(E', g^{E'}) &\delta_Y \\ \text{in } P_{Y \cup Y'}^X / P_{Y \cup Y'}^{X,0}. \end{aligned}$$

Remark 3.6. In [19], Theorem 3.5 is used to evaluate the currents  $T(E, g^E)$  in terms of the arithmetic characteristic classes of Gillet and Soulé [33], [34].

4. ANALYTIC TORSION FORMS AND ANALYTIC TORSION CURRENTS

4.1. COMPOSITION OF AN EMBEDDING AND A SUBMERSION. Let  $i : W \rightarrow V$  be an embedding of complex manifolds, and let  $S$  be a complex manifold. Let  $\pi_{W/S}, \pi_{V/S}$  be holomorphic submersions of  $W, V$  onto  $S$ , with compact fibres  $X, Y$ , so that  $\pi_{V/S} i = \pi_{W/S}$ . Then we have the diagram

$$(4.1) \quad \begin{array}{ccc} Y & \longrightarrow & W \\ \downarrow i & & \downarrow i \quad \searrow \pi_{W/S} \\ X & \longrightarrow & V \xrightarrow{\pi_{V/S}} S \end{array}$$

Let  $F$  be a holomorphic vector bundle on  $W$ . Let  $(E, v)$  be a complex of holomorphic vector bundles on  $V$  as in (3.1), which together with a restriction map  $r : E_{0|V} \rightarrow F$ , provides a resolution of  $i_* F$ . In the sequel we assume that  $R\pi_{W/S*} F$  is locally free. Let  $R\pi_{V/S*} E$  be the direct image of  $E$ . Tautologically,  $R\pi_{V/S*} E \simeq R\pi_{W/S*} F$ . Let  $\omega^V, \omega^W$  be (1,1) closed forms on  $V, W$  which restrict to Kähler forms on the fibres  $X, Y$ . Note that  $N_{W/V} \simeq N_{Y/X}$ . Let  $g^{N_{Y/X}}, g^F$  be Hermitian metrics on  $N_{Y/X}, F$ . Let  $g^E = \bigoplus_{i=0}^m g^{E_i}$  be a Hermitian metric on  $E = \bigoplus_{i=0}^m E_i$ , which verifies (A) with respect to  $g^{N_{Y/X}}, g^F$ .

4.2. FUNCTORIALITY OF THE ANALYTIC TORSION OBJECTS WITH RESPECT TO THE COMPOSITION OF AN EMBEDDING AND A SUBMERSION. Let  $\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$  be the Riemann zeta function. Now we introduce the power series  $R$  of Gillet-Soulé [35].

DEFINITION 4.1. Let  $R$  be the formal power series

$$(4.2) \quad R(x) = \sum_{\substack{n \geq 1 \\ n \text{ odd}}} \left( 2 \frac{\zeta'(-n)}{\zeta(-n)} + \sum_{j=1}^n \frac{1}{j} \right) \zeta(-n) \frac{x^n}{n!}.$$

We identify  $R(x)$  with the corresponding additive genus. The power series  $R$  was obtained by Gillet-Soulé and Zagier by an explicit computation of the analytic torsion of  $\mathbf{P}_n$ , as a correction to the Todd genus  $\widehat{\text{Td}}$  of Gillet-Soulé’s theory, which would fit into a conjectural form of Riemann-Roch-Grothendieck in Arakelov geometry.

Let  $\widehat{\text{Td}}(TX|_Y, g^{TY}, g^{TX}_Y, g^{N_{Y/X}}) \in P^W/P^{W,0}$  be the Bott-Chern class such that

$$(4.3) \quad \frac{\bar{\partial}\partial}{2i\pi} \widetilde{\text{Td}}(TX|_Y, g^{TY}, g^{TX|_Y}, g^{N_{Y/X}}) = \text{Td}(TX|_Y, g^{TX|_Y}) - \text{Td}(TY, g^{TY})\text{Td}(N_{Y/X}, g^{N_{Y/X}}).$$

Let  $T(\omega^V, g^E) \in P^S$  be the analytic torsion forms associated to the family of double complexes  $(\Omega(X, E|_X), (\bar{\partial}^X + v))$ . Observe that  $R\pi_{V/S*}E \simeq R\pi_{W/S*}F$  is now equipped with two  $L_2$  metrics  $g^{R\pi_{V/S*}E}$  and  $g^{R\pi_{W/S*}F}$ . The following result was proved by Lebeau and the author [21] in the case where  $S$  is a point, and extended by the author in [13] to the general case.

THEOREM 4.2. *The following identity holds*

$$(4.4) \quad \begin{aligned} & \widetilde{\text{ch}}(R\pi_{W/S*}F, g^{R\pi_{W/S*}F}, g^{R\pi_{V/S*}F}) - T(\omega^W, g^F) + T(\omega^V, g^E) \\ & - \pi_{V/S*}[\text{Td}(TX, g^{TX})T(E, g^E)] + \pi_{W/S*} \left[ \frac{\widetilde{\text{Td}}(TX|_W, g^{TY}, g^{TX|_W}, g^{N_{Y/X}})}{\text{Td}(N_{Y/X}, g^{N_{Y/X}})} \text{ch}(F, g^F) \right] \\ & - \pi_{V/S*}[\text{Td}(TX)R(TX)\text{ch}(E)] + \pi_{W/S*}[\text{Td}(TY)R(TY)\text{ch}(F)] = 0 \text{ in } P^S/P^{S,0}. \end{aligned}$$

*Remark 4.3.* The main result of [21] is formulated as a formula of comparison of Quillen metrics on the determinant lines  $\lambda(E) \simeq \lambda(F)$ . An important idea in [21],[13] is to replace  $v$  by  $Tv$ , with  $T > 0$ , and to study the behaviour of the corresponding analytic torsion forms as  $T \rightarrow +\infty$ . Then one has to describe the behaviour of the associated harmonic forms, and also the full spectrum of the corresponding Laplacians. In [21], [13], the appearance of the additive genus  $R$  is related to the evaluation in [11] of a characteristic class, the higher analytic torsion forms associated to a short exact sequence of holomorphic vector bundles. The evaluation of this class involves computations on a harmonic oscillator. The coincidence of this class of forms with the genus evaluated by Gillet and Soulé [35] remained unexplained until Bost [24] and Roessler [53] showed that the evaluation of the analytic torsion of  $\mathbf{P}_n$  given in [35] can be obtained as a consequence of [21]. Of course, Theorems 2.17, 3.5 and 4.2 are compatible. In [12], the main result of [21] was interpreted as an excess intersection formula for Bott-Chern currents in infinite dimensions.

4.3. THE RIEMANN-ROCH THEOREM OF GILLET AND SOULÉ. Let  $X$  be an arithmetic variety, i.e. a regular flat scheme over  $\text{Spec}(\mathbf{Z})$ . In [33], [34], Gillet-Soulé constructed an arithmetic Chow group  $\widehat{CH}(X)$ . By definition,  $\widehat{CH}(X) = \widehat{Z}(X)/\widehat{R}(X)$ , where  $\widehat{Z}(X)$  is the group of arithmetic cycles  $(Z, g_Z)$ , with  $Z$  an algebraic cycle, and  $g_Z$  is a Green current on  $X_{\mathbf{C}}$ , i.e. it is a sum of real currents of type  $(p, p)$ , smooth on  $X_{\mathbf{C}} \setminus Z_{\mathbf{C}}$ , such that  $\frac{\partial \bar{\partial}}{2i\pi} g_Z + \delta_Z = \omega_Z$  is a smooth form on  $X$ , and  $\widehat{R}(X)$  is an equivalence relation which refines linear equivalence.

Let  $(E, g^E)$  be an arithmetic vector bundle on  $X$ . Namely  $E$  is an algebraic vector bundle on  $X$ ,  $g^E$  is a Hermitian metric on  $X_{\mathbf{C}}$ . Then Gillet and Soulé constructed arithmetic characteristic classes of  $(E, g^E)$  with values in  $\widehat{CH}(X)_{\mathbf{Q}}$ . More precisely they constructed a Grothendieck group  $\widehat{K}_0(X)$  which contains equivalence classes of vector bundles  $(E, g^E)$ , and also classes of forms of the type  $P^X/P^{X,0}$ , and a Chern character map  $\widehat{\text{ch}} : \widehat{K}_0(X) \rightarrow \widehat{CH}(X)_{\mathbf{Q}}$ .

Let now  $\pi : X \rightarrow S$  be a projective flat morphism of arithmetic varieties. Suppose that  $\pi : X_{\mathbf{Q}} \rightarrow Y_{\mathbf{Q}}$  is smooth. Let  $\omega^X$  be a smooth real  $(1, 1)$  form on  $X_{\mathbf{Q}}$  as in Section 2.3. Let  $(E, g^E) \in \widehat{K}_0(X)$  be such that  $R^i \pi_* E = 0$  for  $i > 0$ . In [35], Gillet and Soulé defined  $\pi_!(E, g^E) \in \widehat{K}_0(S)$  by the formula

$$(4.5) \quad \pi_!(E, g^E) = (R\pi_* E, g^{R\pi_* E}) - T(\omega^X, g^E).$$

This definition is then extended to arbitrary  $(E, g^E) \in \widehat{K}_0(X)$ . Put

$$(4.6) \quad \text{Td}^A(TX/S, g^{TX/S}) = \widehat{\text{Td}}(TX/S, g^{TX/S})(1 - R(TX/S)).$$

The following result was conjectured by Gillet and Soulé in [35] and proved in [36], [37], using Theorem 4.2.

**THEOREM 4.4.** *The following identity holds*

$$(4.7) \quad \widehat{\text{ch}}(\pi_!(E, g^E)) = \pi_*[\text{Td}^A(TX/S, g^{TX/S})\widehat{\text{ch}}(E, g^E)] \text{ in } \widehat{CH}(S)_{\mathbf{Q}}.$$

*Remark 4.5.* Assume that  $S = \text{Spec}(\mathbf{Z})$ . Then (4.7) is an equality in  $\mathbf{R}$ . It expresses the Arakelov degree of  $\det(R\pi_* E)$  in terms of arithmetic characteristic classes.

In [30], Faltings has indicated an alternative strategy to the proof of the Gillet-Soulé theorem, based on the technique of deformation to the normal cone. Then one has to study the behaviour of the analytic torsion forms, as smooth fibres are deformed to the union of two smooth fibres intersecting transversally.

## 5. HIGHER ANALYTIC TORSION AND FLAT VECTOR BUNDLES

Let  $X$  be a smooth manifold, and let  $F$  be a complex flat vector bundle on  $X$ . Then by [28], the bundle  $F$  has Chern classes  $c(F) \in H^{\text{odd}}(X, \mathbf{C}/\mathbf{Z})$ . For  $\text{Re}(c)(F) \in H(X, \mathbf{R})$ , there is a corresponding Chern-Weil theory. In fact let  $\nabla^F$  be the flat connection on  $F$ . Let  $g^F$  be a Hermitian metric on  $F$ . Put  $\theta = (g^F)^{-1} \nabla^F g^F$ . Then for  $k$  odd,  $\text{Re}(c_k)(F, g^F) = (2i\pi)^{-(k-1)/2} 2^{-k} \text{Tr}[\theta^k]$  is a closed form which represents  $\text{Re}(c_k)(F) \in H^k(X, \mathbf{R})$ .

Let  $\pi : X \rightarrow S$  be a submersion of smooth manifolds, with compact fibre  $Z$ . Then  $R\pi_* F$  is a  $\mathbf{Z}$ -graded flat vector bundle on  $S$ . Let  $e(TZ) \in H(X, \mathbf{Q})$  be the Euler class of  $TZ$ .

Now we state a result by Lott and the author [22], which was proved using flat superconnections.

THEOREM 5.1. *For any  $k \in \mathbf{N}$ ,  $k$  odd,*

$$(5.1) \quad \operatorname{Re}(c_k)(R\pi_*F) = \pi_*[e(TZ)\operatorname{Re}(c_k)(F)].$$

Given a metric  $g^F$  and a Euclidean connection  $\nabla^{TZ}$ , let  $g^{R\pi_*F}$  be the  $L_2$  Hermitian metric on  $R\pi_*F$  which is obtained via fibrewise Hodge theory. In [22], higher analytic torsion forms  $T(g^F, \nabla^{TZ})$  are constructed such that

$$(5.2) \quad dT(g^F, \nabla^{TZ}) = \pi_*[e(TZ, \nabla^{TZ})\operatorname{Re}(c_.) (F, g^F)] - \operatorname{Re}(c_.) (R\pi_*F, g^{R\pi_*F}).$$

In degree 0,  $T(g^F, \nabla^{TZ})$  is the Ray-Singer analytic torsion of [50]. The Ray-Singer conjecture, proved by Cheeger [26] and Müller [45] says that for unitarily flat vector bundles, the Ray-Singer analytic torsion coincides with a geometrically defined invariant of the manifold, the Reidemeister torsion [52]. In higher degree, the interpretation of  $T(g^F, \nabla^{TZ})$  is still mysterious. There is a possible link with work by Igusa and Klein [39] on Borel regulators. For related results in an algebraic context, we refer to Bloch and Esnault [23].

ACKNOWLEDGEMENTS *The author is indebted to J.-B. Bost, E. Getzler and C. Soulé for their comments and suggestions on a preliminary version of this paper.*

#### REFERENCES

- [1] Atiyah, M.F., Bott, R., Patodi, V.K. : On the heat equation and the index theorem. *Invent. Math.* 19, 279-330 (1973).
- [2] Atiyah, M.F., Patodi, V.K., Singer I.M. : Spectral asymmetry and Riemannian geometry, I. *Math. Proc. Cambridge Philos. Soc.* 77, 43-69 (1975).
- [3] Atiyah, M.F., Singer, I.M. : The index of elliptic operators. III, *Ann. of Math.* 87, 546-604 (1968).
- [4] Atiyah, M.F., Singer, I.M. : The index of elliptic operators. IV, *Ann. of Math.* 93, 119-138 (1971).
- [5] Berline, N., Getzler E., Vergne, M. : Heat kernels and the Dirac operator. *Grundle. der Math. Wiss. Band 298.* Berlin-Heidelberg-New-York: Springer 1992.
- [6] Berline N., Vergne M. : A proof of Bismut local index theorem for a family of Dirac operators. *Topology* 26, 435-463 (1987).
- [7] Berthelot, P., Grothendieck, A., Illusie, L. : Théorie des intersections et Théorème de Riemann-Roch. *Lecture Notes in Math.* 225. Berlin-Heidelberg-New-York: Springer 1971
- [8] Berthomieu A., Bismut, J.-M. : Quillen metrics and higher analytic torsion forms. *J. reine angew. Math.* 457, 85-184 (1994).
- [9] Bismut, J.-M. : The index Theorem for families of Dirac operators : two heat equation proofs. *Invent. Math.* 83, 91-151 (1986).
- [10] Bismut, J.-M. : Superconnection currents and complex immersions. *Invent. Math.* 99, 59-113 (1990).

- [11] Bismut, J.-M. : Koszul complexes, harmonic oscillators and the Todd class. *J.A.M.S.* 3, 159-256 (1990).
- [12] Bismut, J.-M.: On certain infinite dimensional aspects of Arakelov intersection theory. *Comm. Math. Phys.* 148, 217-248 (1992).
- [13] Bismut, J.-M. : Holomorphic families of immersions and higher analytic torsion forms. *Astérisque* 244. Paris SMF 1997.
- [14] Bismut, J.-M.: Local index theory, eta invariants and holomorphic torsion: a survey. *J. Diff. Geom.* To appear.
- [15] Bismut, J.-M., Cheeger, J. :  $\eta$ -invariants and their adiabatic limits. *J.A.M.S.* 2, 33-70 (1989).
- [16] Bismut, J.-M., Freed D. : The analysis of elliptic families. I. Metrics and connections on determinant bundles. *Comm. Math. Phys.* 106, 159-176 (1986). II. Eta invariants and the holonomy theorem. *Comm. Math. Phys.* 107, 103-163 (1986).
- [17] Bismut, J.-M., Gillet, H., Soulé, C. : Analytic torsion and holomorphic determinant bundles, I. *Comm. Math. Phys.* 115, 49-78 (1988).II. *Comm. Math. Phys.* 115, 79-126 (1988). III. *Comm. Math. Phys.* 115, 301-351 (1988).
- [18] Bismut, J.-M., Gillet, H., Soulé, C. : Bott-Chern currents and complex immersions. *Duke Math. Journal* 60, 255-284 (1990).
- [19] Bismut, J.-M., Gillet, H., Soulé, C. : Complex immersions and Arakelov geometry. *The Grothendieck Festschrift, P. Cartier et al. ed. Vol. I*, pp. 249-331. *Progress in Math.* n° 86. Boston : Birkhäuser 1990.
- [20] Bismut, J.-M., Köhler, K. : Higher analytic torsion forms for direct images and anomaly formulas, *J. Alg. Geom.* 1, 647-684 (1992).
- [21] Bismut, J.-M., Lebeau, G. : Complex immersions and Quillen metrics, *Publ. Math. IHES*, 74, 1-297 (1991).
- [22] Bismut, J.-M., Lott, J. : Flat vector bundles, direct images, and higher real analytic torsion. *J.Am. Math. Soc.* 8, 291-363 (1995).
- [23] Bloch, S., Esnault, H. : A Riemann-Roch theorem for flat bundles, with values in the algebraic Chern-Simons theory, preprint 1998.
- [24] Bost, J.-M. : Analytic torsion of projective spaces and compatibility with immersions of Quillen metrics. *I.M.R.N.* 8, 427-435 (1998).
- [25] Bott, R., Chern, S.S. : Hermitian vector bundles and the equidistribution of the zeroes of their holomorphic sections. *Acta Math.* 114, 71-112 (1965).
- [26] Cheeger J.: Analytic torsion and the heat equation. *Ann. of Math.* 109, 259-322 (1979).
- [27] Cheeger J.:  $\eta$ -invariants, the adiabatic approximation and conical singularities. *J. Diff. Geom.* 26, 175-221 (1987).
- [28] Cheeger, J., Simons, J. : Differential characters and geometric invariants. In *Geometry and Topology*, J. Alexander and J. Harer ed., *Lect. Notes in Math.* n° 1167, p. 50-80. Berlin-Heidelberg-New-York: Springer 1985.
- [29] Dai, X. : Adiabatic limits, nonmultiplicativity of signature and Leray spectral sequence, *J.A.M.S.* 4, 265-321 (1991).

- [30] Faltings G. : Lectures on the arithmetic Riemann-Roch theorem. Ann. Math. Studies 127. Princeton: Princeton University Press 1992.
- [31] Getzler, E. : A short proof of the Atiyah-Singer Index Theorem, *Topology* 25, 111-117 (1986).
- [32] Gilkey, P. : Curvature and the eigenvalues of the Laplacian for elliptic complexes. *Adv. Math.* 10, 344-382 (1973).
- [33] Gillet, H., Soulé, C. : Arithmetic Intersection Theory. *Publ. Math. IHES*, 72, 93-174 (1990).
- [34] Gillet, H., Soulé, C. : Characteristic classes for algebraic vector bundles with hermitian metrics. *Ann. Math. I.* 131, 163-203 (1990). II. 131, 205-238 (1990).
- [35] Gillet, H., Soulé, C. : Analytic torsion and the arithmetic Todd genus. *Topology*, 30, 21-54 (1991).
- [36] Gillet, H. Soulé, C. : An arithmetic Riemann-Roch theorem. *Inv. Math.*, 110, 473-543 (1992).
- [37] Gillet, H., Soulé C. : To appear.
- [38] Harvey, F.R., Lawson, H.B. : A theory of characteristic currents associated with a singular connection. *Astérisque* 213. Paris: S.M.F. (1993).
- [39] Igusa, K., Klein J.: The Borel regulator map on pictures II: An example from Morse theory. *J. of K-theory*, 7, 225-267 (1993)
- [40] Knudsen, F.F., Mumford, D. : The projectivity of the moduli space of stable curves, I: Preliminaries on “det” and “div”. *Math Scand.* 39, 19-55 (1976).
- [41] Ma, X. : Formes de torsion analytique et familles de submersion. *C.R.A.S.* 324 (Série I), 205-210 (1997).
- [42] McKean, H., Singer, I.M. : Curvature and the eigenforms of the Laplacian. *J. Diff. Geom.* 1, 43-69 (1967).
- [43] Mathai, V., Quillen, D. : Superconnections, Thom classes, and equivariant differential forms. *Topology* 25, 85-110 (1986).
- [44] Mazzeo, R., Melrose, R. : The adiabatic limit, Hodge cohomology and Leray’s spectral sequence of a fibration. *J. Diff. Geom.* 31, 185-213 (1990).
- [45] Müller W. : Analytic torsion and  $R$ -torsion of Riemannian manifolds. *Adv. in Math.* 28, 233-305 (1978).
- [46] Patodi, V.K. : Curvature and the eigenforms of the Laplacian. *J. Diff. Geom.* 5, 233-249 (1971).
- [47] Polyakov, A.M.: Quantum geometry of bosonic strings. *Phys. Letters B*, 103, 207-210 (1981).
- [48] Quillen, D. : Superconnections and the Chern character. *Topology* 24, 89-95 (1985).
- [49] Quillen, D. : Determinants of Cauchy-Riemann operators over a Riemannian surface. *Funct. Anal. Appl.* 19, 31-34 (1985).
- [50] Ray, D.B., Singer, I.M. :  $R$ -torsion and the Laplacian on Riemannian manifolds. *Adv. in Math.* 7, 145-210 (1971).



- [51] Ray, D.B., Singer, I.M. : Analytic torsion for complex manifolds. *Ann. of Math.* 98, 154-177 (1973).
- [52] Reidemeister K. : Homotopieringe und Linsenräume. *Hamburger Abhandl.* 11, 102-109 (1935).
- [53] Roessler D.: An Adams-Riemann-Roch theorem in Arakelov geometry. To appear in *Duke Math. Journal* (1999).

Jean-Michel Bismut  
Département de Mathématique  
Université Paris-Sud  
Bâtiment 425  
91405 Orsay Cedex  
France  
bismut@topo.math.u-psud.fr

SOME ANALOGIES BETWEEN NUMBER THEORY  
AND DYNAMICAL SYSTEMS  
ON FOLIATED SPACES

CHRISTOPHER DENINGER<sup>1</sup>

ABSTRACT. In this article we describe what a cohomology theory related to zeta and  $L$ -functions for algebraic schemes over the integers should look like. We then point out some striking analogies with the leafwise reduced cohomology of certain foliated dynamical systems.

1991 Mathematics Subject Classification: Primary 14A20; Secondary 14G10, 14F99, 58F18, 58F20.

Keywords and Phrases:  $L$ -functions of motives, leafwise cohomology, dynamical systems, foliations.

## 1 INTRODUCTION

For the arithmetic study of varieties over finite fields powerful cohomological methods are available which in particular shed much light on the nature of the corresponding zeta functions. These investigations culminated in Deligne's proof of an analogue of the Riemann conjecture for such zeta functions. This had been the hardest part of the Weil conjectures. For algebraic schemes over  $\text{Spec } \mathbb{Z}$  and in particular for the Riemann zeta function no cohomology theory has yet been developed that could serve similar purposes. For a long time it had even been a mystery how such a theory could look like even formally. In this article following [D1–D4] we first describe the shape that a cohomological formalism for algebraic schemes over the integers should take. We then discuss how it would relate to the many conjectures on arithmetic zeta- and  $L$ -functions and indicate a couple of consequences of the formalism that can be proved using standard methods. As it turns out there is a large class of dynamical systems on foliated manifolds whose reduced leafwise cohomology has many of the expected structural properties of the desired cohomology for algebraic schemes. Comparing the arithmetic and dynamical pictures leads to some insight into the basic geometric structures

---

<sup>1</sup>Supported by TMR “Arithmetic Algebraic Geometry”

that dynamical systems relevant for  $L$ -functions of varieties over number fields should have. There is also a very interesting recent approach by Connes [C] to the Riemann conjecture for Hecke  $L$ -series which bears some formal similarities to the preceding considerations. It seems to be closer in spirit to the theory of automorphic  $L$ -functions though.

I would like to thank the Newton Institute in Cambridge for its hospitality during the preparation of part of this article.

## 2 GEOMETRIC ZETA- AND $L$ -FUNCTIONS

Consider the Riemann zeta function

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1} = \sum_{n=1}^{\infty} n^{-s} \quad \text{for } \operatorname{Re} s > 1.$$

It has a holomorphic continuation to  $\mathbb{C} \setminus \{1\}$  with a simple pole at  $s = 1$ . To its finite Euler factors

$$\zeta_p(s) = (1 - p^{-s})^{-1}$$

we add an Euler factor corresponding to the archimedean place  $p = \infty$  of  $\mathbb{Q}$

$$\zeta_{\infty}(s) = 2^{-1/2} \pi^{-s/2} \Gamma(s/2)$$

and introduce the completed zeta function

$$\hat{\zeta}(s) = \zeta(s)\zeta_{\infty}(s).$$

It is holomorphic in  $\mathbb{C} \setminus \{0, 1\}$  with simple poles at  $s = 0, 1$  and satisfies the functional equation:

$$\hat{\zeta}(1-s) = \hat{\zeta}(s).$$

Its zeroes are the so called non-trivial zeroes of  $\zeta(s)$ , i.e. those in the critical strip  $0 < \operatorname{Re} s < 1$ . The famous Riemann conjecture asserts that they all lie on the line  $\operatorname{Re} s = 1/2$ .

Apart from its zeroes, the special values of  $\zeta(s)$ , i.e. the numbers  $\zeta(n)$  for integers  $n \geq 2$ , have received a great deal of attention. Recently, as a special case of the Bloch–Kato conjectures, it has been possible to express them entirely in terms of cohomological invariants of  $\mathbb{Q}$ ; c.f. [BK], [HW]. Together with the theory of  $\zeta$ -functions of curves over finite fields this suggests that the Riemann zeta function should be cohomological in nature. The rest of this article will be devoted to a thorough discussion of this hypothesis in a broader context.

A natural generalization of the Riemann zeta function to the context of arithmetic geometry is the Hasse–Weil zeta function  $\zeta_{\mathcal{X}}(s)$  of an algebraic scheme  $\mathcal{X}/\mathbb{Z}$

$$\zeta_{\mathcal{X}}(s) = \prod_{x \in |\mathcal{X}|} (1 - N(x)^{-s})^{-1}, \quad \operatorname{Re} s > \dim \mathcal{X}$$

where  $|\mathcal{X}|$  is the set of closed points of  $\mathcal{X}$  and  $N(x)$  is the number of elements in the residue field of  $x$ . For  $\mathcal{X} = \text{Spec } \mathbb{Z}$  we recover  $\zeta(s)$ , and for  $\mathcal{X} = \text{Spec } \mathfrak{o}_k$ , where  $\mathfrak{o}_k$  is the ring of integers in a number field  $k$ , the Dedekind zeta function of  $k$ . It is expected that  $\zeta_{\mathcal{X}}(s)$  has a meromorphic continuation to  $\mathbb{C}$  and, if  $\mathcal{X}$  is regular, that

$$\hat{\zeta}_{\mathcal{X}}(s) = \zeta_{\mathcal{X}}(s)\zeta_{\mathcal{X}_{\infty}}(s)$$

has a simple functional equation with respect to the substitution of  $s$  by  $\dim \mathcal{X} - s$ . Here  $\zeta_{\mathcal{X}_{\infty}}(s)$  is a certain product of  $\Gamma$ -factors depending on the Hodge structure on the cohomology of  $\mathcal{X}_{\infty} = \mathcal{X} \otimes \mathbb{R}$ . This is known if  $\mathcal{X}$  is equicharacteristic, i.e. an  $\mathbb{F}_p$ -scheme for some  $p$ , by using the Lefschetz trace formula and Poincaré duality for  $l$ -adic cohomology.

The present strategy for approaching  $\zeta_{\mathcal{X}}(s)$  was first systematically formulated by Langlands. He conjectured that every Hasse–Weil zeta function is up to finitely many Euler factors the product of automorphic  $L$ -functions. One could then apply the theory of these  $L$ -functions which is quite well developed in important cases although by no means in general. For  $\mathcal{X}$  with generic fibre related to Shimura varieties this Langlands program has been achieved in very interesting examples. Another spectacular instance was Wiles’ proof with Taylor of modularity for most elliptic curves over  $\mathbb{Q}$ .

The strategy outlined in section 3 of the present article is completely different and much closer to the cohomological methods in characteristic  $p$ .

By the work of Deligne [De], it is known that for proper regular  $\mathcal{X}/\mathbb{F}_p$  the zeroes (resp. poles) of  $\hat{\zeta}_{\mathcal{X}}(s) = \zeta_{\mathcal{X}}(s)$  have real parts equal to  $\nu/2$  for odd (resp. even) integers  $0 \leq \nu \leq 2 \dim \mathcal{X}$ , and one may expect the same for the completed Hasse–Weil zeta function  $\hat{\zeta}_{\mathcal{X}}(s)$  of an arbitrary proper and regular scheme  $\mathcal{X}/\mathbb{Z}$ .

As for the orders of vanishing at the integers, a conjecture of Soulé [So] asserts that for  $\mathcal{X}/\mathbb{Z}$  regular, quasiprojective connected and of dimension  $d$ , we have the formula

$$\text{ord}_{s=d-n} \zeta_{\mathcal{X}}(s) = \sum_{i=0}^{2n} (-1)^{i+1} \dim \text{Gr}_{\gamma}^n(K_{2n-i}(\mathcal{X}) \otimes \mathbb{Q}) . \quad (1)$$

Here the associated graded spaces are taken with respect to the  $\gamma$ -filtration on algebraic  $K$ -theory. Unfortunately it is not even known, except in special cases, whether the dimensions on the right hand side are finite.

For a (mixed) motive  $M$  over  $\mathbb{Q}$  – intuitively a “piece” in the total cohomology of a variety  $X$ , such as  $H^w(X)$  – analogy with the function field case leads to the following definition of the  $L$ -function:

$$L(M, s) = \prod_p L_p(M, s) \quad \text{where} \quad L_p(M, s) = \det_{\mathbb{Q}_l} (1 - p^{-s} \text{Fr}_p^* | M_l^{I_p})^{-1} .$$

Here  $M_l$  is the  $l$ -adic realization of  $M$  for any  $l \neq p$  and  $\text{Fr}_p, I_p$  are the inverse of a Frobenius automorphism in  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  and an inertia group at  $p$ , respectively. For example, the  $l$ -adic realization of  $M = H^w(X)$  is the  $w$ -th  $l$ -adic cohomology

of  $X \otimes \overline{\mathbb{Q}}$ . Rationality and independence of  $l$  of the characteristic polynomial of  $\text{Fr}_p^*$  are expected for all  $p$ , known in many cases and assumed in the following.

If  $\mathcal{X}$  is proper and flat over  $\text{Spec } \mathbb{Z}$  with smooth generic fibre  $X = \mathcal{X} \otimes \mathbb{Q}$ , then up to finitely many Euler factors we have:

$$\zeta_{\mathcal{X}}(s) = \prod_{w=0}^{2 \dim X} L(H^w(X), s)^{(-1)^w}$$

Adding a suitable product of  $\Gamma$ -factors  $L_{\infty}(M, s)$  defined in [Se] and [F-PR] III which depends only on the real Hodge realization  $M_B$  over  $\mathbb{R}$  we obtain the completed  $L$ -function of the motive

$$\hat{L}(M, s) = L(M, s)L_{\infty}(M, s).$$

In terms of the filtration  $\mathcal{V}$  on  $M_B$  introduced in [D3] § 6, we have

$$L_{\infty}(M, s) = \prod_{n \in \mathbb{Z}} \zeta_{\infty}(s - n)^{d_n}$$

where  $d_n = \dim \text{Gr}_{\mathcal{V}}^n M_B$ .

Define  $\hat{L}_S(M, s)$  by omitting the Euler factors corresponding to a finite set of places  $S$ .

For later purposes we recall the following definition due to Scholl. A motive over  $\mathbb{Q}$  is called integral at  $p$  if the weight filtration on the  $l$ -adic realization for  $l \neq p$  splits as a module under the inertia group at  $p$ . For a finite set  $S$  of prime numbers let  $\mathcal{M}_{\mathbb{Z}, S}$  be the category of motives over  $\mathbb{Q}$  which are integral at all  $p \notin S$ .

The following conjectures are a great challenge to arithmetic geometry. Except for the fourth they have been confirmed in many cases after first identifying the  $L$ -function of a motive with a product of automorphic  $L$ -functions.

**CONJECTURES 2.1** Let  $M$  be a (mixed) motive over  $\mathbb{Q}$ .

1.  $L(M, s)$  and hence  $\hat{L}(M, s)$  have a meromorphic continuation to  $\mathbb{C}$  and there is a functional equation

$$\hat{L}(M, s) = \varepsilon(M, s) \hat{L}(M^*, 1 - s)$$

where  $\varepsilon(M, s) = a e^{bs}$  for some real  $a, b$ .

2.  $\hat{L}(M, s) = \hat{L}_1(M, s) \hat{L}_{02}(M, s)^{-1}$

where  $\hat{L}_1(M, s)$  is entire of genus one and  $\hat{L}_{02}(M, s)$  is a polynomial in  $s$  whose zeroes are integers.

3. (Artin) If  $M$  is simple and not a Tate motive  $\mathbb{Q}(n)$ , the  $L$ -function  $L(M, s)$  has no poles.

4. (Riemann) If  $M$  is pure of weight  $w$ , e.g.  $M = H^w(X)$  for a smooth proper variety  $X/\mathbb{Q}$ , then the zeroes of  $\hat{L}(M, s)$  lie on the line  $\text{Re } s = \frac{w+1}{2}$ .

5. (Deligne, Beilinson, Scholl) For  $M$  in  $\mathcal{M}_{\mathbb{Z}}$

$$\text{ord}_{s=0} L(M, s) = \dim \text{Ext}_{\mathcal{M}_{\mathbb{Z}}}^1(\mathbb{Q}(0), M^*(1)) - \dim \text{Hom}_{\mathcal{M}_{\mathbb{Z}}}(\mathbb{Q}(0), M^*(1)).$$

## 3 THE CONJECTURAL COHOMOLOGICAL FORMALISM

In this section we interpret many of the conjectures about zeta- and  $L$ -functions in terms of an as yet speculative infinite dimensional cohomology theory. We also describe a number of consequences of this very rigid formalism that can be proved directly. Among these there is a formula which expresses the Riemann  $\zeta$ -function as a zeta-regularized product. After giving the definition of regularized determinants in a simple algebraic setting we first discuss the formalism in the case of the Riemann zeta function and then generalize to Hasse–Weil zeta functions and motivic  $L$ -series.

Given a  $\mathbb{C}$ -vector space  $H$  with an endomorphism  $\Theta$  such that  $H$  is the countable sum of finite dimensional  $\Theta$ -invariant subspaces  $H_\alpha$ , the spectrum  $\text{sp}(\Theta)$  is defined as the union of the spectra of  $\Theta$  on  $H_\alpha$ , the eigenvalues being counted with their algebraic multiplicities. The (zeta-)regularized determinant  $\det_\infty(\Theta | H)$  of  $\Theta$  is defined to be zero if  $0 \in \text{sp}(\Theta)$ , and by the formula

$$\det_\infty(\Theta | H) := \prod_{\alpha \in \text{sp}(\Theta)} \alpha := \exp(-\zeta'_\Theta(0)) \quad (2)$$

if  $0 \notin \text{sp}(\Theta)$ . Here

$$\zeta_\Theta(z) = \sum_{0 \neq \alpha \in \text{sp}(\Theta)} \alpha^{-z}, \quad \text{where } -\pi < \arg \alpha \leq \pi,$$

is the spectral zeta function of  $\Theta$ . For (2) to make sense we require that  $\zeta_\Theta$  be convergent in some right half plane, with meromorphic continuation to  $\text{Re } z > -\varepsilon$ , for some  $\varepsilon > 0$ , holomorphic at  $z = 0$ . For an endomorphism  $\Theta_0$  on a real vector space  $H_0$ , such that  $\Theta = \Theta_0 \otimes \text{id}$  on  $H = H_0 \otimes \mathbb{C}$  satisfies the above requirements, we set

$$\det_\infty(\Theta_0 | H_0) = \det_\infty(\Theta | H).$$

On a finite dimensional vector space  $H$  we obtain the ordinary determinant of  $\Theta$ . As an example of a regularized determinant, consider an endomorphism  $\Theta$  whose spectrum consists of the number  $1, 2, 3, \dots$  with multiplicities one. Then

$$\det_\infty(\Theta | H) = \prod_{\nu=1}^{\infty} \nu = \sqrt{2\pi} \quad \text{since } \zeta'(0) = -\log \sqrt{2\pi}.$$

The regularized determinant plays a role for example in Arakelov theory and in string theory. In our context it allows us to write the different Euler factors of zeta- and  $L$ -functions in a uniform way as we will first explain for the Riemann zeta function.

Let  $\mathcal{R}_p$  for  $p \neq \infty$  be the  $\mathbb{R}$ -vector space of real valued finite Fourier series on  $\mathbb{R}/(\log p)\mathbb{Z}$  and set

$$\mathcal{R}_\infty = \mathbb{R}[\exp(-2y)] \quad \text{for } p = \infty.$$

These spaces carry a natural  $\mathbb{R}$ -action  $\sigma^t$  via  $(\sigma^t f)(y) = f(y+t)$  with infinitesimal generator  $\Theta = d/dy$ . The eigenvalues of  $\Theta$  on  $\mathcal{C}_p = \mathcal{R}_p \otimes \mathbb{C}$  are just the poles of  $\zeta_p(s)$ .

PROPOSITION 3.1 *We have  $\zeta_p(s) = \det_\infty \left( \frac{1}{2\pi}(s - \Theta) \mid \mathcal{R}_p \right)^{-1}$  for  $p \leq \infty$ .*

This is easily proved by applying a classical formula of Lerch for the derivative of the Hurwitz zeta function at zero [D3] 2.7.

In a sense  $\overline{\text{Spec}} \mathbb{Z} = \text{Spec} \mathbb{Z} \cup \infty$  is analogous to a projective curve over a finite field. The Grothendieck Lefschetz trace formula in characteristic  $p$  together with the proposition, suggest that a formula of the following type might hold:

$$\hat{\zeta}(s) = \prod_{i=0}^2 \det_\infty \left( \frac{1}{2\pi}(s - \Theta) \mid H^i(\overline{\text{Spec}} \mathbb{Z}, \mathcal{R}) \right)^{(-1)^{i+1}}. \tag{3}$$

Here  $H^i(\overline{\text{Spec}} \mathbb{Z}, \mathcal{R})$  would be some real cohomology vector space equipped with a canonical endomorphism  $\Theta$  associated to some space  $\overline{\text{Spec}} \mathbb{Z}$  corresponding to  $\overline{\text{Spec}} \mathbb{Z}$ . As recalled earlier  $\hat{\zeta}(s)$  has poles only at  $s = 0, 1$  and these are of first order. Moreover the zeroes of  $\hat{\zeta}(s)$  are just the non-trivial zeroes of  $\zeta(s)$ . If we assume that the eigenvalues of  $\Theta$  on  $H^i(\overline{\text{Spec}} \mathbb{Z}, \mathcal{R})$  are distinct for  $i = 0, 1, 2$  it follows therefore that

- $H^0(\overline{\text{Spec}} \mathbb{Z}, \mathcal{R}) = \mathbb{R}$  with trivial action of  $\Theta$ , i.e.  $\Theta = 0$ ,
- $H^1(\overline{\text{Spec}} \mathbb{Z}, \mathcal{R})$  is infinite dimensional, the spectrum of  $\Theta$  consisting of the non-trivial zeroes  $\rho$  of  $\zeta(s)$  with their multiplicities,
- $H^2(\overline{\text{Spec}} \mathbb{Z}, \mathcal{R}) \cong \mathbb{R}$  but with  $\Theta = \text{id}$ .
- For  $i > 2$  the cohomologies  $H^i(\overline{\text{Spec}} \mathbb{Z}, \mathcal{R})$  should vanish.

Formula (3) implies that

$$\xi(s) := \frac{s}{2\pi} \frac{(s-1)}{2\pi} \hat{\zeta}(s) = \prod_{\rho} \frac{1}{2\pi} (s - \rho).$$

This formula turned out to be true [D2], [SchS]. Earlier a related formula had been observed in [K].

If  $H$  is some space with an endomorphism  $\Theta$  let us write  $H(\alpha)$  for  $H$  equipped with the twisted endomorphism  $\Theta_{H(\alpha)} = \Theta - \alpha \text{id}$ . With this notation we expect a canonical “trace”-isomorphism:

$$\text{tr} : H^2(\overline{\text{Spec}} \mathbb{Z}, \mathcal{R}) \xrightarrow{\sim} \mathbb{R}(-1).$$

In our setting the cup product pairing

$$\cup : H^i(\overline{\text{Spec}} \mathbb{Z}, \mathcal{R}) \times H^{2-i}(\overline{\text{Spec}} \mathbb{Z}, \mathcal{R}) \longrightarrow H^2(\overline{\text{Spec}} \mathbb{Z}, \mathcal{R}) \cong \mathbb{R}(-1)$$

induces a pairing for every  $\alpha$  in  $\mathbb{C}$ :

$$\cup : H^i(\overline{\text{Spec}} \mathbb{Z}, \mathcal{C})^{\Theta \sim \alpha} \times H^{2-i}(\overline{\text{Spec}} \mathbb{Z}, \mathcal{C})^{\Theta \sim 1-\alpha} \longrightarrow H^2(\overline{\text{Spec}} \mathbb{Z}, \mathcal{C})^{\Theta \sim 1} \cong \mathbb{C}.$$

Here  $\Theta \sim \alpha$  denotes the subspace of

$$H^i(\overline{\text{Spec } \mathbb{Z}}, \mathcal{C}) = H^i(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R}) \otimes \mathbb{C}$$

of elements annihilated by some power of  $\Theta - \alpha$ . We expect Poincaré duality in the sense that these pairings should be non-degenerate for all  $\alpha$ . This is compatible with the functional equation of  $\hat{\zeta}(s)$ . For the precise relation see [D3] 7.19.

In the next section we will have more to say on the type of cohomology theory that might be expected for  $H^i(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R})$ . But first let us note a nice consequence our approach would have. Consider the linear flow  $\lambda^t = \exp t\Theta$  on  $H^i(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R})$ . It is natural to expect that it is the flow induced on cohomology by a flow  $\phi^t$  on the underlying space  $\overline{\text{Spec } \mathbb{Z}}$ , i.e.  $\lambda^t = (\phi^t)^*$ . This implies that  $\lambda^t$  would respect cup product and that  $\Theta$  would behave as a derivation. Now assume that as in the case of compact Riemann surfaces there is a Hodge  $*$ -operator:

$$* : H^1(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R}) \xrightarrow{\sim} H^1(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R}),$$

such that

$$\langle f, f' \rangle = \text{tr}(f \cup (*f')) \quad \text{for } f, f' \text{ in } H^1(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R}),$$

is positive definite, i.e. a scalar product on  $H^1(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R})$ . It is natural to assume that  $(\phi^t)^*$  and hence  $\Theta$  commutes with  $*$  on  $H^1(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R})$ . From the equality:

$$f_1 \cup f_2 = \Theta(f_1 \cup f_2) = \Theta f_1 \cup f_2 + f_1 \cup \Theta f_2$$

for  $f_1, f_2$  in  $H^1(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R})$  we would thus obtain the formula

$$\langle f_1, f_2 \rangle = \langle \Theta f_1, f_2 \rangle + \langle f_1, \Theta f_2 \rangle,$$

and hence that  $\Theta = \frac{1}{2} + A$  where  $A$  is a skew-symmetric endomorphism of  $H^1(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R})$ . Hence the Riemann conjecture would follow.

The formula  $\Theta = \frac{1}{2} + A$  is also in accordance with numerical investigations on the fluctuations of the spacings between consecutive non-trivial zeroes of  $\zeta(s)$ . It was found that their statistics resembles that of the fluctuations in the spacings of consecutive eigenvalues of random real skew symmetric matrices, as opposed to the different statistics for random real symmetric matrices; see [Sa] for a full account of this story. In fact the comparison was made between hermitian and symmetric matrices, but as pointed out to me by M. Kontsevich, the statistics in the hermitian and real skew symmetric cases agree.

The completion of  $H^1(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R})$  with respect to  $\langle \cdot, \cdot \rangle$ , together with the unbounded operator  $\Theta$  would be the space that Hilbert was looking for, and that Berry [B] suggested to realize in a quantum physical setting.

The following considerations are necessary for comparison with the dynamical picture.

Formula (3) is closely related to a reformulation of the explicit formulas in analytic number theory using the conjectural cohomology theory above, see [I] Kap. 3 and [JL] for the precise relationship. Set  $\mathbb{R}^+ = (0, \infty)$ .



PROPOSITION 3.2 For a test function  $\varphi \in \mathcal{D}(\mathbb{R}^+) = C_0^\infty(\mathbb{R}^+)$  define an entire function  $\Phi(s)$  by the formula

$$\Phi(s) = \int_{\mathbb{R}} \varphi(t) e^{ts} dt .$$

Then we have the “explicit formula”:

$$\Phi(0) - \sum_{\hat{\zeta}(\rho)=0} \Phi(\rho) + \Phi(1) = \sum_p \log p \sum_{k=1}^{\infty} \varphi(k \log p) + \int_0^{\infty} \frac{\varphi(t)}{1 - e^{-2t}} dt .$$

We wish to interpret this well known formula along the lines of [P] §3. For this we require the following elementary notion of a distributional trace. Consider a real or complex vector space  $H$  with a linear  $\mathbb{R}$ -action

$$\lambda : \mathbb{R} \times H \rightarrow H , \quad \lambda(t, h) = \lambda^t(h) ,$$

which decomposes into a countable direct sum of finite dimensional invariant subspaces  $H_n$ . Let  $\text{Tr}(\lambda | H_n)_{\text{dis}}$  be the distribution on  $\mathbb{R}^+$  associated to the function  $t \mapsto \text{Tr}(\lambda^t | H_n)$ , and set

$$\text{Tr}(\lambda | H)_{\text{dis}} = \sum_n \text{Tr}(\lambda | H_n)_{\text{dis}} \tag{4}$$

if the sum converges in the space of distributions  $\mathcal{D}'(\mathbb{R}^+)$ . By assumption  $\lambda$  can be written as  $\lambda^t = \exp t\Theta$  with an endomorphism  $\Theta$  of  $H$ , and we have

$$\text{Tr}(\lambda | H)_{\text{dis}} = \sum_{\alpha \in \text{sp}(\Theta)} \langle e^{t\alpha} \rangle \quad \text{in } \mathcal{D}'(\mathbb{R}^+)$$

if the series converges. Here  $\langle f \rangle \in \mathcal{D}'(\mathbb{R}^+)$  denotes the distribution associated to a locally integrable function  $f$  on  $\mathbb{R}^+$ . Thus

$$\langle \text{Tr}(\lambda | H)_{\text{dis}}, \varphi \rangle = \sum_{\alpha \in \text{sp}(\Theta)} \int_{\mathbb{R}} \varphi(t) e^{t\alpha} dt = \sum_{\alpha \in \text{sp}(\Theta)} \Phi(\alpha)$$

for any test function  $\varphi$  in the Schwartz space  $\mathcal{D}(\mathbb{R}^+)$ . Conjecturally (3.2) can thus be reformulated as the following identity of distributions

$$\sum_i (-1)^i \text{Tr}(\phi^* | H^i(\overline{\text{“Spec } \mathbb{Z}^{\times} \text{”}}, \mathcal{R}))_{\text{dis}} = \sum_p \log p \sum_{k=1}^{\infty} \delta_{k \log p} + \langle (1 - e^{-2t})^{-1} \rangle . \tag{5}$$

Using the Poisson summation formula one sees that

$$\text{Tr}(\sigma | \mathcal{R}_p)_{\text{dis}} = \log p \sum_{k=1}^{\infty} \delta_{k \log p} \quad \text{for finite } p .$$

A direct calculation shows that

$$\text{Tr}(\sigma | \mathcal{R}_{\infty})_{\text{dis}} = \langle (1 - e^{-2t})^{-1} \rangle .$$

Hence (5) can be rewritten as a sheaf theoretic Lefschetz trace formula

$$\sum_i (-1)^i \text{Tr}(\phi^* | H^i(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R}))_{\text{dis}} = \sum_{p \leq \infty} \text{Tr}(\phi^* | \mathcal{R}_p)_{\text{dis}} . \tag{6}$$

For more on this see [D5], [DSch].

We now turn to Hasse–Weil zeta functions of algebraic schemes  $\mathcal{X}/\mathbb{Z}$ . A similar argument as for the Riemann zeta function suggests that

$$\zeta_{\mathcal{X}}(s) = \prod_{i=0}^{2d} \det_{\infty} \left( \frac{1}{2\pi} (s - \Theta) | H_c^i(\mathcal{X}, \mathcal{R}) \right)^{(-1)^{i+1}} \tag{7}$$

where  $H_c^i(\mathcal{X}, \mathcal{R})$  is some real cohomology with compact supports associated to a dynamical system “ $\mathcal{X}$ ” attached to  $\mathcal{X}$  and  $d = \dim \mathcal{X}$ . Here  $\Theta$  should be the infinitesimal generator of the induced flow on cohomology. In particular we would have

$$\text{ord}_{s=\alpha} \zeta_{\mathcal{X}}(s) = \sum_{i=0}^{2d} (-1)^{i+1} \dim H_c^i(\mathcal{X}, \mathcal{C})^{\Theta \sim \alpha} .$$

For a regular connected  $\mathcal{X}$  the Poincaré duality pairing

$$\cup : H_c^i(\mathcal{X}, \mathcal{R}) \times H^{2d-i}(\mathcal{X}, \mathcal{R}) \longrightarrow H_c^{2d}(\mathcal{X}, \mathcal{R}) \xrightarrow{\sim} \mathbb{R}(-d) \tag{8}$$

should identify

$$H_c^i(\mathcal{X}, \mathcal{C})^{\Theta \sim \alpha} \quad \text{with the dual of} \quad H^{2d-i}(\mathcal{X}, \mathcal{C})^{\Theta \sim d-\alpha} .$$

In particular we would get:

$$\text{ord}_{s=d-n} \zeta_{\mathcal{X}}(s) = \sum_{i=0}^{2d} (-1)^{i+1} \dim H^i(\mathcal{X}, \mathcal{C}(n))^{\Theta \sim 0} ,$$

where  $\mathcal{C}(\alpha)$  is the sheaf  $\mathcal{C}$  on “ $\mathcal{X}$ ” with action of the flow twisted by  $e^{-\alpha t}$ . Thus

$$H^i(\mathcal{X}, \mathcal{C}(n))^{\Theta \sim 0} = H^i(\mathcal{X}, \mathcal{C})^{\Theta \sim n} .$$

For a regular  $\mathcal{X}$  we expect formal analogues of Tate’s conjecture

$$H_{\mathcal{M}}^i(\mathcal{X}, \mathbb{C}(n)) := \text{Gr}_{\gamma}^n K_{2n-i}(\mathcal{X}) \otimes \mathbb{C} \xrightarrow{\sim} H^i(\mathcal{X}, \mathcal{C}(n))^{\Theta \sim 0} , \tag{9}$$

and in particular that

$$H^i(\mathcal{X}, \mathcal{C}(n))^{\Theta \sim 0} = 0 \quad \text{for } i > 2n .$$

Note that the latter assertion says that the weights of  $\Theta$  on  $H^i(\mathcal{X}, \mathcal{C})$ , i.e. twice the real parts of its eigenvalues, should be  $\geq i$ . This would imply Soulé’s conjecture

(2.1).

Again the explicit formulas could be expressed in terms of cohomology in the form

$$\sum_i (-1)^i \text{Tr}(\phi^* | H_c^i(\mathcal{X}, \mathcal{R}))_{\text{dis}} = \sum_{x \in |\mathcal{X}|} \log N(x) \sum_{k=1}^{\infty} \delta_{k \log N(x)}. \tag{10}$$

In support of these ideas we have the following result.

**THEOREM 3.3** *On the category of algebraic  $\mathbb{F}_p$ -schemes  $\mathcal{X}$  there is a cohomology theory in  $\mathbb{C}$ -vector spaces with a linear flow such that (7) holds. For a regular connected  $\mathcal{X}$  of dimension  $d$  it satisfies Poincaré duality (8). Moreover (9) reduces to the Tate conjecture for  $l$ -adic cohomology.*

See [D3] §4, [D4] §2 for more precise statements and the simple construction based on  $l$ -adic cohomology. This approach cannot be generalized to non-equi-characteristic  $\mathcal{X}/\mathbb{Z}$ .

If there were a dynamical cohomology theory  $H^i(\overline{\mathcal{X}}, \mathcal{R})$  attached to some Arakelov compactification  $\overline{\mathcal{X}}$  of  $\mathcal{X}$  such that

$$\hat{\zeta}_{\mathcal{X}}(s) = \prod_{i=0}^{2d} \det_{\infty} \left( \frac{1}{2\pi} (s - \Theta) | H^i(\overline{\mathcal{X}}, \mathcal{R}) \right)^{(-1)^{i+1}},$$

then as above Poincaré duality for  $H^i(\overline{\mathcal{X}}, \mathcal{R})$  would be in accordance with the expected functional equation for  $\hat{\zeta}_{\mathcal{X}}(s)$ . A Hodge  $*$ -operator

$$* : H^i(\overline{\mathcal{X}}, \mathcal{R}) \longrightarrow H^{2d-i}(\overline{\mathcal{X}}, \mathcal{R})$$

defining a scalar product via  $\langle f, f' \rangle = \text{tr}(f \cup (*f'))$  and for which

$$\phi^{t*} \circ * = (e^t)^{d-i} * \circ \phi^{t*}, \quad \text{i.e.} \quad \Theta \circ * = * \circ (d - i + \Theta),$$

holds, would imply that  $\Theta - i/2$  is skew symmetric, hence the Riemann hypotheses for  $\hat{\zeta}_{\mathcal{X}}(s)$ . The last equation means that the flow changes the metric defining the  $*$ -operator by the conformal factor  $e^t$ .

As we mentioned above the zeta function  $\zeta_{\mathcal{X}}(s)$  is up to finitely many Euler factors the alternating product of the  $L$ -functions of the motives  $H^i(X)$ . In [D1] we constructed cohomology  $\mathbb{R}$ -vector spaces  $H_{\text{ar}}^w$  with a linear flow on the category of varieties over  $\mathbb{R}$  or  $\mathbb{C}$  such that

$$\zeta_{\mathcal{X}_{\infty}}(s) = \prod_{i=0}^{2 \dim \mathcal{X}_{\infty}} \det_{\infty} \left( \frac{1}{2\pi} (s - \Theta) | H_{\text{ar}}^i(\mathcal{X}_{\infty}) \right)^{(-1)^{i+1}}.$$

Cup product and functoriality turn the spaces  $H_{\text{ar}}^i(\mathcal{X}_{\infty})$  into modules under  $H_{\text{ar}}^0(\mathcal{X}_{\infty}) = H_{\text{ar}}^0(\text{Spec } \mathbb{R}) = \mathcal{R}_{\infty}$  of rank equal to  $\dim H^i(\mathcal{X}_{\infty}, \mathbb{Q})$ . Philosophically the scheme  $\mathcal{X}$  should have bad semistable “reduction” at infinity. In accordance with this idea Consani [Cons] has refined the theory  $H_{\text{ar}}^i$  to a cohomology theory with a linear flow and a monodromy operator  $N$  which contains  $H_{\text{ar}}^i$  as the kernel of  $N$ .

We now turn our attention to motivic  $L$ -series. The first task is to express the local Euler factors  $L_p(M, s)$  in terms of regularized determinants on some spaces functorially attached to  $M$ .

**THEOREM 3.4** *For every  $p \leq \infty$ , there is a left exact additive functor  $\mathcal{F}_p$  from motives over  $\mathbb{Q}$  to the category of  $\mathbb{C}$ -vector spaces with a linear flow such that*

$$L_p(M, s) = \det_{\infty} \left( \frac{1}{2\pi}(s - \Theta) | \mathcal{F}_p(M) \right)^{-1} .$$

*The functor  $\mathcal{F}_p$  commutes with Tate twists, and there are natural flow equivariant maps*

$$\mathcal{F}_p(M) \otimes \mathcal{F}_p(M') \longrightarrow \mathcal{F}_p(M \otimes M') \tag{11}$$

*turning  $\mathcal{F}_p(M)$  into an  $\mathcal{F}_p(\mathbb{Q}(0)) = \mathbb{C}_p$ -module of rank equal to  $\dim M_l^{I^p}$  for finite  $p$  and equal to  $\text{rk} M$  for  $p = \infty$ . On the category of motives integral at  $p$  the functor  $\mathcal{F}_p$  is exact. On motives with good reduction at  $p$  the map (11) is an isomorphism and  $\mathcal{F}_p$  commutes with duals. For  $p = \infty$  it has a real structure  $\mathcal{F}_{\infty}^{\mathbb{R}}$  and there is a natural perfect pairing:*

$$\mathcal{F}_{\infty}^{\mathbb{R}}(M)^{\Theta=0} \times \text{Ext}_{MH_{\mathbb{R}}}^1(\mathbb{R}(0), M_B^*(1)) \longrightarrow \mathbb{R} ,$$

*where  $MH_{\mathbb{R}}$  is the category of real mixed Hodge structures over  $\mathbb{R}$ . For varieties  $X/\mathbb{R}$  we have*

$$H_{\text{ar}}^w(X) = \mathcal{F}_{\infty}^{\mathbb{R}}(H^w(X)) .$$

The proofs – which are quite formal – can be found in [D3]. The functor  $\mathcal{F}_{\infty}$  is constructed from  $M_B$  by a construction á la Fontaine using a simple Barsotti–Tate ring. For finite  $p$ , the construction applies an elementary case of the Riemann–Hilbert correspondence to  $M_l^{I^p} \otimes_{\mathbb{Q}_l} \mathbb{C}$  with the Frobenius action. It can also be viewed as an association of Fontaine’s type.

By the theorem

$$\hat{L}(M, s) = \prod_{p \leq \infty} \det_{\infty} \left( \frac{1}{2\pi}(s - \Theta) | \mathcal{F}_p(M) \right)^{-1} ,$$

and this suggests that

$$\hat{L}(M, s) = \prod_{i=0}^2 \det_{\infty} \left( \frac{1}{2\pi}(s - \Theta) | H^i(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(M)) \right)^{(-1)^{i+1}} \tag{12}$$

for some sheaf with action of the flow  $\mathcal{F}(M)$  on  $\overline{\text{Spec } \mathbb{Z}}$  whose stalks “at the points  $p$ ” should be isomorphic to  $\mathcal{F}_p(M)$ . It should be thought of as an analogue of the sheaf  $\mathcal{F}(\mathcal{M}) = j_*\mathcal{M}$  for a  $\mathbb{Q}_l$ -sheaf  $\mathcal{M}$  on the generic point  $\eta$  of a curve  $Y$  over a finite field, where  $j : \eta \hookrightarrow Y$  is the inclusion.

Formula (12) would represent  $\hat{L}(M, s)$  as a quotient of entire functions – at least

if the regularized determinants are of the Cartier–Voros type [CV].

This together with Poincaré duality for the sheaf cohomologies  $H^i(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(M))$  would explain the first part of conjecture 2.1 c.f. [D3] 7.19.

The assertion about  $\hat{L}_{02}(M, s)$  in the second part of 2.1 means that  $H^0(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(M))$  and  $H^2(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(M))$  should be finite dimensional with  $\Theta$  having only integer eigenvalues.

The Riemann conjecture would follow from purity: For a pure motive  $M$  of weight  $w$  the eigenvalues of  $\Theta$  on  $H^i(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(M))$  should have real part  $\frac{w+i}{2}$ . As before there is a Hodge \*-argument for this c.f. [D3] 7.11.

For  $L(M, s)$  we expect the formula

$$L(M, s) = \prod_{i=0}^2 \det_{\infty} \left( \frac{1}{2\pi} (s - \Theta) \mid H_c^i(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(M)) \right)^{(-1)^{i+1}} \quad (13)$$

and by Poincaré duality

$$L(M, s) = \prod_{i=0}^2 \det_{\infty} \left( \frac{1}{2\pi} (s + \Theta) \mid H^i(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(M^*(1))) \right)^{(-1)^{i+1}}. \quad (14)$$

See [D3] (7.19.1). This implies that

$$\text{ord}_{s=0} L(M, s) = \sum_{i=0}^2 (-1)^{i+1} \dim H^i(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(M^*(1)))^{\Theta \sim 0}.$$

On the category  $\mathcal{M}_{\mathbb{Z}}$  all functors  $\mathcal{F}_p$  are exact by the theorem. Hence  $\mathcal{F}$  should be exact and therefore induce maps for all  $N$  in  $\mathcal{M}_{\mathbb{Z}}$

(15)

$$\mathcal{F} : \text{Ext}_{\mathcal{M}_{\mathbb{Z}}}^i(\mathbb{Q}(0), N) \otimes \mathbb{C} \longrightarrow \text{Ext}_{\overline{\text{Spec } \mathbb{Z}}}^i(\mathcal{C}(0), \mathcal{F}(N))^{\Theta \sim 0} = H^i(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(N))^{\Theta \sim 0}.$$

If these are isomorphisms (2.1) part 5. follows. Note that because  $\text{Spec } \mathbb{Z}$  is an affine curve it is reasonable to expect  $H^i(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(N))$  to vanish for  $i \geq 2$ . Similarly (15) with  $\mathbb{Z}$  replaced by  $\mathbb{Z}_S$  ought to be an isomorphism. The eigenvalues of  $\Theta$  on

$$H^0(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(N)) = H^0(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(N)) \quad (\text{c.f. [D4] § 4})$$

being integers, we have

$$H^0(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(N)) = \bigoplus_{n \in \mathbb{Z}} \text{Hom}(\mathbb{Q}(0), N(n)) \otimes \mathbb{C}$$

by (15) applied to all twists  $N(n)$ . Together with (14) we would get the Artin conjecture (2.1) part 3. Further conjectures on  $L$ -functions and extensions of motives by Deligne, Scholl and Selberg are related to the cohomological formalism in [D4] §§ 4, 9.

Let us now turn to certain consequences of the formalism that have been proved. As for the Riemann zeta function we must have

$$\xi(M, s) := \hat{L}(M, s) \prod_{\tau} \frac{1}{2\pi}(s - \tau) = \prod_{\rho} \frac{1}{2\pi}(s - \rho) \tag{16}$$

where  $\rho$  runs over the zeroes of  $\hat{L}(M, s)$  and  $\tau$  over its finitely many poles. This follows from the theory of [JL] or [I] assuming standard conjectures on the analytic behaviour of  $L$ -series. For example for  $L(E, s)$ , where  $E$  is a modular elliptic curve, formula (16) is a theorem.

As explained above there should be a trace isomorphism

$$\text{tr} : H^2(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R}(1)) = H^2(\overline{\text{Spec } \mathbb{Z}}, \mathcal{R}(1))^{\Theta=0} \xrightarrow{\sim} \mathbb{R} .$$

Comparing this with (15) we are led to search for a category of (mixed) motives  $\mathcal{M}_{\overline{\mathbb{Z}}}$  over  $\overline{\text{Spec } \mathbb{Z}}$  equipped with a non-trivial map

$$\text{Ext}_{\mathcal{M}_{\overline{\mathbb{Z}}}}^2(\mathbb{Q}(0), \mathbb{Q}(1)) \longrightarrow \mathbb{R} .$$

Integrality at a finite prime  $p$  can be expressed in terms of the functor  $\mathcal{F}_p$ , c.f. [DN] appendix. For  $\mathcal{F}_{\infty}$  this condition means that the real Hodge structure  $M_B$  be split. Taking this as our definition of integrality at  $p = \infty$  we define  $\mathcal{M}_{\overline{\mathbb{Z}}}$  to be the subcategory of motives in  $\mathcal{M}_{\mathbb{Q}}$  which are integral at all primes  $p \leq \infty$ . Under the natural injection [Sch] 2.7

$$\mathbb{Q}^* \hookrightarrow \text{Ext}_{\mathcal{M}_{\mathbb{Q}}}^1(\mathbb{Q}(0), \mathbb{Q}(1)) , \tag{17}$$

the motive corresponding to  $\alpha$  is integral at  $p \leq \infty$  iff  $|\alpha|_p = 1$ . In [DN] it was shown that if (17) is an isomorphism rationally then  $\text{Ext}_{\mathcal{M}_{\overline{\mathbb{Z}}}}^2(\mathbb{Q}(0), \mathbb{Q}(1))$  is non-zero. If  $\mathcal{M}_{\overline{\mathbb{Z}}}$  is replaced by the category (1-motives/ $\overline{\text{Spec } \mathbb{Z}}$ )  $\otimes \mathbb{Q}$  then  $\text{Ext}^2(\mathbb{Q}(0), \mathbb{Q}(1))$  is non-zero unconditionally, [J] Cor. 5.5. Furthermore it was shown that the motivic height pairing of [Sch] could be interpreted as a Yoneda pairing followed by the degree map

$$\text{Ext}_{\mathcal{M}_{\overline{\mathbb{Z}}}}^1(\mathbb{Q}(0), M) \times \text{Ext}_{\mathcal{M}_{\overline{\mathbb{Z}}}}^1(\mathbb{Q}(0), M^*(1)) \longrightarrow \text{Ext}_{\mathcal{M}_{\overline{\mathbb{Z}}}}^2(\mathbb{Q}(0), \mathbb{Q}(1)) \longrightarrow \mathbb{R} .$$

This is in accordance with the idea that under a suitable extension of the isomorphism (15) to  $\overline{\text{Spec } \mathbb{Z}}$ , (c.f. [D4] (2.4)), the motivic height pairing will correspond to Poincaré duality

$$H^1(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(M)) \times H^1(\overline{\text{Spec } \mathbb{Z}}, \mathcal{F}(M^*(1))) \longrightarrow H^2(\overline{\text{Spec } \mathbb{Z}}, \mathcal{C}) \stackrel{\text{tr}}{\cong} \mathbb{C}$$

restricted to the  $\Theta \sim 0$  parts.

Apart from local  $L$ -factors there are also local  $\varepsilon$ -factors attached to motives. In [D6] the functors  $\mathcal{F}_p$  and a notion of regularized super-dimension were used among other things to give a comparatively uniform description of these factors at all places.

A motive  $M$  of weight  $w$  with coefficients in a number field  $T$  is called orthogonal if there is a symmetric morphism  $M \otimes M \rightarrow T(-w)$  which induces an isomorphism  $M^* \cong M(w)$ . For example the Artin motive attached to a representation  $\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_N(T)$  is orthogonal if and only if  $\rho$  is orthogonal. Our formalism implies that for orthogonal  $M$  the cup product induces a symplectic form on  $H^1(\overline{\text{Spec}} \mathbb{Z}, \mathcal{F}(M))^{\Theta \sim \frac{w+1}{2}}$  which must therefore be of even dimension. Hence the order of vanishing of  $L(M, s)$  at the central point  $\frac{w+1}{2}$  must be even and the sign in the functional equation therefore be  $+1$  c.f. [D4] §6. For Artin motives this is a theorem of Fröhlich and Queyrut which was extended to more general motives by T. Saito in [S] using crystalline methods.

We close this section with some remarks on trace formulas. If the  $L$ -functions of motives satisfy the expected analytic properties, one can easily extend the explicit formulas of analytic number theory for the  $\hat{L}_S$ -function to this context, see for example [DSch] or [JL]. In terms of our conjectural cohomology theory these can be reformulated – as for the Riemann zeta function – as the following equalities of distributions on  $\mathbb{R}^+$ :

$$\sum_i (-1)^i \text{Tr}(\psi^* | H_c^i(\overline{\text{Spec}} \mathbb{Z} \setminus S, \mathcal{F}(M)))_{\text{dis}} = \sum_{p \notin S} \log p \sum_{k=1}^{\infty} \text{Tr}(\text{Fr}_p^k | M_l^{I_p}) \delta_{k \log p} + \alpha(S) \left\langle \frac{\text{Tr}(e^{\bullet t} | \text{Gr}_{\mathbb{V}} M_B)}{1 - e^{-2t}} \right\rangle \tag{18}$$

and

$$\sum_i (-1)^i \text{Tr}(\psi^* | H_c^i(\overline{\text{Spec}} \mathbb{Z} \setminus S, \mathcal{F}(M)))_{\text{dis}} = \sum_{p \leq \infty, p \notin S} \text{Tr}(\psi^* | \mathcal{F}_p)_{\text{dis}} .$$

Here  $\overline{\text{Spec}} \mathbb{Z} \setminus S$  is the dynamical system corresponding to  $\overline{\text{Spec}} \mathbb{Z} \setminus S$  and we have written  $\psi^{t*}$  for the induced flow on cohomology with sheaf coefficients in accordance with notations in the next section. Moreover  $e^{\bullet t}$  is the map  $e^{nt}$  on  $\text{Gr}_{\mathbb{V}} M_B$  and  $\alpha(S)$  is zero or one according to whether  $S$  contains  $p = \infty$  or not.

In the next section we consider trace formulas for dynamical systems on foliated spaces which bear striking formal similarities with (5) and its generalization (18).

#### 4 DYNAMICAL SYSTEMS ON FOLIATED SPACES

We begin by recalling a formula due to Guillemin and Sternberg [GS] VI §2. Consider a smooth compact manifold  $X$  with a flow  $\phi^t$ , i.e. a smooth action

$$\phi : X \times \mathbb{R} \rightarrow X , \quad \phi^t(x) = \phi(x, t) .$$

The compact orbits are assumed to be non-degenerate in the following sense. If  $x$  is a fixed point of the flow, i.e.  $\phi^t(x) = x$  for all  $t$ , then the tangent map  $T_x \phi^t : T_x X \rightarrow T_x X$  should not have 1 as an eigenvalue for any  $t > 0$ . The vector field  $Y_\phi$  generated by the flow is  $\phi$ -invariant in the sense that  $T_x \phi^t(Y_{\phi, x}) = Y_{\phi, \phi^t(x)}$  for all points  $x$  in  $X$ . Thus for any point  $x$  on a periodic orbit  $\gamma$  of length  $l(\gamma)$

and any positive integer  $k$  the endomorphism  $T_x \phi^{k \cdot l(\gamma)}$  of  $T_x X$  has  $Y_{\phi,x}$  as an eigenvector of eigenvalue 1. Non-degeneracy of  $\gamma$  means that the eigenvalue 1 does not occur on  $T_x X/T_x^0$  where  $T_x^0 = \mathbb{R} \cdot Y_{\phi,x}$ .

Let  $E$  be a smooth vector bundle on  $X$  with an action opposite to  $\phi$ , i.e. a family of maps

$$\psi^t : \phi^{t*} E \longrightarrow E$$

satisfying an obvious cocycle condition. Note that for any  $x \in \gamma$  we get maps

$$\psi_x^{kl(\gamma)} : E_{\phi^{kl(\gamma)}(x)} = E_x \longrightarrow E_x ,$$

and that the traces  $\text{Tr}(\psi_x^{kl(\gamma)} | E_x)$  are independent of the choice of  $x$  on  $\gamma$ . For a fixed point  $x$  the traces  $\text{Tr}(\psi_x^t | E_x)$  are defined for all  $t$ .

Consider the endomorphisms

$$\psi^{t*} : \Gamma(X, E) \xrightarrow{\phi^{t*}} \Gamma(X, \phi^{t*} E) \xrightarrow{\psi^t} \Gamma(X, E)$$

of the Fréchet space  $\Gamma(X, E)$ . In order to define a distributional trace

$$\text{Tr}(\psi^* | \Gamma(X, E)) \quad \text{in } \mathcal{D}'(\mathbb{R}^+) ,$$

Guillemin and Sternberg proceed as follows. Consider the restriction  $\phi : X \times \mathbb{R}^+ \rightarrow X$ , the diagonal map  $\Delta : X \times \mathbb{R}^+ \rightarrow X \times X \times \mathbb{R}^+$ ,  $\Delta(x, t) = (x, x, t)$  and the projections  $p : X \times \mathbb{R}^+ \rightarrow X$ ,  $\pi : X \times \mathbb{R}^+ \rightarrow \mathbb{R}^+$ . View  $\psi$  as a map  $\psi : \phi^* E \rightarrow p^* E$  and let  $K_{\psi^*}$  be the Schwartz kernel of the composite map:

$$\psi^* : \Gamma(X, E) \xrightarrow{\phi^*} \Gamma(X \times \mathbb{R}^+, \phi^* E) \xrightarrow{\psi} \Gamma(X \times \mathbb{R}^+, p^* E) .$$

Thus  $K_{\psi^*}$  is a generalized density on  $X \times X \times \mathbb{R}^+$ . The non-degeneracy assumptions above are equivalent to the image of  $\Delta$  and the graph of  $\phi$  intersecting transversally. Thus by the theory of the wave front set one can pull back  $K_{\psi^*}$  via  $\Delta$  and define

$$\text{Tr}(\psi^* | \Gamma(X, E)) = \pi_* \Delta^* K_{\psi^*} \quad \text{in } \mathcal{D}'(\mathbb{R}^+) .$$

Intuitively,

$$\text{Tr}(\psi^* | \Gamma(X, E)) = \int_X K_{\psi^*}(x, x, t) dx$$

as a distribution in  $t$ .

With this definition of a trace the following result becomes almost a tautology:

PROPOSITION 4.1 (GUILLEMIN, STERNBERG) *Under the assumptions above, the following formula holds in  $\mathcal{D}'(\mathbb{R}^+)$ :*

$$\begin{aligned} \text{Tr}(\psi^* | \Gamma(X, E)) &= \sum_{\gamma} l(\gamma) \sum_{k=1}^{\infty} \frac{\text{Tr}(\psi_x^{kl(\gamma)} | E_x)}{|\det(1 - T_x \phi^{kl(\gamma)} | T_x X/T_x^0)|} \delta_{kl(\gamma)} \\ &+ \sum_x \left\langle \frac{\text{Tr}(\psi_x^t | E_x)}{|\det(1 - T_x \phi^t | T_x X)|} \right\rangle . \end{aligned}$$



Here  $\gamma$  runs over the periodic orbits and in the first sum  $x$  denotes any point on  $\gamma$ . In the second sum  $x$  runs over the stationary points of the flow.

In order to get a formula that is closer in appearance to (5) and (18) we now apply a basic idea which Guillemin [G] and independently Patterson [P] used in the context of Selberg and Ruelle zeta functions. It involves the theory of foliations for which we refer e.g. to [Go]. Assume that  $X$  carries a smooth foliation of codimension one such that  $\phi^t$  maps leaves to leaves. By a theorem of Frobenius this is equivalent to specifying an integrable codimension one subbundle  $T_0 \subset TX$  with  $T\phi^t(T_0) = T_0$  for all  $t$ , the bundle of tangents to the leaves. Let  $U \subset X$  be the open  $\phi^t$ -invariant subset of points  $x$  where the flow line through  $x$  intersects the leaf through  $x$  transversally, i.e. where

$$T_{0x} \oplus T_x^0 = T_x X .$$

We assume that  $U$  contains all periodic orbits.

If  $x$  is a fixed point of  $\phi$  there exists some real constant  $\kappa_x$  such that  $T_x \phi^t$  acts on the one dimensional space  $T_x X / T_{0x}$  by multiplication with  $e^{\kappa_x t}$ . We set

$$\varepsilon_\gamma(k) = \text{sgn det}(1 - T_x \phi^{kl(\gamma)} | T_{0x}) \quad \text{and} \quad \varepsilon_x = \text{sgn det}(1 - T_x \phi^t | T_x X)$$

the latter being independent of  $t > 0$ . From the proposition applied to  $\Lambda^i T_0^* \otimes E$  we get the following formula in  $\mathcal{D}'(\mathbb{R}^+)$ :

$$\begin{aligned} & \sum_i (-1)^i \text{Tr}(\psi^* | \Gamma(X, \Lambda^i T_0^* \otimes E)) \\ &= \sum_\gamma l(\gamma) \sum_{k=1}^\infty \varepsilon_\gamma(k) \text{Tr}(\psi_x^{kl(\gamma)} | E_x) \delta_{kl(\gamma)} + \sum_x \varepsilon_x \left\langle \frac{\text{Tr}(\psi_x^t | E_x)}{1 - e^{\kappa_x t}} \right\rangle . \end{aligned} \tag{19}$$

Here an action  $\psi^t : \phi^{t*} T_0^* \rightarrow T_0^*$  is given by  $\psi_x^t = (T_x \phi^t)^* : T_{0\phi^t(x)}^* \rightarrow T_{0x}^*$ . Together with the action on  $E$  we get an action opposite to  $\phi$  on every  $\Lambda^i T_0^* \otimes E$ . In order to proceed we next assume that  $E$  carries a flat connection along the leaves

$$\delta_0 : \mathcal{E} \longrightarrow T_0^* \otimes \mathcal{E} ,$$

where  $\mathcal{E}$  and  $T_0$  are the sheaves of smooth sections of  $E$  and  $T_0$ . It gives rise to a fine resolution

$$\mathcal{E} \xrightarrow{\delta_0} T_0^* \otimes \mathcal{E} \xrightarrow{\delta_0} \Lambda^2 T_0^* \otimes \mathcal{E} \longrightarrow \dots$$

of the sheaf

$$\mathcal{F} = \text{Ker} (\delta_0 : \mathcal{E} \longrightarrow T_0^* \otimes \mathcal{E})$$

of smooth sections of  $\mathcal{E}$  which are constant along the leaves of the foliation. For the trivial bundle  $E = X \times \mathbb{R}$  with its canonical  $T_0$ -connection we obtain the sheaf

$\mathcal{R}$  of smooth real valued functions on  $X$  which are constant along the leaves. Note that  $\mathcal{F}$  carries a canonical action

$$\psi^t : (\phi^t)^{-1}\mathcal{F} \longrightarrow \mathcal{F}$$

opposite to  $\phi^t$  which is used to define a map on cohomology by composition:

$$\psi^{t*} : H^i(X, \mathcal{F}) \xrightarrow{(\phi^t)^{-1}} H^i(X, (\phi^t)^{-1}\mathcal{F}) \xrightarrow{\psi^t} H^i(X, \mathcal{F}).$$

Then the canonical isomorphism:

$$H^i(X, \mathcal{F}) = H^i((\Gamma(X, \Lambda^\bullet \mathcal{T}_0^* \otimes \mathcal{E}), \delta_0))$$

becomes equivariant under the induced action of the flow and one might hope to replace the alternating sum in (19) by an alternating sum over traces on cohomology.

On the other hand the differential  $\delta_0$  will not have closed image in general, so that the cohomology spaces will not even be Hausdorff [H] 2.1. Let  $\overline{H}^i(X, \mathcal{F})$  be the maximal Hausdorff quotient of  $H^i(X, \mathcal{F})$ , the *reduced* leafwise cohomology. It seems reasonable to expect a dynamical trace formula of the form

$$\begin{aligned} & \sum_i (-1)^i \text{Tr}(\psi^* | \overline{H}^i(X, \mathcal{F})) \\ &= \sum_\gamma l(\gamma) \sum_{k=1}^{\infty} \varepsilon_\gamma(k) \text{Tr}(\psi_x^{kl(\gamma)} | E_x) \delta_{kl(\gamma)} + \sum_x \varepsilon_x \left\langle \frac{\text{Tr}(\psi_x^t | E_x)}{1 - e^{\kappa_x t}} \right\rangle. \end{aligned} \tag{20}$$

Note that for the trivial bundle  $E = X \times \mathbb{R}$  we would get

$$\sum_i (-1)^i \text{Tr}(\psi^* | \overline{H}^i(X, \mathcal{R})) = \sum_\gamma l(\gamma) \sum_{k=1}^{\infty} \varepsilon_\gamma(k) \delta_{kl(\gamma)} + \sum_x \varepsilon_x \langle (1 - e^{\kappa_x t})^{-1} \rangle. \tag{21}$$

For the geodesic flow on the sphere bundle of cocompact quotients of rank one symmetric spaces and the stable foliation, analogous formulas are consistent with the Selberg trace formula, as has been shown by Guillemin [G], Patterson [P] and later workers, e.g. Juhl, Schubert, Bunke, Olbrich and Deitmar. Strictly speaking in these investigations  $\overline{H}^i(X, \mathcal{F})$  is replaced by a sum of representations suggested by this cohomology.

If  $X$  is the suspension of a diffeomorphism on a compact manifold  $M$ , the leafwise cohomologies turn out to be Hausdorff and hence Fréchet spaces, and (20) holds with the straightforward definition of a distributional trace given in (4). This consequence of the ordinary Lefschetz trace formula seems to be well known. A proof is written up in [D7] § 3.

Apart from these cases which do not involve stationary points the formula (20) does not seem to be established. One of the main problems is of course the definition of a good trace on the cohomology spaces  $\overline{H}^i(X, \mathcal{F})$  these being infinite dimensional

in general [AH]. Even if all of the  $\overline{H}^i(X, \mathcal{F})$  are finite dimensional, (20) does not seem to be known. However it appears that at least for Riemannian foliations something can be done using the recent Hodge theorem of Alvarez-Gomez and Kordyukov for leafwise cohomology. In this case there is also a Hodge  $*$ -operator on cohomology which is induced by the metrics on the leaves.

Let  $U$  be the dynamical system obtained by removing all the leaves containing stationary points. Then a trace formula of the form

$$\sum_i (-1)^i \text{Tr}(\psi^* | \overline{H}_c^i(U, \mathcal{F})) = \sum_\gamma l(\gamma) \sum_{k=1}^{\infty} \varepsilon_\gamma(k) \text{Tr}(\psi_x^{kl(\gamma)} | E_x) \delta_{kl(\gamma)}$$

is expected. For  $E = U \times \mathbb{R}$  in particular we should have

$$\sum_i (-1)^i \text{Tr}(\psi^* | \overline{H}_c^i(U, \mathcal{R})) = \sum_\gamma l(\gamma) \sum_{k=1}^{\infty} \varepsilon_\gamma(k) \delta_{kl(\gamma)}. \quad (22)$$

It seems to be quite a challenge to establish such dynamical trace formulas in any generality and also for more general foliations. This would also be a major contribution to the theory of periodic solutions of ordinary differential equations.

Given a closed orbit  $\gamma$  and a point  $x$  on  $\gamma$  consider the isomorphism

$$\overline{\gamma} = (\gamma, x) : \mathbb{R}/l(\gamma)\mathbb{Z} \xrightarrow{\sim} \gamma, \quad \bar{t} \mapsto \phi^t(x).$$

The functor

$$\mathcal{F} \mapsto \mathcal{F}_{\overline{\gamma}} = \Gamma(\mathbb{R}/l(\gamma)\mathbb{Z}, \overline{\gamma}^{-1}\mathcal{F})$$

from  $\mathcal{R}$ -modules to  $C^\infty(\mathbb{R}/l(\gamma)\mathbb{Z})$ -modules is exact [D7] 3.22. We view  $\mathcal{F}_{\overline{\gamma}}$  as the stalk of  $\mathcal{F}$  in the “geometric point”  $x$  of  $\gamma$ . The Poisson summation formula implies that

$$\text{Tr}(\psi^* | \mathcal{F}_{\overline{\gamma}})_{\text{dis}} = l(\gamma) \sum_{k=1}^{\infty} \text{Tr}(\psi_x^{kl(\gamma)} | E_x) \delta_{kl(\gamma)}.$$

For a stationary point  $x$  a suitable interpretation of the trace on  $\mathcal{F}_x$  gives:

$$\text{Tr}(\psi^* | \mathcal{F}_x)_{\text{dis}} = \left\langle \frac{\text{Tr}(\psi_x^t | E_x)}{1 - e^{\kappa_x t}} \right\rangle \quad \text{c.f. [D8]}.$$

Thus the right hand side of the trace formulas can be rewritten in more sheaf theoretical terms as the sum of distributional traces of the flow on the stalks of  $\mathcal{F}$  in the compact orbits of the flow. Incidentally, note that our former ring  $\mathcal{R}_p$  is just the dense subalgebra of finite Fourier series in  $C^\infty(\mathbb{R}/(\log p)\mathbb{Z})$ .

Formula (21) resp. (22) resembles the cohomological version of the explicit formulas for the Riemann zeta function (5) resp. for the Hasse Weil zeta function (10). However, as we will see, the setting of this section and in particular the assumption that we are dealing with compact manifolds is too restrictive for the goal of realizing (5) and (10) as special cases of (21) and (22). Nonetheless

we are led to expect the following structures on the searched for dynamical systems (“ $\text{Spec } \mathbb{Z}$ ”,  $\phi^t$ ) and (“ $\mathcal{X}$ ”,  $\phi^t$ ) corresponding to  $\text{Spec } \mathbb{Z}$  resp. the algebraic scheme  $\mathcal{X}/\mathbb{Z}$ . The space “ $\text{Spec } \mathbb{Z}$ ”, whatever its nature, infinite dimensional, a Grothendieck topology, ..., should have some compactness property. The closed orbits  $\gamma$  should correspond to the prime numbers such that  $l(\gamma) = \log p$  if  $\gamma \hat{=} p$ . More generally on “ $\mathcal{X}$ ” they should correspond to the closed points of  $\mathcal{X}$  with  $l(\gamma) = \log N(x)$  if  $\gamma \hat{=} x$ . On “ $\text{Spec } \mathbb{Z}$ ” there should be a stationary point  $x_\infty$  corresponding to the infinite prime  $p = \infty$ . All these compact orbits must appear with positive sign in the dynamical trace formulas. Of course there could also be more periodic orbits and stationary points if their contributions in the trace formula vanish because of opposite signs.

There are to be one-codimensional foliations on “ $\text{Spec } \mathbb{Z}$ ” and “ $\mathcal{X}$ ” such that the open subset of points where the leaf is transversal to the flow contains all periodic orbits. Moreover  $\kappa_{x_\infty} = -2$ , i.e.  $T_{x_\infty} \phi^t$  operates on  $T_{x_\infty}/T_{0x_\infty}$  by multiplication with  $e^{-2t}$ .

The cohomologies conjectured in section two should be the dense spaces of smooth vectors in the corresponding reduced leafwise cohomologies. Here a vector is smooth if it is contained in the sum of generalized eigenspaces of the induced flow on cohomology.

The leaves on “ $\text{Spec } \mathbb{Z}$ ” (resp. “ $\mathcal{X}$ ”) should be two (resp.  $2 \dim \mathcal{X}$ ) dimensional in a suitable sense since for foliated manifolds  $H^i(X, \mathcal{R}) = 0$  for  $i > d$  where  $d$  is the dimension of the leaves, and  $\overline{H}^d(X, \mathcal{R}) \neq 0$  if there exists a non trivial holonomy invariant current on  $X$ . Thus “ $\text{Spec } \mathbb{Z}$ ” (resp. “ $\mathcal{X}$ ”) should have dimension three (resp.  $2 \dim \mathcal{X} + 1$ ) in that sense. These dimensions agree with the étale cohomological dimensions of  $\text{Spec } \mathbb{Z}$  (resp.  $\mathcal{X}$ ).

As for the structure of “ $\overline{\mathcal{X}}$ ” \ “ $\mathcal{X}$ ” possibly the set of stationary points of the flow on “ $\overline{\mathcal{X}}$ ” is  $\mathcal{X}_\infty(\mathbb{C})/\langle F_\infty \rangle$ , where  $F_\infty$  is complex conjugation. This would generalize what we expect for  $\mathcal{X} = \text{Spec } \mathbb{Z}$  and more generally for  $\mathcal{X} = \text{Spec } \mathfrak{o}_k$ . Note also that the set of closed points of  $\mathcal{X}$  over  $p$  can be identified with the set  $\mathcal{X}_p(\overline{\mathbb{F}}_p)/\langle \text{Fr}_p \rangle$  of Frobenius orbits on  $\mathcal{X}_p(\overline{\mathbb{F}}_p)$ , where  $\mathcal{X}_p = \mathcal{X} \otimes \mathbb{F}_p$ .

We now discuss the basic theory of flows with an integrable invariant complement. This is relevant for us since they appear as subsystems in the above. Let us define an  $F$ -flow  $\phi^t$  to consist of a (Banach-)manifold  $U$  with a flow generated by a smooth vector field which exists for all positive but possibly not for all negative times. By definition an  $F$ -system is an  $F$ -flow with a one-codimensional foliation  $T_0$  which is everywhere transversal to the flow. In particular there are no fixed points. These systems form a category in an obvious way. Their theory is essentially well known and recalled for example in [D7] §3. The foliation corresponds uniquely to a closed flow-invariant one form  $\omega_\phi$  with  $\langle \omega_\phi, Y_\phi \rangle = 1$ , via  $\ker \omega_\phi = T_0$ . The period group  $\Lambda \subset \mathbb{R}$  is defined as the image of the length homomorphism

$$l : \pi_1^{\text{ab}}(U) \longrightarrow \mathbb{R} \quad , \quad l(c) = \int_c \omega_\phi .$$

If there is a morphism  $U \rightarrow U'$  of  $F$ -systems then  $\Lambda_U \subset \Lambda_{U'}$ . Periodic orbits  $\gamma$  give well defined elements  $[\gamma]$  of  $\pi_1^{\text{ab}}(U)$  and one has  $l([\gamma]) = l(\gamma)$ , the length of  $\gamma$ .

For a variety  $V/\mathbb{F}_q$  there is an analogous map

$$l : \hat{\pi}_1^{\text{ab}}(V) \longrightarrow \hat{\pi}_1(\text{Spec } \mathbb{F}_q) = \hat{\mathbb{Z}}$$

induced by the projection  $V \rightarrow \text{Spec } \mathbb{F}_q$ . Closed points  $x$  of  $V$  give Frobenius conjugacy classes and hence well defined elements  $[F_x]$  of  $\hat{\pi}_1^{\text{ab}}(V)$ . They satisfy the equation  $l([F_x]) = \deg x = \log_q N(x)$ .

On an  $F$ -system the following three categories are equivalent:

- vector bundles  $E$  with a flat  $T_0$ -connection  $\delta_0$  and a compatible action  $\psi$  which is opposite to  $\phi$ ;
- locally free  $\mathcal{R}$ -modules  $\mathcal{F}$  with an action  $\psi$  opposite to  $\phi$ ;
- local systems  $F$  of  $\mathbb{R}$ -vector spaces.

Here  $\mathcal{E} \leftrightarrow \mathcal{F} = \text{Ker}(\delta_0 : \mathcal{E} \rightarrow \mathcal{T}_0^* \otimes \mathcal{E}) \leftrightarrow F = \text{Ker}(\Theta_{\mathcal{F}} : \mathcal{F} \rightarrow \mathcal{F})$ , where  $\Theta_{\mathcal{F}} : \mathcal{F} \rightarrow \mathcal{F}$  is the derivative of  $\psi$  at  $t = 0$ . Let  $\alpha$  be a real number. To the twist  $\mathcal{F}(\alpha)$ , defined as  $\mathcal{F}$  with action  $\psi_{\mathcal{F}(\alpha)}^t = e^{-t\alpha}\psi_{\mathcal{F}}^t$ , there corresponds a local system  $F(\alpha)$ . For  $\mathcal{F} = \mathcal{R}$  it is denoted  $\mathbb{R}(\alpha)$ . Its monodromy representation is  $\exp(\alpha l)$ . Hence  $\Lambda \subset \log \mathbb{Q}_+^*$  if and only if there is a local system  $\underline{\mathbb{Q}}(1)$  of  $\mathbb{Q}$ -vector spaces such that  $\underline{\mathbb{R}}(1) = \underline{\mathbb{Q}}(1) \otimes \mathbb{R}$ .

If we complexify we get analogous equivalences of categories.

There is an exact sequence

$$0 \longrightarrow H^{i-1}(U, \mathcal{F})/\text{Im } \Theta \longrightarrow H^i(U, F) \longrightarrow H^i(U, \mathcal{F})^{\Theta=0} \longrightarrow 0$$

where  $\Theta = (\Theta_{\mathcal{F}})_*$ . This is analogous to the exact sequence

$$0 \longrightarrow H^{i-1}(\overline{V}, \overline{F})_{\text{Fr}_q} \longrightarrow H^i(V, F) \longrightarrow H^i(\overline{V}, \overline{F})^{\text{Fr}_q} \longrightarrow 0$$

for a  $\mathbb{Q}_l$ -sheaf  $F$  on  $V$  where  $\overline{V} = V \otimes \overline{\mathbb{F}_q}$ . In the language of arithmetic geometry,  $H^*(U, F)$  is the arithmetic cohomology and  $H^*(U, \mathcal{F})$  with its action of the flow the geometric cohomology. As usual the latter commutes with twists but not the former.

There is a classification theorem: Every  $F$ -system is canonically contained as an open subsystem in a complete such system, i.e. one where the flow exists for all times in  $\mathbb{R}$ ; c.f. [D8]. All complete connected  $F$ -systems are obtained as follows: Let  $M$  be any leaf of  $U$ . Then  $M$  is connected and  $\Lambda = \{t \in \mathbb{R} \mid \phi^t(M) = M\}$  so that  $\Lambda$  operates on  $M$ . The system  $U$  is then isomorphic to the suspension  $M \times_{\Lambda} \mathbb{R}$  where  $\Lambda$  acts on  $\mathbb{R}$  by translation and the foliation is by the images of  $M \times \{t\}$  for  $t$  in  $\mathbb{R}$ .

### 5 FURTHER COMPARISON

For “Spec  $\mathbb{Z}$ ” the period group  $\Lambda$  must contain the numbers  $\log p$  as they should be lengths of closed orbits. Hence  $\Lambda \supset \log \mathbb{Q}_+^*$ . On the other hand  $\underline{\mathbb{R}}(1)$  will have a rational structure (see below) and hence  $\Lambda \subset \log \mathbb{Q}_+^*$ , so that  $\Lambda = \log \mathbb{Q}_+^*$ . Writing

the flow multiplicatively we therefore expect “Spec  $\mathbb{Z}$ ”, if its flow is complete, to have the form  $M \times_{\mathbb{Q}_+^*} \mathbb{R}_+^*$  for some “space” with  $\mathbb{Q}_+^*$ -action  $M$  reminiscent of the idèlic picture. A similar argument for varieties  $V/\mathbb{F}_q$  with a rational point suggests that “ $V$ ”  $\cong N \times_{q^z} \mathbb{R}_+^*$ .

As mentioned above, the leafwise cohomology of “ $V$ ” should be isomorphic to a theory constructed from the  $\mathbb{Q}_l$ -cohomology of  $\bar{V}$  after the choice of an embedding  $\mathbb{Q}_l \subset \mathbb{C}$ . Comparing the kernels of  $\Theta$ , it follows on combining [D3] (2.4) and §4 with [D7] (3.19) that the singular cohomology of  $N$  with  $\mathbb{C}$ -coefficients, endowed with the automorphism  $q^*$ , must be isomorphic to  $H^*(\bar{V}, \mathbb{Q}_l) \otimes \mathbb{C}$  with  $\text{Fr}_q^*$ -action. It follows that  $H^d(N, \mathbb{Z})$ , where  $d = \dim N$ , must be a  $\mathbb{Z}[q^{-1}]$ -module, since  $\text{Fr}_q^*$  acts by multiplication with  $q^d$  on  $H^d(\bar{V}, \mathbb{Q}_l)$ .

The natural way to obtain such  $N$  is to take a compact manifold  $\tilde{N}$  with a finite map  $q : \tilde{N} \rightarrow \tilde{N}$  of degree  $q$  and set  $N = \varprojlim (\dots \rightarrow \tilde{N} \xrightarrow{q} \tilde{N} \rightarrow \dots)$ . Note the continuity theorems for cohomology in this regard, c.f. [Br] II.14. The most naive way to obtain  $(\tilde{N}, q)$  would be by lifting  $(V, \text{Fr}_q)$  to  $\mathbb{C}$ . For cellular varieties and ordinary abelian varieties over  $\mathbb{F}_q$  this is possible but of course not in general.

It seems possible that in the above isomorphism “Spec  $\mathbb{Z}$ ”  $\cong M \times_{\mathbb{Q}_+^*} \mathbb{R}_+^*$  the leaf  $M$  is obtained from a “space”  $\tilde{M}$  with commuting operators for every prime number  $p$ , by an analogous projective limit. This puts  $M \times_{\mathbb{Q}_+^*} \mathbb{R}_+^*$  even closer to the idèlic view point.

Allowing such more general spaces removes a difference between dynamical trace formulas and explicit formulas in cohomological form: Both can be extended to test functions on  $\mathbb{R}^*$ , but whereas for compact manifolds the former become symmetric under  $t \leftrightarrow -t$ , the latter exhibit a twisted symmetry. A closely related point is this: For a finite dimensional  $F$ -system the flow acts with weight zero on the top leafwise reduced cohomology with compact supports. This follows by looking at the invariant currents and noting that automorphisms act by  $\pm 1$  on top compactly supported cohomology with  $\mathbb{Z}$ -coefficients. Since we want weights different from zero, e.g. equal to one for Spec  $\mathbb{Z}$ , we are forced to allow more general spaces than finite dimensional manifolds as leaves. For ordinary abelian varieties over  $\mathbb{F}_p$  the theory of the zeta function can in fact be established dynamically using pro-manifolds but in general – at least in characteristic  $p$  – even pro-manifolds as leaves are not the right kind of space.

If the association from schemes to foliated dynamical systems is functorial one has a natural construction of sheaves  $\mathcal{F}(M)$  for any motive  $M$ . For a variety  $\pi : X_0 \rightarrow \text{Spec } \mathbb{Q}$  let  $\pi = “\pi” : X = “X_0” \rightarrow “\text{Spec } \mathbb{Q}”$  be the associated morphism of foliated dynamical systems. The functors

$$X_0 \longmapsto R^i \pi_* (\mathcal{R}_X) \quad \text{and} \quad X_0 \longmapsto R^i \pi_* (\mathbb{R}_X)$$

define cohomology theories which by universality factor over the category of motives. They are denoted  $M \mapsto \mathcal{G}(M)$  and  $M \mapsto G(M)$ . The morphism  $j_0 : \text{Spec } \mathbb{Q} \rightarrow \text{Spec } \mathbb{Z}$  will induce a morphism  $j = “j_0”$  of dynamical systems and we get functors  $\mathcal{F} = j_* \circ \mathcal{G}$  and  $F = j_* \circ G$ . The two constructions are related by  $F = \text{Ker}(\Theta : \mathcal{F} \rightarrow \mathcal{F})$ . Moreover  $F$  has a natural  $\mathbb{Q}$ -structure  $F_{\mathbb{Q}}$  obtained by starting with rational coefficients. In fact over “Spec  $\mathbb{Z}_S$ ”, where  $S$  is a finite or

cofinite set of prime numbers, we should get a  $\mathbb{Z}[l^{-1} \mid l \notin S]$ -structure on  $F$  by taking  $\mathbb{Z}_X$ -coefficients<sup>2</sup> above. For  $n \in \mathbb{Z}$ , we get  $\mathcal{F}(\mathbb{Q}(n)) = \mathcal{R}(n)$ ,  $F(\mathbb{Q}(n)) = \mathbb{R}(n)$  and  $F_{\mathbb{Q}}(\mathbb{Q}(1))$  provides the rational structure on  $\mathbb{R}(1)$  alluded to above.

Comparing formulas (18) and (20) over “Spec  $\mathbb{Z}_S$ ”, we see that the semisimplifications of  $(M_l^{I_p}, \text{Fr}_p)$  and  $(E_x, \psi_x^{\log p})$  for  $x \in \gamma \cong p \notin S$  should be isomorphic. Since  $E$  is a vector bundle the dimensions of  $M_l^{I_p}$  must be constant, i.e.  $M$  must have good reduction at the finite primes  $p \notin S$ . Note that via the equivalence of categories above,  $(E_x, \psi_x^{\log p})$  is isomorphic to  $F_x$  with its monodromy representation along  $\gamma$ . The rational structure  $F_{\mathbb{Q},x}$  on  $F_x$  thus implies that the characteristic polynomial of the monodromy representation has rational coefficients. The same must therefore hold for the Frobenius action on  $M_l$  if our picture is correct. This is well known for many motives by the work of Deligne and conjectured in general.

We now reinterpret part of (2.1) 5. as a fully faithfulness assertion. For finite  $S$  consider a motive  $M$  over  $\mathbb{Q}$  with good reduction outside of  $S$ . Using the expected isomorphism (15) over Spec  $\mathbb{Z}_S$  we get a commutative diagram

$$\begin{CD} \text{Hom}(\mathbb{Q}(0), M) \otimes \mathbb{R} @>{\mathcal{F}}>> H^0(\text{“Spec } \mathbb{Z}_S\text{”}, \mathcal{F}(M))^{\Theta \sim 0} \\ @V{F}VV @A{\uparrow}A \\ H^0(\text{“Spec } \mathbb{Z}_S\text{”}, F(M)) @>{\sim}>> H^0(\text{“Spec } \mathbb{Z}_S\text{”}, \mathcal{F}(M))^{\Theta \sim 0}, \end{CD}$$

noting that  $H^0$  is Hausdorff. Hence all arrows must be isomorphisms. Replacing  $M$  by  $M_1^* \otimes M_2$ , it follows that the exact tensor functor  $F_{\mathbb{Q}}$  from motives with good reduction on Spec  $\mathbb{Z}_S$  to  $\mathbb{Q}$ -local systems on “Spec  $\mathbb{Z}_S$ ”, must be fully faithful. The map induced by Tannakian duality fits very nicely into a diagram comparing topological fundamental groups and Galois groups of number fields, see [D7] (42).

The constructions in the real manifold setting of section three, even if we allow infinite-dimensional or pro-manifolds, always lead to sheaves of real vector spaces  $\mathcal{F}$ . On the other hand the spaces  $\mathcal{F}_p(M)$  are by construction ([D3] §3) complex vector spaces with no evident real structure. For motives over  $\mathbb{Q}$  this is not a contradiction, but the analogue for motives over finite fields is impossible. This is so because the functors  $F_x$  would give exact faithful tensor functors into  $\mathbb{R}$ -vector spaces which are known not to exist. On the other hand on the subcategory of ordinary motives over finite fields the predictions of the dynamical formalism work out correctly by a result of Deligne, see [D7] 4.7.

CONCLUSION

Apart from stating his famous conjectures on zeta functions, A. Weil also explained how they could be attacked given a cohomology theory for varieties in characteristic  $p$  with properties similar to those of singular cohomology. For varieties over number fields the analogues of the Weil conjectures and further conjectures have by now been checked in numerous cases except for the Riemann conjecture 2.1 part 4 of course. In this article we have outlined a strategy to approach them. This program requires a cohomology theory for algebraic schemes over the integers

---

<sup>2</sup>This is not a misprint.

with properties similar to those of the reduced leafwise cohomology of a class of dynamical systems with one-codimensional foliations by pro-manifolds.

## REFERENCES

- [AH] J.A. Alvarez Lopez, S. Hurder, Pure-point spectrum for foliation geometric operators, preprint 1995
- [B] M. Berry, Riemann's zeta function: a model of quantum chaos, Lecture Notes in Physics 263, Springer 1986
- [Br] G. Bredon, Sheaf theory. Springer 1997
- [BK] S. Bloch, K. Kato,  $L$ -functions and Tamagawa numbers of motives. (Grothendieck Festschrift I) 333–400, Birkhäuser 1991
- [CV] P. Cartier, A. Voros, Une nouvelle interprétation de la formule des traces de Selberg, (Grothendieck Festschrift II) 1–67, Birkhäuser 1991
- [C] A. Connes, Formule de trace en géométrie non-commutative et hypothèse de Riemann. C.R. Acad. Sci. 323 (1996), 1231–1236
- [Cons] K. Consani, Double complexes and Euler  $L$ -factors, Compos. Math. 111 (1998), 323–358
- [De] P. Deligne, La conjecture de Weil I. Inst. Hautes Études Sci. Publ. Math. 43 (1974), 273–307
- [D1] C. Deninger, On the  $\Gamma$ -factors attached to motives. Invent. Math. 104 (1991), 245–261
- [D2] C. Deninger, Local  $L$ -factors of motives and regularized determinants. Invent. Math. 107 (1992), 135–150
- [D3] C. Deninger, Motivic  $L$ -functions and regularized determinants. Proc. Symp. Pure Math. 55, 1 (1994), 707–743
- [D4] C. Deninger, Motivic  $L$ -functions and regularized determinants II. In: F. Catanese (ed.), Arithmetic Geometry, Cortona, 1994, Symp. Math. 37, 138–156, Cambridge Univ. Press 1997
- [D5] C. Deninger, Lefschetz trace formulas and explicit formulas in analytic number theory. J. Reine Angew. Math. 441 (1993), 1–15
- [D6] C. Deninger, Motivic  $\varepsilon$ -factors at infinity and regularized dimensions. Indag. Math., N.S. 5 (4), (1994), 403–409
- [D7] C. Deninger, On Dynamical systems and their Possible Significance for Arithmetic Geometry. To appear in a conference proceedings on regulators
- [D8] C. Deninger, On Dynamical systems and their Possible Significance for Arithmetic Geometry II. In preparation
- [DN] C. Deninger, E. Nart, On  $\text{Ext}^2$  of motives over arithmetic curves. Amer. J. of Math. 117 (1995), 601–625
- [DSch] C. Deninger, M. Schröter, A distribution theoretic interpretation of Guinand's functional equation for Cramér's  $V$ -function and generalizations. J. London Math. Soc. (2) 52 (1995) 48–60
- [F-PR] J-M. Fontaine, B. Perrin-Riou, Autour des conjectures de Bloch et Kato, cohomologie galoisienne et valeurs de fonctions  $L$ , Proc. Symp. Pure Math. 55, 1 (1994), 599–706
- [Go] C. Godbillon, Feuilletages, Etudes géométriques. Progress in Math. 98, Birkhäuser 1991



- [G] V. Guillemin, Lectures on spectral theory of elliptic operators. Duke Math. J. 44 (1977), 485–517
- [GS] V. Guillemin, S. Sternberg, Geometric asymptotics, Math. Surveys 14, Amer. Math. Soc., Providence, R.I. 1977
- [H] A. Haefliger, Some remarks on foliations with minimal leaves. J. Diff. Geo. 15 (1980), 269–284
- [HW] A. Huber, J. Wildeshaus, Classical motivic polylogarithm according to Beilinson and Deligne, Doc. Math. J. DMV 3 (1998) 27–133
- [I] G. Illies, Regularisierte Produkte, Spurformeln und Cramér-Funktionen, Schriftenreihe des Mathematischen Instituts der Univ. Münster, 3. Serie, Heft 22, 1998
- [J] U. Jannsen, Mixed motives, motivic cohomology, and Ext-groups. Proc. ICM Zürich 1994, pp. 667–679, Birkhäuser 1995
- [JL] J. Jorgenson, S. Lang, Explicit formulas and regularized products, Lecture Notes in Mathematics 1593, Springer 1994
- [K] N. Kurokawa, Parabolic components of zeta function. Proc. Japan Acad. Ser. A64 (1988) 21–24
- [P] S.J. Patterson, On Ruelle’s zeta function. Israel Math. Conf. Proc. 3 (1990), 163–184
- [S] T. Saito, The sign of the functional equation of the  $L$ -function of an orthogonal motive. Invent. Math. 120 (1995), 119–142
- [Sa] P. Sarnak, Quantum Chaos, Symmetry and Zeta Functions, Lecture I: Quantum Chaos, Lecture II: Zeta Functions, Curr. Dev. Math. 84–115, International Press 1997
- [Sch] A.J. Scholl, Height pairings and special values of  $L$ -functions. Proc. Symp. Pure Math. 55, 1 (1994), 571–598
- [SchS] M. Schröter, C. Soulé, On a result of Deninger concerning Riemann’s zeta function, Proc. Sympos. Pure Math. 55 (1994), 745–747
- [Se] J-P. Serre, Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures), Sémin. Delange-Pisot-Poitou, exp. 19 (1969/70)
- [So] C. Soulé,  $K$ -théorie et zéros aux points entiers de fonctions zêta, Proc. ICM, Warsaw, 1983, pp. 437–445

Christopher Deninger  
Mathematisches Institut  
Westf. Wilhelms-Universität  
Einsteinstr. 62  
48149 Münster  
deninge@math.uni-muenster.de

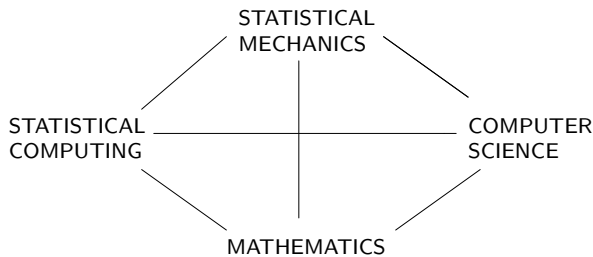
FROM SHUFFLING CARDS  
TO WALKING AROUND THE BUILDING:  
AN INTRODUCTION TO MODERN MARKOV CHAIN THEORY

PERSI DIACONIS

ABSTRACT. This paper surveys recent progress in the classical subject of Markov chains. Sharp rates of convergence are available for many chains. Examples include shuffling cards, a variety of simulation procedures used in physics and statistical work, and random walk on the chambers of a building. The techniques used are a combination of tools from geometry, PDE, group theory and probability.

0 INTRODUCTION

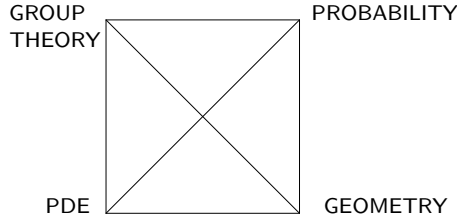
The classical subject of Markov chains has seen spectacular progress in the past ten years. Progress is seen through theoretical advances and practical applications. These may be roughly depicted as the interactions between:



Briefly, Markov chain Monte Carlo is a mainstay of the computational side of statistical mechanics. There, one wants to draw samples from probability measures on high dimensional state spaces (e.g., the Ising model). One practical way to proceed is to run a fancy kind of random walk (the Metropolis algorithm or Glauber dynamics) [50] which reaches equilibrium at the desired measure. Similar procedures have created a revolution in the computational side of statistics (the Gibbs sampler)[22], [40]. In theoretical computer science, a slew of intractable problems (#-p-complete) problems like computing the permanent of a matrix or

the volume of a convex polyhedron) have provably accurate approximations in polynomial time because simple Markov chains can be constructed and proved to converge rapidly [58]. All of this rests on new mathematical developments.

The new mathematics uses ideas from diverse areas.



Probabilistically, new ideas like coupling [48] and stopping time techniques [3], [19] give ‘pure thought’ solutions to previously intractable problems. Techniques from PDE and spectral geometry allow bounds on the eigenvalues of the basic operators in terms of the geometry of the underlying chain (bottleneck measures, discrete curvatures, and volume growth). Comparison techniques allow study of a chain of interest by comparison with a neat chain which can be analyzed through group representations. The various areas interact so there are probabilistic proofs of results in classical geometry and group theory and vice versa.

The present paper offers a thread through this maze by following the development of a single example: mixing  $n$  cards by repeatedly removing the top card and inserting it at random.

The example is studied in Section 1 which introduces basic notation, shows what a theorem in the subject looks like, and proves that  $n \log n$  shuffles suffice to mix up  $n$  cards. Thus, when  $n = 52$ , about 200 shuffles are necessary and suffice. The argument introduces coupling arguments and shows that the underlying non self adjoint operators are explicitly diagonalizable. Section 2 offers a variety of extensions where a similar analysis obtains. These include the usual method of shuffling cards. Section 3 extends things to random walk on the chambers of a hyperplane arrangement and then to walks on the chambers of a building. These examples show an intimate connection between probability, algebra, and geometry.

Section 4 gives pointers to many topics not covered, a brief example of the geometric theory of Markov chains (again applied to shuffling cards), some open problems, and a beginner’s guide to the literature.

## 1 SOME MARKOV CHAINS ON PERMUTATIONS.

### 1.1 THE TSETLIN LIBRARY.

Picture a pile of file-folders which are used from time to time. The  $i^{\text{th}}$  folder is used with weight  $w_i$  with  $w_i > 0$ ,  $w_1 + \cdots + w_n = 1$ . It is natural to want frequently used folders near the top. A scheme which achieves this, even if the  $w_i$  are unknown, is simply to replace the most recently used folder on top. To put this into a mathematical framework, label the folders  $1, 2, \dots, n$  and let an

arrangement of these labels be denoted by a permutation  $\sigma$  say with  $\sigma(i)$  the label at position  $i$ . Moving folder  $i$  to the top changes  $\sigma$  by a cycle  $(1, 2 \cdots \sigma^{-1}(i))$ . The chance of moving from  $\sigma$  to  $\zeta$  in one step is

$$K(\sigma, \zeta) = \begin{cases} w_i & \text{if } \zeta = (1, 2 \cdots \sigma^{-1}(i)) \sigma \\ 0 & \text{otherwise.} \end{cases} \tag{1.1}$$

It helps some of us to think of  $K(\sigma, \zeta)$  as the  $(\sigma, \zeta)$  entry of an  $n!$  by  $n!$  matrix. Then, making repeated moves is represented by matrix multiplication. Thus, the chance of going from  $\sigma$  to  $\zeta$  in two steps is

$$K^2(\sigma, \zeta) = \sum_{\eta} K(\sigma, \eta) K(\eta, \zeta)$$

After all, to get from  $\sigma$  to  $\zeta$ , one must go to some possible  $\eta$  and then from  $\eta$  to  $\zeta$ . Similarly,  $K^l(\sigma, \zeta)$  is defined.

A matrix of form (1.1) with  $K(\sigma, \zeta) \geq 0$ ,  $\sum_{\zeta} K(\sigma, \zeta) = 1$  is called a stochastic matrix and the process of successive arrangements is called a Markov chain. The Peron-Frobenius theorem implies that under mild regularity conditions (connectedness and aperiodicity, satisfied in all examples here), such a Markov chain has a unique stationary distribution  $\pi(\sigma) > 0$ ,  $\sum_{\sigma \in S_n} \pi(\sigma) = 1$ . This is characterized as the unique left eigenvector of  $K$  with eigenvalue 1 (so  $\sum_{\sigma \in S_n} \pi(\sigma) K(\sigma, \zeta) = \pi(\zeta)$ ). It is also characterized by the limiting result as  $l$  tends to infinity

$$\lim K^l(\sigma, \zeta) = \pi(\zeta) \text{ for all } \sigma \tag{1.2}$$

Algebraically, this says that if the matrix  $K$  is raised to a high power, all the rows are approximately equal to  $\pi$ . Probabilistically, this says that for any starting state  $\sigma$ , after many steps, the chance that the chain is in state  $\zeta$  is approximately equal to  $\pi(\zeta)$ , no matter what the starting state is.

For the Tsetlin Library (1.1), the stationary distribution  $\pi$  is easy to describe. One description is “sample from the weights  $\{w_i\}$  without replacement.” That is, form a random permutation  $\sigma$  by choosing  $\sigma(1) = j$  with probability  $w_j$ . This first choice being made, delete weight  $w_{\sigma(1)}$ , renormalize the remaining weights to sum to one, and sample from these to determine  $\sigma(2)$ . Continuing in this way gives  $\sigma$ . Formally:

$$\pi(\sigma) = \frac{w_{\sigma_1}}{1 - w_{\sigma_1}} \frac{w_{\sigma_2}}{1 - w_{\sigma_1} - w_{\sigma_2}} \cdots \frac{w_{\sigma_{n-1}}}{1 - w_{\sigma_1} - \cdots - w_{\sigma_{n-2}}}. \tag{1.3}$$

This natural probability measure arises in dozens of applied contexts from psychophysical experiments (as the Luce model) to oil and gas exploration [17].

The standard way of quantifying the rate of convergence of  $K^l$  to  $\pi$  is to use the total variation distance; let  $K_\sigma^l(A) = \sum_{\zeta \in A} K^l(\sigma, \zeta)$ ,

$$\|K_\sigma^l - \pi\| = \max_{A \in \mathcal{S}_n} |K_\sigma^l(A) - \pi(A)| = \frac{1}{2} \sum_{\zeta \in \mathcal{S}_n} |K^l(\sigma, \zeta) - \pi(\zeta)|$$

These equalities are easily proved.

As an example of the kind of theorem that emerges, we show

**THEOREM 1.1.** *For the Tsetlin library chain (1.1)*

$$\|K_\sigma^l - \pi\| \leq \sum_{i=1}^n (1 - w_i)^l \tag{1.4}$$

*Remark 1.* Consider the simple case where all  $w_i = \frac{1}{n}$ . This gives a simple shuffling scheme: Cards are repeatedly removed at random and placed on top. This is the inverse of top to random described before (the rates are the same). The bound on the right side of (1.4) becomes  $n(1 - \frac{1}{n})^l$ . Using  $1 - x \leq e^{-x}$ , we see that when  $l = n(\log n + c)$  with  $c > 0$ ,  $\|K_\sigma^l - \pi\| \leq e^{-c}$ . It is not hard to see this is sharp: If  $l = n(\log n - c)$  with  $c > 0$  the distance to stationarity is essentially at its maximum value of 1. A graph of the distance to stationarity versus  $l$  appears in Figure 1. The limiting shape of this graph is derived in [19]. This shows an example of the cutoff phenomenon [17]. While the distance  $\|K^l - \pi\|$  is monotone decreasing in  $l$ , the transition from one to zero happens in a short interval centered at  $n \log n$ . In [17] similar cutoffs are proved for many other choices of weights, e.g.,  $w_i = \frac{c}{(i+1)^s}$ .

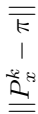


Figure 1: Distance to stationarity for top to random shuffle

*Proof of Theorem 1.1* The proof uses a coupling argument. Picture two decks of cards. The first starts in order  $1, 2, \dots, n$ . The second starts in random order drawn from the stationary distribution (1.2). At each time  $t = 1, 2, 3 \dots$  choose a label  $i$  with probability  $w_i$  and move card  $i$  to the top of both decks. Note that

this forces the two decks to be in the same order in the top positions. Once cards labeled  $i$  are in the same position in the two decks, they stay that way under further moves. It follows that the first time  $T$  that all indices have been chosen at least once, the two decks are in the same order. The second deck began in stationarity, and repeated moves preserve stationarity. Thus at time  $T$  the first deck is distributed in the stationary distribution.

The time  $T$  is called a coupling time [48]. It is easy to prove the formal bound

$$\|K_\sigma^l - \pi\| \leq P\{T > l\}.$$

A further simple argument shows  $P\{T > l\} \leq \sum (1 - w_i)^l$ . □

*Remark 2.* There is a large literature on the move to front scheme as a method of dynamic storage allocation. See [36].

*Remark 3.* The Markov chain (1.1) is not self-adjoint. Nonetheless, Phaterfod [52] shows that the matrix  $K$  has real eigenvalues  $\beta_s = \sum_{i \in S} w_i$  with multiplicity the number of permutations with fixed-point set  $S$ . Here  $S$  runs over subsets of  $[n] = \{1, 2, \dots, n\}$ . It is curious that we have no analytic tools to use these eigenvalues for deriving bounds such as (1.3).

## 2 MORE VIGOROUS SHUFFLES.

The Tsetlin library scheme can be varied by choosing a subset  $S \subset [N]$  with weight  $w_s$  and moving the folders with labels in  $S$  to the top, keeping them in the same relative order.

**THEOREM 2.1.** *Suppose the weights  $w_s$  separate in the sense that for every  $i$  and  $j$ ,  $w_s > 0$  for some  $s$  with  $i \in S, j \notin S$  or  $i \notin S, j \in S$ . Then the subset to top chain has a unique stationary distribution  $\pi$  and*

$$\|K_\sigma^l - \pi\| \leq \sum_{\substack{i \in S, j \notin S \\ j \in S, i \notin S}} (1 - w_s)^l$$

*Proof.* Theorem 2.1 is proved by the following coupling: Let  $T$  be the first time every pair of labels,  $i, j$  have been separated at least once. This is a coupling time and theorem 1.2 follows. □

*Remark 4.* Again, all the eigenvalues are real, known, and useless [9].

There is a special case of Theorem (2.1) that is of general interest. Suppose that all the weights  $\{w_s\}_s$  are equal to  $\frac{1}{2^n}$ . The shuffling scheme amounts to choosing a random subset and moving these labels to the top. The inverse process is the Gilbert-Shannon-Reeds (G-S-R) distribution for riffle shuffling ordinary playing cards. Here, one cuts off the top  $j$  cards with probability  $\binom{n}{j}/2^n$ . The top and

$l$	1	2	3	4	5	6	7	8	9	10
$\ K^l - \pi\ $	1.000	1.000	1.000	1.000	.924	.614	.334	.167	.085	.043

Table 1: Total variation distance after riffing 52 cards  $l$  times

bottom halves are riffled together according to the following scheme: At a given time, if one half has  $A$  cards, the second half has  $B$  cards, drop the next card from the first half with probability  $\frac{A}{A+B}$ . It is not hard to see these are inverse descriptions. The G-S-R distribution is quite a realistic description of the way real people shuffle real cards. Of course, in this case  $\pi(\sigma) = 1/n!$  is the uniform distribution.

The chance of separating  $i$  and  $j$  in one shuffle is evidently  $1/2$ . Thus the bound of theorem (1.2) is

$$\|K_\sigma^l - \pi\| \leq \binom{n}{2} \left(\frac{1}{2}\right)^l$$

The right side of this bound is small when  $l$  is larger than  $2 \log_2 n$ .

In joint work with David Bayer [8], more accurate estimates of the distance are derived. We prove the sharp result that  $\frac{3}{2} \log_2 n$  shuffles are necessary and suffice:

**THEOREM 2.2.** *For the G-S-R model of riffle shuffles, let  $l = \frac{3}{2} \log_2 n + c$ . Then*

$$\|K_\sigma^l - \pi\| = 1 - 2\Phi\left(\frac{-2^{-c}}{4\sqrt{3}}\right) + o\left(\frac{1}{\sqrt{n}}\right).$$

with  $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-t^2/2} dt$ .

When  $n = 52$  we derive the following exact result shown in Table 1 above.

Theory shows that the total variation distance continues to decrease by a power of 2 for larger  $l$ . Evidently, there is a sharp threshold centered at about seven shuffles. Theorem 2.2 says that for large  $n$ , a graph of total variation versus  $l$  looks like Figure 1 with a cutoff at  $3/2 \log_2 n$ .

Table 1 is derived from a simple closed form expression: The chance that the deck is in position  $\sigma$  after  $l$  shuffles equals  $\binom{2^l + n - d}{n} / 2^{nl}$  with  $d$  the number of descents in  $\sigma^{-1}$ . This close connection between descents and shuffling lends to new formulae in combinatorics—enumeration of permutations by descents and cycle structure [40], [23]. It is also closely connected to Hodge type decompositions for Hochschild homology [42]. This rich circle of interconnections feeds back into probability: While it takes  $\frac{3}{2} \log_2 n$  shuffles to make all aspects of a permutation match the uniform distribution, features depending on long cycles are essentially random after one shuffle.

As a final generalization, consider shuffling driven by a block ordered partition  $[B_1, B_2, \dots, B_k]$ . To shuffle, remove cards with labels in  $B_1$ , and place them on

top, keeping them in their same relative order. These are followed by cards with labels in  $B_2$ , and so on. Choosing weights for each block ordered partition leads to a shuffling scheme that includes the Tsetlin library (weight  $w_i$  on  $[i, [n] \setminus i]$ ) and the G-S-R model (weight  $1/2^n$  on  $[s, [n] \setminus s]$ ). These general shuffling schemes were suggested by Bidigare, Hanlon and Rockmore [9]. They permit an essentially complete analysis [12], [13]. As will be seen next, these shuffles too are a very special case of random walk on a hyperplane arrangement.

### 3 RANDOM WALKS ON THE CHAMBERS OF A HYPERPLANE ARRANGEMENT.

We work in  $\mathbb{R}^d$ . Let  $A = \{H_1, \dots, H_k\}$  be a finite collection of affine hyperplanes. These divide space into chambers  $C$  and faces  $F$ . For example, Fig. 2 shows three hyperplanes in  $\mathbb{R}^2$ .

Figure 2: 3 lines in the plane

There are seven chambers, nine half-line faces (one labeled  $F$ ), and three point faces. There is a natural action of faces on chambers denoted  $F * C$ : This is the unique chamber adjacent to  $F$  and closest to  $C$  (in the sense of crossing the fewest number of hyperplanes). For example, in Figure 2 the product of the chamber  $C$ , with the face  $F$  is the chamber  $F * C$ . This has distance two from  $C$ , while the other chamber adjacent to  $F$  is at distance three.

Bidigare, Hanlon, and Rockmore (B-H-R) [9] suggested choosing weights  $\{w_F\}$  and defining a random walk defined on  $C$  by repeatedly multiplying by faces drawn from these weights. They found the eigenvalues of these chains were positive sums of the weights. Brown and Diaconis [13] showed the chains are diagonalizable, determined the stationary distribution, and gave reasonably sharp coupling bounds for convergence to stationarity.

The B-H-R results extend the shuffling results of Section 2 above: In  $\mathbb{R}^n$ , the *braid arrangement* has hyperplanes  $\{H_{ij}\}_{i < j}$  with  $H_{ij} = \{(x_1 \cdots x_n) : x_i = x_j\}$ . The chambers of the braid arrangement are naturally labeled by the  $n!$  permutations (the relative order of the coordinates inside the chamber). The faces of the braid arrangements are determined by various equalities among coordinates. They are easily seen to be labeled by block ordered partitions discussed in Section 2.



Moreover, the action of faces on chambers is just the shuffling scheme described in Section 2.

There are many hyperplane arrangements where the chambers can be labeled with natural combinatorial objects such as trees or tilings of various regions [13] [59]. The face walks give natural Markov chains on these spaces which permit a complete analysis. There is a useful description of the stationary distribution, the operators are diagonalizable with positive eigenvalues which are partial sums of the weights. Finally, there are good rates of convergence using a coupling argument.

For this expository account, I content myself with a single geometric example drawn from joint work with Louis Billera and Ken Brown [11]. Consider  $n$  planes (through zero) in  $\mathbb{R}^3$ . These are most easily pictured by their intersection with the unit sphere. For example, Figure 2 shows the northern hemisphere cut into chambers or regions by 4 planes—one being the plane of the picture.

The projection of  $C$  on  $v$ .

Figure 3: 4 planes in  $\mathbb{R}^3$ .

The chambers are the open regions shown together with a matching set “under” the sphere. There are 14 chambers altogether ( $\binom{n}{2} + 2$  for  $n$  planes in general position). Consider the random walk on chambers generated by picking a random vertex of the arrangement uniformly. The walk moves from its current chamber to the chamber adjacent to the chosen vertex. It is intuitively clear that the chance of winding up in a given region  $c$  depends on the number  $i(c)$  of sides of the region, regions with large values of  $i(c)$  being more likely. In [11] we showed that  $\pi(c) = (i(c) - 2) / (2(f_0 - 2))$  with  $f_0$  the total number of vertices in the arrangement. Thus in Fig. 2  $f_0 = 14$  and the 8 triangular regions have  $\pi = 1/14$  while the 6 quadrilaterals have  $\pi = 1/7$ . We have no intuitive explanation for this; we just observed it was true in small cases and proved it beginning with a rather indirect description of the stationary distribution given by sampling from the vertices *without* replacement. We find the result surprising; for example, there are four essentially different configurations of six planes in  $\mathbb{R}^3$ . These are shown in Table 2 together with their vital statistics. In all cases, the stationary distribution for an  $i$ -gon is proportional to  $i - 2$ . Note that some configurations don't have any  $i$ -gons. The eigenvalues and coupling for this example show that the walk reaches stationarity after two steps!

These examples show that hyperplane walks have some remarkable properties. They do not yet explain what makes things tick. The next two sections give

$i$	A	B	C	D
3	20	14	12	12
4	0	12	16	18
5	12	6	4	0
6	0	0	0	2

Figure 4: Table 2: Six great circles in general position with number of  $i$ -gons

random walks on buildings where things start to break and random walks on semi-groups, the current ultimate generalization.

#### 4 RANDOM WALKS ON THE CHAMBERS OF A BUILDING.

There is a natural extension of the walks of a hyperplane arrangement generated by a reflexion group such as the braid arrangement. This gives random walks on the chambers of a building; we will work with finite objects (spherical buildings). This section reports work of Ken Brown.

A building is a simplicial complex given with a set of subcomplexes called apartments. These apartments must be (isomorphic to) the chambers of a euclidean hyperplane arrangement generated by a finite reflexion group. The top dimensional cells of the complex are called chambers. As an example, the following complex is a building.

Figure 5: An  $A_2$  building

The vertices (one-cells) are numbered  $a, b, c, d, e, f, x, y$ . The two-cells are the edges shown; these are the chambers. There are three apartments

Each of these may be identified with the braid arrangement in  $\mathbb{R}^3$ .

There is a natural action of a face of a building on the chambers. One of the building axioms says that any two faces are in an apartment. Thus any face and chamber are in an apartment and it makes sense to multiply them using the procedure described in Section 3. In the  $A_2$  building pictured in Fig. 5, consider the chamber  $\{a, b\}$  and the vertex  $d$ ;  $d * \{a, b\} = \{d, c\}$  because  $\{c, d\}$  is the closest chamber to  $\{a, b\}$  adjacent to  $d$  (distance 2). Any finite tree is a building, and the product of an edge with a vertex may be similarly defined.

A Markov chain on the chambers of a building may be defined by choosing an arbitrary system of weights on the lower dimensional simplices. This generalizes the shuffling scheme of Section B but does not include general hyperplane arrangements.

For the  $A_2$  building pictured in Figure 5, the walk may be pictured as a service discipline where a single server occupies an edge. Customers arrive at vertices with given propensities and the server slides over to the edge closest to the next customer. One may ask how much time the server spends on a given edge in the long run.

This class of examples introduces some new behavior: It is no longer true that the eigenvalues are positive or even sums of the weights. As an example, consider Figure 5 with equal weights on  $b, f, x$ . The eigenvalues are real and the matrix is diagonalizable, but the eigenvalues are algebraic numbers which are no longer linear in the weights. It is an open problem to find examples of random walks on buildings where the eigenvalues are complex. Despite all this, the following example shows that these walks have some elegant special cases where everything works out neatly:

Consider a vector space  $V$  which is  $n$ -dimensional over a finite field  $\mathbb{F}_q$  with  $q = p^a$  elements for some prime  $p$ . A flag is a maximal increasing sequence of subspaces. Thus it consists of a line in a plane in a three-space and so on up to an  $n-1$  space. We will describe a simple random walk on the space of flags which is a direct analog of the random to top chains in Section 1 above. The walk is driven by a system of weights for each line  $l : \{w_l\} l \in \mathbb{P}_{n-1}$ . Here  $w_l \geq 0$ ,  $\sum_l w_l = 1$ . The

walk proceeds as follows: Suppose it is currently at the flag  $v_1 \subset v_2 \cdots \subset v_{n-1}$ . Choose a line with probability  $w_l$ . Modify the flag to begin with  $l$ :

$$l \subset l + v_1 \subset l + v_2 \cdots \subset l + v_n$$

If  $l \notin v_{i-1}$  but  $l \in v_i$ , the chain of subspaces repeats since  $l + v_{i-1} = l + v_i$ . Strike out this repetition to get a new maximal flag. This defines a random walk in maximal flags which “moves a random vector to the front.” As  $q \rightarrow 1$ ; a subspace becomes a subset and a flag becomes a permutation; the walk becomes move to front.

Brown [12] gives an elegant analysis of these chains which perfectly parallels the analysis of Section 3.

**THEOREM 4.1.** [Brown] *For the random line to front with weights  $\{w_l\}$ , there is an eigenvalue for each subspace  $x$  (including  $\phi, \mathbb{P}^n$ )*

$$\lambda_x = \sum_{l \in x} w_l.$$

*This has multiplicity  $m_j(q) = \sum q^{MAJ(\pi)} = [j]! \sum_{k=0}^j \frac{(-1)^k q^{\binom{k}{2}}}{[k]}$ , with  $j = \text{codim}(x)$ , and the first sum over derangements  $\pi$  in  $S_j$ . If  $w_j$  is uniform*

$$\|K_x^m - \pi\| \leq \frac{(q^n - 1)(q^{n-1} - 1)}{(q^2 + 1)(q - 1)} \left( \frac{q^{n-2} - 1}{q^n - 1} \right)^m.$$

*Remark 5.* The last bound shows that  $m = n - 1$  steps suffice to achieve randomness when  $n$  is large and  $q$  is fixed. This is clearly the minimum by dimension arguments so the bound is sharp in this case.

#### 4.1 WHAT IS THE ULTIMATE GENERALIZATION?

The results in Sections 1–4 have a marked similarity; it is natural to try to derive a common generalization. In all cases one is “multiplying something” by an associative product (the one case where things went wrong for the  $A_2$  building of Fig. 5, it turns out the product isn’t associative). This suggests random walk on a semigroup as a possible general setting. Let  $\mathcal{X}$  be a semigroup and  $w_x$  a probability on  $\mathcal{X}$ . Let  $\rho$  be an ideal in  $\mathcal{X}$  (so  $xc \in \rho$  for all  $x \in \mathcal{X}, c \in \rho$ ). Then generate a random walk by repeatedly choosing elements from  $\{w_x\}$  and multiplying. While there is some general theory for these random walks [53] [20], they are too general to hope that results such as real eigenvalues go through. Indeed, any Markov chain on a set  $S$  can be represented as a random walk on the set of all functions from  $S$  to  $S$ .

Ken Brown [12] has shown that results of Sections 1–4 above and many others are captured by semigroups which have all elements idempotent ( $x^2 = x$ ) and further satisfy the cancellation property  $xyx = xy$  for all  $x, y$ . These are called

“left regular bands” in the semigroup business. Brown’s proof introduces the semigroup algebra and studies its representations. The irreducible representations of a left regular band turn out to be one-dimensional, and this leads to a complete description of the eigenvalues and multiplicities. The coupling bound had been carried out earlier. [13]

Are these semigroup walks the ultimate generalization? It seems too early to tell. Further, the tools available for hyperplane, building, and semigroup walks are still not sharp enough to prove the cutoff phenomenon as in Theorems 1.1 and 2.2. These seem to need the more refined setting of the descent algebra. There is much yet to understand, but the above developments give a flavor of some exciting mathematics in progress.

## 5 TOPICS NOT COVERED

The results in Sections 1–5 show the developments of a single theme. There are many other themes that have led to exciting developments. This brief section gives pointers to the literature. It may be supplemented by browsing through the preprint service for Monte Carlo Markov chains: <http://www.stats.bris.ac.uk/~maspb/mcmc>. Throughout,  $\mathcal{X}$  is a finite set,  $K(x, y)$  is a stochastic matrix, and  $\pi$  is the stationary distribution.

### 5.1 COUPLING

Coupling techniques are available in some generality. In *principle* there is a maximal coupling which is sharp in the sense the  $\|K^l - \pi\| = P\{T > l\}$  for  $l = 1, 2, 3, \dots$ . These are usually impossible to find. At present, finding useful couplings is an art. Lindvall [48] is a book-length introduction to coupling. Examples can be found in Aldous [1] and in [16]. Recently, couplings have been used to solve extremely tough problems. Finally, the coupling from the past method of Propp-Wilson [60] has been used to allow exact generation for several distributions of interest. There is a useful bound on the spectral gap given a coupling bound [43], [2]. All of this said, it is still quite difficult to generate useful bounds for many chains of interest using coupling. This is why the geometric theory of Markov chains has been actively developed.

### 5.2 THE GEOMETRIC THEORY OF MARKOV CHAINS

Suppose that the underlying chain is reversible:  $\pi(x)K(x, y) = \pi(y)K(y, x)$  for all  $x, y$ . Form a graph with vertex set  $\mathcal{X}$  and an undirected edge from  $x$  to  $y$  if  $K(x, y) > 0$ . The geometric theory relates geometric properties of this graph such as diameter, volume growth and various measures of bottlenecks (curvature) to the convergence rates of the chain. This borrows tools from spectral geometry and PDE such as the following inequalities

Poincaré, Cheeger, Nash, Sobolev, Log Sobolev.

Useful introductions to these ideas with many examples may be found in [5], [56], [58]. Along with others, I have written about these things in [35], [27], [29], [30]. Expositions in graph theoretic language appear in [10][15]. The computer science community has also written about such geometric bounds with [49], [46] being surveys with extensive references.

The theory has been adapted to nonreversible chains [38][29]. Here is a simple example which illustrates the geometric tools. Consider  $\mathcal{X} = S_n$  all permutations. Let  $n$  be odd. Let  $S = \{(1, 2), (1, 2, \dots, n)\}$ : A transposition and an  $n$ -cycle.

Define  $K(\sigma, \eta) = \begin{cases} \frac{1}{2} & \text{if } \eta\sigma^{-1} \in S \\ 0 & \text{otherwise} \end{cases}$ . This is the Markov chain described informally

as “either transpose the top two cards or move the top card to the bottom.” This simple chain should be easy to analyze, but no coupling bound is known. The results show that there are universal constants  $A_1, A, B$  such that

$$Ae^{-Bl/n^3 \log n} \leq \|K^l - \pi\| \leq Ae^{-Bl/n^3 \log n}$$

Roughly, this says order  $n^3 \log n$  shuffles suffice. When  $n = 52$ ,  $n^3 \log n$  is more than half a million. Thus, this shuffling scheme is much slower than “top to random.” Here is a brief outline of the argument:

Let  $L^2 = \{f : \mathcal{X} \rightarrow \mathbb{R} \text{ with } (f, g) = \sum_x f(x)g(x)\pi(x)\}$ . For this example  $\pi(x) = \frac{1}{n!}$ . Let  $K$  operate linearly on  $L^2$  by  $Kf(x) = \sum_y K(x, y)f(y)$ . If  $K, \pi$  were

reversible,  $K$  would be self-adjoint. In the present example,  $K$  is *not* self-adjoint. We first symmetrize  $K$ , forming  $\tilde{K} = KK^*$ . This is a self-adjoint operator with a simple description: Set  $T = \{(1, 2)(1 \cdots n)^{-1}, (1 \cdots n)(1, 2)\}$ . Then  $\tilde{K}(\sigma, \sigma) = \frac{1}{2}$ ,  $\tilde{K}(\sigma, \zeta) = \frac{1}{4}$  if  $\zeta\sigma^{-1} \in T$ ,  $\tilde{K}(\sigma, \zeta) = 0$  otherwise.

The eigenvalues  $\tilde{\beta}_i$  of  $\tilde{K}$  can be characterized through the quadratic form  $\tilde{E}(f, g) = \langle (I - \tilde{K})f, g \rangle$ . As shown in [29], Section 2, convergence rates for the original chain  $K$  can be expressed in terms of  $\tilde{\beta}$ .

$$\|K^l - \pi\|^2 \leq \frac{1}{4} \sum_{\beta=1}^{n!-1} \tilde{\beta}^{2l}$$

Here  $\tilde{\beta}_0 = 1$  does not appear in the sum.

Finally, one can get good bounds on the eigenvalues  $\tilde{\beta}_i$  by comparison with a third chain: random transpositions.  $\tilde{K}(\sigma, \zeta) = \frac{1}{n}$  if  $\sigma = \zeta, 2/n^2$  if  $\sigma\zeta^{-1}$  is a transposition and zero otherwise.

For this third chain, a formula for the eigenvalues and their multiplicities is available using character theory [33]. To compare  $\tilde{K}$  and  $\tilde{K}$  one shows  $\tilde{E} \leq An^2 \tilde{E}$  for universal  $A$ . This in turn is accomplished by writing  $(1, 2)(1, \dots, n)^{-1}$  and  $(1 \cdots n)(1, 2)$  in terms of transpositions. Many examples of this sort appear in [25]. Details for the present example can be found in [29], Section 2.

The argument sketched above shows the interactions between probability, geometry, group theory, and PDE. More sophisticated examples appear in [37], [47], [55].

### 5.3 GENERAL STATE SPACES

I have principally been involved with bounding Markov chains on finite state spaces. There has also been much work on general state spaces. At present writing very little of this is quantitative and what is available is often too crude to be useful to practitioners. Meyn and Tweedie [51] is a book-length development of the asymptotic theory, and Rosenthal [54] is a recent example of the quantitative theory with references to related work.

### 5.4 SOME OPEN PROBLEMS

The present article does not do justice to perhaps the most exciting development; the infinite variety of tricks and techniques that practitioners develop to give believable answers in practical problems. Even the most basic techniques in widespread use—the Metropolis algorithm [32] and the Gibbs sampler are beyond current theoretical understanding. There has been spectacular progress in special cases such as the Ising model (work of Stroock-Zegarlinski, Martinelli, Schoneman, and others). However, the following kind of problem is completely open: On the symmetric group consider  $\pi(\sigma) = Z(\theta)\theta^{d(\sigma, \sigma_0)}$ . Here  $0 < \theta \leq 1$ ,  $d$  is a metric on permutations such as  $\sum |\sigma_0(i) - \sigma(i)|$ ,  $\sigma_0$  is a fixed, known permutation, and  $Z$  is a normalization factor. The problem is to generate from  $\pi$ . One simple method: Use the Metropolis algorithm with base chain random transpositions. Analysis of the time to stationarity is beyond theory at present writing. It seems natural to conjecture that order  $n \log n$  steps are necessary and suffice to reach stationarity. See [21] for such a result for a special choice of metric.

In a similar vein; trying to make mathematical sense out of any widely used Monte Carlo Markov chain procedure from umbrella sampling to hybrid Monte Carlo offers very challenging mathematics problems.

### 5.5 MORE OPEN PROBLEMS.

Section 5.2 showed how to bound the rate of convergence of a non-reversible chain in terms of the eigenvalues of its multiplicative reversibilization. These in turn were bounded by comparison with a random transpositions chain. Comparison only works for reversible chains. The problem is, find a way of using the explicit eigenvalues of the chains in Sections 2-4 above. Here are three explicit questions. *First*, is there any way of using the eigenvalues to derive explicit bounds on total variation. There are useful bounds for reversible chains [35]. *Second*, can one relate the eigenvalues of a non-reversible chain  $K$  to the eigenvalues of its multiplicative reversibilization? For example, for random to top, the reversibilization becomes random to random. For riffle shuffles, the reversibilization becomes 'remove a random subset and shuffle it back at random.' This is a natural model of traffic where two lanes merge into one and then split into two. *Third*, in the hyperplane

setting of Section 3 a local walk can be defined on the chambers. Choose a weight  $w_i$  for each hyperplane. From a region  $C$  choose one of its bounding hyperplanes with probability proportional to its weight and reflect to the adjacent chamber. This gives a reversible Markov chain with stationary distribution proportional to the sum of the weights of hyperplanes bounding a chamber. Such walks are used to generate random tilings and elsewhere. Is there any way to use the known eigenvalues of the chamber walks of Section 3 to analyze the local walks? These questions go through as stated for buildings.

## REFERENCES

- [1] Aldous D. (1983) *Random walks on finite groups and rapidly mixing Markov chains*. In Séminaire de Probabilités, XVII, LNM 986, Springer, Berlin.
- [2] Aldous D. (1982) *Some inequalities for reversible Markov chains*. Jour. Lond. Math. Soc. 25, 564-576.
- [3] Aldous D. and Diaconis P. (1987) *Strong uniform times and finite random walks*. Adv. Appl. Math. 8, 69-97.
- [4] Aldous D. and Diaconis P. (1986) *Shuffling cards and stopping times*. American Math Monthly, 93, 333-348.
- [5] Aldous D. and Fill J. (1996) Preliminary version of a book on finite Markov chains available via homepage <http://www.stat.berkeley.edu/users/aldous>
- [6] Alon N. and Milman V. (1985)  $\lambda_1$ , *isoperimetric inequalities for graphs and superconcentrators*. J. Comb. Th. B, 38, 78-88.
- [7] Bakry D. (1994) *L'hypercontractivité et son utilisation en théorie des semi-groups*. In Ecole d'été de Saint Flour 1992, Springer LNM 1581.
- [8] Bayer D. and Diaconis P. (1992) *Trailing the dovetail shuffle to its lair*. Ann. Appl. Prob. 2, 294-313.
- [9] Bidigare, P., Hanlon, P. and Rockmore, D. (1998) *A combinatorial description of the spectrum for the Tsetlin library*. Duke Math Journal. To appear.
- [10] Biggs, N. (1993) *Algebraic graph theory*, 2nd ed. Cambridge, Cambridge University Press.
- [11] Billera, L., Brown, K., Diaconis, P. (1998) *Geometry and probability in three dimensions*. American Mathematical Monthly. To appear.
- [12] Brown, K. (1998) *Random walk on semi-groups*. Unpublished manuscript.
- [13] Brown, K. and Diaconis, P. (1998) *Random walks and hyperplane arrangements*. Annals Probab. To appear.
- [14] Cheeger J. (1970) *A lower bound for the smallest eigenvalue of the Laplacian*. Problems in Analysis, Symposium in Honor of S. Bochner. Princeton University Press. 195-199.
- [15] Chung, F. (1997) *Spectral graph theory*. American Math. Soc. Providence.
- [16] Diaconis P. (1986) *Group representations in probability and statistics*. IMS, Hayward.
- [17] Diaconis P. (1996) *The cutoff phenomenon in finite Markov chains*. Proc. Natl. Acad. Sci. USA, 93, 1659-1664.



- [18] Diaconis P. and Fill J. (1990) *Strong stationary times via a new form of duality*. Ann. Prob. 18, 1483-1522.
- [19] Diaconis, P., Fill, J. and Pitman, J. (1992) *Analysis of top to random shuffles*. Combinatorics, Probability and Computing, 1, 135-155.
- [20] Diaconis, P. and Freedman, D. (1998) *Iterated random functions*. SIAM Journal. To appear.
- [21] Diaconis, P. and Hanlon, P. (1992) *Eigen analysis for some examples of the Metropolis algorithm*. Contemporary Math. 138, 989-117.
- [22] Diaconis P. and Holmes S. (1995) *Three Examples of Monte-Carlo Markov Chains: at the Interface between Statistical Computing, Computer Science and Statistical Mechanics*. In Discrete Probability and Algorithms, (Aldous et al, ed.) 43-56. The IMA volumes in Mathematics and its Applications, Vol. 72, Springer-Verlag.
- [23] Diaconis P., McGrath M, and Pitman J. (1993) *Riffle shuffles, cycles, and descents* Combinatorica 15, 1, 11-29.
- [24] Diaconis P. and Saloff-Coste L. (1993) *Comparison theorems for reversible Markov chains*. Ann. Appl. Prob. 3, 696-730.
- [25] Diaconis P. and Saloff-Coste L. (1993) *Comparison techniques for random walk on finite groups*. Ann. Prob. 21, 2131-2156.
- [26] Diaconis P. and Saloff-Coste L. (1994) *Moderate growth and random walk on finite groups*. G.A.F.A., 4, 1-36.
- [27] Diaconis P. and Saloff-Coste L. (1995) *An application of Harnack inequalities to random walk on nilpotent quotients.*, J. Fourier Anal. Appl., Kahane special issue, 187-207.
- [28] Diaconis P. and Saloff-Coste L. (1995) *Random walks on finite groups: a survey of analytical techniques*. In Probability on groups and related structures XI, H. Heyer (ed), World Scientific.
- [29] Diaconis P. and Saloff-Coste L. (1996) *Nash inequalities for finite Markov chains.*, J. Th. Prob. 9, 459-510.
- [30] Diaconis P. and Saloff-Coste L. (1996) *Logarithmic Sobolev inequalities and finite Markov chains*. Ann. Appl. Prob. 6, 695-750.
- [31] Diaconis P. and Saloff-Coste L. (1995) *Walks on generating sets of Abelian groups*. Prob. Th. Rel. Fields. 105, 393-421.
- [32] Diaconis P. and Saloff-Coste L. (1995) *What do we know about the Metropolis algorithm*. Jour. Comp. Sys. Sci. To appear.
- [33] Diaconis D. and Shahshahani M. (1981) *Generating a random permutation with random transpositions*. Z. Wahrsch. Verw. Geb., 57, 159-179.
- [34] Diaconis P. and Shahshahani M. (1987) *Time to reach stationarity in the Bernoulli-Laplace diffusion model*. SIAM Jour. Math. Anal., 18, 208-218.
- [35] Diaconis P. and Stroock D. (1991) *Geometric bounds for eigenvalues for Markov chains*. Ann. Appl. Prob. 1, 36-61.
- [36] Dobrow, R. and Fill, J. (1995) *The move to the front rule for self-organizing lists. With Markov dependent records*. In Discrete Probability and Algorithms, Springer, New York, pp. 57-80.

- [37] Dyer M. and Frieze A. (1991) *Computing the volume of convex bodies: a case where randomness provably helps*. Probabilistic Combinatorics and its applications, Proceedings of the AMS Symposia in Applied Mathematics 44, 123-170.
- [38] Fill J. (1991) *Eigenvalue bounds on convergence to stationarity for nonreversible Markov chains, with application to the exclusion process*. Ann. Appl. Probab., 1, 62-87.
- [39] Frieze A., Kannan R. and Polson N. (1994) *Sampling from log concave distributions*. Ann. Appl. Prob. 4, 812-837.
- [40] Gessel, I. and Reutenrue, C. (1993) *Counting permutations with given cycle structure and descent set*. Journal Combin. Th. A. 64, 184-215.
- [41] Gross L. (1993) *Logarithmic Sobolev inequalities and contractivity properties of semigroups*. In Lecture Notes in Math. 1563. Springer.
- [42] Hanlon, P. (1990). *The action of  $S_n$  on the components of the Hodge decompositions of Hochschild homology*. Mich. J. Math, 37, 105-124.
- [43] Holley, R. (1985) *Rapid convergence to equilibrium in one-dimensional stochastic Ising models*. Ann. Prob. 13
- [44] Jerrum M. and Sinclair A. (1993) *Polynomial time approximation algorithms for the Ising model*, SIAM Journal of Computing, 22, 1087-1116.
- [45] Jerrum M. and Sinclair A. (1997) *The Markov chain Monte Carlo method: an approach to approximate counting and integration*. In Approximation algorithms for NP-hard problems, D.S. Hochbaum (Ed.), PWS Publishing, Boston.
- [46] Kannan R. (1994) *Markov chains and polynomial time algorithms*. Proceedings of the 35th IEEE Symposium on Foundations of Computer Science, Computer Society Press, 656-671.
- [47] Lawler G. and Sokal A. (1988) *Bounds on the  $L^2$  spectrum for Markov chains and Markov processes: a generalization of Cheeger inequality*. Trans. AMS, 309, 557-580.
- [48] Lindvall, T. (1992) *Lectures on the coupling method*. Wiley, N.Y.
- [49] Lovász L. and Simonovits M. (1993). *Random walks in a convex body and an improved volume algorithm*. Random Structures and Algorithms, 4, 359-412.
- [50] Metropolis N., Rosenbluth A., Rosenbluth M., Teller A. and Teller E. (1953) *Equations of state calculations by fast computing machines*. J. Chem. Phys. 21, 1087-1092.
- [51] Meyn, S. and Tweedie, R. (1993) *Markov chains and stochastic stability*. Springer, New York.
- [52] Phatarfod, R. (1991) *On the matrix occurring in a linear search problem*. J. Appl. Probab. 28, 336-346.
- [53] Rosenblatt, M. (1986) *Random walk on semigroups* Contemporary Math, 50, 115-120.
- [54] Rosenthal, J. (1995) *Minorization conditions and convergence rates for Markov chain Monte Carlo*. Jour. American Statis. Assoc., 90, 558-566.

- [55] Saloff-Coste L. (1996) *Simple examples of the use Nash inequalities for finite Markov chains*. In Semstat III, Current Trends in Stochastic Geometry and its Applications. W.S. Kendall, O.E. Barndorff-Nielsen and MC. van Lieshout, Eds. Chapman & Hall.
- [56] Saloff-Coste L. (1997) *Lectures on finite Markov chains*. In Springer Lecture Notes in Mathematics 1665, 301-408.
- [57] Sinclair A. (1992) *Improved bounds for mixing rates of Markov chains and multicommodity flow*. Combinatorics, Probability and Computing, 1, 351-370.
- [58] Sinclair A. (1993) *Algorithms for random generation and counting: a Markov chain approach*. Birkhäuser, Boston.
- [59] Stanley, R. (1996) *Hyperplane arrangements, interval orders and trees*. Proc. Nat. Acad. Sci., USA, 93.
- [60] Wilson, D. and Propp, J. (1996) *How to get an exact sample from a generic Markov chain and sample a random spanning tree from a directed graph*. Proc. Seventh Annual ACM-SIAM Symposium on Discrete Algorithms. ACM, NY, 448-457.

Persi Diaconis  
Departments of Mathematics  
and Statistics  
Stanford University  
Stanford, California 94305  
USA

CHAOTIC HYPOTHESIS AND UNIVERSAL  
LARGE DEVIATIONS PROPERTIES

GIOVANNI GALLAVOTTI

ABSTRACT. Chaotic systems arise naturally in Statistical Mechanics and in Fluid Dynamics. A paradigm for their modelization are smooth hyperbolic systems. Are there consequences that can be drawn simply by assuming that a system is hyperbolic? here we present a few model independent general consequences which may have some relevance for the Physics of chaotic systems.

Keywords and Phrases: Chaotic hypothesis, Anosov maps, Reversibility, Large deviations, Chaos

§1. CHAOTIC MOTIONS.\*

A typical system exhibiting chaotic motions is a gas in a box whose particles interact via short range forces with a repulsive core, *e.g.* a hard core. No hope to ever be able to solve the evolution equations.

In the very simple case of pure hard cores it has been possible to prove, mathematically at least in some cases, that the system is ergodic, [Si1], [Sz], but ergodicity in itself is only a beginning of the qualitative theory of the motion. A similar situation arises in Fluid Mechanics: is a qualitative theory of Turbulence possible as, clearly, there are hopes to be able, in the near future, to prove an existence–uniqueness theorem but there is no hope for exact solutions of Navier Stokes equations?

Equilibrium Statistical Mechanics is a brilliant example of a very successful quantitative theory derived from a comprehensive qualitative hypothesis, the *ergodic hypothesis*. The key to its success is a *general* expression for the probability distribution  $\mu$  on phase space  $M$  providing us with the *statistics* of the motions corresponding to given values of the macroscopic parameters determining the state of the system.

The statistics  $\mu$  is defined in terms of the time evolution map  $S$  via the relation:

$$\lim_{T \rightarrow \infty} \frac{1}{T} \sum_{j=0}^{T-1} F(S^j x) = \int_M F(y) \mu(dy) \quad (1.1)$$

---

\* Expanded text of the talk at the ICM98 in Berlin, 26 August 1998.

for all smooth *observables*  $F$  and for almost all, in the sense of volume measure on  $M$ , initial data  $x \in M$ . In Equilibrium Statistical Mechanics the distribution  $\mu$  is identified with the uniform distribution on the surface of constant energy (the macroscopic state of the system being determined by the volume  $V$  of the container box and by the energy  $U$ ), which is an obviously invariant distribution by Liouville's theorem of Hamiltonian Mechanics: this is a necessary consequence of the ergodic hypothesis.

The success of Equilibrium Statistical Mechanics can be traced back to the fact that the ergodic hypothesis provides us with a concrete general, *model independent*, expression for the statistics of the motions. An expression that can be used to derive relations among *time averages* of various observables without even dreaming of ever being able to actually compute any of such averages.

The Boltzmann's *heat theorem*, the positivity of compressibility and specific heat are simple, but great, examples of such relations. They are relations which hold for any model, provided one makes the ergodicity hypothesis, see [Ga1]. A classical argument that can be used to derive the heat theorem (*i.e.* the second law of Thermodynamics) from ergodicity is provided us by Boltzmann, see Appendix A2 and [Ga2].

Consider a mechanical system: viewing its phase space as a discrete set of points the ergodic hypothesis says that motion is a one cycle permutation of the points. Given a initial datum with energy  $U$  and with volume  $V$  we define *temperature* the time average of kinetic energy  $T = \langle K \rangle$  and *pressure* the time average of the derivative of the potential  $\varphi$  with respect to the volume  $V$  (note that the force acting on the particles consists of the internal pair forces *and* of the force that the walls exercise upon the particles which depends on the position of the walls, hence it does change when the volume varies). Here and below  $\langle F \rangle$  will denote the time average of the observable  $F$ .

A general elementary property of a system whose motion on each energy surface is a single periodic motion is that if one calls  $p = \langle \partial_V \varphi \rangle$  then:

$$\frac{dU + p dV}{T} = \text{exact} \quad (1.2)$$

which means that if the energy  $U$  and a parameter  $V$  on which the potential depends (it will be the volume in our case) are varied by  $dU$  and  $dV$  respectively *then the differential in (1.2) is exact.*

An elementary classical calculation shows that  $p$ , see Appendix A2, in the case of a gas in a box, has the meaning of average force exercised per unit surface on the walls of the container as a consequence of the particles collisions: thus we see that the ergodic hypothesis plus a general, trivial, identity among the averages of suitable mechanical quantities yields a relation ("equality of cross derivatives") holding without free parameters.

The reason why such relation is physically relevant for macroscopic systems is that the time necessary for the averages defining  $T, p$  to be reached within a good approximation by the finite time averages of  $K, \partial_V \varphi$  is not the unobservable *recurrence time* (*i.e.* the superastronomic time for the system to complete a single tour of the energy surface  $U$ ) but it is a much shorter physically observable time

(whose theory is also due to Boltzmann being the essence of the Boltzmann's equation) because the quantities  $K, \partial_V \varphi$  have an essentially constant value on the energy surface if the number of particles is large (so that the average of such observables "stabilizes" very rapidly compared to the recurrence times).

To summarize: a simple hypothesis allows us to find the statistics of the motions of an equilibrium system: this implies simple parameterless relations among averages of physically relevant quantities (*i.e.*  $\partial_V \frac{1}{T} = \partial_U \frac{p}{T}$ ) which are observable in large systems because such quantities average very quickly compared to the recurrence times (being practically constant on the surface of given energy if the system is large).

Thus a natural question arises: is there anything analogous in Non Equilibrium Statistical Mechanics? and in developed Turbulence?

The first problem is "what is the analogue of the uniform Liouville's distribution?". This is a really non trivial question that, once answered, will possibly allow us to try to find relations between time averages of mechanical quantities. The nontriviality is due to the fact that as soon as a system is out of equilibrium, *i.e.* nonconservative forces act upon it, dissipation is necessary in order to be able to reach a stationary state. But this means that *any* model used will be necessarily described by an evolution equation which will have a nonzero divergence: so that phase space will necessarily contract, in the average, and the statistics of the motion will be concentrated on a set of zero Lebesgue volume, see [Ru3].

Ruelle's proposal in the early 1970's was that one should regard such systems as *hyperbolic* so that there would be a unique stationary distribution describing the statistics of almost all initial data (chosen with the uniform distribution on phase space), [Ru1]. The ideas of Krylov, [Kr79], inspired Sinai in his development of the theory of Anosov systems via Markov partitions and, see [Si2], in conceiving complex mechanical systems as hyperbolic, and Ruelle's new ideas and his principle emerged, profiting of the important technical and conceptual achievements of Sinai.

This principle has been interpreted in [GC] as the following:

*Chaotic hypothesis: A chaotic mechanical system can be regarded for practical purposes as a topologically mixing Anosov system.*

This means that the closure of the attractor is a smooth surface on which the evolution is a Anosov system: of course assuming Axiom A instead of Anosov would be more natural, particularly in few degrees of freedom systems, [Ru1]. However I prefer to formulate the hypothesis in terms of Anosov system as fractality of the closure of the attractor seems to be of little relevance in systems with large number of degrees of freedom occurring in Statistical Mechanics.

The locution *practical purposes* is deliberately ambiguous as we know that even in Equilibrium Statistical Mechanics the corresponding ergodic hypothesis may fail while its consequences, at least some of them, will not (like the heat theorem in a free gas or in a harmonic chain).

The above physical discussion serves as a quick motivation of the mathematical question: *are there general properties shared by mechanical systems that are transitive or mixing Anosov systems?*

In the next sections I provide some affirmative answer in the class of *time reversible Anosov maps* and of *weakly interacting chains of Anosov maps*. Recall: a *time reversal* symmetry for a dynamical system  $(M, S)$  is *any* isometric diffeomorphism  $I$  such that:

$$I^2 = 1, \quad IS = S^{-1}I \quad (1.3)$$

Examples in Hamiltonian mechanical systems are the velocity reversal, or the composition of the velocity reversal and the parity symmetry, or the composition of the velocity reversal, parity symmetry and charge conjugation symmetry. In general a time reversal may be a symmetry quite different from the naive one that can be imagined, see [BG].

Hamiltonian systems on which further anholonomic constraints are imposed via Gauss' principle of *least constraint* often generate systems which show a time reversal symmetry, see Appendix A1, thus providing the simplest examples.

## §2. TIME REVERSIBLE DISSIPATIVE ANOSOV SYSTEMS. FLUCTUATION THEOREM.

We now study a  $C^\infty$ , topologically mixing, Anosov system  $(M, S)$  on a compact manifold  $M$ .

Let  $M$  be a  $d$ -dimensional,  $C^\infty$ , compact manifold and let  $S$  be a  $C^\infty$ , mixing (transitive would suffice) Anosov diffeomorphism, [AA], [Si1]. If  $W_x^u, W_x^s$  denote the *unstable* or *stable* manifold at  $x \in M$ , we call  $W_x^{u,\delta}, W_x^{s,\delta}$  the connected parts of  $W_x^u, W_x^s$  containing  $x$  and contained in the sphere with center  $x$  and radius  $\delta$ . Let  $d_u, d_s$  be the *dimensions* of  $W_x^u, W_x^s$ :  $d = d_u + d_s$ . We shall take  $\delta$  always smaller than the smallest curvature radius of  $W_x^u, W_x^s$  for  $x \in M$ . Transitivity implies that  $W_x^u, W_x^s$  are dense in  $M$  for all  $x \in M$ .

The map  $S$  can be regarded, locally near  $x$ , either as a map of  $M$  to  $M$  or of  $W_x^u$  to  $W_{Sx}^u$ , or of  $W_x^s$  to  $W_{Sx}^s$ . The *Jacobian matrices* of the "three" maps will be  $d \times d$ ,  $d_u \times d_u$  and  $d_s \times d_s$  matrices denoted respectively  $\partial S(x)$ ,  $\partial S(x)_u$ ,  $\partial S(x)_s$ . The absolute values of the respective determinants will be denoted  $\Lambda(x)$ ,  $\Lambda_u(x)$ ,  $\Lambda_s(x)$  and are Hölder continuous functions, strictly positive (in fact  $\Lambda(x)$  is  $C^\infty$ ), [Si1], [AA], [Ru4]. Likewise one can define the Jacobians of the  $n$ -th iterate of  $S$ ; they are denoted by appending a label  $n$  to  $\Lambda, \Lambda_u, \Lambda_s$  and are related to the latter by the differentiation chain rule:

$$\begin{aligned} \Lambda_n(x) &= \prod_{j=0}^{n-1} \Lambda(S^j x), & \Lambda_{u,n}(x) &= \prod_{j=0}^{n-1} \Lambda_u(S^j x), \\ \Lambda_{s,n}(S^j x) &= \prod_{j=0}^{n-1} \Lambda_{s,n}(S^j x), & \Lambda_n(x) &= \Lambda_{u,n}(x) \Lambda_{s,n}(x) \chi_n(x) \end{aligned} \quad (2.1)$$

and  $\chi_n(x) = \frac{\sin \alpha(S^n x)}{\sin \alpha(x)}$  is the ratio of the sines of the *angles*  $\alpha(S^n x)$  and  $\alpha(x)$  between  $W^u$  and  $W^s$  at the points  $S^n x$  and  $x$ . Hence  $\chi_n(x)$  is bounded above and below in terms of a constant  $B > 0$ :  $B^{-1} \leq \chi_n(x) \leq B$ , for all  $x$  (by the transversality of  $W^u$  and  $W^s$ ).

We can define the *forward* and *backward statistics* or “SRB distributions”  $\mu_+, \mu_-$  of the volume measure  $\mu_0$  via the limits:

$$\lim_{T \rightarrow \infty} \frac{1}{T} \sum_{k=0}^{T-1} F(S^{\pm k}x) = \int_C \mu_{\pm}(dy)F(y) \equiv \mu_{\pm}(F) \tag{2.2}$$

which exist for all smooth functions  $F$  on  $M$  and for all but a set of zero volume of initial points  $x$ , see [S1].

Therefore it is the probability distribution  $\mu_+$  that is the *statistics*  $\mu$  of the motions (almost surely with respect to the volume measure  $\mu_0$  on  $M$ ), see (1.1): *it plays the role of the Gibbs distribution, or microcanonical ensemble, of equilibrium Statistical Mechanics.* Hence we are looking for general properties of  $\mu_+$ , independent of the system considered, if possible.

Let  $\Lambda(x) = |\det \partial S(x)|$ ; let  $\mu_{\pm}$  be the forward and backward statistics of the volume measure  $\mu_0$  (*i.e.* the SRB distributions for  $S$  and  $S^{-1}$ ).

*Definition:* The system  $(M, S)$  is dissipative if:

$$- \int_M \mu_{\pm}(dx) \log \Lambda^{\pm 1}(x) = \bar{\eta}_{\pm} > 0 \tag{2.3}$$

*Remarks:* 1) Existence of a time reversal symmetry  $I$ , see (1.3), implies  $\bar{\eta}_+ = \bar{\eta}_-$  and  $\Lambda(x) = \Lambda^{-1}(Ix)$ ; furthermore  $I W_x^u = W_{Ix}^s$  and the dimensions of the stable and unstable manifolds  $d_s, d_u$  are equal:  $d_u = d_s$  and  $d = d_u + d_s$  is even.

2) if  $\Lambda_u(x), \Lambda_s(x)$  denote the absolute values of the Jacobian determinants of  $S$  as a map of  $W_x^u$  to  $W_{Sx}^u$  and of  $W_x^s$  to  $W_{Sx}^s$ , then  $\Lambda_u(x) = \Lambda_s(Ix)^{-1}$ .

3) If a system  $(M, S)$  is dissipative then the system  $(M', S')$  with  $M' = M \times M$  and  $S'(x, y) = (Sx, S^{-1}y)$  provides us with an example, setting  $I(x, y) = (y, x)$ , of a dynamical system in the general class of “reversible” Anosov maps considered in §1. It is remarkable that for Anosov systems it is  $\bar{\eta}_{\pm} \geq 0$ , see [Ru3].

*From now on only reversible dissipative Anosov dynamical systems  $(M, S)$  will be considered:* it is for such systems that it will be possible to derive general model independent properties.

*Definition:* The “dimensionless entropy production rate” or the “phase space contraction rate” at  $x \in M$  and over a time  $\tau$  is the function  $\varepsilon_{\tau}(x)$ :

$$x \rightarrow \varepsilon_{\tau}(x) = \frac{1}{\bar{\eta}_{+\tau}} \sum_{j=-\tau/2}^{\tau/2-1} \log \Lambda^{-1}(S^j x) = \frac{1}{\bar{\eta}_{+\tau}} \log \bar{\Lambda}_{\tau}^{-1}(x) \tag{2.4}$$

with  $\bar{\Lambda}_{\tau}(x) \stackrel{def}{=} \prod_{j=-\tau/2}^{\tau/2-1} \Lambda(S^j x)$ . Hence (see (2.2)) it is, with  $\mu_0$ -probability 1:

$$\langle \varepsilon_{\tau} \rangle_+ = \lim_{T \rightarrow +\infty} \frac{1}{T} \sum_{j=0}^{T-1} \varepsilon_{\tau}(S^j x) \equiv \int_M \mu_+(dy) \varepsilon_{\tau}(y) = 1 \tag{2.5}$$



From the general theory of Anosov systems, [Si1], it follows that the  $\mu_+$ -probability that  $p = \varepsilon_\tau(x)$  is in the interval  $[p - \delta, p + \delta]$  can be written as  $\max_{q \in [p - \delta, p + \delta]} e^{\tau \bar{\zeta}(q)}$  for some suitably chosen function  $\bar{\zeta}(p)$  and up to a factor bounded by  $B^{\pm 1}$  with  $0 < B < +\infty$ . This is a deep result of Sinai that holds because the statistics  $\mu_+$  can be regarded as a Gibbs distribution and one can use the large deviation theory for such distributions: see Appendix A3 below for details. Then the following theorem holds, see [GC]:

*Fluctuation theorem: The “large deviation function”  $\bar{\zeta}(p)$  is analytic in an interval  $(-p^*, +p^*)$  with  $p^* \geq 1$  and verifies the relation:*

$$\frac{\bar{\zeta}(p) - \bar{\zeta}(-p)}{p\bar{\eta}_+} = 1 \quad |p| < p^* \quad (2.6)$$

*i.e. the odd part of  $\bar{\zeta}(p)$  is in general linear and its slope is equal to the average entropy creation rate.*

What one really checks, see [Ga3], is the existence of  $p^* \geq 1$  such that the SRB distribution  $\mu_+$  verifies:

$$p - \delta \leq \lim_{\tau \rightarrow \infty} \frac{1}{\bar{\eta}_+\tau} \log \frac{\mu_+(\{\varepsilon_\tau(x) \in [p - \delta, p + \delta]\})}{\mu_+(\{\varepsilon_\tau(x) \in -[p - \delta, p + \delta]\})} \leq p + \delta \quad (2.7)$$

for all  $p$ ,  $|p| < p^*$  and for any  $\delta > 0$ .

The above theorem was first informally proved in [GC] where its interest for nonequilibrium statistical mechanics was pointed out. The theorem can be regarded as a large deviation result for the probability distribution  $\mu_+$ . Although I think that the physical interest of the theorem far outweighs its mathematical aspects it is useful to see a formal proof. A proof is reproduced in Appendix A3 below: it is taken from [Ga3].

The relation (2.6) has been tested numerically in several cases: it was in fact discovered in a numerical experiment, see [ECM2], and tested in other experiments, see [BGG], [BCL], [LLP]. Why does one need to test a theorem? the reason is that in concrete cases not only it is not known whether the system is Anosov but, in fact, it is usually clear that it is not, see [RT]. Hence the test is necessary to check the Chaotic Hypothesis which says that the failure of the Anosov property should be irrelevant for “practical purposes”.

Another interesting aspect, that cannot be treated here for limitations of time, of the above theorem is that it can be interpreted as an extension to non zero forcing (*i.e.*  $\bar{\eta}_+ > 0$ ) of the Green–Kubo relations: see [Ga6].

### §3. FLUCTUATIONS IN LARGE SYSTEMS.

An important drawback of the above fluctuation theorem, besides the reversibility assumption which is not verified in many important cases, is that it can be practically verified, for physical as well as mathematical reasons, only in (relatively) small systems.

In fact the logarithm of the entropy creation rate distribution  $\tau \bar{\zeta}(p)$  is, usually, not only proportional to  $\tau$ , *i.e.* to the time interval over which the entropy creation fluctuation is observed, but *also to the spatial extension of the system*, *i.e.* to the number of degrees of freedom; so that it is extremely unlikely that observing  $p$  in a large system one can see a value  $p$  which is appreciably different from 1 (note that the normalizing constant  $\bar{\eta}_+$  in (2.4) is so chosen that the average of  $p$  in the stationary state is 1).

For this reason in macroscopic (or just “large”) systems the phase space contraction rate is essentially constant (and its physical interpretation is of strength of the friction) much as the density is constant in gases at equilibrium. Therefore one can hope to see entropy creation rate fluctuations only if one can define a *local entropy creation rate*  $\eta_{V_0}(x)$  associated with a microscopic region  $V_0$  of space.

I now discuss, heuristically, why one should expect that a *local entropy creation rate can be defined, at least in some cases, and verifies a local version of the fluctuation law* (2.6). This is discussed in a special example, see [Ga7], as in general one can doubt that a local version of the fluctuation law holds, see [BCL].

The special example that we select is the *chain* of weakly coupled Anosov maps, well studied in the literature, [PS]. The system has a translation invariant spatial structure, *i.e.* it is a chain (or a lattice) of weakly interacting chaotic (mixing Anosov) system. This can be described as follows.

Let  $(M', S')$  be a dynamical system whose phase space  $M'$  is a product of  $2N + 1$  identical analytic manifolds  $\bar{M}_0$ :  $M' = \bar{M}_0^{2N+1}$  and  $S' : M' \rightarrow M'$  is a small perturbation of a product map  $\bar{S}_0 \times \dots \times \bar{S}_0 \stackrel{def}{=} \tilde{S}_0$  on  $M'$ . We assume that  $(\bar{M}_0, \bar{S}_0)$  is a mixing Anosov systems. The size  $N$  (an integer) will be called the “spatial size” of the system.

For  $x, y, z \in \bar{M}_0$  let  $F_\varepsilon(x, z, y)$  be analytic and such that  $z \rightarrow F_\varepsilon(x, z, y)$  is a map, of  $\bar{M}_0$  into itself,  $\varepsilon$ -close to the identity and  $\varepsilon$ -analytic for  $|\varepsilon|$  small enough. We suppose that, if  $\underline{x} = (x_{-N}, \dots, x_N) \in M'$ :

$$(S' \underline{x})_i = F_\varepsilon(x_{i-1}, x_i, x_{i+1}) \circ S_0 x_i \quad (3.1)$$

where  $x_{\pm(N+1)}$  is *identified* with  $x_{\mp N}$  (*i.e.* we regard the chain as periodic); we call such a dynamical system a *chain of interacting Anosov maps* coupled by nearest neighbors. It is a special example of the class of maps considered in [PS].<sup>1</sup>

It is difficult, maybe even impossible, to construct a (non trivial) reversible system of the above form: we therefore (see [Ga3]) consider the system  $(M, S)$  where  $M = M' \times M'$  and define  $S_0 \stackrel{def}{=} \tilde{S}_0 \times (\tilde{S}_0)^{-1}$  and  $S \stackrel{def}{=} S' \times (S')^{-1}$ , called hereafter the *free evolution* and the *interacting evolution*, respectively. So that the system can be considered as time reversible with a time reversal map  $I(\underline{x}, \underline{y}) = (\underline{y}, \underline{x})$ . Note that the inverse map to (3.1) does not have the same form. The map  $S$  is, however, still in the class considered in [PS] because it can be written

<sup>1</sup> In the paper [PS] it is assumed that *also*  $\bar{S}_0$  (hence  $S_0$ ) is close to the identity, *e.g.* within  $\varepsilon$ : such condition does not seem necessary for the purposes of the present paper, hence it will not be assumed.

as  $S(\underline{x}, \underline{y})_i = (S(\underline{x}, \underline{y})_{i1}, S(\underline{x}, \underline{y})_{i2})$  with:

$$\begin{aligned} S(\underline{x}, \underline{y})_{i1} &= F_\varepsilon(x_{i-1}, x_i, x_{i+1}) \circ S_0 x_i \\ S(\underline{x}, \underline{y})_{i2} &= G_{\varepsilon,i}(\underline{y}) \circ S_0^{-1} y_i \end{aligned} \tag{3.2}$$

where  $G$  has “short range”, *i.e.*  $|G_\varepsilon(\underline{y})_i - G_\varepsilon(\underline{y}')_i|$  is of order  $\varepsilon^k$  if  $\underline{y}$  and  $\underline{y}'$  coincide on the sites  $j$  with  $|j - i| \leq k$ . By definition the system  $(M, S)$  is “reversible”, *i.e.* the volume preserving diffeomorphism  $I$  verifies (1.3) above.

Therefore the points of the phase space  $M$  will be  $(\underline{x}, \underline{y}) = (x_{-N}, y_{-N}, \dots, x_N, y_N)$ : however, to simplify notations, we shall denote them by  $\underline{x} = (x_{-N}, \dots, x_N)$ , with  $x_j$  denoting, of course, a pair of points in  $\overline{M}_0$ .

If  $\varepsilon$  is small enough the interacting system will still be hyperbolic, *i.e.* for every point  $\underline{x}$  it will be possible to define a stable and an unstable manifolds  $W_{\underline{x}}^s, W_{\underline{x}}^u$ , [PS], so that the key notion of “Markov partition”, [Si1], will make sense and it will allow us to transform, following the work [PS], the problem of studying the statistical properties of the dynamics of the system into an equivalent, but much more familiar, problem in equilibrium statistical mechanics of lattice spin systems interacting with short range forces. The reader will recognize below that this method is the natural extension to chains of the method used in Appendix A3 to study a single Anosov system.

The main notion that we want to introduce for our chain is the notion of *local entropy creation rate*  $\eta_{V_0}(\underline{x})$ , the entropy creation rate inside a fixed finite set  $V_0 \subset [-N, N]$  of Anosov systems among the  $2N + 1$  composing the chain.

*Definition:* Fixed a point  $\underline{x} = (\dots, x_{\ell-1}, x_\ell, x_{\ell+1}, \dots)$  consider the map (3.1) as a map of  $\underline{x}_{V_0} \stackrel{\text{def}}{=} (x_j)_{j \in V_0} = (x_{-\ell}, \dots, x_\ell)$  into:

$$\underline{x}'_{V_0} = S(\dots, x_{-\ell-1}, \underline{x}_{V_0}, x_{\ell+1}, \dots)_{V_0} \tag{3.3}$$

defined by (3.1) for  $i \in [-\ell, \ell]$ . We call “local entropy production rate” associated with the “space like box”  $V_0 = [-\ell, \ell]$  at the phase space point  $\underline{x} = (\dots, x_{\ell-1}, x_\ell, x_{\ell+1}, \dots)$  the quantity  $\eta_{V_0}(\underline{x})$  equal to minus the logarithm of the determinant of the  $2(2\ell + 1) \times 2(2\ell + 1)$  Jacobian matrix of the map (3.3).

Given a finite region  $V_0$  centered at the origin and a time interval  $T_0$ , let  $\eta_+$  denote the average density of entropy creation rate, *i.e.*  $\eta_+ = \lim_{V_0, T_0 \rightarrow \infty} \frac{1}{|T_0|} \frac{1}{|V_0|} \sum_{j=0}^{|T_0|-1} \eta_{V_0}(S^j x)$ , then we set:

$$p = \frac{1}{\eta_+ |V|} \sum_{j=-\frac{1}{2}|T_0|}^{\frac{1}{2}|T_0|} \eta_{V_0}(S^j x), \quad V = V_0 \times T_0 \tag{3.4}$$

where  $\eta_{V_0}(x)$  denotes the entropy creation rate in the region  $V_0$ .

Calling  $\pi_V(p)$  the probability distribution of  $p$  in the stationary state  $\mu_+$ , *i.e.* in the SRB distribution, and assuming that the system is a weakly coupled chain of Anosov systems I shall show, heristically, that:

*Proposition:* It is  $\pi_V(p) = e^{\zeta(p)|V|+O(|\partial V|)}$  where  $|\partial V|$  denotes the size of the boundary of the space-time region  $V$  and  $\zeta(p)$  is a function analytic in  $p \in (-p^*, p^*)$  for some  $p^* \geq 1$ . And:

$$\begin{aligned} \frac{\zeta(p) - \zeta(-p)}{p\eta_+} &= 1, & |p| < p^* \\ \bar{\zeta}(p) &= r\zeta(p), & \bar{\eta}_+ = r\eta_+ \end{aligned} \quad (3.5)$$

where  $r$  is the total “volume”  $(2N + 1)$  of the system, i.e. the “global” and “local” distributions are trivially related if appropriately normalized.

Note that this implies that if  $V_0$  is an interval of length  $L = |V_0|$  and if  $H = |T_0|$  then the relative size of the error and of the leading term will be, for some length  $R$ , of order  $(L + H)R$  compared to order  $LH$ . Hence a relative error  $O(H^{-1} + L^{-1})$  is made by using simply  $\zeta(p)$  to evaluate the logarithm of the probability of  $p$  as defined by (3.4).

The interest of the above statements lies in their independence on the total size  $2N + 1$  of the systems and the relevance of the above proposition for concrete applications should be clear.

*It means that the fluctuation theorem leads to observable consequences if one looks at the far more probable microscopic fluctuations of the local entropy creation rate.* One can test the relation (3.5) in a small region  $V_0$  even when the system is very large: in such regions the entropy creation rate fluctuations will be frequent enough to be observable and carefully measurable. These fluctuations behave, therefore, just as ordinary density fluctuations at equilibrium: also the latter are not macroscopically observable but they are easily observable in small volumes.

The key results for the analysis leading to the above proposition are the papers [GC], [Ga3] and, mainly, [PS]: the latter paper provides us with a deep analysis of chains of Anosov systems and it contains, I believe, all the ingredients necessary to make the analysis mathematically rigorous: however I do not attempt at a mathematical proof here. The analysis is presented in Appendix A4 below.

Other types of fluctuation theorems (concerning non SRB distributions) had been previously found, see [ES]; extensions to stochastic systems have been recently discussed, see [Ku], [LS].

*ACKNOWLEDGMENTS:* I have profited of stimulating discussions with F. Perroni, who also helped with numerical tests of the above ideas, with F. Bonetto and D. Ruelle. This work is part of the research program of the European Network on: “Stability and Universality in Classical Mechanics”, # ERBCHRXCT940460; partially supported also by Rutgers University and CNR-GNFM.

## APPENDIX A1: THE GAUSS' MINIMAL CONSTRAINT PRINCIPLE.

Let  $\varphi(\dot{\underline{x}}, \underline{x}) = 0$ ,  $\underline{x} = \{\dot{x}_j, x_j\}$  be a constraint and let  $\underline{R}(\dot{\underline{x}}, \underline{x})$  be the constraint reaction and  $\underline{F}(\dot{\underline{x}}, \underline{x})$  the active force, see also Appendix A1 of [Ga3].

Consider all the possible accelerations  $\underline{a}$  compatible with the constraints and a given initial state  $\dot{\underline{x}}, \underline{x}$ . Then  $\underline{R}$  is *ideal* or *verifies the principle of minimal constraint* if the actual accelerations  $\underline{a}_i = \frac{1}{m_i}(\underline{F}_i + \underline{R}_i)$  minimize the *effort*:

$$\sum_{i=1}^N \frac{1}{m_i} (\underline{F}_i - m_i \underline{a}_i)^2 \longleftrightarrow \sum_{i=1}^N (\underline{F}_i - m_i \underline{a}_i) \cdot \delta \underline{a}_i = 0 \quad (\text{A1.1})$$

for all possible variations  $\delta \underline{a}_i$  compatible with the constraint  $\varphi$ . Since all possible accelerations following  $\dot{\underline{x}}, \underline{x}$  are such that  $\sum_{i=1}^N \partial_{\dot{x}_i} \varphi(\dot{\underline{x}}, \underline{x}) \cdot \delta \underline{a}_i = 0$  we can write:

$$\underline{F}_i - m_i \underline{a}_i - \alpha \partial_{\dot{x}_i} \varphi(\dot{\underline{x}}, \underline{x}) = \underline{0} \quad (\text{A1.2})$$

with  $\alpha$  such that  $\frac{d}{dt} \varphi(\dot{\underline{x}}, \underline{x}) = 0$ , *i.e.* :

$$\alpha = \frac{\sum_i (\dot{x}_i \cdot \partial_{\dot{x}_i} \varphi + \frac{1}{m_i} \underline{F}_i \cdot \partial_{\dot{x}_i} \varphi)}{\sum_i m_i^{-1} (\partial_{\dot{x}_i} \varphi)^2} \quad (\text{A1.3})$$

which is the analytic expression of the Gauss' principle, see [LA].

Note that if the constraint is even in the  $\dot{x}_i$  then  $\alpha$  is odd in the velocities: therefore if the constraint is imposed on a system with Hamiltonian  $H = K + V$ , with  $K$  quadratic in the velocities and  $V$  depending only on the positions, and if on the system act other purely positional forces (conservative or not) then the resulting equations of motion are reversible if time reversal is simply defined as velocity reversal.

The gaussian principle has been somewhat overlooked in the Physics literature in Statistical Mechanics: its importance has been only recently brought again to the attention, see the review [HHP]. A notable, though ancient by now, exception is a paper of Gibbs, [Gi], which develops variational formulas which he relates to the Gauss principle of least constraint.

APPENDIX A2. HEAT THEOREM FOR MONOCYCLIC SYSTEMS. EVALUATION OF THE AVERAGE  $\langle \partial_V \varphi \rangle$ .

Consider a 1-dimensional system with potential  $\varphi(x)$  such that  $|\varphi'(x)| > 0$  for  $|x| > 0$ ,  $\varphi''(0) > 0$  and  $\varphi(x) \xrightarrow{x \rightarrow \infty} +\infty$  (in other words a 1-dimensional system in a confining potential). There is only one motion per energy value (up to a shift of the initial datum along its trajectory) and all motions are periodic so that the system is *monocyclic*. Assume also that the potential  $\varphi(x)$  depends on a parameter  $V$ .

One defines *state* a motion with given energy  $E$  and given  $V$ . And:

$U$  = total energy of the system  $\equiv K + \varphi$

$T$  = time average of the kinetic energy  $K$

$V$  = the parameter on which  $\varphi$  is supposed to depend

$p$  = - time average of  $\partial_V \varphi$

A state is parameterized by  $U, V$  and if such parameters change by  $dU, dV$  respectively we define:

$$dL = -pdV, \quad dQ = dU + pdV \quad (A2.1)$$

then:

*Theorem (Helmholtz): the differential  $(dU + pdV)/T$  is exact.*

In fact let:

$$S = 2 \log \int_{x_-(U,V)}^{x_+(U,V)} \sqrt{K(x; U, V)} dx = 2 \log \int_{x_-(U,V)}^{x_+(U,V)} \sqrt{U - \varphi(x)} dx \quad (A2.2)$$

( $\frac{1}{2}S$  is the logarithm of the action), so that:

$$S = \frac{\int (dU - \partial_V \varphi(x) dV) \frac{dx}{\sqrt{K}}}{\int K \frac{dx}{\sqrt{K}}} \quad (A2.3)$$

and, noting that  $\frac{dx}{\sqrt{K}} = \sqrt{\frac{2}{m}} dt$ , we see that the time averages are given by integrating with respect to  $\frac{dx}{\sqrt{K}}$  and dividing by the integral of  $\frac{1}{\sqrt{K}}$ . We find therefore:

$$dS = \frac{dU + pdV}{T} \quad (A2.4)$$

Boltzmann saw that this was not a simple coincidence: his interesting (and healthy) view of the continuum (which he probably never really considered more than a convenient artifact, useful for computing quantities describing a discrete world) led him to think that in some sense *monocyclicity was not a strong assumption*.

In general one can call *monocyclic* a system with the property that there is a curve  $\ell \rightarrow x(\ell)$ , parameterized by its curvilinear abscissa  $\ell$ , varying in an interval  $0 < \ell < L(E)$ , closed and such that  $x(\ell)$  covers all the positions compatible with the given energy  $E$ .

Let  $x = x(\ell)$  be the parametric equations so that the energy conservation can be written:

$$\frac{1}{2} m \dot{\ell}^2 + \varphi(x(\ell)) = E \quad (A2.5)$$

then if we suppose that the potential energy  $\varphi$  depends on a parameter  $V$  and if  $T$  is the average kinetic energy,  $p = -\langle \partial_V \varphi \rangle$  it is, for some  $S$ :

$$dS = \frac{dE + pdV}{T}, \quad p = -\langle \partial_V \varphi \rangle, \quad T = \langle K \rangle \quad (A2.6)$$

where  $\langle \cdot \rangle$  denotes time average.

The above can be applied to a gas in a box. Imagine the box containing the gas to be covered by a piston of section  $A$  and located to the right of the origin at distance  $L$ : so that  $V = AL$ .

The microscopic model for the piston will be a potential  $\bar{\varphi}(L - \xi)$  if  $x = (\xi, \eta, \zeta)$  are the coordinates of a particle. The function  $\bar{\varphi}(r)$  will vanish for  $r > r_0$ , for some  $r_0$ , and diverge to  $+\infty$  at  $r = 0$ . Thus  $r_0$  is the width of the layer near the piston where the force of the wall is felt by the particles that happen to roam there.

Noting that the potential energy due to the walls is  $\varphi = \sum_j \bar{\varphi}(L - \xi_j)$  and that  $\partial_V \varphi = A^{-1} \partial_L \varphi$  we must evaluate the time average of:

$$\partial_L \varphi(x) = - \sum_j \bar{\varphi}'(L - \xi_j) \quad (\text{A2.7})$$

As time evolves the particles with  $\xi_j$  in the layer within  $r_0$  of the wall will feel the force exercised by the wall and bounce back. Fixing the attention on one particle in the layer we see that it will contribute to the average of  $\partial_L \varphi(x)$  the amount:

$$\frac{1}{\text{total time}} 2 \int_{t_0}^{t_1} -\bar{\varphi}'(L - \xi_j) dt \quad (\text{A2.8})$$

if  $t_0$  is the first instant when the point  $j$  enters the layer and  $t_1$  is the instante when the  $\xi$ -component of the velocity vanishes "against the wall". Since  $-\bar{\varphi}'(L - \xi_j)$  is the  $\xi$ -component of the force, the integral is  $-2m|\dot{\xi}_j|$  (by Newton's law), provided  $\dot{\xi}_j > 0$  of course.

The number of such contributions to the average per unit time are therefore given by  $\rho_{wall} A \int_{v>0} 2mv f(v) v dv$  if  $\rho_{wall}$  is the density (average) of the gas near the wall and  $f(v)$  is the fraction of particles with velocity between  $v$  and  $v + dv$ . Using the ergodic hypothesis (*i.e.* the microcanonical ensemble) and the equivalence of the ensembles to evaluate  $f(v)$  it follows that:

$$p \stackrel{def}{=} \langle \partial_V \varphi \rangle = \rho_{wall} \beta^{-1} \quad (\text{A2.9})$$

where  $\beta^{-1} = k_B T$  with  $T$  the absolute temperature and  $k_B$  the Boltzmann's constant. That the (A2.9) yields the correct value of the pressure is well known, see [MP], in Classical Statistical Mechanics; in fact often it is even taken as microscopic definition of the pressure.

### APPENDIX A3. A PROOF OF THE FLUCTUATION THEOREM.

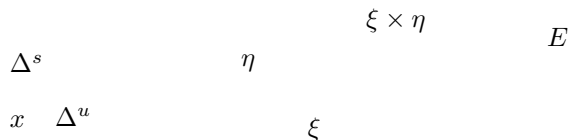
#### (A) Description of the SRB statistics.

A set  $E$  is a *rectangle* with center  $x$  and axes  $\Delta^u, \Delta^s$  if:

- 1)  $\Delta^u, \Delta^s$  are two connected surface elements of  $W_x^u, W_x^s$  containing  $x$ .
- 2) for any choice of  $\xi \in \Delta^u$  and  $\eta \in \Delta^s$  the local manifolds  $W_\xi^{s,\delta}$  and  $W_\eta^{u,\delta}$  intersect in one and only one point  $x(\xi, \eta) = W_\xi^{s,\delta} \cap W_\eta^{u,\delta}$ . The point  $x(\xi, \eta)$  will also be denoted  $\xi \times \eta$ .

- 3) the boundaries  $\partial\Delta^u$  and  $\partial\Delta^s$  (regarding the latter sets as subsets of  $W_x^u$  and  $W_x^s$ ) have zero surface area on  $W_x^u$  and  $W_x^s$ .
- 4)  $E$  is the set of points  $\Delta^u \times \Delta^s$ .

Note that *any*  $x' \in E$  can be regarded as the center of  $E$  because there are  $\Delta'^u, \Delta'^s$  both containing  $x'$  and such that  $\Delta^u \times \Delta^s \equiv \Delta'^u \times \Delta'^s$ . Hence each  $E$  can be regarded as a rectangle centered at any  $x' \in E$  (with suitable axes). See figure.



The circle is a small neighborhood of  $x$ ; the first picture shows the axes; the intermediate picture shows the  $\times$  operation and  $W_{\eta}^{u,\delta}, W_{\xi}^{s,\delta}$ ; the third picture shows the rectangle  $E$  with the axes and the four marked points are the boundaries  $\partial\Delta^u$  and  $\partial\Delta^s$ . The picture refers to a two dimensional case and the stable and unstable manifolds are drawn as flat, *i.e.* the  $\Delta$ 's are very small compared to the curvature of the manifolds. The center  $x$  is drawn in a central position, but it can be *any* other point of  $E$  provided  $\Delta^u$  and  $\Delta^s$  are correspondingly redefined. One should meditate on the symbolic nature of the drawing in the cases of higher dimension.

The *unstable boundary* of a rectangle  $E$  will be the set  $\partial_u E = \Delta^u \times \partial\Delta^s$ ; the *stable boundary* will be  $\partial_s E = \partial\Delta^u \times \Delta^s$ . The boundary  $\partial E$  is therefore  $\partial E = \partial_s E \cup \partial_u E$ . The set of the *interior points* of  $E$  will be denoted  $E^0$ . A *pavement* of  $M$  will be a covering  $\mathcal{E} = (E_1, \dots, E_{\mathcal{N}})$  of  $M$  by  $\mathcal{N}$  rectangles with pairwise disjoint interiors. The *stable (or unstable) boundary*  $\partial_s \mathcal{E}$  (or  $\partial_u \mathcal{E}$ ) of  $\mathcal{E}$  is the union of the stable (or unstable) boundaries of the rectangles  $E_j$ :  $\partial_u \mathcal{E} = \cup_j \partial_u E_j$  and  $\partial_s \mathcal{E} = \cup_j \partial_s E_j$ .

A pavement  $\mathcal{E}$  is called *markovian* if its stable boundary  $\partial_s \mathcal{E}$  retracts on itself under the action of  $S$  and its unstable boundary retracts on itself under the action of  $S^{-1}$ , [Sil], [Bo], [Ru1]; this means:

$$S\partial_s \mathcal{E} \subseteq \partial_s \mathcal{E}, \quad S^{-1}\partial_u \mathcal{E} \subseteq \partial_u \mathcal{E} \tag{A3.1}$$

Setting  $M_{j,j'} = 0, j, j' \in \{1, \dots, \mathcal{N}\}$ , if  $SE_j^0 \cap E_{j'}^0 = \emptyset$  and  $M_{j,j'} = 1$  otherwise we call  $C$  the set of sequences  $\underline{j} = (j_k)_{k=-\infty}^{\infty}, j_k \in \{1, \dots, \mathcal{N}\}$  such that  $M_{j_k, j_{k+1}} \equiv 1$ . The transitivity of the system  $(M, S)$  implies that  $M$  is *transitive*: *i.e.* there is a power of the matrix  $M$  with all entries positive. The space  $C$  will be called the space of the *compatible symbolic sequences*. If  $\mathcal{E}$  is a markovian pavement and  $\delta$  is small enough the map:

$$X : \underline{j} \in C \rightarrow x = \bigcap_{k=-\infty}^{\infty} S^{-k} E_{j_k} \in M \tag{A3.2}$$

is continuous and 1 - 1 between the complement  $M_0 \subset M$  of the set  $N = \cup_{k=-\infty}^{\infty} S^k \partial \mathcal{E}$  and the complement  $C_0 \subset C$  of  $X^{-1}(N)$ . This map is called the



*symbolic code* of the points of  $M$ : it is a code that associates with each  $x \notin N$  a sequence of symbols  $\underline{j}$  which are the labels of the rectangles of the pavement that are successively visited by the motion  $S^j x$ .

The symbolic code  $X$  transforms the action of  $S$  into the *left shift*  $\vartheta$  on  $C$ :  $SX(\underline{j}) = X(\vartheta \underline{j})$ . A key result, [Si1], is that it transforms the *volume measure*  $\mu_0$  on  $M$  into a *Gibbs distribution*, [LR], [Ru2],  $\bar{\mu}_0$  on  $C$  with formal Hamiltonian:

$$H(\underline{j}) = \sum_{k=-\infty}^{-1} h_-(\vartheta^k \underline{j}) + h_0(\underline{j}) + \sum_{k=0}^{\infty} h_+(\vartheta^k \underline{j}) \tag{A3.3}$$

where, see (2.1):

$$\begin{aligned} h_-(\underline{j}) &= -\log \Lambda_s(X(\underline{j})), & h_+(\underline{j}) &= \log \Lambda_u(X(\underline{j})), \\ h_0(\underline{j}) &= -\log \sin \alpha(X(\underline{j})) \end{aligned} \tag{A3.4}$$

If  $F$  is Hölder continuous on  $M$  the function  $\bar{F}(\underline{j}) = F(X(\underline{j}))$  can be represented in terms of suitable functions  $\Phi_k(j_{-k}, \dots, j_k)$  as:

$$\bar{F}(\underline{j}) = \sum_{k=1}^{\infty} \Phi_k(j_{-k}, \dots, j_k), \quad |\Phi_k(j_{-k}, \dots, j_k)| \leq \varphi e^{-\lambda k} \tag{A3.5}$$

where  $\varphi > 0, \lambda > 0$ . In particular  $h_{\pm}$  (and  $h_0$ ) enjoy the property (A3.5) (*short range*).

If  $\bar{\mu}_+, \bar{\mu}_-$  are the Gibbs states with formal Hamiltonians:

$$\sum_{k=-\infty}^{\infty} h_+(\vartheta^k \underline{j}), \quad \sum_{k=-\infty}^{\infty} h_-(\vartheta^k \underline{j}) \tag{A3.6}$$

the distributions  $\mu_{\pm}$  on  $M$ , images of  $\bar{\mu}_{\pm}$  via the code  $X$  in (A3.2), will be the *forward* and *backward statistics* of the volume distribution  $\mu_0$  (corresponding to  $\bar{\mu}_0$  via the code  $X$ ), [Si1]. This means that:

$$\lim_{T \rightarrow \infty} \frac{1}{T} \sum_{k=0}^{T-1} F(S^{\pm k} x) = \int_M \mu_{\pm}(dy) F(y) \equiv \mu_{\pm}(F) \tag{A3.7}$$

for all smooth  $F$  and for  $\mu_0$ -almost all  $x \in M$ . The distributions  $\mu_{\pm}$  are often called the *SRB distributions*, [ER]; the above statements and (A3.6),(A3.7) constitute the content of a well known theorem by Sinai, [Si1].

An approximation theorem for  $\mu_+$  can be given in terms of the *coarse graining* of  $M$  generated by the markovian pavement  $\mathcal{E}_T = \bigvee_{k=-T}^T S^{-k} \mathcal{E}$ .<sup>3</sup> If  $E_{j_{-T}, \dots, j_T} \equiv \bigcap_{k=-T}^T S^{-k} E_{j_k}$  and  $x_{j_{-T}, \dots, j_T}$  is a point chosen in the coarse grain set  $E_{j_{-T}, \dots, j_T}$ , so that its symbolic sequence is obtained by attaching to the right

---

<sup>3</sup> Where  $\vee$  denotes the operation which, given two pavements  $\mathcal{E}, \mathcal{E}'$  generates a new pavement  $\mathcal{E} \vee \mathcal{E}'$ : the rectangles of  $\mathcal{E} \vee \mathcal{E}'$  simply consist of all the intersections  $E \cap E'$  of pairs of rectangles  $E \in \mathcal{E}$  and  $E' \in \mathcal{E}'$ .

and to the left of  $j_{-T}, \dots, j_T$  arbitrary compatible sequences depending only on the symbols  $j_{\pm T}$  respectively. We define the distribution  $\mu_{T,\tau}$  by setting:

$$\mu_{T,\tau}(F) \equiv \int_M \mu_{T,\tau}(dx)F(x) = \frac{\sum_{j_{-T}, \dots, j_T} \bar{\Lambda}_{u,\tau}^{-1}(x_{j_{-T}, \dots, j_T})F(x_{j_{-T}, \dots, j_T})}{\sum_{j_{-T}, \dots, j_T} \bar{\Lambda}_{u,\tau}^{-1}(x_{j_{-T}, \dots, j_T})} \tag{A3.8}$$

$$\bar{\Lambda}_{u,\tau}(x) \stackrel{def}{=} \prod_{k=-\tau/2}^{\tau/2-1} \Lambda_u(S^k x)$$

Then for all smooth  $F$  we have:  $\lim_{T \geq \tau/2, \tau \rightarrow \infty} \mu_{T,\tau}(F) = \mu_+(F)$ . Note that equation (A3.8) can also be written:

$$\mu_{T,\tau}(F) = \frac{\sum_{j_{-T}, \dots, j_T} e^{-\sum_{k=-\tau/2}^{\tau/2-1} h_+(\vartheta^k \underline{j}^0)} F(X(\underline{j}^0))}{\sum_{j_{-T}, \dots, j_T} e^{-\sum_{k=-\tau/2}^{\tau/2-1} h_+(\vartheta^k \underline{j}^0)}} \tag{A3.9}$$

where  $\underline{j}^0 \in C$  is the compatible sequence agreeing with  $j_{-T}, \dots, j_T$  between  $-T$  and  $T$  (i.e.  $X(\underline{j}^0) = x_{j_{-T}, \dots, j_T} \in E_{j_{-T}, \dots, j_T}$ ) and continued outside as above.

*Notation:* to simplify the notations we shall write, when  $T$  is regarded as having a fixed value,  $\underline{q}$  for the elements  $\underline{q} = (j_{-T}, \dots, j_T)$  of  $\{1, \dots, \mathcal{N}\}^{2T+1}$ ; and  $E_{\underline{q}}$  will denote  $E_{j_{-T}, \dots, j_T}$  and  $x_{\underline{q}}$  the above point of  $E_{\underline{q}}$ .

*Remark:* Note that the weights in (A3.9) depend on the special choices of the centers  $x_{\underline{q}}$  (i.e. of  $\underline{j}^0$ ); but if  $x_{\underline{q}}$  varies in  $E_{\underline{q}}$  the weight of  $x_{\underline{q}}$  changes by at most a factor, bounded above by some  $B < \infty$  and below by  $B^{-1}$ , for all  $T \geq 0$ , and essentially depending only on the symbols corresponding to the sites close to  $\pm T$ .

The last formula shows that the forward statistics of  $\mu_0$  can be regarded as a Gibbs state for a *short range one dimensional spin chain with a hard core interaction*. The spin at  $k$  is the value of  $j_k \in \{1, \dots, \mathcal{N}\}$ ; the short range refers to the fact that the function  $h_+(j) \equiv \log \Lambda_u(X(\underline{j}))$ , ( $\Lambda_u(x)$  being Hölder continuous), can be represented as in (A3.5) where the  $\bar{\Phi}_k$  play the role of "many spins" interaction potentials and the hard core refers to the fact that the only spin configurations  $\underline{j}$  allowed are those with  $M_{j_k, j_{k+1}} \equiv 1$  for all integers  $k$ .

(B) *A Legendre transform.*

First the function (2.4) is converted to a function on the spin configurations  $\underline{j} \in C$ :

$$\tilde{\varepsilon}_\tau(\underline{j}) = \varepsilon_\tau(X(\underline{j})) = \frac{1}{\tau} \sum_{k=-\tau/2}^{\tau/2-1} L(\vartheta^k \underline{j}) \tag{A3.10}$$

where  $L(\underline{j}) \equiv \frac{1}{\eta_+} \log \Lambda^{\pm 1}(X(\underline{j}))$  has a *short range* representation of the type (A3.5).

The SRB distribution  $\mu_+$  is regarded (see above) as a Gibbs state  $\bar{\mu}_+$  with short range potential on the space  $C$  of the compatible symbolic sequences, associated with a Markov partition  $\mathcal{E}$ , [Si1], [Ru2]. Therefore, by general large deviations properties of short range Ising systems ([La], [El], [Ol], there is a function  $\bar{\zeta}(s)$  real analytic in  $s$  for  $s \in (-p^*, p^*)$  for a suitable  $p^* > 0$ , strictly convex and such that if  $p < p^*$  and  $[p - \delta, p + \delta] \subset (-p^*, p^*)$  we have:

$$\frac{1}{\tau} \log \bar{\mu}_+(\{\tilde{\varepsilon}_\tau(\underline{j}) \in [p - \delta, p + \delta]\}) \xrightarrow{\tau \rightarrow \infty} \max_{s \in [p - \delta, p + \delta]} \bar{\zeta}(s) \tag{A3.11}$$

and the difference between the r.h.s. and the l.h.s. tends to 0 bounded by  $D\tau^{-1}$  for a suitable constant  $D$ . The function  $\bar{\zeta}(s)$  is the Legendre transform of the function  $\lambda(\beta)$  defined as:

$$\lambda(\beta) = \lim_{\tau \rightarrow \infty} \frac{1}{\tau} \log \int e^{\tau \beta \tilde{\varepsilon}_\tau(\underline{j})} \bar{\mu}_+(d\underline{j}) \tag{A3.12}$$

*i.e.*  $\lambda(\beta) = \max_{s \in (-p^*, p^*)} (\beta s + \bar{\zeta}(s))$ , where the quantity  $p^*$  can be taken  $p^* = \lim_{\beta \rightarrow +\infty} g\beta^{-1}\lambda(\beta)$  and the function  $\lambda(\beta)$  is a real analytic, [CO], strictly convex function of  $\beta \in (-\infty, \infty)$  and  $\beta^{-1}\lambda(\beta) \xrightarrow{\beta \rightarrow \pm\infty} \pm p^*$ , *i.e.* it is asymptotically linear.

The above (A3.11) is a "large deviations theorem" for one dimensional spin chains with short range interactions, [La].

Hence it will be sufficient to prove the following; if  $I_{p,\delta} = [p - \delta, p + \delta]$ :

$$\frac{1}{\eta_+ \tau} \log \frac{\bar{\mu}_+(\{\tilde{\varepsilon}_\tau(\underline{j}) \in I_{p,\delta \mp \eta(\tau)}\})}{\bar{\mu}_+(\{\tilde{\varepsilon}_\tau(\underline{j}) \in I_{-p,\delta \pm \eta(\tau)}\})} \begin{cases} < p + \delta + \eta'(\tau) \\ > p - \delta - \eta'(\tau) \end{cases} \tag{A3.13}$$

with  $\eta(\tau), \eta'(\tau) \xrightarrow{\tau \rightarrow \infty} 0$ .

(C) *Thermodynamic formalism informations.*

In this section  $X$  will denote a lattice interval, *i.e.* a set of consecutive integers  $X = (x, x + 1, \dots, x + n - 1)$ : hence it should not be confused with the code  $X$  of (A3.2).

Let  $\underline{j}_X = (j_x, j_{x+1}, \dots, j_{x+n-1})$  if  $X = (x, x + 1, \dots, x + n - 1)$  and  $n$  is odd, and call  $\bar{X} = x + (n - 1)/2$  the *center* of  $X$ . If  $\underline{j} \in C$  is an infinite spin configuration we also denote  $\underline{j}_X$  the set of the spins with labels  $x \in X$ . The left shift of the interval  $X$  will be denoted by  $\vartheta$ ; *i.e.* by the same symbol of the left shift of a (infinite) spin configuration  $\underline{j}$ .

Let  $l_X(\underline{j}_X) = l^{(n)}(j_x, j_{x+1}, \dots, j_{x+n-1})$ , and  $h_X^+(\underline{j}_X) = h_+^{(n)}(j_x, j_{x+1}, \dots, j_{x+n-1})$  be translation invariant, *i.e.* functions such that  $l_{\vartheta X}(\underline{j}) \equiv l_X(\underline{j})$  and  $h_{\vartheta X}^+(\underline{j}) = h_X^+(\underline{j})$ , and such that the functions  $h_+(\underline{j})$ , see (2.4), and  $L(\underline{j})$ , see (A3.10), can be written for suitably chosen constants  $b_1, b_2, b, b'$ :

$$\begin{aligned}
 L(\underline{j}) &= \sum_{\bar{X}=0} l_X(\underline{j}_X), & h_+(\underline{j}) &= \sum_{\bar{X}=0} h_X^+(\underline{j}_X) \\
 |l_X(\underline{j}_X)| &\leq b_1 e^{-b_2 n}, & |h_X^+(\underline{j}_X)| &\leq b e^{-b'n}
 \end{aligned}
 \tag{A3.14}$$

Then  $\tau\tilde{\varepsilon}_\tau(\underline{j})$  can be written as  $\sum_{\bar{X}\in[-\tau/2, \tau/2-1]} l_X(\underline{j}_X)$ .

Hence  $\tau\tilde{\varepsilon}_\tau(\underline{j})$  can be approximated by  $\tau\tilde{\varepsilon}_\tau^M(\underline{j}) = \sum^{(M)} l_X(\underline{j}_X)$  where  $\sum^{(M)}$  means summation over the sets  $X \subseteq [-\frac{1}{2}\tau - M, \frac{1}{2}\tau + M]$ , while  $\bar{X}$  is in  $[-\frac{1}{2}\tau, \frac{1}{2}\tau - 1]$ . The approximation is described by:

$$|\tau\tilde{\varepsilon}_\tau^M(\underline{j}) - \tau\tilde{\varepsilon}_\tau(\underline{j})| \leq b_3 e^{-b_4 M} \tag{A3.15}$$

for suitable<sup>4</sup>  $b_3, b_4$  and for all  $M \geq 0$ . Therefore if  $I_{p,\delta} = [p - \delta, p + \delta]$  and  $M = 0$  we have:

$$\mu_+(\{\varepsilon_\tau(x) \in I_{p,\delta}\}) \begin{cases} \leq \bar{\mu}_+(\{\tilde{\varepsilon}_\tau^0 \in I_{p,\delta+b_3/\tau}\}) \\ \geq \bar{\mu}_+(\{\tilde{\varepsilon}_\tau^0 \in I_{p,\delta-b_3/\tau}\}) \end{cases} \tag{A3.16}$$

It follows from the general theory of 1-dimensional Gibbs distributions, [Ru2], that the  $\bar{\mu}_+$ -probability of a spin configuration which coincides with  $\underline{j}_{[-\tau/2, \tau/2]}$  in the interval  $[-\frac{1}{2}\tau, \frac{1}{2}\tau]$ ,<sup>5</sup> is:

$$\frac{[e^{-\sum^* h_X^+(\underline{j}_X)}]}{\sum_{\underline{j}'_{[-\tau/2, \tau/2]}} [\cdot]} P(\underline{j}_{[-\tau/2, \tau/2]}) \tag{A3.17}$$

where  $\sum^*$  denotes summation over all the  $X \subseteq [-\tau/2, \tau/2 - 1]$ ; the denominator is just the sum of terms like the numerator, evaluated at a generic (compatible) spin configuration  $\underline{j}'_{[-\tau/2, \tau/2]}$ ; finally  $P$  verifies the bound, [Ru2]:

$$B_1^{-1} < P(\underline{j}_{[-\tau/2, \tau/2]}) < B_1 \tag{A3.18}$$

with  $B_1$  a suitable constant independent of  $\underline{j}_{[-\tau/2, \tau/2]}$  and of  $\tau$  ( $B_1$  can be explicitly estimated in terms of  $b, b'$ ). Therefore from (A3.16) and (A3.17) we deduce for any  $T \geq \tau/2$ :

$$\begin{aligned}
 \mu_+(\{\varepsilon_\tau(x) \in I_{p,\delta}\}) &\leq \bar{\mu}_+(\{\tilde{\varepsilon}_\tau^0 \in I_{p,\delta+b_3/\tau}\}) \leq \\
 &\leq B_2 \mu_{T,\tau}(\{\tilde{\varepsilon}_\tau^0 \in I_{p,\delta+b_3/\tau}\}) \leq B_2 \mu_{T,\tau}(\{\tilde{\varepsilon}_\tau \in I_{p,\delta+2b_3/\tau}\})
 \end{aligned}
 \tag{A3.19}$$

for some constant  $B_2 > 0$ ; and likewise a lower bound is obtained by replacing  $B_2$  by  $B_2^{-1}$  and  $b_3$  by  $-b_3$ .

<sup>4</sup> One can check from (A3.14), that the constants  $b_3, b_4$  can be expressed as simple functions of  $b_1, b_2$ .

<sup>5</sup> *i.e.* the spin configurations  $\underline{j}'$  such that  $j'_x = j_x, x \in [-\frac{1}{2}\tau, \frac{1}{2}\tau]$ .

Then if  $p < p^*$  and  $I_{p,\delta} \subset (-p^*, p^*)$  the set of the rectangles  $E \in \bigvee_{-T}^T S^{-k} \mathcal{E}$  with center  $x$  such that  $\varepsilon_\tau(x) \in I_{p,\delta}$  is not empty, as it follows from the strict convexity and the asymptotic linearity of the function  $\lambda(\beta)$  in (A3.12).

We immediately deduce the lemma:

*Lemma 1: the distributions  $\mu_+$  and  $\mu_{T,\tau}$ ,  $T \geq \frac{1}{2}\tau$ , verify:*

$$\frac{1}{\tau\bar{\eta}_+} \log \frac{\mu_+(\{\varepsilon_\tau(x) \in I_{p,\delta \mp 2b_3/\tau}\})}{\mu_+(\{\varepsilon_\tau(x) \in -I_{p,\delta \pm 2b_3/\tau}\})} \begin{cases} < \frac{\log B_2^2}{\tau\bar{\eta}_+} + \frac{1}{\tau\bar{\eta}_+} \log \frac{\mu_{T,\tau}(\{\tilde{\varepsilon}_\tau \in I_{p,\delta}\})}{\mu_{T,\tau}(\{\tilde{\varepsilon}_\tau \in -I_{p,\delta}\})} \\ > -\frac{\log B_2^2}{\tau\bar{\eta}_+} + \frac{1}{\tau\bar{\eta}_+} \log \frac{\mu_{T,\tau}(\{\tilde{\varepsilon}_\tau \in I_{p,\delta}\})}{\mu_{T,\tau}(\{\tilde{\varepsilon}_\tau \in -I_{p,\delta}\})} \end{cases} \tag{A3.20}$$

for  $I_{p,\delta} \subset [-p^*, p^*]$  and for  $\tau$  so large that  $p + \delta + 2b_3/\tau < p^*$ .

Hence (A3.13) will follow if we can prove:

*Lemma 2: there is a constant  $\bar{b}$  such that the approximate SRB distribution  $\mu_{T,\tau}$  verifies:*

$$\frac{1}{\bar{\eta}_+\tau} \log \frac{\mu_{T,\tau}(\{\tilde{\varepsilon}_\tau \in I_{p,\delta}\})}{\mu_{T,\tau}(\{\tilde{\varepsilon}_\tau \in -I_{p,\delta}\})} \begin{cases} \leq p + \delta + \bar{b}/\tau \\ \geq p - \delta - \bar{b}/\tau \end{cases} \tag{A3.21}$$

for  $\tau$  large enough (so that  $\delta + \bar{b}/\tau < p^* - p$ ) and for all  $T \geq \tau/2$ .

The latter lemma will be proved in §4 and it is the only statement that does not follow from the already existing literature.

*(D) Time reversal symmetry implications*

The relation (A3.20) holds for any choice of the Markov partition  $\mathcal{E}$ . Note that if  $\mathcal{E}$  is a Markov pavement so is  $i\mathcal{E}$  (because  $iS = S^{-1}i$  and  $iW_x^u = W_{ix}^s$ ); furthermore if  $\mathcal{E}_1$  and  $\mathcal{E}_2$  are Markov pavements then  $\mathcal{E} = \mathcal{E}_1 \vee \mathcal{E}_2$  is also markovian. Therefore:

*Lemma 3: there exists a time reversal Markov pavement  $\mathcal{E}$ , i.e. a Markov pavement such that  $\mathcal{E} = i\mathcal{E}$ .*

This can be seen by taking any Markov pavement  $\mathcal{E}_0$  and setting  $\mathcal{E} = \mathcal{E}_0 \vee i\mathcal{E}_0$ . Alternatively one could construct the Markov pavement in such a way that it verifies automatically the symmetry [G2]. Since the center of a rectangle  $E_q \in \mathcal{E}_T$  can be taken to be any point  $x_q$  in the rectangle  $E_q$  we can and shall suppose that the centers of the rectangles in  $\mathcal{E}_T$  have been so chosen that the center of  $iE_q$  is  $ix_q$ , i.e. the time reversal of the center  $x_q$  of  $E_q$ .

For  $\tau$  large enough the set of configurations  $\underline{q} = \underline{j}_{[-T,T]}$  such that  $\varepsilon_\tau(x) \in I_{p,\delta}$  for all  $x \in E_{\underline{q}}$  is not empty<sup>6</sup> and the ratio in (A3.21) can be written, if  $x_{\underline{q}}$  is the center of  $E_{\underline{q}} \in \mathcal{E}_T$ , as:

---

<sup>6</sup> Note that  $p^* = \sup_x \limsup_{\tau \rightarrow +\infty} \varepsilon_\tau(S^{\tau/2}x)$  and let  $p \in (-p^* + \delta, p^* - \delta)$ ; furthermore  $\zeta(s)$  is smooth, hence  $> -\infty$ , for all  $|s| < p^*$ .

$$\frac{\sum_{\varepsilon_\tau(x_q) \in I_{p,\delta}} \bar{\Lambda}_{u,\tau}^{-1}(x_q)}{\sum_{\varepsilon_\tau(x_q) \in -I_{p,\delta}} \bar{\Lambda}_{u,\tau}^{-1}(x_q)} = \frac{\sum_{\varepsilon_\tau(x_q) \in I_{p,\delta}} \bar{\Lambda}_{u,\tau}^{-1}(x_q)}{\sum_{\varepsilon_\tau(x_q) \in I_{p,\delta}} \bar{\Lambda}_{u,\tau}^{-1}(ix_q)} \tag{A3.22}$$

Define  $\bar{\Lambda}_{s,\tau}(x)$  as in (A3.8) with  $s$  replacing  $u$ : then the time reversal symmetry implies that  $\bar{\Lambda}_{u,\tau}(x) = \bar{\Lambda}_{s,\tau}^{-1}(ix)$ , see remark 2) following definition (B), §2.<sup>7</sup> This permits us to change (A3.22) into:

$$\frac{\sum_{\varepsilon_\tau(x_q) \in I_{p,\delta}} \bar{\Lambda}_{u,\tau}^{-1}(x_q)}{\sum_{\varepsilon_\tau(x_q) \in I_{p,\delta}} \bar{\Lambda}_{s,\tau}(x_q)} \begin{cases} < \max_q \bar{\Lambda}_{u,\tau}^{-1}(x_q) \bar{\Lambda}_{s,\tau}^{-1}(x_q) \\ > \min_q \bar{\Lambda}_{u,\tau}^{-1}(x_q) \bar{\Lambda}_{s,\tau}^{-1}(x_q) \end{cases} \tag{A3.23}$$

where the maxima are evaluated as  $q$  varies with  $\varepsilon_\tau(x_q) \in I_{p,\delta}$ .

By (2.1) we can replace  $\bar{\Lambda}_{u,\tau}^{-1}(x) \bar{\Lambda}_{s,\tau}^{-1}(x)$  with  $\bar{\Lambda}_\tau^{-1}(x) B^{\pm 1}$ , see (A3.8), (2.4); thus noting that by definition of the set of  $q$ 's in the maximum in (A3.23) we have  $\frac{1}{\eta_+} \log \bar{\Lambda}_\tau^{-1}(x_q) \in I_{p,\delta}$ , we see that (A3.21) follows with  $\bar{b} = \frac{1}{\eta_+} \log B$ .

*Corollary: the above analysis gives us a concrete bound on the speed at which the limits in (2.6) are approached. Namely the error has order  $O(\tau^{-1})$ .*

This is so because the limit (A3.11) is reached at speed  $O(\tau^{-1})$ ; furthermore the regularity of  $\lambda(s)$  in (A3.11) and the size of  $\eta(\tau), \eta'(\tau)$  and the error term in (A3.21) have all order  $O(\tau^{-1})$ .

The above analysis proves a large deviation result for the probability distribution  $\mu_+$ : since  $\mu_+$  is a Gibbs distribution, see (A3.6), various other large deviations theorems hold for it, [DV], [El], [Ol], but unlike the above they are not related to the time reversal symmetry.

APPENDIX A4: HEURISTIC PROOF OF THE LOCAL FLUCTUATION THEOREM.

(A) Markov partitions and symbolic dynamics for the chain.

The reduction of the dynamical nonequilibrium problem of a weakly interacting chain of Anosov maps, see §3, to a short range lattice spin system equilibrium problem is the content of (A), (B) of this appendix, see [Ga7]. This is an extension of the corresponding analysis in Appendix A3 for the case of a single Anosov map: it is necessary to discuss it again in order to exploit the short range nature of the coupling and its weakness in order to obtain results independent on the size  $N$  of the chain.

Let  $\bar{\mathcal{P}}_0 = (E_1^0, \dots, E_{N_0}^0)$  be a Markov partition, see [Sil], for the unperturbed "single site" system  $(\bar{M}_0 \times \bar{M}_0, \bar{S}_0 \times \bar{S}_0^{-1})$ . Then  $\bar{\mathcal{P}}_0^{2N+1} = \{E_\alpha\}$ ,

---

<sup>7</sup> Here it is essential that  $\bar{\Lambda}_{u,\tau}(x)$  is the expansion of the unstable manifold between the initial point  $S^{-\tau/2}x$  and the final point  $S^{\tau/2}x$ : i.e. it is a trajectory of time length  $\tau$ , which at its central time is in  $x$ .

$\alpha = (\rho_{-N}, \dots, \rho_N)$  with  $E_\alpha = E_{\rho_{-N}}^0 \times E_{\rho_{-N+1}}^0 \times \dots \times E_{\rho_N}^0$  is a Markov partition of  $(\overline{M}_0^{2(2N+1)}, S_0)$ .

The perturbation, *if small enough*, will deform the partition  $\overline{\mathcal{P}}_0^{2N+1}$  into a Markov partition  $\mathcal{P}$  for  $(M, S)$  changing only “slightly” the partition  $\overline{\mathcal{P}}_0^{2N+1}$ . The work [PS] shows that the above “ $\varepsilon$  small enough” *mean that  $\varepsilon$  has to be chosen small but that it can be chosen  $N$ -independent*, as we shall always suppose in what follows.

Under such circumstances we can establish a correspondence between points of  $M$  that have the same “symbolic history” (or “symbolic dynamics”) along  $\overline{\mathcal{P}}_0^{2N+1}$  under  $S_0$  and along  $\mathcal{P}$  under  $S$ ; we shall denote it by  $h$ ; see [PS].

The Markov partition  $\overline{\mathcal{P}}_0^{2N+1}$  for  $S_0$  associates with each point  $\underline{x} = (x_{-N}, \dots, x_N)$  a sequence  $(\sigma_{i,j})$ ,  $i \in [-N, N], j \in (-\infty, \infty)$  of symbols so that  $(\sigma_{i,j})_{j=-\infty}^\infty$  is the free symbolic dynamics of the point  $x_i$ . We call the first label  $i$  of  $\sigma_{i,j}$  a “space-label” and the second a “time-label”. Not all sequences can arise as histories of points: however (by the definition of  $h$ , see above) precisely the same sequences arise as histories of points along  $\mathcal{P}_0$  under the free evolution  $S_0$  or along  $\mathcal{P}$  under the interacting evolution  $S$ .

The map  $h$  is Hölder continuous and “short ranged”:

$$|h(\underline{x})_i - h(\underline{x}')_i| \leq C \sum_j \varepsilon^{|i-j|\gamma'} |x_j - x'_j|^\gamma \tag{A4.1}$$

for some  $\gamma, \gamma', C > 0$ , [PS], if  $|x - y|$  denotes the distance in  $\overline{M}_0 \times \overline{M}_0$  (*i.e.* in the single site phase space).

Furthermore the code  $\underline{x} \leftrightarrow \underline{\sigma}$  associating with  $\underline{x}$  its “history” or “symbolic dynamics”  $\underline{\sigma}(\underline{x})$  along the partition  $\mathcal{P}$  under the map  $S$  is such that, fixed  $j$ :

$$\underline{\sigma}(\underline{x})_i = \underline{\sigma}(\underline{x}')_i \text{ for } |i - j| \leq \ell \quad \Rightarrow \quad |x_j - x'_j| \leq C\varepsilon^{\gamma\ell} \tag{A4.2}$$

The inverse code associating with a history  $\underline{\sigma}$  a point with such history will be denoted  $\underline{x}(\underline{\sigma})$ .

If  $\underline{x} = (x_{-N}, \dots, x_N)$  is coded into  $\underline{\sigma}(\underline{x}) = (\underline{\sigma}_{-N}, \dots, \underline{\sigma}_N) = (\sigma_{i,j})$ , with  $i = -N, \dots, N$ , and  $j \in (-\infty, +\infty)$ , the short range property holds also in the time direction. This means that, fixed  $i_0$ :

$$\sigma_{i,j} = \sigma'_{i,j} \text{ for } |i - i_0| < k, |j| < p \quad \Rightarrow \quad |\underline{x}(\underline{\sigma})_{i_0} - \underline{x}(\underline{\sigma}')_{i_0}| \leq C\varepsilon^{\gamma k} e^{-\kappa p} \tag{A4.3}$$

for some  $\kappa, \gamma, C > 0$ , see lemma 1 of [PS]. The constants  $\kappa, \gamma, C, C', B, B' > 0$  above and below should not be thought to be the same even when denoted by the same symbol: however they could be *a posteriori* fixed so that to equal symbols correspond equal values.

By construction the codes  $\underline{x} \leftrightarrow \underline{\sigma}(\underline{x})$  commute with time evolution.

The sequences  $(\sigma_{i,j})$  which arise as symbolic dynamics along  $\overline{\mathcal{P}}_0$  under the free single site evolution of a point  $x_i$  are subject to constraints, that we call “vertical”, imposing that  $T_{\sigma_{i,j}, \sigma_{i,j+1}}^0 \equiv 1$  for all  $j$ , if  $T_{\sigma, \sigma'}$  denotes the “compatibility matrix”

of the “free single site evolution” (*i.e.*  $T_{\sigma,\sigma'}^0 = 1$  if the  $\bar{S}_0 \times \bar{S}_0^{-1}$  image of  $E_\sigma$  intersects the interior of  $E_{\sigma'}$  and  $T_{\sigma,\sigma'}^0 = 0$  otherwise). We call the latter condition a “compatibility condition” for the spins in the  $i$ -th column.

The mixing property of the free evolution immediately implies that a large enough power of the compatibility matrix  $T^0$  has all entries positive. This means that for each symbol  $\sigma$  we can find semiinfinite sequences:

$$\begin{aligned} \sigma_B(\sigma) &= (\dots, \sigma_{-1}, \sigma_0 \equiv \sigma), & T_{\sigma_{i-1}, \sigma_i}^0 &= 1, & \text{for all } i \leq 0 \\ \sigma_T(\sigma) &= (\sigma \equiv \sigma_0, \sigma_1, \dots), & T_{\sigma_i, \sigma_{i+1}}^0 &= 1, & \text{for all } i \geq 0 \end{aligned} \quad (A4.4)$$

and defines two functions  $\sigma_B, \sigma_T$ , called “compatible extensions”, defined on the set  $\{1, \dots, \mathcal{N}_0\}$  of labels of the single site Markov partition  $\mathcal{P}_0$ , with values in the compatible semiinfinite sequences.

In fact there are (uncountably) many ways of performing such compatible extensions “from the bottom” and “from the top” of the symbol  $\sigma$  into semiinfinite compatible sequences of symbols. We imagine to select one pair  $\sigma_B, \sigma_T$  arbitrarily, once and for all, and call such a selection a “choice of boundary conditions” or “of extensions”, on symbolic dynamics, for reasons that should become clear shortly. All this seems unavoidable and it is closely parallel to the corresponding discussion in the analysis of the simpler case of a single Anosov system discussed in Appendix A3, see the discussion preceding (A3.8).

We shall therefore be able to “extend in a standard way” any finite compatible block<sup>8</sup>  $Q$  of spins:

$$\underline{\sigma}_Q = (\sigma_{i,j})_{i \in L, j \in K}, \quad L = (a - \ell, a + \ell), \quad K = (b - m, b + m) \quad (A4.5)$$

by setting  $\sigma_{i,j} = \sigma_B(\sigma_{i,b-n})_{b-n-j}$  for  $j < b - n$  and  $\sigma_{i,j} = \sigma_T(\sigma_{i,b+n})_{j-b-n}$  for  $j > b + n$ . Here  $a, b, \ell, m$  are integers.

In the free evolution there are no “horizontal” compatibility constraints; hence it is always possible to extend the finite block  $\underline{\sigma}_Q = (\sigma_{i,j})_{i \in L, j \in K}$  to a “full spin configuration” sequence  $(\sigma_{i,j})_{i \in [-N, N], j \in (-\infty, \infty)}$ , obtained by continuing the columns in the just described standard way, using the boundary extensions  $\sigma_B, \sigma_T$ , above the top and below the bottom, into a biinfinite sequence and also by extending the spin configuration to the right and to the left to a sequence with spatial labels running over the full spatial range  $[-N, N]$ . One simply defines  $\sigma_{i,j}$  for  $i \notin L$  as *any* (but prefixed once and for all) compatible biinfinite sequence of symbols (the same for each column).

The allowed symbolic dynamics sequences for the free dynamics (on  $\mathcal{P}_0$ ) and for the interacting dynamics (on  $\mathcal{P}$ ) *coincide* because the free and the interacting dynamics are conjugated by the map  $h$ , [PS]. Therefore the above operations make sense *also* if the sequences are regarded as symbolic sequences of the interacting dynamics, as we shall do from now on.

To conclude: given a “block”  $\underline{\sigma}_Q$  of symbols, with space–time labels  $(i, j) \in Q = L \times K$ , we can associate with it a point  $\underline{x} \in M$  whose symbolic dynamics

<sup>8</sup> A block  $(\sigma_{i,j})$ ,  $(i, j) \in Q$ , is naturally said to be “compatible” if  $T_{\sigma_{i,j}, \sigma_{i,j+1}}^0 = 1$  for all  $(i, j) \in Q$  such that  $(i, j + 1)$  is also in  $Q$ .



is the above described standard extension of  $\underline{\sigma}_Q$ . The latter depends only on the values of  $\sigma_{i,j}$  for  $j$  at the top or at the bottom of  $Q$  and, of course, on the boundary conditions  $\sigma_B, \sigma_T$  chosen to begin with.

(B) *Expansion and contraction rates.*

Consider the rates of variation of the phase space volume,  $\lambda_0(\underline{x})$ , or, respectively, of the surface elements of the stable and unstable manifolds  $\lambda_s(\underline{x})$  and  $\lambda_u(\underline{x})$  at the point  $\underline{x}$ : they are the logarithms of the Jacobian determinants  $\partial S(\underline{x}), \partial_{(\alpha)} S(\underline{x}), \alpha = s, u$ , where  $\partial_{(\alpha)}$  denotes the Jacobian of  $S$  as a map of  $W_{\underline{x}}^{\alpha}$  to  $W_{S\underline{x}}^{\alpha}$  where  $\alpha = u, s$  distinguishes the unstable manifold  $W_{\underline{x}}^u$  of  $\underline{x}$  or the stable manifold  $W_{\underline{x}}^s$  of  $\underline{x}$ :

$$\lambda_{\alpha}(\underline{x}) = -\log |\det \partial_{(\alpha)} S(\underline{x})|, \quad \alpha = 0, u, s \tag{A4.6}$$

where  $\partial_{(0)} S(\underline{x}) \stackrel{def}{=} \partial S(\underline{x})$ .

A hard technical problem is to represent  $\lambda_{\alpha}(\underline{x})$  in terms of the “symbolic history” of  $\underline{x}$  along  $\mathcal{P}$ , *i.e.* in terms of compatible sequences  $\underline{\sigma} = (\sigma_{i,j})$  with  $i \in (-N, N), j \in (-\infty, \infty)$ . The rates  $\lambda_{\alpha}(\underline{x})$  can be expressed as:

$$\lambda_{\alpha}(\underline{x}) = -\log \left| \det \frac{\partial S}{\partial \underline{x}} \Big|_{W^{\alpha}(\underline{x})} \right| = \sum_{L \subset [-N, N]} \tilde{\delta}_L^{(\alpha)}(\underline{x}_L) \tag{A4.7}$$

where  $L$  is an interval in  $[-N, N]$  (with  $\pm(N+1)$  identified with  $\mp N$ ), [PS].

For  $\alpha = 0$  this can be done by noting that the matrix  $J = \frac{\partial S}{\partial \underline{x}}$  has an almost diagonal structure:  $J(\underline{x}) = J_0(\underline{x})(1 + \Delta(\underline{x}))$  where  $J_0(\underline{x})$  is the Jacobian matrix of the free motion  $J_0(\underline{x}) = \bar{J}_0(x_{-N}) \times \bar{J}_0(x_{-N+1}) \times \dots \times \bar{J}_0(x_N)$  if  $\underline{x} = (x_{-N}, \dots, x_N)$  and if  $D = (\prod_{j=-N}^N \det \bar{J}_0(x_j))$ :

$$\det J = D \cdot e^{\text{Tr} \log(1 + \Delta(\underline{x}))} = D \cdot e^{\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} \text{Tr} \Delta(\underline{x})^k} \tag{A4.8}$$

which leads to (A4.7) if one uses that the matrix elements  $\Delta_{p,q} = J_0^{-1}(\underline{x}) \partial_{x_p} \partial_{x_q} J(\underline{x})$  are essentially local, *i.e.* bounded by  $B(C\varepsilon)^{|p-q|\gamma}$  for some  $\gamma, C, B > 0$  (see (3.1), (3.2), (A4.3)).

For  $\alpha = u, s$  (A4.7) can be derived in a similar way using also that:

(1) the stable and unstable manifolds of  $\underline{x}$  consist of points  $\underline{y}$  which have eventually, respectively towards the future or towards the past, the same history of  $\underline{x}$ ,

(2) they are described in a local system of coordinates around  $\underline{x} = (\dots, x_{-1}, x_0, x_1, \dots)$  by smooth “short range” functions. Suppose, in fact, that on each factor  $M_0$  we introduce a local system of coordinates  $(\alpha, \beta)$  around the point  $x_i \in M_0$ , such that the unperturbed stable and unstable manifolds are described locally by graphs  $(\alpha, f_s(\alpha))$  or  $(f_u(\beta), \beta)$ .

The unperturbed stable and unstable manifolds will be smooth graphs  $(\alpha_i, f_s(\alpha_i))$  or  $(f_u(\beta_i), \beta_i)$  with  $\alpha_i$  varying close to  $\bar{\alpha}_i$  and  $\beta_i$  close to  $\bar{\beta}_i$ , with  $(\bar{\alpha}_i, \bar{\beta}_i)$  being the coordinates of  $x_i$ .

Fixed a point  $\underline{x} = (x_{-N}, \dots, x_N)$  with coordinates  $(\bar{\alpha}_i, \bar{\beta}_i)_{i=-N, \dots, N}$  the perturbed manifolds of the point  $\underline{x}$  will be described by smooth (at least  $C^2$  and in fact of any prefixed smoothness if  $\varepsilon$  is sufficiently small) functions  $W^s(\underline{\alpha}), W^u(\underline{\beta})$  of  $\underline{\alpha} = (\alpha_i)_{i=-N, N}$  or of  $\underline{\beta} = (\beta_i)_{i=-N, N}$  which are “local”; *i.e.* if  $\underline{\alpha}$  and  $\underline{\alpha}'$  agree on the sites  $i - \ell, i + \ell$  or if  $\underline{\beta}$  and  $\underline{\beta}'$  agree on the sites  $i - \ell, i + \ell$  then:

$$\begin{aligned} \|W^u(\underline{\beta})_i - f_u(\beta_i)\|_{C^2} &< C\varepsilon, & \|W^u(\underline{\beta})_i - W^u(\underline{\beta}')_i\|_{C^2} &< C\varepsilon^\ell \\ \|W^s(\underline{\alpha})_i - f_s(\alpha_i)\|_{C^2} &< C\varepsilon, & \|W^s(\underline{\alpha})_i - W^s(\underline{\alpha}')_i\|_{C^2} &< C\varepsilon^\ell \end{aligned} \tag{A4.9}$$

for some  $C > 0$ , see [PS] lemmata 1,2. Here the norms in the first column are the norms in  $C^2$  as functions of the arguments  $\underline{\beta}$  or respectively  $\underline{\alpha}$ , while the norms in the second column are  $C^2$  norms evaluated (of course) after identifying the arguments of  $\underline{\beta}$  (or  $\underline{\alpha}$ ) and  $\underline{\beta}'$  (or  $\underline{\alpha}'$ ) with labels  $j$  such that  $|i - j| \leq \ell$ .

(3) If we consider the dependence of the planes tangent to the stable and unstable manifolds  $W^s_{\underline{x}}, W^u_{\underline{x}}$  at  $\underline{x}$  we find that they are Hölder continuous as functions of  $\underline{x}$ :

$$|(dW^{\alpha}_{\underline{x}})_i - (dW^{\alpha}_{\underline{y}})_i| < C \sum_j \varepsilon^{|i-j|\kappa} |x_j - y_j|^\gamma, \quad \alpha = u, s \tag{A4.10}$$

where  $(dW^{\alpha}_{\underline{x}})_i$  denoted the components relative to the  $i$ -th coordinate of  $\underline{x}$  of the tangent plane to  $W^{\alpha}_{\underline{x}}$  and  $C, \kappa, \gamma > 0$ .

The above properties and the Hölder continuity (A4.1), (A4.2), (A4.3) imply that the “horizontal potentials”  $\tilde{\delta}_L^{(\alpha)}(\underline{x}_L)$  in (A4.7) are “short ranged”:

$$|\tilde{\delta}_L^{(\alpha)}(\underline{x}_L)| \leq B (C\varepsilon)^{(|L|-1)\gamma}, \quad \alpha = u, s \tag{A4.11}$$

for some  $B, C, \gamma > 0$ ; we denote  $|L|$  the number of points in the set  $L$ .

We shall use the symbolic representation of  $\underline{x} \in M$  to express the rates  $\lambda^{(\alpha)}(\underline{x})$ . For this purpose let  $\underline{x} = (x_i)_{i=-N, N}$  and suppose that such  $\underline{x}$  corresponds to the symbolic dynamics sequence  $\underline{\sigma} = (\underline{\sigma}_j)_{j=-\infty}^{\infty}$  where  $\underline{\sigma}_j = (\sigma_{-N, j}, \dots, \sigma_{N, j})$ . We denote  $\underline{\sigma}_L$  the sequence  $\underline{\sigma}_L = (\sigma_{i, j})_{i \in L, j = -\infty, \infty}$ .

Then  $\underline{\sigma}_L$  *does not* determine  $\underline{x}_L$  (unless there is no interaction, *i.e.*  $\varepsilon = 0$ ): however the short range property, (A4.3), of the symbolic codes and of the map  $h$  conjugating the free evolution and the interacting evolution shows that, if  $L'$  is a larger interval containing  $L$  and centered around  $L$ , then the sequence  $\underline{\sigma}_{L'}$  determines each point of  $\underline{x}_L$  within an approximation  $\leq (C\varepsilon)^{(|L'|-|L|)\gamma}$ . Hence we can define  $\widehat{\delta}_L^{(\alpha)}(\underline{\sigma}_L)$  so that:

$$\begin{aligned} \tilde{\delta}_L^{(\alpha)}(\underline{x}_L) &= \sum_{L' \supset L} \widehat{\delta}_{L'}^{(\alpha)}(\underline{\sigma}_{L'}), & |\widehat{\delta}_L^{(\alpha)}(\underline{\sigma}_L)| &< B' (C'\varepsilon^\gamma)^{|L|-1} \\ \lambda_\alpha(\underline{x}) &= \sum_L 2^{|L|} \widehat{\delta}_L^{(\alpha)}(\underline{\sigma}_L) \end{aligned} \tag{A4.12}$$

for some  $B', C', \gamma$ . This leads to expressing  $\lambda_\alpha(\underline{x})$  in terms of the symbolic dynamics of  $\underline{x}$  and of the “space-localized” potentials  $\widehat{\delta}_L^{(\alpha)}(\underline{\sigma}_L)$ .

Let  $Q_n = L \times K$  where  $K = [-n, n]$  is a “time–interval” and set

$$\mathcal{L}_{Q_n}^\alpha(\underline{\sigma}_{Q_n}) \stackrel{def}{=} \widehat{\delta}_L^{(\alpha)}([\underline{\sigma}_{Q_n}]) - \widehat{\delta}_L^{(\alpha)}([\underline{\sigma}_{Q_{n-1}}]) \tag{A4.13}$$

if  $n \geq 1$  and  $[\underline{\sigma}_{Q_n}]$  denotes a *standard extension* (in the sense of §3) of  $\underline{\sigma}_{Q_n}$ ; or just set  $\mathcal{L}_{Q_0}^\alpha \stackrel{def}{=} \widehat{\delta}_L^{(\alpha)}([\underline{\sigma}_{Q_0}])$  for  $n = 0$ . We define  $\mathcal{L}_Q^\alpha(\underline{\sigma}_Q)$  for  $Q = L \times K$  and  $K$  not centered (*i.e.*  $K = (a - n, a + n)$ ,  $a \neq 0$ ) so that it is translation invariant with respect to space time translations (of course the horizontal translation invariance is already implied by the above definitions and the corresponding translation invariance of  $\widehat{\delta}_L^{(\alpha)}$ ).

The *remarkable property*, consequence of the Hölder continuity of the functions in (A4.6) and of the (A4.3),(A4.12), see [PS], is that for some  $\gamma, \kappa, B, C > 0$ :

$$|\mathcal{L}_Q^\alpha(\underline{\sigma}_Q)| \leq B(C\varepsilon^\gamma)^i e^{-\kappa j} \tag{A4.14}$$

if  $i, j$  are the horizontal and vertical dimensions of  $Q$ .

In this way we define a “space–time local potential”  $\mathcal{L}_Q^{(\alpha)}$  which is, by construction, translation invariant and such that, if  $\Lambda$  denotes the box  $\Lambda = [-N, N] \times [-M, M]$  the following representations for the rates in (A4.6) hold:

$$-\log |\det \partial_{(\alpha)} S^{2M+1}(S^{-M} \underline{x})| = \sum_{Q \subset \Lambda} \mathcal{L}_Q^\alpha(\underline{\sigma}_Q) + O(|\partial\Lambda|) \tag{A4.15}$$

where  $O(|\partial\Lambda|)$  is a “boundary correction” due to the fact that in (A4.15) one should really extend the sum over the  $Q$ ’s centered at height  $\leq M$  and contained in the infinite strip  $[-N, N] \times [-\infty, \infty]$  rather than restricting  $Q$  to the region  $\Lambda$ . Hence the remainder in (A4.15) can, in principle, be explicitly written, in terms of the potentials  $\mathcal{L}_Q^{(\alpha)}$ , in the boundary term form usual in Statistical Mechanics of the 2–dimensional short range Ising model and it can be estimated to be of  $O(|\partial\Lambda|)$  by using (A4.14).

(C) *Symmetries. SRB states and fluctuations.*

Besides the obvious translation invariance symmetry the dynamical system has a *time reversal symmetry*; this is the diffeomorphism  $I$ , see (1.3), which *anti-commutes* with  $S$  and  $S_0$ :

$$IS = S^{-1}I, \quad IS_0 = S_0I^{-1}, \quad I^2 = 1 \tag{A4.16}$$

We can suppose that the Markov partition is time reversible, *i.e.* to each element  $E_{\underline{\sigma}}$  of the partition  $\mathcal{P}$  one can associate an element  $E_{\underline{\sigma}'} = IE_{\underline{\sigma}}$  which is *also* an element of the partition. Here we simply use the invariance of the Markov partition property under maps that either commute or anticommute with the evolution  $S$ : hence it is not restrictive, see [Ga5],[Ga3], to suppose that for each  $\underline{\sigma}$  one can define a  $\underline{\sigma}'$  so that  $E_{\underline{\sigma}'} = IE_{\underline{\sigma}}$ . We shall denote such  $\underline{\sigma}'$  as  $I\underline{\sigma}$  or also  $-\underline{\sigma}$ . For

$\varepsilon = 0$ , *i.e.* for vanishing perturbation, the map  $I$  will act independently on each column of spins of  $\underline{\sigma}$ . This property remains valid for small perturbations; hence:

$$I \underline{\sigma} = \{\sigma'_{i,j}\} = \{-\sigma_{i,-j}\} \stackrel{def}{=} - \underline{\sigma}^I \tag{A4.17}$$

*i.e.* time reversal simply reflects the spin configuration corresponding to a phase space point and changes “sign” of each spin.

The functions  $\lambda_\alpha(\underline{x})$  and their “potentials”  $\mathcal{L}_Q^\alpha(\underline{\sigma}_Q)$  verify, as a consequence, if  $Q = [-\ell, \ell] \times [-k, k]$  is a centered rectangle:

$$\lambda_\alpha(I \underline{x}) = -\lambda_{\alpha'}(\underline{x}), \quad \mathcal{L}_Q^\alpha(\underline{\sigma}_Q) = -\mathcal{L}_Q^{\alpha'}(-\underline{\sigma}_Q^I) \tag{A4.18}$$

where  $\alpha' = s$  if  $\alpha = u$  and  $\alpha' = u$  if  $\alpha = s$ ,  $\alpha' = 0$  if  $\alpha = 0$ . The above symmetries will be translated into remarkable properties of the SRB distribution.

The “local entropy production rate” associated with the “space like box”  $V_0 = [-\ell, \ell]$  at the phase space point  $\underline{x} = (\dots, x_{\ell-1}, x_\ell, x_{\ell+1}, \dots)$  has been defined in §3 in terms of the Jacobian matrix of the map  $S$ . We can likewise consider the corresponding Jacobian determinants of the restriction of the map  $S$  to the stable and unstable manifolds of  $\underline{x}$ . Such determinants will depend not only from  $x_i$ ,  $i \in V_0$ , and on the nearest neighbors variables  $x_{\pm\ell}$  but *also* on the other ones  $x_k$  with  $|k| > \ell + 1$ : however their dependence from the variables with labels  $|k| > \ell$  is exponentially damped as  $\varepsilon^{(|k|-\ell)\gamma}$ , by (A4.14). Thus we can define  $\eta_{V_0}^s, \eta_{V_0}^u$  in a way completely analogous to  $\eta_{V_0}^0$  in (3.3).

If we look at the average phase space variation rates  $\eta_{V_0}^0, \eta_{V_0}^s, \eta_{V_0}^u$  between the time  $-\vartheta$  and  $\vartheta$  we can find, via a power expansion like the one in (A4.8) along the lines leading from (A4.8) to (A4.15), a mathematical expression as:

$$\eta_{V_0}^\alpha(\underline{x}) \simeq \sum_Q^* \mathcal{L}_Q^\alpha(\underline{\sigma}_Q) \tag{A4.19}$$

where the  $\sum_Q^*$  runs over rectangles  $Q$  centered at 0-time  $Q = [a-\ell, a+\ell] \times [-k, k]$  with  $[a-\ell, a+\ell] \subseteq V_0$ . This could be taken as an alternative *definition* of  $\eta_{V_0}^\alpha$ , as it is a rather natural expression. For our purposes, if  $V = V_0 \times [-\vartheta, \vartheta]$ , one needs to note that (A4.19) holds at least in the sense that:

$$\frac{1}{V_0 \cdot (2\vartheta + 1)} \sum_{j=-\vartheta}^{\vartheta} \eta_{V_0}^{(\alpha)}(S^j \underline{x}) = \frac{1}{V_0 \cdot (2\vartheta + 1)} \sum_{Q \subset V} \mathcal{L}_Q^\alpha(\underline{\sigma}_Q) + \frac{O(|\partial V|)}{|V|} \tag{A4.20}$$

*i.e.* expression (A4.19) can be used to compute the average local entropy creation rate in the space-time region  $V$  up to boundary corrections  $O(|\partial V|)$  (that can be neglected for the purposes of the following discussion).

We now study the SRB distribution  $\mu$ : denoting by  $\langle F \rangle_+$  the average value with respect to  $\mu$  of the observable  $F$  we can say, see [Si1], [PS], that if  $\Lambda = [-N, N] \times [-T, T]$ :

$$\langle F \rangle_+ = \lim_{T \rightarrow \infty} \frac{\sum_{\underline{\sigma}} F(\underline{\sigma}) e^{\sum_{Q \subset \Lambda} \mathcal{L}_Q^u(\underline{\sigma}_Q)}}{\sum_{\underline{\sigma}} e^{\sum_{Q \subset \Lambda} \mathcal{L}_Q^u(\underline{\sigma}_Q)}} \tag{A4.21}$$

We want to study the properties of the fluctuations of:

$$p = \frac{1}{V\eta_+} \sum_{Q \subset V} \mathcal{L}_Q^u(\underline{\sigma}_Q), \quad \text{if } \eta_+ = \lim_{V \rightarrow \infty} \frac{1}{V} \sum_{Q \subset V} \langle \mathcal{L}_Q^u \rangle_+ \tag{A4.22}$$

for which we expect a distribution of the form  $\pi_V(p) = \text{const } e^{V\zeta(p)+O(\partial V)}$ . The SRB distribution gives to the event that  $p$  is in the interval  $dp$  the probability  $\pi_V(p)dp$  with:

$$\pi_V(p) = \text{const} \sum_{\text{at fixed } p} \sum_{Q \subset \Lambda} e^{\sum_{Q \subset \Lambda} \mathcal{L}_Q^u(\underline{\sigma}_Q)} \tag{A4.23}$$

and (defining implicitly  $U^u$ ):

$$\begin{aligned} \sum_{Q \subset \Lambda} \mathcal{L}_Q^u(\underline{\sigma}_Q) &= \sum_{Q \subset V} \mathcal{L}_Q^u(\underline{\sigma}_Q) + \sum_{Q \subset \Lambda/V} \mathcal{L}_Q^u(\underline{\sigma}_Q) + O(|\partial V| \kappa^{-1}) \stackrel{def}{=} \\ &\stackrel{def}{=} U_V^u(\underline{\sigma}_V) + U_{\Lambda/V}^u(\underline{\sigma}_{\Lambda/V}) + O(|\partial V| \kappa^{-1}) \end{aligned} \tag{A4.24}$$

with  $\kappa > 0$ , having used the ‘‘short range’’ properties (A4.14) of the potential.

In the sums in (A4.21) we would like to sum over  $\underline{\sigma}_V$  and over  $\underline{\sigma}_{\Lambda/V}$  as if such spins were independent labels. This is not possible because of the vertical compatibility constraints. However the mixing property supposed on the free evolution implies that the compatibility matrix  $T^0$  raised to a large power  $R$  has positive entries. Hence if we leave a gap of width  $R$  above and below  $V$  we can regard as independent labels the labels  $\sigma_{i,j}$  with  $i$  in the space part  $V_0$  of the region  $V = V_0 \times [-\vartheta, \vartheta]$  and with  $|j| > \vartheta + R$ , by a distance  $\geq R$  above or below the region  $V$ . Denoted  $V + R \stackrel{def}{=} V_0 \times [-\vartheta - R, \vartheta + R]$  remark that:

$$\sum_{Q \subset \Lambda} \mathcal{L}_Q^u(\underline{\sigma}_Q) = U_V^u(\underline{\sigma}_V) + U_{\Lambda/(V+R)}^u(\underline{\sigma}_{\Lambda/(V+R)}) + O(|\partial V| (R + \kappa^{-1})) \tag{A4.25}$$

Hence, proceeding as in [GC1], we change the sum over (the dummy label)  $\underline{\sigma}$  in the denominator to a sum over  $-\underline{\sigma}^I$  and using  $\mathcal{L}_{Q^I}^u(-\underline{\sigma}^I_Q) = -\mathcal{L}_Q^s(\underline{\sigma}_Q)$ :

$$\frac{\pi_V(p)}{\pi_V(-p)} = \frac{\sum_{\text{at fixed } p} \sum_{Q \subset V} e^{\mathcal{L}_Q^u(\underline{\sigma}_Q)} e^{U_{\Lambda/(V+R)}^u(\underline{\sigma}_{\Lambda/(V+R)})}}{\sum_{\text{at fixed } p} \sum_{Q \subset V} e^{-\mathcal{L}_Q^s(\underline{\sigma}_Q)} e^{U_{\Lambda/(V+R)}^u((-\underline{\sigma}^I)_{\Lambda/(V+R)})}} e^{O(|\partial V|)} \tag{A4.26}$$

with the summation being over the spin configurations in the ‘‘whole space–time’’  $\Lambda$ , subject to the specified constraint of having the same value for  $p$ , *i.e.* the same average local entropy creation rate in the space–time region  $V$ . The latter expression becomes, since the labels  $\underline{\sigma}, -\underline{\sigma}^I$  (respectively in the numerator and denominator of (A4.26)) are independent *dummy labels*:

$$\frac{\sum_{\text{at fixed } p} \sum_{Q \subset V} e^{\mathcal{L}_Q^u(\underline{\sigma}_Q)} Z(\Lambda/(V + R))}{\sum_{\text{at fixed } p} \sum_{Q \subset V} e^{-\mathcal{L}_Q^s(\underline{\sigma}_Q)} Z(\Lambda/(V + R))} e^{O(|\partial V|)} \tag{A4.27}$$

so that by the (A4.20), (A4.22) and since the symmetry relations above imply the relation  $\sum_{Q \subset V} (\mathcal{L}_Q^u(\underline{\sigma}_Q) + \mathcal{L}_Q^s(\underline{\sigma}_Q)) = V \eta_+ p$ , up to corrections of size  $O(|\partial V| \kappa^{-1})$  we find, (note the repetition of the comparison argument given in [GC]):

$$\frac{\pi_V(p)}{\pi_V(-p)} = e^{\eta_+ V p} e^{O(|\partial V|)} \quad (\text{A4.28})$$

yielding a *local fluctuation law*, i.e. the first of (3.5). The second line of (3.5) is a (simple) consequence of the above analysis but we do not discuss it here.

#### REFERENCES.

- [AA] Arnold, V., Avez, A.: *Ergodic problems of classical mechanics*, Benjamin, 1966.
- [BCL] Bonetto, F., Chernov, N., Lebowitz, J.: , preprint, 1998.
- [BG] Bonetto, F., Gallavotti, G.: *Reversibility, coarse graining and the chaoticity principle*, Communications in Mathematical Physics, 189, 263–276, 1997.
- [BGG] Bonetto, F., Gallavotti, G., Garrido, P.: *Chaotic principle: an experimental test*, Physica D, 105, 226–252, 1997
- [Bo] Bowen, R.: *Markov partitions for Axiom A diffeomorphisms*, American Journal of Mathematics, 92, 725–747, 1970.
- [CO] Cassandro, M., Olivieri, E.: *Renormalization group and analyticity in one dimension. A proof of Dobrushin's theorem*, Communications in mathematical physics, 80, 255–269, 1981.
- [DV] Donsker, M.D., Varadhan, S.R.S.: *Asymptotic evolution of certain Markov processes expectations for large time*, Communications in Pure and Applied Mathematics, 28, 279–301, 1975; 29, 389–461, 1976; 36, 182–212, 1983.
- [ECM2] Evans, D.J., Cohen, E.G.D., Morriss, G.P.: *Probability of second law violations in shearing steady flows*, Physical Review Letters, 71, 2401–2404, 1993.
- [El] Ellis, R.S.: *Entropy, large deviations and statistical mechanics*, New York, Springer Verlag, 1985.
- [ER] Eckmann, J.P., Ruelle, D.: *Ergodic theory of strange attractors*, Reviews in Modern Physics, 57, 617–656, 1985.
- [ES] Evans, D.J., Searles, D.J.: *Equilibrium microstates which generate second law violating steady states*, Physical Review E, 50E, 1645–1648, 1994.
- [Ga1] Gallavotti, G.: *Chaotic dynamics, fluctuations, nonequilibrium ensembles*, Chaos, 8, 384–392, 1998.
- [Ga2] Gallavotti, G.: *Statistical Mechanics*, Springer–Verlag, in print.
- [Ga4] Gallavotti, G.: *Chaotic hypothesis: Onsager reciprocity and fluctuation–dissipation theorem*, Journal of Statistical Phys., 84, 899–926, 1996.
- [Ga3] Gallavotti, G.: *Reversible Anosov maps and large deviations*, Mathematical Physics Electronic Journal, MPEJ, (<http://mpej.unige.ch>), 1, 1–12, 1995.
- [Ga5] Gallavotti, G.: *New methods in nonequilibrium gases and fluids*, Proceedings of the conference *Let's face chaos through nonlinear dynamics*, U. of Maribor, 24

June– 5 July 1996, ed. M. Robnik, in print in *Open Systems and Information Dynamics*, Vol. 5, 1998 (also in mp\_arc@ math. utexas.edu #96-533 and chao-dyn #9610018).

[Ga6] Gallavotti, G.: *Extension of Onsager's reciprocity to large fields and the chaotic hypothesis*, Physical Review Letters, 77, 4334–4337, 1996.

[Ga7] Gallavotti, G.: *A local fluctuation theorem*, in chao-dyn 9808005.

[GC] Gallavotti, G., Cohen, E.G.D.: *Dynamical ensembles in nonequilibrium statistical mechanics*, Physical Review Letters, 74, 2694–2697, 1995. And *Dynamical ensembles in stationary states*, Journal of Statistical Physics, 80, 931–970, 1995.

[Gi] Gibbs, J. W.: *On the fundamental formula of dynamics*, American J. of Mathematics, Vol.II, 49–64, 1879. See also Volume II, Part 2 of Gibbs' *Collected Works*.

[HHP] Holian, B.L., Hoover, W.G., Posch. H.A.: *Resolution of Loschmidt's paradox: the origin of irreversible behavior in reversible atomistic dynamics*, Physical Review Letters, 59, 10–13, 1987.

[Kr] Krylov, N.S.: *Works on the foundations in statistical physics*, Princeton University Press, 1979, (english translations of selected papers).

[Ku] Kurchan, J.: *Fluctuation theorem for stochastic dynamics*, Journal of Physics A, 31, 3719–3729, 1998.

[LA] Levi-Civita, T., Amaldi, U.: *Lezioni di Meccanica Razionale*, Zanichelli, Bologna, 1927 (reprinted 1974), volume 3.

[La] Lanford, O.: *Entropy and equilibrium states in classical statistical mechanics*, ed. A. Lenard, Lecture notes in Physics, Springer Verlag, vol. 20, p. 1–113, 1973.

[LLP] Lepri. S., Livi, R., Politi, A. *Energy transport in anharmonic lattices close and far from equilibrium*, preprint, cond-mat@xyz. lanl. gov #9709156, to appear on Physica D.

[LR] Lanford, O., Ruelle, D.: *Observables at infinity and states with short range correlations in statistical mechanics*, Communications in Mathematical Physics, 13, p. 194–215, 1969.

[LS] Lebowitz, J.L., Spohn, H.: *The Gallavotti-Cohen Fluctuation Theorem for Stochastic Dynamics*, preprint, Rutgers University, June 1998.

[MP] Marchioro, C., Presutti, E.: *Thermodynamics of particle systems in presence of external macroscopic fields*, Communications in Mathematical Physics, 27, 146–154, 1972. And 29, 265–284, 1973.

[MR] Morriss, G.P., Rondoni, L.: *Applications of periodic orbit theory to  $N$ -particle systems*, Journal of Statistical Physics, 86, 991, 1997.

[Ol] Olla, S.: *Large deviations for Gibbs random fields*, Probability Theory and related fields, 77, 343–357, 1988.

[PS] Pesin, Y.B., Sinai, Y.G.: *Space-time chaos in chains of weakly interacting hyperbolic mappings*, Advances in Soviet Mathematics, 3, 165–198, 1991.

[RT] Rom-Kedar, V., Turaev, D.: *Big islands in dispersing billiard-like potentials*, preprint, Weizmann Institute, April 2, 1998.

- [Ru1] Ruelle, D.: *A measure associated with axiom A attractors*, American Journal of Mathematics, 98, 619–654, 1976. And *Sensitive dependence on initial conditions and turbulent behavior of dynamical systems*, Annals of the New York Academy of Sciences, 356, 408–416, 1978.
- [Ru2] Ruelle, D.: *Statistical mechanics of a one dimensional lattice gas*, Communications in Mathematical Physics, 9, 267–278, 1968.
- [Ru3] Ruelle, D.: *Positivity of entropy production in nonequilibrium statistical mechanics*, Journal of Statistical Physics, 85, 1–25, 1996. And: *Entropy production in nonequilibrium statistical mechanics*, Communications in Mathematical Physics, 189, 365–371, 1997.
- [Ru4] Ruelle, D.: *Elements of differentiable dynamics and bifurcation theory*, Academic Press, 1989.
- [Si1] Sinai, Y.: *Gibbs measures in ergodic theory*, Russian Mathematical Surveys, 27, 21–69, 1972 and *Lectures in ergodic theory*, Lecture notes in Mathematics, Princeton U. Press, Princeton, 1977.
- [Si2] Sinai, Y.G.: *Development of Krylov's ideas*, in Krylov, N.S.: *Works on the foundations in statistical physics*, Princeton University Press, 1979, p. 239–281.

Giovanni Gallavotti  
Fisica, Università La Sapienza  
Roma, Italy  
giovanni@ipparco.roma1.infn.it





FROM CLASSICAL NUMERICAL MATHEMATICS  
TO SCIENTIFIC COMPUTING

WOLFGANG HACKBUSCH

ABSTRACT. The challenge of Numerical Mathematics by the fast development of the computer technology has changed this field continuously. The need of efficient algorithms is described. Their development is supported by certain principles as “hierarchical structures”, and “adaptivity”, “decomposition”. These principles and their interactions are demonstrated in the lecture.

1991 Mathematics Subject Classification: AMS 65N, 65R, 65Y, 35A40, 45L10

Keywords and Phrases: Scientific Computing, Algorithms, pde, boundary value problems, Adaptivity, Decomposition

## 1 INTRODUCTION

This paper tries to sketch the structural changes in Numerical Mathematics. Due to the page restrictions, the illustrating examples must be omitted.

### 1.1 THE SCOPE OF NUMERICAL MATHEMATICS

First, we characterise the typical topics which already appeared in Numerical Mathematics when this field developed in the mid of this century. Two essential keywords are the *approximation* (or discretisation) and the *algorithm*.

The algorithm<sup>1</sup> establishes the constructive part of Numerical Mathematics. In the following, we will often refer to the solution of the linear system

$$Ax = b \quad (x, b \in \mathbb{R}^n) \quad (1)$$

as a standard example of a problem to be solved. A possible (but slow) algorithm would be the Gauß elimination performing the mapping  $b \mapsto x$ .

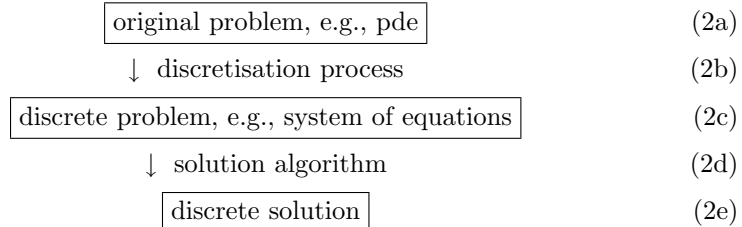
Since, in general, the mathematical problems are not solvable by finitely many elementary operations, one needs some kind of approximation. The following examples are chosen from the field of *partial differential equations* (pde). Since the solution is sought in infinitely dimensional spaces, a ‘discretisation’ is needed

---

<sup>1</sup>Formally, an algorithm is a function, which maps input data  $x \in X$  into the desired output data  $y \in Y$  and which is explicitly described by a *finite* product of *elementary* operations.

before an algorithm can be applied. The usual discretisation of a (linear) partial differential equation is a linear system (1).<sup>2</sup>

We obtain the following picture:



In the classical form of Numerical Mathematics the processes (2b) and (2d) are well separated.

Finally, the discretisation process (2b) as well as the solution algorithm (2d) are subjects of a Mathematical Analysis. The analysis of the discretisation process concerns, e.g., the discretisation error. The analysis of an algorithm may investigate its stability or its convergence speed (for iterative algorithms) etc.

## 1.2 CHALLENGE BY LARGE SCALE PROBLEMS

Large scale computations are those which are almost too large to be computed on present machines.<sup>3</sup> Then, improvements are required to make the problem feasible. In the field of pde's it is always possible to pose larger and more complex problems than those treated at present. The increasing demands concern not only the problem dimension but also the mathematical complexity. One source of mathematical complexity is the fact that simplified models are replaced by more and more realistic ones. This may, e.g., lead to

- nonlinear problems (in the simplest case this requires a series of linear auxiliary problems to be solved, in more complicated situations the solution structure may cause further difficulties and needs respective strategies),
- complicated geometries (although the mathematical analysis of a pde for a simple two-dimensional and a complicated three-dimensional domain may be similar from a theoretical point of view, the implementation of the algorithm is by far much more involved).

Often the solution of a (discretised) pde is only a small part of the whole computation. This happens for inverse problems which may be well-posed or ill-posed. Examples are

- parameter identification problems,
- optimisation of various parameters (coefficients, shape, etc.).

---

<sup>2</sup>Another kind of approximation occurs on a lower level: the exact arithmetical operation with real number must be replaced by approximate operations in the set of machine numbers.

<sup>3</sup>Here, 'large scale' is to be understood in a relative sense: large compared with the computer capacity available today. In this sense, all present large scale computations will become small under future conditions.

### 1.3 SCIENTIFIC COMPUTING

It is the challenge by large scale problems which have changed Numerical Mathematics continuously into its present form. The changes cannot be described only by great strides made in the algorithms and in the discretisation techniques. The modern approach is characterised by a *combined* design of both, discretisations and algorithms. Even the modelling is more and more involved in the whole process. Computer Science is involved, e.g., by the modern computer architecture but also by the implementation process, which more and more becomes the bottleneck.

This paper tries to show the main strategies which have been developed and led to the present structure. In particular, we name the

- hierarchical structures,
- adaptive approaches,
- (de)composition techniques.

Hierarchies are very successful for algorithms (see §2.3), but also important for the discretisation and modelling process. Adaptive techniques are indispensable for large scale problems (see §3.2). The composition and decomposition techniques have theoretical aspects in mathematics as well as quite practical aspects as the use of parallel computers (see §4.1).

## 2 EFFICIENT ALGORITHMS

It may be self-evident that we would like the algorithms to be as efficient as possible, i.e., they should yield the desired results for lowest computational costs. This vague request can be made more precise. Below, we explain why in the case of large scale computations, the development of the computer technology leads to the need of algorithms with linear complexity. The notation of complexity is recalled below.

### 2.1 ALGORITHMS AND THEIR COMPLEXITY

In the following, we fix the discretisation (2b) and discuss the algorithm (2d).

While the structural properties of algorithms are quite similar to those of proofs in mathematics, two algorithms  $\alpha, \beta : X \rightarrow Y$  mapping the input  $x$  into the same output  $\alpha(x) = \beta(x)$  are not considered to be equal but are valued according to their costs. Typical cost criteria are the required computer time and storage. Since the time needed for the computation depends on the speed of the computer, we may take the number of elementary arithmetical operations as a measure.<sup>4</sup> Since, by definition, each algorithm  $\alpha : X \rightarrow Y$  is a well-defined product  $\alpha = \alpha_k \circ \dots \circ \alpha_1$  of elementary operations  $\alpha_i$ , the arithmetical costs  $C(\alpha)$  of an algorithm is well-defined, too.

Usually, the data sets  $X, Y$  are not fixed but can be parametrised (e.g.,  $X = R^n$ ). Let  $n$  be the maximum of the number of input and output data. The complexity of an algorithm  $\alpha$  is  $O(\varphi(n))$ , if  $C(\alpha) = O(\varphi(n))$  as  $n \rightarrow \infty$ .

---

<sup>4</sup>This is a simplifying assumption. In fact, on modern computers the relation between the number of arithmetical operations and the computer time is no more linear, e.g., because of pipelining effects.

There are difficult problems, for which it is considered as a success if the complexity is polynomial (i.e.,  $\varphi(n) = n^p$  for some  $p$ ). To this respect, problems from Linear Algebra are simple. For instance, the  $n \times n$  system (1) can be solved by Gauß elimination with complexity  $O(n^3)$ . But as we will see below, the  $O(n^3)$  complexity is quite unsatisfactory.

Since, except trivial counter-examples,  $n$  data require at least one operation per datum, the *linear complexity*  $O(n)$  is the best possible (as a lower bound). Whether linear complexity can be achieved is often an open problem.

Instead of the polynomial complexity behaviour  $O(n^p)$ , one often finds the asymptotic behaviour<sup>5</sup>  $O(n^p \log^q n)$ . Because of the slow increase<sup>6</sup> of the logarithm, the logarithmic factor is considered as less important. We say that the complexity is *almost linear* if  $p = 1$ , while  $q > 0$  is allowed.

To simplify the discussion, we have concentrated on the number of arithmetical operations (computer time) and have not mentioned the storage requirements. If nothing else is said, we suppose that the storage requirement is (almost) linear in  $n$ .

## 2.2 WHY LINEAR COMPLEXITY IS NECESSARY

The asymptotic description of the algorithmic complexity is uninteresting as long as we are not forced to increase  $n$ . This need is caused by the computer technology. In the former times of hand calculations or mechanical calculators, there were obvious reasons why  $n$  was rather small. This is why Numerical Mathematics did not appear as a discipline of its own before the help of electronic computers was available.

As pointed out in §1.2, we would like to compute problems as large as the computer resources allow. Assuming a storage requirement of  $O(n)$ , we conclude that the dimension  $n$  of the largest problem we can handle increases directly with the storage of the computer.

The steady improvement of the computer technology can be described quantitatively. In spite of the technological jumps, the improvement of the storage size is rather uniform over the past decades. One observes an improvement by a factor about 100 over 10 years. A similar factor can be found for the increase in speed. The only interesting fact from these data is that *storage and speed increase by almost the same factor per time*. This has an immediate impact on the computer time for the problems to be solved.

Suppose an algorithm with complexity  $O(n^p) \approx Cn^p$ . Replacing the old computer by a new one with storage and speed improved by the factor  $c > 1$ , we want to solve problems of dimension  $cn$  instead of  $n$  (due to the increased storage). This requires  $C(cn)^p$  operations. Because of the improved speed, the computer time is now  $C(cn)^p/c = Cc^{p-1}n^p$  instead of  $Cn^p$  previously. We conclude that an improvement of the computer facilities by  $c$  increases the computer time by  $c^{p-1}$ . Hence, only if the algorithm has (almost) linear complexity, the run time does not deteriorate.

<sup>5</sup>Or more general  $O(n^{q+\varepsilon})$  for any  $\varepsilon > 0$ .

<sup>6</sup>In fact, the constants in two  $O(n^p \log^q n)$  terms can be more important than the logarithm.

The conclusion for algorithms with complexities worse than the linear one is that either the algorithm can only be used for small size problems or one has to tolerate larger and larger computational times.

## 2.3 HIERARCHICAL STRUCTURES

One basic principle that may lead to efficient algorithms is the use of hierarchies. A typical advantage of a hierarchical structure is the possibility of recursive algorithms. Below, we give a well-known example.

### 2.3.1 EXAMPLE: FFT

Consider Eq. (1) with matrix entries  $a_{jk} = \omega^{jk}$  ( $0 \leq j, k \leq n-1$ ), where  $\omega = \exp(\pm 2\pi i/n)$ . Then the matrix-vector multiplication  $x \mapsto b = Ax$  describes the mapping from the vector coefficients  $x$  into the Fourier coefficients of  $b = \mathcal{F}_n(x)$  (or vice versa, depending on the  $\pm$  sign).

The standard matrix-vector multiplication algorithm has  $O(n^2)$  complexity. Let  $n = 2^q$ . The idea of the Fast Fourier Transform (FFT), which can be traced back to Gauß, is to split the unknown Fourier coefficients  $b = (b_0, b_1, \dots, b_{n-1})$  into  $b_{odd} = (b_1, b_3, \dots, b_{n-1})$  and  $b_{even} = (b_0, b_2, \dots, b_{n-2})$  and to construct the related  $x_{odd}, x_{even}$  with  $b_{odd} = \mathcal{F}_{n/2}(x_{odd})$ ,  $b_{even} = \mathcal{F}_{n/2}(x_{even})$ . This allows a recursive application: One problem of dimension  $n = 2^q$  (level  $q$ ) is transferred into 2 problems of dimension  $n/2 = 2^{q-1}$  (level  $q-1$ ), etc. until it is reduced to  $n = 2^q$  problems of the trivial dimension 1 (level 0). The costs per step are  $O(n)$ . Since  $q = \log_2 n$  is the number of levels, we result in the almost linear complexity  $O(n \log n)$ .

Here, the vector spaces  $X_\ell = \mathbb{R}^{n_\ell}$  of dimension  $n_\ell = 2^\ell$  ( $\ell = 0, 1, \dots$ ) form the hierarchy. The typical characteristics of the FFT algorithm are: (i) The problem is trivial at level 0, while (ii) it is easy (and cheap) to reformulate the problem of level  $\ell$  by those of level  $\ell-1$ . In more general cases, (ii) takes the form that an essential part of the algorithm is the solution of problems on the lower level.

### 2.3.2 EXAMPLE: WAVELETS

The fact that the number of involved hierarchy levels grows like  $\log_2 n$  does not necessarily imply that this logarithmical factor must appear in the complexity. The wavelet transformation, which is quite close to the Fourier Transform, relies much stronger on the hierarchical structure (functions  $f$  of level<sup>7</sup>  $\ell$  define functions  $f(2\cdot)$  of level  $\ell+1$  and vice versa). Supposing a finite filter length, the wavelet transform and its back transform have exactly *linear* complexity.

The hierarchy for wavelets defined on  $\mathbb{R}$  is the family  $\{G_\ell = \{x = k2^{-\ell} : k \in \mathbb{Z}\} : \ell \in \mathbb{Z}\}$  of uniform grids. Since the wavelets are a part of Mathematical Analysis and a tool for the approximation, we see that the concept of hierarchies is also essential for the discretisation process.

<sup>7</sup>In wavelet terminology 'level' is called 'scale'.

## 2.3.3 EXAMPLE: SOLUTION OF SPARSE SYSTEMS BY MULTI-GRID

Most of the discretisation methods for pde produce a so-called *sparse* matrix  $A$  in (1), i.e., the number of non-zero entries is much smaller than  $n^2$ ; in the following, we assume that there are  $O(n)$  non-zero entries. A trivial consequence is that the matrix-vector multiplication  $x \mapsto Ax$  is cheap (linear complexity). Therefore, the hope is to approximate<sup>8</sup> the solution by an iterative process using only a fixed ( $n$ -independent) number of such matrix-vector multiplications.

Although  $A$  is sparse, the inverse  $A^{-1}$  is, in general, a full matrix. This allows the following illustration of the difficulty about linear complexity. Even if we would be able to get the inverse matrix  $A^{-1}$  for free, the computation of  $x$  by  $x := A^{-1}b$  involves the multiplication of a full matrix by a vector and is therefore of complexity  $O(n^2)$ .

Linear iterations for solving  $Ax = b$  are of the form<sup>9</sup>

$$x^{m+1} = \Phi(x^m, b) := Mx^m + Nb = x^m - N(Ax^m - b)$$

with the iteration matrix  $M = I - NA$  ( $N$  arbitrary). The iteration converges,  $x^m \rightarrow x = A^{-1}b$ , if the convergence speed which equals the spectral radius  $\rho(M)$  of the matrix  $M$  is  $< 1$ . In order to get the best results for minimal costs, one has to minimise the *effective work*

$$Eff(\Phi) := \frac{\text{cost per iteration step}}{-\log \rho(M)} = \min$$

over all linear iterations  $\Phi$ . It turns out that  $\Phi$  leads to an almost  $O(n^p)$  complexity for the solution of (1) if  $Eff(\Phi) = O(n^p)$ . Due to the sparsity, we may assume 'cost per iteration step' =  $O(n)$ ; hence,  $Eff(\Phi) = O(n^p)$  is equivalent to  $\rho(M) = 1 - O(n^{1-p})$ . In particular, linear complexity requires  $\rho(M) \leq \bar{\rho} < 1$  for all  $n$ .

Unfortunately, there is no iteration known so far which ensures linear complexity for *all* sparse matrices  $A$ . Instead one looks for fast iterations that work for *certain classes of matrices*.

Such a class are the sparse matrices resulting from the discretisation of elliptic partial differential equations, where the *multi-grid iteration* leads to linear complexity. The characteristic structure of the multi-grid method is the use of a hierarchy of discrete problems. The standard hierarchy parameter is the grid size  $h$ . Denote the discrete problem on hierarchy level  $\ell$  by  $A_\ell x_\ell = b_\ell$  for decreasing mesh sizes  $h_0 > h_1 > \dots > h_\ell > \dots$ . The iteration for solving a discrete problem of level  $\ell$  involves the lower levels  $0, 1, \dots, \ell - 1$  as auxiliary problems. A brief explanation of the fast convergence is as follows: Standard classical iterations have a local range and reduce very well the oscillatory iteration errors. Long range errors need long range corrections which can be performed efficiently

<sup>8</sup>There is no need to compute the discrete solution too accurate, since we are interested in the solution of the problem (2a). The discrete solution is affected with the discretisation error in any way. Hence, an additional approximation error of the size of the discretisation error is acceptable.

<sup>9</sup>For details see Hackbusch: Iterative solution of large sparse systems of equations. Springer, New York 1994.

only by coarser grids corresponding to lower levels. Algebraic properties of  $A$  like positive definiteness, symmetry, etc. are less important<sup>10</sup>. The main properties needed in the convergence proof is the fact that the family of matrices  $A_\ell$  stems from a discretisation of an elliptic pde.

### 2.3.4 DIFFICULTIES DUE TO COMPLICATED GEOMETRIES

Large scale problems involve possibly an increasingly detailed geometry, since now more and more data are available for the geometric description. While technical objects have a comparably simple shape, problems from medicine or geography etc. may be rather complicated.

We recall that the multi-grid method requires a hierarchy of grids of size  $h_\ell$  starting with a quite coarse grid size  $h_0$ . Although these grids can be constructed by the very flexible finite elements, the existence of such a grid hierarchy seems to be in conflict with a detailed geometry, since a complicated geometry requires that all describing grids are small enough. Here, a progress can be reported. Independent of the smallness of the geometrical details, one can construct a hierarchy of nested (conforming) finite element spaces

$$V_0 \subset V_1 \subset \dots \subset V_{\ell-1} \subset V_\ell \subset \dots \subset H^1(\Omega)$$

(so-called *composite finite elements*<sup>11</sup>) so that  $\dim V_0$  can be a small number (equivalently, the corresponding mesh size  $h_0$  can be rather larger, e.g.,  $h_0$  can be of the diameter of the domain). Although the size  $h_\ell$  may be much larger than the size of the geometrical details, one can prove the standard approximation  $\inf\{\|u - u_\ell\|_{H^1(\Omega)} : u_\ell \in V_\ell\} \leq Ch_\ell \|u\|_{H^2(\Omega)}$  for all  $u \in H^2(\Omega)$ , which is fundamental for the error estimation and multi-grid convergence.

## 2.4 ROBUSTNESS VERSUS EFFICIENCY

The example of the multi-grid method has shown that, in order to obtain efficiency, one has to make use of the special properties of the considered subclass of problems. In the case of multi-grid, the strength of ellipticity is one of these properties. In singular perturbation problems, ellipticity is fading out. Furthermore, there are other problem parameters which can have a negative influence on the convergence speed of the iteration. As soon as convergence can turn into divergence, the method becomes unreliable.

We call an algorithm *robust* (with respect to a certain set and range of parameters) if its performance does not fail when the problem parameters vary. Often,

<sup>10</sup>This is underlined by the fact that even *nonlinear* systems can be solved by (nonlinear) multi-grid iterations with asymptotically the same speed.

<sup>11</sup>Details in a) Hackbusch, Sauter: Composite finite elements for the approximation of PDEs on domains with complicated micro-structures. *Numer. Math.* 75 (1997) 447-472; b) Hackbusch, Sauter: Composite finite elements for problems containing small geometrical details. Part II: Implementation and numerical results. *Computing and Visualization in Science* 1 (1997) 15-25; c) Sauter: Composite finite elements for problems with complicated boundary. Part III: Essential boundary conditions. Report 97-16, Universität zu Kiel.



one has to find a compromise between quite efficient but non-robust and very robust but inefficient methods. There are various approaches to robust multi-grid variants, e.g., the ‘algebraic multi-grid method’. The term ‘algebraic’ indicates that the method uses only the information of the algebraic data in (1) and does not require details about the underlying pde and the discretisation process. Such a method comes closer to a ‘black-box method’, but it has to be emphasised that the algebraic multi-grid methods are still restricted to a subclass of systems.<sup>12</sup>

The preference for robust or for very efficient but more specialised methods also depends on the kind of user. While the numerical mathematician likes highly efficient algorithms for a special application, other users prefer robust methods since either the mathematical background is not well-understood or not available.

### 3 EFFICIENT DISCRETISATION METHODS

It is not enough that the solution method is efficient. Also the discretisation of the partial differential equation must be considered. In academic situations, the order of the discretisation is essential and new kinds of approximations can be proposed (see next Subsection). Nevertheless, in general, one needs adaptive methods. The reasons for adaptivity and the tools for its implementation are considered in §3.2.

#### 3.1 COMPARISON OF DIFFERENT DISCRETISATION METHODS

So far, we have taken the discrete problem as given and were looking for an efficient solution algorithm. Hence, the discretisation process in (2b) was considered to be fixed. Instead, one should also compare different discretisation methods. The success of an discretisation can be judged by the *discretisation error*, the difference<sup>13</sup> between the exact and approximate solution, or a suitable norm of the discretisation error. Here, it is to be emphasised that the discretisation method does not produce only one particular discrete problem, but at least a sequence (or as we shall see later, even a larger set) of discrete problems. Using the dimension  $n$  as an index, we may write the discretisation method  $\mathcal{D}$  as the sequence  $(P_n)_{n \in \mathbb{N}' \subset \mathbb{N}}$  of discrete problems  $P_n$  with solution  $x_n$  and discretisation error  $\varepsilon_n$ .

Usually, the aim is to reach the best accuracy for minimal costs. To be more precise, two particular strategies are of interest:

- *Accuracy oriented choice:* Let an accuracy  $\varepsilon > 0$  be given. For a fixed discretisation choose the minimal dimension  $n = n_\varepsilon$  such that the discretisation error is  $\lesssim \varepsilon$ . The arithmetical costs are denoted by  $\text{Costs}(P_{n_\varepsilon})$ . Choose that discretisation method for which  $\text{Costs}(P_{n_\varepsilon})$  is minimal.<sup>14</sup>

---

<sup>12</sup>The scope of the method is not easy to describe, since one observes that it performs well even for situations where convergence proofs are still missing.

<sup>13</sup>The definition of this ‘difference’ is not quite unique since the discrete and the continuous solution are elements from different sets.

<sup>14</sup>If the discrete problems of the different discretisations are of the same kind (hence, the costs depend only on  $n$ ), the discretisation with minimal  $n_\varepsilon$  is sought.

- *Memory oriented choice*: Let a maximal data size  $N$  be given (e.g., the whole memory of the computer). Choose that discretisation method which yields a discrete solution  $x_N$  (for the particular  $N$ ) with best accuracy  $\varepsilon_N$ .

The accuracy oriented choice is the more advanced one. The difficulty in practice is twofold. The first difficulty concerns the prediction of  $\varepsilon$ . Often it is not easy to tell how accurate (with respect to what – global or weighted – norm) the solution should be. Second, it is not trivial to judge the error of the discrete solution, i.e., to check whether  $error \lesssim \varepsilon$ .

The memory oriented choice is a lazy choice. The whole computer capacity may be used although the result will be much too accurate for the purpose in mind.

These alternatives can be illustrated for two discretisation methods of different order. Let  $\mathcal{D}_I$  be a first discretisation of order  $\alpha$ , i.e., the discretisation error  $\varepsilon_{I,N}$  behaves like<sup>15</sup>  $O(n^{-\alpha})$ , when the dimension  $n$  varies. Similarly, let  $\mathcal{D}_{II}$  be a second discretisation method of order  $\beta$ . For the accuracy oriented choice,  $\varepsilon = O(n_I^{-\alpha}) = O(n_{II}^{-\beta})$  yields  $n_I = O(\varepsilon^{-1/\alpha})$  and  $n_{II} = O(\varepsilon^{-1/\beta})$ . Hence,  $\alpha < \beta$  implies that (at least asymptotically)  $n_{II} < n_I$  and therefore the higher order discretisation is more efficient. For the memory oriented choice,  $n = N$  is fixed. Again, the higher order  $\beta > \alpha$  is preferred, since the accuracy  $\varepsilon_I = O(N^{-\alpha})$  is (asymptotically) smaller than  $\varepsilon_{II} = O(N^{-\beta})$ .

Attempts have been made to improve the polynomial behaviour  $\varepsilon = O(n^{-p})$ . One approach is the *p-finite element method*, where the step size  $h$  remains fixed, while the order  $p = p(n)$  is increasing. Under perfect conditions, an exponential behaviour  $\varepsilon = O(\exp(-cn^\alpha))$  ( $c, \alpha > 0$ ) is obtained.<sup>16</sup>

Another approach are the *sparse grids*, where the discretisation error is almost of the order  $\varepsilon_h = O(h^p)$ , whereas the grid has only  $n = O(h^{-1})$  grid points even if the domain is a subset of  $\mathbb{R}^d$ . Then, the discretisation error equals  $\varepsilon_h = O(n^{-p})$  instead of  $O(n^{-p/d})$ . Since  $d = 3$  is the standard spatial dimension, this approach promises a much better accuracy for the same dimension  $n$ .

In practice, both of the methods mentioned above cannot be applied to general boundary value problems, but only to local parts. In the case of the p-method, the solution must be very smooth, which may happen in the interior of the domain with a fixed distance from the boundary but is in general not true at the boundary. This gives rise to the *hp-method* which combines the standard finite element method with the p-method in an adaptive manner. In the case of sparse grids, these grids correspond to a special domain (square, cube etc. or their smooth image), which is usually only a part of the whole domain. Therefore, in general, the use of p- and sparse-grid methods require in addition adaptive techniques as they are explained below.

<sup>15</sup>This definition is simplified. Usually the order is defined by  $O(h^{-\alpha})$ , where  $h$  is the mesh size.  $h$  and  $n$  are connected by  $n = O(h^{-d})$ , where  $d$  is the dimension of the domain  $\Omega \subset \mathbb{R}^d$ .

<sup>16</sup>To be precise, one has also to take into account that the p-method requires much more accurate quadratures for the system matrix entries and that the resulting linear system is harder to solve than standard finite element systems.

## 3.2 ADAPTIVITY

### 3.2.1 ABSTRACT SETTING

To be precise, the result of a discretisation is a *family* of discrete problems  $\mathcal{P} = \{P_i : i \in I\}$ , where the index set  $I$  usually coincides with  $\mathbb{N}$  or an infinite subset of  $\mathbb{N}$ . If  $x_i$  is the solution of  $P_i$ , we expect a certain of convergence of  $x_i$  to the solution  $x$  of the continuous problem, i.e., the discretisation error  $\varepsilon_i$  should tend to 0. In the case of the ‘accuracy oriented choice’ from §3.1, we want to find the minimiser  $P_{i_{opt}}$  of  $\min\{\text{costs}(P_i) : i \in I \text{ and } \varepsilon_i \leq \varepsilon\}$ . The trivial strategy for finding  $i_{opt}$  is to test the solution  $x_i$  and to proceed to index  $i + 1$  (this can, e.g., mean a halving of the mesh size) if  $\varepsilon_i > \varepsilon$ .

In the adaptive case, the index set  $I$  has a much more general structure, e.g., it may be a graph. Then, given a discrete problem  $P_i$ , there are several next finer discrete problems  $\{P_j : j \text{ successors of } i\}$ . The solution of the minimisation problem  $\min\{\text{Costs}(P_i) : i \in I \text{ and } \varepsilon_i \leq \varepsilon\}$  must be avoided.<sup>17</sup> Instead, one needs a heuristic  $H$  selecting a convergent subsequence  $\{P_{i_k} : k \in \mathbb{N}\}$ ,  $i_k = H(x_{i_{k-1}})$ .

If, in the Galerkin case, adaptation is understood more generally as the optimal approximation by any kind of function spaces, the theoretical background traces back to the *n-widths* introduced by Kolmogorov.

### 3.2.2 WHAT PARAMETERS CAN BE ADAPTED?

The finite element discretisation decomposes the whole domain into triangles (tetrahedra) or other geometric elements. Starting with a given (coarse) finite element triangulation of a domain with step size  $h_0$ , we can consider a uniform refinement (e.g., each triangle is regularly divided into four smaller ones). This yields a sequence of discrete problems with the uniform step size  $h_\ell = 2^{-\ell}h_0$ . On the other hand, the finite element discretisation allows to choose *different* element sizes at different locations, i.e., the mesh size may become a function  $h(x)$ . Among all finite element discretisations one has to select a sequence satisfying  $\lim \max_x h(x) = 0$ . Usually, the triangulations  $\tau_i$  of this sequence are not chosen independently, but given a triangulation  $\tau_i$  the next one,  $\tau_{i+1}$ , is obtained by *local* refinement. The question arises where to refine the grid.

The adaptation by local grid refinement is the most important example which we shall discuss below. For completeness, also other subjects of adaptation are mentioned. (i) Another possibility is to adapt the order of the finite element functions (hp-method). (ii) Usually, one avoids flat (almost degenerated) triangles. However, under certain circumstances, flat triangles with a prescribed direction of the longest side are desired. Therefore, the orientation and degree of degeneration is a possible subject of adaptation. (iii) The kind of discretisation technique may change in different subregions of the boundary value problem.

---

<sup>17</sup>The minimisation over certain discretisation parameters is a problem of a much higher complexity than the original task. Hence, the final costs is not  $\text{Costs}(p_i)$  for a suitable  $i$ , but  $\text{Costs}(p_i)$  plus a large overhead for the minimisation.

### 3.2.3 WHY SHOULD BE ADAPTED?

A uniform step size is (almost) optimal, if the function to be approximated is uniformly smooth. In practice, one has to approximate functions with different smoothness in different parts, e.g., (i) very smooth in one part  $\Omega_{(i)}$  of the domain and (ii) less smooth in another part  $\Omega_{(ii)}$ . Then the mesh size might be constant ( $= h_{(i)}^*$ ) in  $\Omega_{(i)}$  and constant ( $= h_{(ii)}^*$ ) in  $\Omega_{(ii)}$  but with  $h_{(i)}^* \gg h_{(ii)}^*$ . Choosing the uniform but coarse mesh size  $h = h_{(i)}^*$  everywhere, we result in a large discretisation error because of the bad approximation in  $\Omega_{(ii)}$ . On the other hand, the uniform choice  $h = h_{(ii)}^*$  gives (by definition) a satisfactory discretisation error, but because of  $h_{(ii)}^* \ll h_{(i)}^*$ , this grid is much too fine in  $\Omega_{(i)}$  and leads to a total dimension much larger than necessary.

Often, a further situation arises: (iii) The function has singular derivatives at a certain point  $x_0$ . Then, one needs a mesh with  $h^*(x)$  decaying in a certain way as  $x$  approaches  $x_0$ . Note that  $h^*(x)$  takes very small values only in very small parts of the domain. Choosing such a fine grid everywhere would be a huge waste of computer time.

Altogether, one has to construct a mesh with local mesh width  $h(x) \leq h_{(i)}^*, h_{(ii)}^*, h^*(x)$  in the respective parts.

### 3.2.4 WHAT MAKES ADAPTATION DIFFICULT?

The reason for the different choices of  $h(x)$  is the smoothness of the function  $u(x)$  to be approximated. In simple cases like quadrature, the function  $u$  and possibly its derivatives are explicitly available. A different situation occurs in the case of differential equations. Here, the function  $u$  is the quantity we are looking for. The question arises whether we can get the information about the smoothness of  $u$  before we have computed the approximation of  $u$ .

The answer to the latter question is that an iterative approach is used. Starting with a rough approximation of  $u^0$ , one tries to find informations for adapting the mesh from which the next approximation  $u^1$  is computed, etc.

This iteration combines the discretisation process and the solution process, since they are performed in a cyclic manner.

### 3.2.5 HOW TO CONTROL THE ADAPTATION?

There are cases, where the adaptation to the problem can be designed *a priori*, but, usually, the adaptation process is done *a posteriori*, more precisely, during the computational process. For the *a posteriori* adaptation, we have to describe the control mechanism steering the details of the adaptation.

A general strategy to this respect consists of two fundamental considerations:

- The discretisation error is to be described as a sum of *local errors*. Usually, the local residuum is such a tool.
- The desired situation is the *equidistribution* of the local errors. That means, one tries to adapt the mesh so that all local errors are equally sized. The

argument is that a locally small error is a waste of computation without improving the global error essentially.

The control mechanism is first explained for the ‘memory oriented choice’ explained in §3.1. In this case, one refines as long as further storage is available. The only critical decision is where to refine the finite element grid. For this purpose, a lot of ‘error indicators’ exist which indicate where (possibly) the error is dominating. Many of these criteria are heuristic. The theory-based error estimators are explained below.

The ‘accuracy oriented choice’ from §3.1 requires two decisions. First, we need an indication that the discretisation error is below the required accuracy  $\varepsilon$ . In the negative case, we have to decide where to refine locally (as discussed above). Both decisions are supported by the error estimators explained in the next Subsection.

In particular in time dependent problems, not only an adaptive refinement but also a *coarsening* may be necessary.

### 3.3 ERROR INDICATORS AND ESTIMATORS

The *a posteriori error estimators*, first introduced by Babuška and Rheinboldt<sup>18</sup>, are a fundamental tool for the adaptive refinement. Let  $\tau$  be a triangulation of the domain  $\Omega$ , i.e.,  $\Omega$  is the disjoint union of the elements  $\Delta \in \tau$ . The finite element solution for the triangulation  $\tau$  is denoted by  $u_\tau$ . Then, the error estimator has the form

$$\Phi(u_\tau) = \sqrt{\sum_{\Delta \in \tau} \varphi_\Delta(u_\tau)},$$

where  $\varphi_\Delta$  is a computable<sup>19</sup> function depending only on the data restricted to  $\Delta$  (or its neighbourhood). Denoting the error of  $u_\tau$  by  $e(u_\tau)$  (e.g.,  $e(u_\tau) = \|u - u_\tau\|$  for a suitable norm  $\|\cdot\|$ ), we would like to have constants  $A, B$  such that

$$A\Phi(u_\tau) \leq e(u_\tau) \leq B\Phi(u_\tau).$$

If  $e(u_\tau) \leq B\Phi(u_\tau)$  holds,  $\Phi$  is called *reliable* since knowing its value we can guarantee an error estimate. If  $A\Phi(u_\tau) \leq e(u_\tau)$ ,  $\Phi$  is called *efficient* since we avoid overestimation.

### 3.4 COMBINATION OF THE DISCRETISATION AND SOLUTION PROCESS

In the beginning, we said that in the classical form of Numerical Mathematics the discretisation of the continuous problem and the algorithm for the discrete

<sup>18</sup>See Babuška-Rheinboldt: A posteriori error estimates for the finite element method. *Int. J. Numer. Meth. Engrg.* 12 (1978) 1597-1615. For a recent survey see Verfürth: A review of a posteriori error estimation and adaptive mesh-refinement techniques. Wiley-Teubner 1996.

<sup>19</sup>To be quite precise, there are two alternatives to be considered. 1) If  $\varphi_\Delta$  is a mathematical expression including integration, we can obtain reliable error estimates. 2) For computational purposes, such a  $\varphi_\Delta$  (e.g., the integration contained in  $\varphi_\Delta$ ) must be discretised and yields an algorithm  $\tilde{\varphi}_\Delta$ . Then,  $\Phi$  cannot be reliable in general without (a priori) assumptions on the smoothness of the integrands.

problem were well separated. With the adaptive approach we have reached a new level, where a new kind of algorithm is *directly applied to the continuous problem*, i.e., the design of the discretisation has become a part of the solution algorithm itself.

The reason for this development is not only the efficacy we want to obtain, but also the huge amount of data. As long as we compute only few numbers, we may be able to judge their quality and possibly improve the discretisation. However, when we compute a massive set of data corresponding, e.g., to a relative dense three-dimensional grid, we have already problems to perceive the data. We need special visualisation tools to interpret the computed results. The judgement of their accuracy is even more difficult. Therefore, it is an obvious consequence that the control over the discretisation process is given to the algorithm itself.

The new kind of algorithm can be considered as a triple  $(\mathcal{D}, \mathcal{A}, \mathcal{H})$ , where  $\mathcal{D}$  is the discretisation method (offering a large variety of discrete problems, e.g., all finite element triangulations),  $\mathcal{A}$  are the algorithms for solving the discrete problems produced by  $\mathcal{D}$ , while the heuristic  $\mathcal{H}$  is the adaptive strategy controlling the discretisation process.

### 3.5 HIERARCHY PLUS ADAPTIVITY

In the following, we discuss the hierarchy of grids used by the multi-grid method. Then adaptive approaches can be realised in two ways.

1) *Global grids.* Let  $\{G_\ell : \ell = 0, 1, \dots\}$  be the sequence of grids (finite element meshes etc.), where  $G_{\ell+1}$  is constructed adaptively from the solution  $x_\ell$  in grid  $G_\ell$ .

2) *Local grids.* Let  $G'_0 = G_0$  be a starting grid and denote by  $G'_\ell$  the regular refinement ( $\ell$  partitioning steps in all elements). An adaptive (local) refinement  $G_1$  of  $G_0$  can be considered as a union of  $G_{10} := G'_0$  and of a subset  $G_{11} \subset G'_1$ . In general, a local refinement  $G_\ell$  is a union of subsets  $G_{\ell,k} \subset G'_k$  ( $0 \leq k \leq \ell$ ).

The second approach works also for the wavelet hierarchy: There the local refinement is replaced by adding the wavelet functions  $\psi(2^\ell x - k)$  of level  $\ell$  for only few shifts  $k$ .

So far, the hierarchical structure does allow adaptivity. Of course, extra overhead occurs to administrate the additional description of the local grid details.

## 4 PARALLELISM

The costs of an algorithm are not determined by mathematics but by kind of computing tools. If the technology is changing also the valuation of algorithms might change. For instance, on a vector computers  $\text{Costs}(A_I) < \text{Costs}(A_{II})$  may hold, although algorithm  $A_I$  requires more scalar operations than  $A_{II}$ , provided that  $A_I$  exploits the vector operations.

In the last decade, the parallel computer became available which allows to perform the computation in parallel on a number of processors, provided the computations are independent. In the optimal case (optimal balance, no overhead) the computation time decreases by the factor  $p$ =number of processors. Another effect

is the enlarged storage ( $p$  times the storage of each processor), provided that the algorithm can use the distributed memory. Since, in the optimal case, speed and storage increases by the same factor, the considerations of §2.1 show that also the parallel algorithms must be of linear complexity.

Let a sequential algorithm  $A_s$  be given. One can try to construct a parallel algorithm  $A_p$  which yields identical results. For its construction, one needs at least a *data decomposition*.

Usually, one tries to construct a special parallel algorithm. One strategy for its construction is the *problem decomposition* of the full problem into subtasks.

## 4.1 COMPOSITION, DECOMPOSITION

### 4.1.1 COMPOSITION

Often, large scale problem are obtained by composing subproblems. Difficulties in the decomposition process may possibly arise from

- a) different kinds of differential equations and/or integral equations in the subproblems,
- b) different coordinate systems in the subproblems,
- c) different discretisations in the subproblems,
- d) non-fitting meshes even when all subproblems are discretised by the same kind of finite elements.

The coupling conditions, which are similar to the boundary conditions, must be integrated into the complete problem. If the meshes do not fit, one has to ensure the connection in a weak sense, e.g., by Lagrange multipliers (so-called ‘mortar element method’).

### 4.1.2 DECOMPOSITION

The decomposition of the whole problem into subproblems can have different reasons:

- 1) software is available for the specific subproblems,
- 2) the iterative scheme makes use of the solution of the subproblems,
- 3) the problem must be decomposed to use a parallel computer.

Another question is how the complete problem can be divided. Two different approaches are relevant:

- a) The given problem is already a composed problem, then the obvious candidates for the subproblems are the basic components.
- b) If the given problem is uniform, a partitioning must be defined. Differently from a), the number of subtasks can be chosen according to the number of available processors.

Reason 1) is, in particular, important for large scale problems which are implemented by a team where each expert is responsible for a particular subtask.

Reason 2): For iterative schemes<sup>20</sup>, it is a standard approach to correct the

---

<sup>20</sup>Details in Chapter 11 of Hackbusch: Iterative solution of large sparse systems of equations. Springer, New York 1994.

actual approximation by a solution of a simpler problem<sup>21</sup>, where the ‘simpler problem’ is obtained by neglecting the coupling of subproblems. The simplest subproblems of a system (1) are the separate  $n$  scalar equations. Solving the  $i$ th scalar equations with respect to  $x_i$  yields the classical Jacobi and Gauß-Seidel iteration. Since a partitioning according to Approach a) is obvious, we consider the Approach b). In the context of elliptic pde’s discretised over a mesh in the domain  $\Omega$ , one can partition  $\Omega$  into subdomains  $\Omega_i$  (together with their meshes) such that  $\cup \Omega_i = \Omega$ . This leads to the *domain decomposition method*. The decomposition may also use overlapping domains. Since the first domain decomposition method (with two overlapping domains) was used by H. A. Schwarz (1870) to prove the existence of a holomorphic function in a composed domain, these iterations are also called *Schwarz iteration*.

The use of parallel computers for domain decomposition methods is obvious: The solution of the  $i$ th subproblem on  $\Omega_i$  involves intensive computations on the  $i$ th processor. Afterwards communication is needed to initialise the next iteration step, but the communication concerns only the overlapping region or in the simplest case only the common interior boundary. Since the communication involves only a rather small part of all unknowns, there is a hope for a good speed-up factor.

However, the use of the domain decomposition principle *only* cannot be successful. If  $p$  is the number of subdomains (and parallel processors), the overlapping Schwarz method does lead to a speed-up by  $p$ , but the convergence speed of the iteration slows down by the same factor. Therefore, in the meantime it is well-accepted that one has to add a coarse-grid subspace.<sup>22</sup> This makes the domain decomposition approach very similar to the multi-grid method: The coarse-grid correction has a larger step size ratio  $h_{fine}/h_{coarse}$ , while the subspace solutions form the smoothing process of the two-grid iteration.

The addition of the coarse-grid subspace leads to a generalisation of the domain decomposition principle: The decomposition of the vector space into subspaces. The resulting notation of a *subspace iteration* is general enough to describe the domain decomposition methods as well as the multi-grid iterations. The theory developed so far<sup>23</sup> is more or less restricted to positive definite system matrices  $A$ . Applied to multi-grid iterations, the results use weaker assumptions but yield also weaker convergence results.

## 4.2 INTERACTION OF THESE PRINCIPLES

### 4.2.1 HIERARCHY PLUS DECOMPOSITION

The hierarchy can be considered as a vertical structure providing problems of different discretisation levels, whereas the decomposition yields an horizontal structure.

<sup>21</sup>Let  $W$  be ‘close’ to  $A$  but such that  $Wy = d$  is easy to solve. Then the iterative scheme  $x^{new} = x^{old} - W^{-1}(Ax^{old} - b)$  requires the solution of  $Wy = d$  with  $d = Ax^{old} - b$ .

<sup>22</sup>Divide the domain  $\Omega$  into pieces  $\Omega_i$  of size  $H$  and introduce a global mesh of size  $h$ . Then the coarse-grid mesh has size  $H$ .

<sup>23</sup>Survey in Xu: Iterative methods by space decompositions and subspace correction. *SIAM Review* 34 (1992) 581-613.



These structures are essentially orthogonal and do not conflict with each other.

The traditional domain decomposition method has two hierarchy levels, the global problem and many local subproblems. It is possible to repeat the domain decomposition principle for each subproblem. Another possibility is to use the same decomposition structure over all levels on the hierarchy. This is the standard approach for *data decomposition* for the purpose of parallel computations.

Hierarchy plus parallelism may create a specific problem. Usually, the algorithm works sequentially over the hierarchy levels. If the lower levels are connected with coarser grids and therefore less computational work, the communication part may predominate.

#### 4.2.2 DECOMPOSITION PLUS ADAPTIVITY

When using the decomposition for parallelising, the idea is to associate each subproblem with one of the processors. At the starting time of each iteration step, all processors must get the new (boundary and right-hand side) data for the subproblems. Since the iteration cannot proceed before all results are collected, one should ensure that all subtask computations need almost the same time. This requirement can be satisfied by creating subdomains with nearly the same number of unknowns.

In this case, adaptivity leads to a severe conflict. By definition, the adaptive refinement yields locally different changes. One subdomain may be strongly refined, whereas another one remains unchanged. Obviously, even if the dimensions of the subtasks are equidistributed initially, the subproblems may lose their balance. Without a rearrangement of the subdomains, the parallel algorithm becomes poor.

The rearrangement process is called *load balancing*. On the one hand side, the load balancing must be cheap in order not to spoil the overall performance time. On the other hand, the load balancing is a very delicate task because a) the optimal decomposition is NP-hard, b) the subdomain data to be rearranged on one processor are distributed over different processors. It becomes even more difficult in the multi-grid case where also the vertical level structure is to be considered.<sup>24</sup>

If the load balancing is successfully implemented, the algorithm decides not only about the termination (when the accuracy is reached) and local refinement, but also about the decomposition structure.

## 5 MODELLING AND IMPLEMENTATIONAL ASPECTS

### 5.1 MODELLING

We started with an approximation (discretisation) separated from the algorithm for the discrete problem. As shown in §3.4, both have become more and more intertwined. However, the mathematical problem from (2a) is not really fixed. Usually, it is the result of a modelling process for some problem from outside

---

<sup>24</sup>See Bastian: Parallele adaptive Mehrgitterverfahren. Teubner, Stuttgart 1996.

mathematics (e.g., mechanics; see (3a)). The modelling process may be an approximation<sup>25</sup> by itself. The model might be more or less involved, certain aspects may be neglected or simplified or represented in full detail. Often, the details of the modelling process should be related to the accuracy required for the discrete problem. This gives rise to a hierarchy of models.

physical (chemical etc.) problem (3a)

↓ modelling process (3b)

mathematical problem, e.g., pde (3c)

↓ discretisation process (3d)

discrete problem, e.g., system of equations (3e)

computer ↔ ↓ solution algorithm (3f)

discrete solution (3g)

From the mathematical point of view it is very interesting when the model hierarchy leads to *different scales* in the solution. Such different scales may be *time scales* for time-dependent problem: Certain processes are much faster than others (e.g., mechanical changes faster than thermal ones or chemical reactions faster than the flow dynamics). This gives rise to interesting discretisation techniques. The consideration of scales in the discretisation can also be regarded as an adaptation process (using the smallest time scale for *all* components would be a waste of computer time).

Details in a model may also lead to *geometric scales*. The diameter of the domain (of the boundary value problem  $Lu = f$ ) is the coarsest scale. The coefficient function of  $L$  may be oscillatory giving rise to the wavelength as next geometric scale. In regular cases, the *homogenisation technique* offers a tool to split the true solution into a sum of a homogenised part and the details.

## 5.2 IMPLEMENTATION

In (3f) the box ‘computer’ should indicate the interaction of the solution algorithm with the computer. This includes that the algorithm depends on the computer architecture. Another important software aspect is mentioned next.

The steadily increasing volume of the data and the increasing problem complexity on the one hand and the development in the computer architecture on the other hand have made the implementation more and more involved. Although algorithms and computers have become faster, the act of implementation consumes an increasing time of work. Since Scientific Computing needs extensive software, its production (i.e., the implementation process) must become a scientific topic of Scientific Computing by its own.<sup>26</sup>

<sup>25</sup>This approximation process is meant when engineers speak about a *simulation*.

<sup>26</sup>For a positive example see Bastian et al.: UG - A flexible software toolbox for solving partial differential equations. *Computing and Visualization in Science* 1 (1997) 27-40.

## 6 TREATMENT OF NON-SPARSE MATRICES

The request of linear complexity is very restrictive and seems to exclude, e.g., the treatment of linear systems with a *full* matrix, since then even simple operations like the matrix-vector multiplication are of quadratic complexity. The survey is concluded by a discussion of this problem.

## 6.1 BOUNDARY INTEGRAL EQUATIONS

A linear and homogeneous boundary value problem  $Lu = 0$  in a domain  $\Omega \subset \mathbb{R}^d$  can be reformulated as an integral equation of the form  $\lambda u(x) = (Ku)(x) + g(x)$  for  $x \in \Gamma$  with the boundary integral operator

$$(Ku)(x) := \int_{\Gamma} k(x, y)u(y)d\Gamma_y$$

defined on the boundary  $\Gamma = \partial\Omega$ . The kernel  $k$  is the fundamental solution of  $L$  or some derivative.

The advantage of the boundary integral representation is due to the fact that the domain  $\Omega$  with spatial dimension  $d$  is replaced by a manifold of dimension  $d - 1$ . Using elements of size  $h$ , the discretisation of  $\Omega$  requires  $O(h^{-d})$  elements, whereas  $\Gamma$  leads to only  $n = O(h^{1-d})$  elements. In particular for exterior problems (where  $\Omega$  is infinite), the integral equation is much simpler.

The disadvantage of the integral equation is caused by the fact that a discretisation of an integral operator (the so-called *boundary element method*) leads to full matrices (instead of the sparse ones for the local differential operators). For the interesting case  $d = 3$ , one finds that the boundary element method with dimension  $n = O(h^{1-d})$  is cheaper than the standard finite element method only if the complexity is better than  $O(n^{3/2})$ . In particular,  $O(n^2)$  complexity cannot be accepted.

This is a typical situation, where the full matrix  $A$  with its  $n^2$  entries seems to prevent any algorithm from better complexity than  $O(n^2)$ . Indeed, yet the computation of the system matrix  $A$  consumes  $O(n^2)$  operations where the constant may be rather large. Hence, first of all the use of the full matrix  $A$  must be avoided and replaced by a matrix (linear mapping) which can be described by (almost)  $O(n)$  data. One might ask why this should be possible. The reason is that the pseudo-differential operator  $K$  has quite similar properties as standard differential operators. The latter ones can be approximated by sparse matrices depending on only  $O(n)$  data.

Essentially, there are two different approaches for a realisation:

- *Matrix compression.* One can look for a special discretisation of  $K$  such that most of the entries of  $A$  are extremely small so that their replacement by zero yields an (almost) sparse matrix  $\tilde{A}$ . Such a discretisation can be obtained by a Galerkin approach based on suitable wavelet functions.<sup>27</sup>

<sup>27</sup>The delicate requirement is that the entries which should be suppressed must be known *before*

- *Panel clustering.* Given any discretisation of  $K$  with system matrix  $A$ , one can try to approximate  $A$  by another matrix  $\tilde{A}$  which is easily describable by almost  $O(n)$  data. This ensures that only almost  $O(n)$  data are to be stored. Furthermore, the matrix-vector multiplication  $x \mapsto \tilde{A}x$  must be performable by almost  $O(n)$  operations. This is achieved by the panel clustering method.<sup>28</sup> The main idea is the replacement of the (smooth) kernel function  $k$  in the far-field. Different from the wavelet matrix compression, the panel clustering method is not a discretisation by itself but can be combined with any collocation or Galerkin method. Further, it is independent of the smoothness of the boundary  $\Gamma$ .

In both cases, one can prove that the replacement of  $A$  by  $\tilde{A}$  yields an additional error which is of the same size as the discretisation error or even smaller.

## 6.2 GENERAL NON-SPARSE SYSTEMS

Recently, L. N. Trefethen (Oxford) posed a number of maxims of which the twenty first one reads as follows:

- Is there an  $O(n^{2+\epsilon})$  algorithm<sup>29</sup> for solving an  $n \times n$  system  $Ax = b$ ? This is the biggest unsolved problem in numerical analysis, but nobody is working on it.<sup>30</sup>

Since the multiplication of a full matrix times a vector costs  $O(n^2)$  operations, a sufficient condition would be that the inverse  $A^{-1}$  can be computed by an  $O(n^{2+\epsilon})$  algorithms. Unfortunately, I cannot offer such an algorithm. Instead, I would like to ask whether for a restricted (but interesting) subclass of problems, the following related question can be answered:

- Is it possible to compute a good approximate  $B$  of the inverse  $A^{-1}$  by almost  $O(n)$  operations such that  $B$  requires a storage of almost  $O(n)$  and such that the multiplication of  $B$  by an  $n$ -vector  $b$  costs almost  $O(n)$ ?

At first sight, this seems impossible, since in general  $A^{-1}$  is a full matrix with  $n^2$  entries. Indeed, for the exact inverse  $B = A^{-1}$  we find only very few positive examples. However, as in the panel clustering method mentioned above, it may be possible to find an approximation  $B \approx A^{-1}$  with this property.

In fact, it is possible to give a positive answer to the latter question if  $A$  is a discretisation of an elliptic operator including pseudo-differential operators. Because of the hierarchical structure of the applied matrix representation, we call the set of approximating matrices  $\mathcal{H}$ -matrices.<sup>31</sup> The precise results are as follows:

---

their computation. For details see, e.g., Schneider: Multiskalen- und Wavelet-Matrixkompression. Teubner, Stuttgart 1998.

<sup>28</sup>See, e.g., §9.7 in Hackbusch: Integral equations. ISNM 120, Birkhäuser, Basel 1995.

<sup>29</sup>Obviously, it is meant that  $\epsilon$  may be any positive number. For a system with a full matrix  $A$ , which cannot be represented by less than  $n^2$  data,  $N = n^2 + n$  is the data size of the input data  $(A, b)$ . Therefore, an  $O(n^2) = O(N)$  complexity for solving  $Ax = b$  is linear complexity!

<sup>30</sup>SIAM News, vol 31, No 1 (1998) page 4.

<sup>31</sup>Details will be in a forthcoming paper.

- the storage of the  $\mathcal{H}$ -matrix data is of the size  $O(n \log n)$ ,
- the (approximate) sum of two  $\mathcal{H}$ -matrices costs  $O(n \log n)$ ,
- the (approximate) product of two  $\mathcal{H}$ -matrices costs  $O(n \log^2 n)$ ,
- the (approximate) product of an  $\mathcal{H}$ -matrix with an  $n$ -vector costs  $O(n \log n)$ .

Since the inverse can be obtained by multiplications (by suitable transformation matrices), also the (approximate) inversion of an  $\mathcal{H}$ -matrix costs  $O(n \log^2 n)$  operations.

Even if one wants to perform the usual iterative techniques, often a Schur complement occurs which is of the form  $S = D - BA^{-1}C$ . Since the Schur complement contains the inverse matrix  $A^{-1}$ ,  $S$  is usually a full matrix. Therefore, one can neither represent the matrix  $S$  nor its inverse in the standard form. Up to now, the only remedy is to know a good preconditioner for  $S$ . Then it is enough to have an efficient algorithm for the matrix-vector multiplication  $x \mapsto Sx$  which can make use of the representation  $S = D - BA^{-1}C$ . The  $\mathcal{H}$ -matrix algorithm opens new possibilities, since the explicit approximate computation of  $S = D - BA^{-1}C$  can be performed, provided that  $A, B, C, D$  are  $\mathcal{H}$ -matrices.

Wolfgang Hackbusch  
Universität zu Kiel  
Olshausenstr. 40  
D-24098 Kiel, Germany  
wh@numerik.uni-kiel.de

## DYNAMICS, TOPOLOGY, AND HOLOMORPHIC CURVES

HELMUT H. W. HOFER

ABSTRACT. In this paper we describe the intimate interplay between certain classes of dynamical systems and a holomorphic curve theory. There are many aspects touching areas like Gromov-Witten invariants, quantum cohomology, symplectic homology, Seiberg-Witten invariants, Hamiltonian dynamics and more. Emphasized is this interplay in real dimension three. In this case the methods give a tool to construct global surfaces of section and generalizations thereof for the large class of Reeb vector fields. This class of vector fields, includes, in particular, all geodesic flows on surfaces.

1991 Mathematics Subject Classification: 32, 34, 35, 49, 58, 70

Keywords and Phrases: Hamiltonian dynamics, contact forms, Reeb vector fields, quantum cohomology, Gromov-Witten invariants, Arnold conjecture, Weinstein conjecture, holomorphic curves, symplectic homology, surfaces of section.

## 1 PERIODIC ORBITS OF DYNAMICAL SYSTEMS

Symplectic and contact geometry as well as Hamiltonian dynamics experienced in the last decade a tremendous growth. In order to cover some aspects in a certain depth one faces the serious dilemma of making a selection. Rather than touching many areas, it seems more appropriate to focus only on a few aspects. The choice made here was to describe the subtle relationship between Hamiltonian dynamics, topology and a theory of holomorphic curves. So many aspects are only briefly mentioned or even ignored. However, they are being dealt with in other papers contained in the proceedings of the ICM Berlin. In particular the contributions by S. Donaldson, Y. Eliashberg, K. Kuperberg, D. McDuff, J. Moser, L. Polterovich, Y. Ruan and C. Taubes.

The aim of this paper is to explain some of the recent progress at the interface of Hamiltonian dynamics and symplectic geometry. In order to appreciate the special features of (certain) Hamiltonian dynamics versus general dynamics we begin with the following classical problem.

In 1950 Seifert, [79], raised the question if a given non-singular vector field  $X$  on the three-sphere admits a periodic orbit:

$$\dot{x} = X(x) \text{ and } x(0) = x(T), \quad T > 0.$$

As it turned out this is a subtle problem. In higher dimensions Wilson, [87], provided in 1966 examples of non-singular vector fields on  $S^{2n-1}$ ,  $n \geq 3$ , without periodic orbits. However, dimension three poses more difficulties due to lack of room in order to make some of the higher dimensional ideas work. After all, destroying periodic orbits, which are 1-dimensional sets, should be easier in higher dimensions.

In 1974 Schweizer, [77], showed that there exist non-singular  $C^1$ -vector fields on  $S^3$  without any periodic orbits. The regularity of the counterexample was strengthened to  $C^2$  in [36]. In 1994 the question was finally settled by K. Kupferberg, [59], who constructed a real analytic counterexample.

**THEOREM 1.1 (K. KUPERBERG)** *There exists a nowhere vanishing real analytic vector field on  $S^3$  without any periodic orbit.*

So, asking for periodic orbits, given an arbitrary smooth vector field on  $S^3$  (and as the method shows on any three-manifold) is not a good question if we only know little about the dynamical system. On the other hand, at the end of the seventies most notably by Rabinowitz, [74, 75], and Weinstein, [85], there were some positive results concerning special vector fields coming from Hamiltonian systems. Rabinowitz's somewhat more general result is the following:

**THEOREM 1.2 (RABINOWITZ)** *A regular energy surface of an autonomous Hamiltonian system in  $\mathbf{R}^{2n}$ , which bounds a star-shaped domain, carries a periodic orbit.*

Weinstein proved a slightly weaker result assuming that the energy surface bounds a convex domain.

Figure 1: *A starshaped energy surface is diffeomorphic to a sphere centered at some point via radial transformation.*

We note that from a symplectic purist's point of view the results are not satisfactory, since the assumptions are not invariant under symplectic (or canonical) transformations.

Abstractly speaking we have here an existence result for certain non-singular vector fields on spheres  $S^{2n-1}$ . What is interesting now, of course, is the cut-off line between "Guaranteed Existence" and "Possible Non-Existence".

Based on the above mentioned results by Rabinowitz and his own contribution, Weinstein made in 1978 a conjecture, [86], which together with the earlier Arnold conjectures, [2], in symplectic fixed point theory had a tremendous impact.

Rabinowitz's result were extremely important, in particular psychologically, since the degenerate and indefinite classical Hamiltonian variational principle was used for the first time to study existence problem of periodic orbits in Hamiltonian

dynamics. One should keep in mind that this variational principle was thought to be only formal and completely useless for existence questions.

There were a certain number of difficulties to overcome. First of all one had to find a suitable functional analytic set-up, secondly one had to deal with the problem that a priori the Morse indices of the critical points of the functional had infinite Morse-index and co-index, so that (Palais-Smale type) Morse-theory in infinite-dimensional spaces would indicate that there is no relationship between the critical points and the topology of the underlying space, which in our case is the free loop space of the underlying symplectic manifold. Shortly afterwards Conley and Zehnder, [15], showed how the action principle by means of the Conley-index theory could be used to do symplectic fixed point theory, by proving a symplectic fixed point theorem for tori. Extensions of the methods for more general manifolds were however obstructed by immense technical difficulties. In 1985, Gromov, [34], introduced PDE-methods to symplectic geometry (the theory of pseudoholomorphic curves), “ignoring” however the underlying variational structure. (The word “ignoring” might be somewhat too strong here. The variational structure enters in the theory in the disguise of area bounds, which are of course extremely (in fact intrinsically) important in Gromov’s theory.)

Then in 1987, Floer, [25], brought together the Conley-Zehnder variational point of view and Gromov’s PDE methods and constructed his famous (symplectic) Floer homology theory. After that there were still some serious obstacles to overcome. For example, that the symplectic fixed point problem is not variational in general, but rather comparable with doing Morse-theory for a closed 1-form. (This calls for a Novikov-type Floer-theory, which was carried out in [43].) Besides that, the notorious difficulty of understanding holomorphic spheres in symplectic manifolds and in particular multiple covered spheres hindered progress for quite a while. Recently these difficulties were overcome, see in particular [30, 64, 63].

After this historical excursion let us state the Weinstein conjecture.

**CONJECTURE 1.3 (WEINSTEIN)** *Let  $M^{2n-1}$  be a  $(2n-1)$ -dimensional closed manifold and  $X$  a non-singular smooth vector field. Assume there exists a 1-form  $\lambda$  having the following properties:*

$$\begin{aligned} \lambda \wedge d\lambda^{n-1} & \text{ is a volume form,} \\ d\lambda(X, \cdot) & = 0, \\ \lambda(X) & > 0. \end{aligned}$$

*Then  $X$  has a periodic orbit.*

We call a 1-form  $\lambda$  a contact form if  $\lambda \wedge d\lambda^{n-1}$  is a volume form. We observe that a contact form defines a non-singular vector field  $X$  by

$$i_X d\lambda = 0 \text{ and } i_X \lambda = 1. \tag{1}$$

This uniquely determined vector field  $X$  is called the Reeb vector field associated with the contact form  $\lambda$ . Clearly, if  $f : M \rightarrow (0, \infty)$  is a smooth function, then the vector field  $X$  admits a periodic orbit if and only if  $fX$  admits a periodic orbit.



Therefore there is no loss of generality assuming in the Weinstein conjecture that  $X$  is a Reeb vector field. Note that  $\lambda$  defines a hyperplane distribution  $\xi \rightarrow M$  by

$$\xi = \ker(\lambda).$$

This plane field distribution is completely non-integrable. It is called a contact structure. We refer the reader to Arnold's book, [3], appendix 4, for more basic information about contact structures.

For our purposes we note here, that given a contact form on a three-dimensional manifold, there can always be introduced local coordinates  $(x, y, z)$  in which the contact form  $\lambda$  is given by  $\lambda = dz + xdy$ .

Figure 2: *The local model for a contact structure in dimension three*

At first glance the hypothesis in the Weinstein conjecture seems mysterious. However, some work reveals that it has a geometrically compelling meaning. Namely  $M$  may be viewed as an element of a smooth 1-parameter family of mutually different Hamiltonian energy surfaces  $M_\delta$ ,  $\delta \in [-\delta_0, \delta_0]$  (with  $M_0 = M$ ) in  $[-\delta_0, \delta_0] \times M$  equipped with a suitable symplectic structure, so that flows on two different energy surfaces are conformally symplectically the same. In particular the flows on any two such energy surfaces are conjugated.

So, for example, if one of these energy surfaces contains a periodic orbit, so do the others. One can reformulate the Weinstein conjecture as follows.

**CONJECTURE 1.4 (WEINSTEIN)** *Assume  $(W, \omega)$  is a symplectic manifold and  $H : W \rightarrow \mathbf{R}$  a smooth Hamiltonian, so that  $M := H^{-1}(E)$  is a compact regular energy surface (for some energy  $E$ ). If there exists a 1-form  $\lambda$  on  $M$  such that  $\lambda(X_H(x)) \neq 0$  for  $x \in M$  and  $d\lambda = \omega|_M$ , then there exists a periodic orbit on  $M$ .*

Here  $X_H$  is the Hamiltonian vector field defined by

$$i_{X_H}\omega = -dH.$$

Both formulations of the Weinstein conjecture are equivalent.

Having this in mind one can appreciate the following result. Consider the symplectic vector space  $(\mathbf{R}^{2n}, \omega)$ . The symplectic form is defined by

$$\omega = \sum_{j=1}^n dq_j \wedge dp_j.$$

Recall, that given an autonomous Hamiltonian  $H : \mathbf{R}^{2n} \rightarrow \mathbf{R}$  we have the associated Hamiltonian system

$$\dot{z} = X_H(z). \quad (2)$$

Denote by  $\Sigma_H$  the set of all  $E \in \text{image}(H)$  such that there exists no periodic solution  $(z, T)$  of (2) with  $H(z) = E$ . Now the following almost existence result holds, which tells us that periodic orbits are a common phenomenon and that there are usually many of them.

**THEOREM 1.5** *Let  $H : \mathbf{R}^{2n} \rightarrow \mathbf{R}$  be a smooth Hamiltonian satisfying  $H(z) \rightarrow \infty$  if  $|z| \rightarrow \infty$ . Then  $\text{measure}(\Sigma_H) = 0$ .*

This theorem was essentially proved by Hofer and Zehnder, [54], where it was shown that the complement of  $\Sigma_H$  is dense. The same approach was then pushed to its limits by Struwe, [81], showing that  $\text{measure}(\Sigma_H) = 0$ .

This almost existence phenomenon can be understood best within the symplectic capacity theory, see [56]. It holds for more general symplectic manifolds. However, not for all manifolds, see [37] for some very interesting phenomena.

Nevertheless one might ask if a regular compact energy surface necessarily carries a periodic orbit. We begin with a positive application. Using Theorem 1.5 we can recover Viterbo's landmark result, namely the proof of the Weinstein conjecture in  $\mathbf{R}^{2n}$ , [84]:

**COROLLARY 1.6 (VITERBO)** *Given a closed, connected hypersurface  $M$  in  $(\mathbf{R}^{2n}, \omega)$ , admitting a contact form  $\lambda$  such that  $d\lambda = \omega|_M$ , any Hamiltonian system having  $M$  as a regular energy surface admits a periodic orbit on  $M$ .*

The proof, based on Theorem 1.5 is obvious. Foliate the neighborhood of  $M$  by conformally symplectic images  $M_\delta$ ,  $\delta \in [-1, 1]$  by using the contact hypothesis. Assume that  $M_{-1}$  is contained in the bounded component  $B$  of  $\mathbf{R}^{2n} \setminus M$ .

Now define a Hamiltonian  $H$  having the property that  $H^{-1}(\delta) = M_\delta$  for  $\delta \in [-\frac{1}{2}, \frac{1}{2}]$ , so that these  $M_\delta$  are regular energy surfaces. In addition  $H(z) \rightarrow \infty$  for  $|z| \rightarrow \infty$ .

Figure 3: *The level sets for the constructed Hamiltonian  $H$ . The Hamiltonian is constant between a big sphere  $S$  and  $M_1$ .*

An application of Theorem 1.5 shows that for some  $\delta \in [-\frac{1}{2}, \frac{1}{2}]$  there exists a periodic orbit. Since all these hypersurfaces are conformally symplectically equivalent there is also one on  $M_0 = M$ . So the theorem can be used to prove existence results. But is the theorem optimal?

By results of Ginzburg, [31, 32], and Herman, [38, 39] the following holds.

**THEOREM 1.7** *For  $n \geq 3$  there exists a smooth embedding  $\Phi$  of  $[-1, 1] \times S^{2n-1}$  into  $(\mathbf{R}^{2n}, \omega)$ , such that  $M_0 = \Phi(\{0\} \times S^{2n-1})$  does not contain any periodic solution.*

By the almost existence theorem, of course,

$$\text{measure}\{\delta \in [-1, 1] \mid M_\delta \text{ contains a periodic orbit}\} = 2.$$

So, in some sense, in  $\mathbf{R}^{2n}$ , for  $n \geq 3$ , the almost existence result is the best possible. Nevertheless it is still an open question if Theorem 1.7 holds for  $n = 2$ .

At this point we have almost existence results and non-existence results and an existence result for closed contact type hypersurfaces in  $\mathbf{R}^{2n}$ .

Are there manifolds for which one can say that every Reeb vector field on them has a periodic orbit?

**THEOREM 1.8 (HOFER)** *Assume that  $X$  is a Reeb vector field on a closed three-manifold  $M$ . Then  $X$  admits a periodic orbit if either  $M$  is finitely covered by  $S^3$ , or if  $\pi_2(M) \neq \{0\}$ , or if the underlying contact structure is overtwisted.*

The notion of an overtwisted contact structure is important in three-dimensional contact geometry.

**DEFINITION 1.9** *Let  $\lambda$  be a contact structure on the three-manifold  $M$  with underlying contact structure  $\xi = \text{kern}(\lambda)$ . The contact structure  $\xi$  is said to be overtwisted if there exists an embedded disk  $\mathcal{D} \subset M$ , such that*

$$T(\partial\mathcal{D}) \subset \xi|(\partial\mathcal{D}) \tag{3}$$

$$T_z\mathcal{D} \not\subset \xi_z \text{ for all } z \in \partial\mathcal{D}. \tag{4}$$

*We call a contact structure tight if it is not overtwisted. (Figure 4 gives an example of an overtwisted disk).*

It is a fundamental result by Bennequin, [6], that the so-called standard contact structure on  $S^3$

$$\lambda_0 = \frac{1}{2}[q \cdot dp - p \cdot dq]|S^3$$

is tight.<sup>1</sup>

In a deep paper (which stunned many of the experts), [20], Eliashberg classified all overtwisted contact structures for a closed three-manifold  $M$ . This classification can be done in purely homotopy theoretic terms.<sup>2</sup> In addition he showed

<sup>1</sup>Here  $S^3$  is viewed as the unit sphere in  $\mathbf{C}^2$ , where the latter is equipped with the coordinates  $z = q + ip$ ,  $q, p \in \mathbf{R}^2$ .

<sup>2</sup>There is an ‘‘h-principle’’ in the background.

Figure 4: *An overtwisted contact structure on  $\mathbf{R}^3$ .*

that up to diffeomorphism there is only one (positive) tight contact structure on  $S^3$  but a countable number of overtwisted contact structures and also classified the contact structures on  $\mathbf{R}^3$ , see [22, 23]. One should also mention the work by Giroux, most notably [33], which had a great impact on contact geometry.

## 2 PERIODIC ORBITS IN HAMILTONIAN DYNAMICS AND RIGIDITY

As the preceding discussion shows, finding periodic orbits is an “ill-posed” problem in general, but well-posed” for a certain class of dynamical systems.

From a dynamical systems point of view periodic orbits allow to study the flow in a neighborhood by means of a return map. In the case of a Hamiltonian system one can expect already very striking phenomena as Figure 5 shows. The fixed point 0 in the middle is surrounded by smooth curves, which are invariant under the return map. These curves were discovered by Moser, [71]. Between these curves there are orbits of elliptic and hyperbolic periodic points. The stable and unstable manifolds starting from these hyperbolic points intersect transversally in so-called homoclinic points. Due to these homoclinic points we have invariant hyperbolic sets on which the iterates of the return map behave like a Bernoulli shift. The dotted lines represent the recently discovered Mather-sets, [66]. The generic existence of the homoclinic orbits was rigorously established by Zehnder, [90].

Particularly interesting are hyperbolic periodic orbits if they come together with a (global) homoclinic orbit. Then, if the stable and unstable manifold intersect transversally, a very rich dynamics unfolds near the union of the periodic and the homoclinic orbit.

Surprisingly, there is an additional dimension to the periodic orbits, which only in the last ten years has become apparent. Namely the importance of periodic orbits in a symplectic rigidity theory. They are the objects which carry important symplectic information. Let us mention two of these constructions. The first is a symplectic capacity introduced by Hofer and Zehnder, [55]. Consider the category  $\mathcal{S}^{2n}$  consisting of all of all  $2n$ -dimensional symplectic manifolds (with or without boundary) as objects and the symplectic embeddings as morphisms.

For every symplectic manifold  $(W, \omega)$  in  $\mathcal{S}^{2n}$  we consider the collection

Figure 5: *The dynamical complexity near a generic elliptic periodic orbit, as seen for the return map of a transversal section.*

$\mathcal{H}(W, \omega)$  of all smooth maps  $H : W \rightarrow (-\infty, 0]$  with compact support  $\text{supp}(H)$  such that:

- $\text{supp}(H) \cap \partial W = \emptyset$ .
- There exists a nonempty open set  $U$  with  $H|_U \equiv \text{const.} = \inf_{x \in W} H(x)$ .
- Every periodic orbit of the Hamiltonian system  $\dot{x} = X_H(x)$  with period  $T \in (0, 1]$  is constant.

Then define a number  $c(W, \omega) \in [0, \infty) \cup \{\infty\}$  by

$$c(W, \omega) := \sup_{H \in \mathcal{H}(W, \omega)} \|H\|_{C^0}.$$

These numbers are new symplectic invariants called symplectic capacities and are by their very nature 2-dimensional invariants of the symplectic manifold  $(W, \omega)$ . Of course the volume  $\text{vol}(W, \omega) = \int_W \omega^n$  is a  $2n$ -dimensional invariant. The formal properties of  $c$  are:

- If  $(W, \omega) \rightarrow (V, \tau)$  then  $c(W, \omega) \leq c(V, \tau)$ .
- $c(W, \alpha\omega) = |\alpha| \cdot c(W, \omega)$  for  $\alpha \in \mathbf{R} \setminus \{0\}$ .
- $c(B^{2n}) = c(Z^{2n}) = \pi$ .

Here  $B^{2n}$  is the Euclidean unit ball in  $\mathbf{R}^{2n}$  and  $Z^{2n}$  the unit-cylinder  $B^2 \times \mathbf{R}^{2n-2}$ , both equipped with the induced symplectic structure.<sup>3</sup>

If  $(\phi_t)$  is a Hamiltonian flow on some symplectic manifold and  $U$  is an open subset then not only the volume of  $\text{vol}(\phi_t(U))$  is independent of  $t$  but also the symplectic capacity  $c(\phi_t(U))$ .

---

<sup>3</sup>The definition of a symplectic capacity is motivated by Gromov's celebrated (non-)squeezing theorem, [34, 35]. His theorem leads to a capacity called "Gromov's width".

As it turns out there are many different constructions for symplectic capacities. Some involve the theory of pseudoholomorphic curves, [34], some the least action principle in Hamiltonian dynamics, [18], and there is even one using a symplectic homology theory, [27]. In reference [18] symplectic rigidity phenomena were shown for the first time to be related to periodic orbit problems.

Symplectic homology is a realization of the following idea. Assume that we consider the usual homology theory, but restricted to the category  $\mathcal{S}^{2n}$ . Since the spaces have an additional symplectic structure and the morphisms are symplectic embeddings it seems plausible that the restricted standard (topological) homology functor is obtained by composing a forgetful functor with some (much more complex) symplectic homology functor. Indeed, along these lines a symplectic homology functor can be constructed depending on three parameters, namely an integer  $k$  and a pair of real numbers  $a \leq b$ . As it turns out the symplectic homology for sufficiently nice symplectic manifolds  $W$  with boundary is constructed out of the topology of  $M$  and the periodic orbits for the Hamiltonian flow on  $\partial W$ . The action of the periodic orbits gives a real filtration (leading to the  $a, b$ -dependence) and the Conley-Zehnder indices of the periodic orbits (a substitute for the Morse index, when seeing periodic orbits as critical points of some Morse function on a suitable loop space) lead to the integer grading. For more details the reader is referred to [27], or to [56] for a short overview.

### 3 HOLOMORPHIC CURVES AND THE WEINSTEIN CONJECTURE

As it turns out there is a subtle relationship between the dynamics of Reeb vector fields and an holomorphic curve theory. In order to explain this “holomorphic connection” we start with a specific example. View  $S^{2n-1}$  as the unit sphere in  $\mathbf{C}^n$ . We write the coordinates in  $\mathbf{C}^n$  as

$$z = (z_1, \dots, z_n) = (q_1 + ip_1, \dots, q_n + ip_n)$$

with  $z_j \in \mathbf{C}$  and  $q_j, p_j \in \mathbf{R}$ . The standard contact form  $\lambda_0$  on  $S^{2n-1}$  is defined by:

$$\lambda_0 = \frac{1}{2} \sum_{j=1}^n [q_j dp_j - p_j dq_j] |S^3.$$

The Reeb vector field is given by  $X_0(z) = 2iz$ , which generates the Hopf fibration and the contact structure  $\xi_0$  is the bundle of complex  $(n-1)$ -planes in  $TS^{2n-1}$ .

The idea, which is difficult to motivate a priori, is now the following. Introduce on  $\mathbf{R} \times S^{2n-1}$  the complex structure  $\tilde{J}$  by requiring that the diffeomorphism

$$\Phi : \mathbf{C}^n \setminus \{0\} \rightarrow \mathbf{R} \times S^{2n-1}, z \rightarrow \left( \frac{1}{2} \ell n |z|, \frac{z}{|z|} \right)$$

is biholomorphic, i.e.

$$T\Phi \circ i = \tilde{J} \circ T\Phi.$$

Then, one easily verifies that  $\tilde{J}$  is given by

$$\tilde{J}(a, u)(h, k) = (-\lambda_0(u)(k), i\pi_0 k + hX_0(u)), \quad (5)$$

where  $\pi_0 : TS^{2n-1} \rightarrow \xi_0$  is the projection along  $X_0$ . Of course under  $\Phi$  the study of holomorphic curves in  $\mathbf{C}^n$ , which avoid the origin is equivalent to studying holomorphic curves in  $\mathbf{R} \times S^{2n-1}$ . In  $\mathbf{C}^n$  there is a very nice class of holomorphic curves, namely the affine algebraic curves. In which way are they distinguished from an arbitrary holomorphic curve? Denote by  $\Sigma$  the collection of all smooth maps  $\mathbf{R} \rightarrow [0, 1]$  having non-negative derivative and associate to  $\varphi \in \Sigma$  the 2-form on  $\mathbf{R} \times S^{2n-1}$  defined by

$$\omega_\varphi = d(\varphi\lambda_0),$$

where  $(\varphi\lambda_0)(a, u)(h, k) = \varphi(a)\lambda_0(u)(k)$ .

The interesting observation is now, [42]:

PROPOSITION 3.1 *Assume that  $A$  is a connected closed subset of  $\mathbf{C}^n \setminus \{0\}$ . Then the following statements are equivalent:*

1. *The closure of  $A$  in  $\mathbf{C}^n$  is an irreducible 1-dimensional affine algebraic curve.*
2. *There exists a connected closed Riemann surface  $(S, j)$ , and a finite subset  $\Gamma \subset S$ , and a smooth map  $\tilde{u} : S \setminus \Gamma \rightarrow \mathbf{R} \times S^{2n-1}$  such that*

$$\tilde{J} \circ T\tilde{u} = T\tilde{u} \circ j, \tag{6}$$

$$0 < E(\tilde{u}) := \sup_{\varphi \in \Sigma} \int_{S \setminus \Gamma} \tilde{u}^* \omega_\varphi < \infty,$$

$\tilde{u}$  cannot be smoothly extended over any point in  $\Gamma$ ,

$$\Phi(S) = \tilde{u}(S \setminus \Gamma).$$

Clearly  $T\tilde{u} \circ j = \tilde{J} \circ T\tilde{u}$  is a non-linear Cauchy-Riemann type equation. If  $\tilde{u}$  is a solution, then necessarily  $\tilde{u}^* \omega_\varphi$  is a non-negative integrand, so that the definition of  $E(\tilde{u})$  makes sense. The estimate  $E(\tilde{u}) > 0$  implies that  $\tilde{u} \not\equiv const..$  The finiteness of the energy means analytically that given a solution  $\tilde{u}$  of the Cauchy-Riemann equation and an  $\mathbf{R}$ -invariant metric on  $\mathbf{R} \times S^{2n-1}$ , the area of the image of  $\tilde{u}$  in any set  $[c, c + 1] \times S^{2n-1}$  is uniformly bounded independent of  $c \in \mathbf{R}$ . This, of course, corresponds to polynomial growth if we view the corresponding curve in  $\mathbf{C}^n$ . What is the behavior near the points in  $\Gamma$  (the punctures)?

Near a (non-removable) puncture  $z_0$  the image of a tiny punctured disk around  $z_0$  is approximately a half-cylinder  $[R, \infty) \times P$ , where  $P$  is a Hopf circle. There is a suggestive way to generalize the above situation. Namely, consider a closed manifold  $M$  of dimension  $2n - 1$ , equipped with a contact form  $\lambda$ . Make one choice, by taking a complex multiplication  $J : \xi \rightarrow \xi$ , where  $\xi = \text{kern}(\lambda)$ , so that

$$g_J(u)(k, k') = d\lambda(u)(k, J(u)k')$$

defines fibre-wise a positive inner product for the bundle  $\xi \rightarrow M$ . Then define an  $\mathbf{R}$ -invariant almost complex structure on  $\mathbf{R} \times M$  by

$$\tilde{J}(a, u)(h, k) = (-\lambda(u)(k), J(u)\pi k + hX(u)),$$

where  $X$  is the Reeb vector field associated to  $\lambda$  and  $\pi : TM \rightarrow \xi$  the projection along  $X$ . The definition of  $E$  generalizes by replacing  $\varphi\lambda_0$  by  $\varphi\lambda$ . So our new

equation becomes

$$\begin{aligned}\tilde{u} : S \setminus \Gamma &\rightarrow \mathbf{R} \times M \\ T\tilde{u} \circ j &= \tilde{J} \circ T\tilde{u} \\ 0 &< E(\tilde{u}) < \infty.\end{aligned}\tag{7}$$

What is the behavior near a puncture  $z_0 \in \Gamma$ ? There are three mutually exclusive possibilities.

1. Positive puncture:  $\lim_{z \rightarrow z_0} a(z) = \infty$
2. Negative puncture:  $\lim_{z \rightarrow z_0} a(z) = -\infty$
3. Removable puncture:  $\lim_{z \rightarrow z_0} a(z) =: a_0 \in \mathbf{R}$

In the last case the map  $\tilde{u}$  can be smoothly extended over  $z_0$ . Let us assume that for the following  $\tilde{u}$  has been extended over all removable punctures. We note that for a solution of (7) the set  $\Gamma$  cannot be empty. Indeed, otherwise by Stokes' theorem  $E(\tilde{u}) = 0$ .

The relationship between the solutions of (7) and the periodic orbits of  $X$  is contained in

**THEOREM 3.2 (HOFER)** *Let  $\lambda$  be a contact form on the closed  $(2n - 1)$ -dimensional manifold  $M$  and  $J$  be an admissible complex multiplication for the underlying contact structure  $\xi$ . If (7) has a solution, then there exists a periodic orbit for the Reeb vector field with period  $T \leq E(\tilde{u})$ .*

For generic  $\lambda$  the finite energy surface approximates near a puncture a cylinder over a periodic orbit. Figure 6 on the next page shows a finite energy surface with two positive punctures and one negative puncture.

In order to use that theorem, one needs to develop methods to find holomorphic curves solving (7). Whereas the first existence results were based on ad hoc methods it meanwhile became clear for specialists that there is a (Floer-type) homology theory in the background. It has already been christened "Contact Homology", but doesn't yet exist as "hard copy". This theory was envisioned by Eliashberg and the author in 1993 after the paper [40], and some talks about special cases were given at various places, in particular at the IAS/Park City summer institute on symplectic geometry, [24]. To create such a homology theory for general closed contact manifolds, one encounters certain analytical problems in counting holomorphic curves, quite familiar from the Arnold conjectures. However, since the recent solution of the Arnold conjectures overcomes these difficulties one should be able deal with these problems.

By the previous discussion the Weinstein conjecture has been reduced to finding nontrivial holomorphic curves. The following theorem is the first, dealing with the solvability of (7). The method used is an Eliashberg-type disk-filling, [21], based on Gromov's pseudoholomorphic curve theory. These type of methods are familiar in the theory of several complex variables, where they are used to study envelopes of holomorphy, see [5]. The main point here is, however, that it is a priori known that the analysis involved in the disk-filling has to fail.



Figure 6: A finite energy surface with 2 positive punctures and one negative puncture

**THEOREM 3.3 (HOFER)** *Assume  $M$  is a closed three-manifold and  $\lambda$  a contact form. Let  $J : \xi \rightarrow \xi$  be an admissible complex multiplication for the underlying contact structure and denote by  $\tilde{J}$  the associated almost complex structure on  $\mathbf{R} \times M$ . If either  $M = S^3$ , or  $\pi_2(M) \neq 0$ , or  $\xi$  is overtwisted there exists a solution  $\tilde{u}$  of (7) with  $S = S^2$  and  $\Gamma = \{\infty\}$ . In other words there exists a finite energy plane.*

We note that Theorem 3.3 implies Theorem 1.8. The proof is based on a careful analysis of certain nonlinear boundary value problems involving a non-linear Cauchy-Riemann type operator on the disk. One knows for topological reasons that there cannot be apriori estimates and studies carefully how the estimates fail. A bubbling-off analysis making extensive use of the  $\mathbf{R}$ -invariance of  $\tilde{J}$  then allows via reparametrizations to construct these solutions. We refer the reader to the upcoming book [1] for a very detailed description of the methods, and to [40, 41, 42] for the original proof and some discussion of the underlying ideas.

In dimension three we can sometimes say more about the nature of the periodic orbits to which the holomorphic curves are asymptotic. For example, for

every Reeb vector field on  $S^3$  there exists an unknotted periodic orbit, see [52].

Many interesting and surprising examples illustrating how bad arbitrary Hamiltonian flows can behave in contrast to Reeb flows can be found in [11].

#### 4 GLOBAL SYSTEMS OF SURFACES OF SECTION

One might wonder, if one can say more about the dynamics. Here we restrict ourselves to the three-dimensional cases for the sole reason that the methods cannot be employed in higher dimensions.

Assume we are given a closed three-manifold  $M$  and a nowhere vanishing vector field  $X$ . We would like to understand the dynamics. A successful idea going back to Poincaré and Birkhoff, [7], is to find a global surface of section, reducing the understanding of the dynamics to the problem of understanding a self-map of a surface. Of course there are topological and dynamical obstructions in finding such a surface.

**DEFINITION 4.1** *A global surface of section for  $(M, X)$  is a compact surface (perhaps with boundary)  $\Sigma \subset M$ , such that  $\partial\Sigma$  consists of periodic orbits and  $\dot{\Sigma} = \Sigma \setminus \partial\Sigma$  is transversal to  $X$ , so that in addition every orbit other than those in  $\partial\Sigma$  hit  $\dot{\Sigma}$  in forward and backward time.*

The surface of section allows to define a return map  $\psi : \dot{\Sigma} \rightarrow \dot{\Sigma}$ . Then the dynamics is encoded in  $\psi$ . Of course, having in mind how complicated flows are, one really doesn't expect the existence of such a surface of section. For example, any surface of section for  $(S^3, X)$  must necessarily have a boundary. Indeed, if there is no boundary component,  $S^3$  would necessarily fiber over  $S^1$ , which by the exact homotopy sequence for a fibration would imply that  $\pi_1(S^3) \neq \{1\}$ . On the other hand if there is a boundary component there has to be a periodic orbit, which however need not to exist by Kuperberg's result. Also, in the volume-preserving case it is doubtful if something sensible can be said. However, as it turns out, for Reeb flows on three-dimensional manifolds, a whole theory of surfaces of section almost intrinsically exists. This theory, which will be discussed now, should be possible for every (or at least many) three-manifold. However, details have only been carried out so far for  $S^3$ .

Let us begin with  $S^3$  equipped with the standard structure  $\lambda_0$ . Again we let ourselves be inspired by the model problem. Denote by

$$\Phi : \mathbf{C}^2 \setminus \{0\} \rightarrow \mathbf{R} \times S^3$$

the diffeomorphism

$$z \rightarrow \left( \frac{1}{2} \ell n |z|, \frac{z}{|z|} \right)$$

previously defined.

Consider the sets  $\Phi(\mathbf{C} \times \{c\})$ , where  $c \in \mathbf{C} \setminus \{0\}$ , and  $\Phi((\mathbf{C} \setminus \{0\}) \times \{0\})$ . The union of these sets is a smooth foliation  $\mathcal{F}$  of  $\mathbf{R} \times S^3$  consisting of finite energy surfaces. Observe that we have a natural  $\mathbf{R}$ -action:

$$\mathbf{R} \times \mathcal{F} \rightarrow \mathcal{F}, (a, F) \rightarrow a + F,$$

Figure 7: *The collection of projected surfaces establishes an open book decomposition of  $S^3$*

where

$$a + F := \{(a + b, m) \mid (b, m) \in F\}.$$

There is one fixed point  $F_0$  of this action corresponding to a cylinder over the periodic orbit  $P = S^1 \times \{0\}$ :

$$F_0 = \mathbf{R} \times P.$$

If the surfaces are projected into  $S^3$  the fixed point  $F_0$  projects onto the Hopf circle  $P$  and all other surfaces onto open disks bounded by  $P$ . The collection of projected surfaces in fact establishes an open book decomposition of  $S^3$  with disk-like pages, see Figure 7.

What happens if we modify the contact form, but keep the contact structure, i.e. replace  $\lambda_0$  by  $\lambda = f\lambda_0$ ?

In order to study this question it is useful to make the following definition.

**DEFINITION 4.2** *Let  $M$  be a closed three-manifold,  $\lambda$  a contact form on  $M$  and  $J$  a complex multiplication for the associated contact structure. A finite energy foliation  $\mathcal{F}$  for  $(M, \lambda, J)$  is a 2-dimensional smooth foliation for  $\mathbf{R} \times M$  such that the following holds:*

- *There exists a universal constant  $C > 0$  such that for every leaf  $F \in \mathcal{F}$  there exists an embedded finite energy curve  $(S, \Gamma, \tilde{u})$  for  $(M, \lambda, J)$  satisfying*

$$F = \tilde{u}(S \setminus \Gamma)$$

*and  $E(\tilde{u}) \leq C$ . All punctures  $\Gamma$  are assumed to be non-removable.*

- *For every  $a \in \mathbf{R}$  and  $F \in \mathcal{F}$  also  $a + F$  belongs to  $\mathcal{F}$ . In particular either  $F = F_a$  or  $F \cap (a + F) = \emptyset$ .*

Let us call a contact form  $\lambda$  non-degenerate if all the periodic orbits  $(x, T)$  for  $X_\lambda$  are non-degenerate in the following sense. Denote by  $\eta_t$  the flow associated to

$X$  and observe that it preserves  $\lambda$ , so that the tangent map  $T\eta_t(x(0))$  induces a map

$$L_{(x,t)} := T\eta_t(x(0))|_{\xi_{x(0)}} : \xi_{x(0)} \rightarrow \xi_{x(T)}.$$

For every period  $T > 0$  we therefore obtain a self map of  $x_{\xi(0)}$ , which is symplectic with respect to the structure  $d\lambda(x(0))$ . We say  $(x, T)$  is non-degenerate if 1 does not belong to the spectrum of  $L_{(x,T)}$ .

We assume that we are given a closed three-manifold  $M$  and a contact form  $\lambda$  with associated Reeb vector field  $X$  and contact structure  $\xi$ . Assuming that the contact form  $\lambda$  is non-degenerate is a generic condition. Indeed, the following holds.

**PROPOSITION 4.3** *Fix a contact form  $\tau$  on the closed three manifold  $M$ . Consider the subset  $\Xi_1 \subset C^\infty(M, (0, \infty))$  consisting of all those  $f$  such that  $\lambda = f\tau$  is non-degenerate. Let  $\Xi_2$  consist of all those  $f \in \Xi_1$  such in addition the stable and unstable manifold of hyperbolic orbits intersect transversally. Then  $\Xi_1$  and  $\Xi_2$  are Baire subsets of  $C^\infty(M, (0, \infty))$ .*

The question is now if finite energy foliations exist for given data  $(M, \lambda, J)$ . The answer to this question in general is not known. However, as we will see, we have existence for  $M = S^3$  and generic contact forms  $\lambda = f\lambda_0$ , where  $\lambda_0$  is the standard contact form and  $f \in \Xi_1$ , provided  $J$  is generic as well. In the  $S^3$ -case it makes sense to impose more conditions on the finite energy foliation.

First of all one needs to define some index  $\mu(x, T)$  for a non-degenerate periodic solutions  $(x, T)$ . This index, the so-called Conley-Zehnder index, [14], is some kind of Morse index for a periodic orbit of a Hamiltonian system. In our low-dimensional case the Conley-Zehnder index can be interpreted as an integer-measure of how orbits infinitesimally close to a periodic orbit twist around it with respect to some natural framing, see [42] for a detailed discussion.

Next one defines another index for a finite energy surface by

$$\text{ind}(\tilde{u}) = \mu(\tilde{u}) - \chi(S) + \sharp\Gamma,$$

where  $\chi(S)$  is the Euler characteristic of the underlying closed Riemann surface,  $\sharp\Gamma$  is the number of punctures, and  $\mu(\tilde{u}) = \mu^+ - \mu^-$  is the total Conley-Zehnder index, which is computed as follows. The number  $\mu^\pm$  is the sum of the Conley-Zehnder indices of the periodic orbits associated to the positive and negative punctures, respectively.

The index  $\text{ind}(\tilde{u})$  has an interpretation as a Fredholm index, describing the dimension of the moduli space of nearby finite energy surfaces, having the same topological type and number of punctures, which are allowed to move as well as the complex structure on  $S$  in Teichmüller space, see [49]. In the following we shall call a solution

$$\tilde{u} : S^2 \setminus \Gamma \rightarrow \mathbf{R} \times M$$

of the non-linear Cauchy-Riemann equation with finite (but nontrivial) energy having only non-removable punctures a finite energy sphere. If  $\Gamma = \{\infty\}$  we call it a finite energy plane.

DEFINITION 4.4 *Let  $\lambda = f\lambda_0$  be a non-degenerate contact form on  $S^3$  and  $J$  a complex multiplication for  $\xi_0$ . A stable finite energy foliation for  $(S^3, \lambda, J)$  is a finite energy foliation with the following properties:*

1. *Every leaf of the foliation is the image of an embedded finite energy sphere.*
2. *For every leaf the asymptotic limits are simply covered, their Conley-Zehnder indices are contained in  $\{1, 2, 3\}$  and they have self-linking number  $-1$ .*<sup>4</sup>
3. *Every leaf has precisely one positive puncture, but an arbitrary number of negative punctures.*
4. *For every leaf  $F$ , parametrized by a finite energy sphere  $\tilde{u}$ , which is not a fixed point for the  $\mathbf{R}$ -action, we have  $\text{ind}(\tilde{u}) \in \{1, 2\}$ .*

Figure 8 on the next page shows an example.

The following result gives the existence of finite energy foliations.

THEOREM 4.5 *For every choice of  $f \in \Xi_1$  there exists a Baire set of admissible complex multiplications  $J$  admitting a stable finite energy foliation  $\mathcal{F}$  of  $(S^3, f\lambda_0, J)$ .*

We shall not give a proof of the results concerning finite energy foliations in this overview, but refer the reader to the forthcoming paper [53].

Given a stable finite energy foliation of  $S^3$ , one can show that the projected surfaces establish a singular foliation of  $S^3$  which gives a smooth foliation transverse to the flow in the complement of a finite number of distinguished periodic orbits.

Using this system of surfaces one can prove, [53]:

THEOREM 4.6 *Let  $f \in \Xi_2$ . Then the Reeb flow of  $X_\lambda$  on  $S^3$  associated to  $\lambda = f\lambda_0$  has the following properties.*

- *Either  $X_\lambda$  has precisely two geometrically distinct periodic orbits or infinitely many.*
- *If  $X_\lambda$  does not admit a disk-like global surface of section there exists a hyperbolic periodic orbit with orientable stable manifold and a homoclinic orbit converging in forward and backward time to the hyperbolic orbit. In particular there are infinitely many geometrically distinct periodic orbits and the topological entropy of the flow is positive.*

This gives the following corollary.

COROLLARY 4.7 *Let  $f \in \Xi_2$ . If the associated Reeb flow admits a periodic orbit  $(x, T)$ , with  $T$  the minimal period, so that  $x_T : \mathbf{R}/(T\mathbf{Z}) \rightarrow S^3$  is knotted, then there exist infinitely many geometrically distinct periodic orbits.*

---

<sup>4</sup>Presumably one can also require the asymptotic limits to be unknotted. However, our existence result Theorem 4.5 so far does not give this additional property.

Figure 8: *The figure shows the trace of the projection of a finite energy foliation on a two-dimensional plane. Here we have two spanning orbits  $E_1$  and  $E_2$  which are elliptic and a hyperbolic one denoted by  $H$ . Moreover the foliation contains planes and cylinders. The dashed lines are the traces of the stable and unstable manifold of the hyperbolic orbit  $H$ . We assume the non-generic situation that they precisely match up creating several invariant sets. The dotted lines are periodic orbits for the Reeb vector field. The fat lines represent rigid pieces of the finite energy foliation. Namely two cylinders and two planes. The three-sphere is viewed as  $\mathbf{R}^3 \cup \{\infty\}$ .*

It is worthwhile to give some ideas about the proof of Corollary 4.7. Given  $\lambda = f\lambda_0$  take a generic  $J$  and the associated stable finite energy foliation  $\mathcal{F}$  for  $(S^3, \lambda, J)$ . Assume that the  $\mathbf{R}$ -action has precisely one fixed point. In this case we have a disk-like surface of section  $\mathcal{D}$  and a return map

$$\Psi : \dot{\mathcal{D}} \rightarrow \dot{\mathcal{D}},$$

which preserves the area form  $d\lambda|_{\mathcal{D}}$ . This map has a fixed point as a consequence of Brouwer's translation theorem. Recall that the translation theorem asserts that an orientation preserving homeomorphism  $h$  of  $\mathbf{R}^2$  either has a fixed point or there exists a non-empty open set  $U$  such that  $U \cap h^j(U) = \emptyset$  for all  $j \in \{1, 2, \dots\}$ . Clearly all  $h^j(U)$  and  $h^k(U)$  are mutually disjoint for  $j \neq k$ . If in our case  $\Psi$  does not have a fixed point we immediately obtain a contradiction to the fact that  $\Psi$  preserves area. Removing this fixed point we obtain an area preserving self-map of the open annulus, which by a striking result due to Franks, [29], has the following property:

**THEOREM 4.8 (FRANKS)** *Let  $\Psi$  be an area- and orientation-preserving self-map of the open annulus. If  $\Psi$  admits a periodic point, then it admits infinitely many periodic points.*

In order to finish the argument for the corollary we may assume arguing indirectly that there are precisely two periodic orbits. In that case both are unknotted

Figure 9: *The figure shows the situation if there is a disk-like surface of section, but only two periodic orbits.*

and mutually linked, as depicted in Figure 9. However, since we have one knotted orbit this is impossible.

There are also results without any genericity assumption. If  $M \subset \mathbf{R}^4$  is a compact energy surface enclosing a strictly convex domain, then one can show by methods similar to those outlined above that there exists a global disk-like surface of section. More precisely, see [48],

**THEOREM 4.9** *The Hamiltonian flow on a sphere-like energy surface in  $\mathbf{R}^4$ , bounding a strictly convex domain admits a global disk-like surface of section. In particular it has precisely two geometrically distinct periodic orbits or infinitely many.*

## 5 TOPOLOGY AND REEB DYNAMICS

After the previous results and discussions one might wonder, if it is possible to use the theory of finite energy surfaces and some knowledge of the Reeb dynamics in order to learn something about the topology of the underlying manifold. There has been not much research in that direction, but the results so far indicate that there are some nontrivial connections.

We begin by showing that tight contact forms feel the topology. Let  $M$  be a closed three manifold. For every tight contact form  $\lambda$  denote by  $[\lambda]$  the infimum of all periods  $T$  of contractible periodic orbits  $(x, T)$  for  $X_\lambda$ .<sup>5</sup> For a closed oriented surface  $F \subset M$  denote by  $v_\lambda(M)$  the number

$$v_\lambda(F) = \frac{\frac{1}{2} \int_F |d\lambda|}{[\lambda]}.$$

This is the normalized positive area of  $F$ .<sup>6</sup> Then define the virtual area of  $F$  by

$$v(F) = \inf_{\lambda \in \mathcal{T}} v_\lambda(F).$$

<sup>5</sup>If there are no contractible periodic orbits we take the infimum over the empty set leading to  $[\lambda] = \infty$ . For simple geometrical reasons we always have  $[\lambda] > 0$ .

<sup>6</sup>Obviously  $\int_F d\lambda = 0$ , so that the positive area and the negative area cancel each other.

Here  $\mathcal{T}$  is the collection of all tight contact forms on  $M$ .

One has the following result, see [40].

**THEOREM 5.1** *Assume  $M$  is a closed orientable three-manifold and  $F$  an embedded sphere. If  $v(F) < 1$  then  $F$  is contractible in  $M$ .*

If the Poincaré conjecture holds one can show that  $v(F) < 1$  implies  $v(F) = 0$  and even that  $v(F) = 0$  if and only if  $F$  is contractible. The criterion is extremely sharp. For  $F = \{\text{point}\} \times S^2$  in  $M = S^1 \times S^2$  we have  $v(F) = 1$ .<sup>7</sup>

The next result shows that we are even sometimes able to recover the topology of the space. For more general results see [46, 47].

**THEOREM 5.2** *Assume that  $\lambda$  is a contact form on the closed three-manifold  $M$ , so that the periodic orbits of the associated Reeb vector field are all non-degenerate. Assume that there exists an embedded disk  $\mathcal{D}$  in  $M$  so that the boundary  $\partial\mathcal{D}$  is a periodic orbit of minimal period  $T_0$ , say, and  $\mathcal{D} \setminus \partial\mathcal{D}$  is transverse to the flow. Then, if all periodic orbits with periods  $T \leq T_0$  are elliptic or hyperbolic with non-orientable stable manifold, necessarily  $M$  is diffeomorphic to  $S^3$  and the contact form  $\lambda$  is tight.*

Now leaving firm grounds one might foresee some of the possible developments in contact geometry and topology as follows. Assume a contact form  $\lambda$  on a closed three-manifold  $M$  is given. Fixing an admissible complex multiplication for the underlying contact structure  $\xi$  gives an almost complex structure  $\tilde{J}$  for  $\mathbf{R} \times M$ . Studying the finite energy surfaces for  $\tilde{J}$  will lead<sup>8</sup> to some Floer type homology theory, called contact homology, build on a  $\mathbf{Z}_2$ -graded algebra generated by the periodic orbits. The analytical difficulties comprise those familiar in the Arnold conjectures, [30, 63, 64]. The underlying techniques are those from [40, 50, 49, 51, 48, 52]. As it turns out, contact homology only depends on the underlying co-oriented contact structure  $\xi$ . This theory can be carried out in any (odd) dimension. Symplectic cobordisms compatible with the contact structures induce morphisms in this theory.

Focusing now on dimension three the following can be said. The contact homology for overtwisted contact structures is presumably trivial, and, if  $\xi$  is tight, an interesting invariant for  $(M, \xi)$ . Given a Legendrian knot, i.e. a knot with tangent space contained in  $\xi$ , certain surgeries are possible to lead to new tight contact manifolds. It is important to understand how the contact groups change. Of course, it is necessary to introduce a contact homology group for

---

<sup>7</sup>As a parenthetical remark we observe that for every tight contact form

$$v(F) \cdot [\lambda] \leq \frac{1}{2} \int_F |d\lambda|.$$

In case, there exists an embedded non-contractible sphere, which always holds if  $\pi_2(M) \neq \{0\}$  by the sphere theorem, we have that  $v(F) \geq 1$ . Therefore the inequality implies the existence of a contractible periodic orbit.

<sup>8</sup>The details for such a theory are formidable and are just being carried out by Y. Eliashberg and H. Hofer.



Legendrian knots, [24], which would be based on Arnold's chord problem, [4] and would have to generalize [13].

Since the contact homology for  $(M, \xi)$  should be computable for every generic contact form inducing  $\xi$  it will be important to develop methods to simplify the contact form by eliminating short periodic orbits for the Reeb vector field, which algebraically should not be there.

Thirdly, some of the finite energy surfaces occurring for a given contact form, might be used for finite energy foliations, which lead to generalizations of open book decompositions, but indeed carrying more structure.

It is feasible that some program as out-lined above will be useful for studying the topology of three-dimensional manifolds. There is, of course, no doubt that this program leads in any case to a deeper understanding of the dynamics of Reeb vector fields. This is particularly interesting, since we also obtain new tools for studying geodesic flows on surfaces.

## 6 RELATIONSHIP TO OTHER AREAS

In a nutshell one can say that study of the Reeb dynamics or certain aspects of it is closely related to be able to count and handle holomorphic curves. How to use holomorphic spheres in order to prove cases of the Weinstein conjecture was shown by Hofer and Viterbo, [45]. Of course meanwhile there are very well-developed methods for counting holomorphic curves in a systematic way, leading to the Gromov-Witten invariants, see [30, 63]. That these invariants can be effectively used for proving certain cases of the Weinstein conjecture has been shown recently in [65].

**THEOREM 6.1** *Let  $(V, \omega)$  be any compact symplectic manifold. Then the Weinstein conjecture holds for every hypersurface of contact type in  $(\mathbf{C} \times V, \omega_{\mathbf{C}} \oplus \omega)$ .*

In dimension four Gromov-Witten invariants are closely related to Seiberg-Witten theory by the important results of Taubes, see [82, 83]. These results guarantee that in a four-dimensional symplectic manifold certain two-dimensional cohomology classes can be represented by a holomorphic curve.

How one can bring all these theories nicely together has been demonstrated by Weimin Chen, [10].

**THEOREM 6.2 (WEIMIN CHEN)** *Let  $M \subset (V, \omega)$  be a compact hypersurface of contact type in a closed symplectic four-manifold with  $b_2^+(V) \geq 2$ . Let  $\lambda$  be a contact form on  $M$ , so that  $d\lambda = \omega|_M$ . Assume  $M$  carries the orientation induced by  $\lambda \wedge d\lambda$ . Then the first Chern class of the induced contact structure  $\xi = \ker(\lambda)$  equipped with a complex structure compatible with  $d\lambda$  is Poincaré dual to a finite union of periodic orbits on  $M$  oriented by  $-\lambda$ . In particular if  $c_1(\xi) \neq 0$  there has to be a periodic orbit.*

The key ingredient is a the following theorem of Taubes.

**THEOREM 6.3 (TAUBES)** *Let  $(V, \omega)$  be a closed symplectic four-manifold with  $b_2^+(V) \geq 2$  and a nontrivial canonical bundle  $K$ . Then for a generic  $\omega$ -compatible*

almost complex structure  $J$ , the Poincaré dual to  $c_1(K)$  is represented by the fundamental class of an embedded  $J$ -holomorphic curve  $\Sigma$  in  $V$  (not necessarily connected).

This result follows from the relationship between Seiberg-Witten and Gromov-Witten invariants and the nontriviality of the Seiberg-Witten invariants for closed symplectic manifolds, see [82, 83].

The proof of Theorem 6.2 has a certain number of technical ingredients. Nevertheless a proof by pictures gives an idea.

Figure 10: *Stretching of a holomorphic curve*

The compact hypersurface  $M$  sits inside  $V$  and has an open neighborhood  $[-\varepsilon, \varepsilon] \times M$  with symplectic structure  $d(e^t \lambda)$ . We take an almost complex structure  $\tilde{J}_N$  compatible with  $\omega$ , which behaves on  $[-\varepsilon, \varepsilon] \times M$  in such a way that in suitable coordinates the neighborhood looks like  $[-N, N] \times M$  equipped with  $\tilde{J}^9$ . Taubes' result guarantees for every  $N$  a holomorphic curve  $C_N$ . The additional information guarantees certain bounds on the area as well as on the genus. In the limit  $N \rightarrow \infty$  the curve converges near  $\{0\} \times M$  to some cylinders over periodic orbits.

#### ACKNOWLEDGEMENT

I would like to thank K. Wysocki and E. Zehnder for helpful discussions.

#### REFERENCES

- [1] C. Abbas and H. Hofer. Holomorphic curves and global questions in contact geometry. To appear in Birkhäuser.
- [2] V.I. Arnold. Sur une propriété topologique des applications globalement canoniques de la mécanique classique. C. R. Acad. Paris 261, 3719-3722, 1965.

---

<sup>9</sup>This is some kind of a stretching construction.

- [3] V.I. Arnold. *Mathematical methods of classical mechanics*. Graduate texts in mathematics, Vol 60, Springer.
- [4] C. Abbas. Finite energy surfaces and the chord problem. To appear in *Duke Math. J.* Vol. 96.
- [5] E. Bedford and B. Gaveau. Envelopes of holomorphy of certain 2-spheres in  $\mathbf{C}^2$ . *Amer. J. Math.* 105, no. 4, 975–1009, 1983.
- [6] D. Bennequin. Entrelacements et équations de Pfaff. *Astérisque*, 107-108:83–161, 1983.
- [7] G.D. Birkhoff. *Dynamical Systems*. Colloquium Publ. A.M.S., Vol. 9, 1927.
- [8] E. Bishop. Differentiable manifolds in complex Euclidean space. *Duke Math. J.*, 32 (1965) 1–22.
- [9] S. Bolotin. Invariant sets of Hamiltonian systems and variational methods. Proceedings of the International Congress of Mathematicians Zürich 1994, Vol. 1, 2: 1169–1178, Birkhäuser, Basel, 1995.
- [10] Weimin Chen. Pseudoholomorphic curves and the Weinstein conjecture. Preprint 1997.
- [11] K. Cieliebak. Symplectic boundaries: Creating and destroying closed characteristics. *GAF* 7, No. 2:269–322, 1997.
- [12] Yu. Chekanov. Hofer’s symplectic energy and Lagrangian intersections. Publ. Newton Inst., 8, 296–306, Cambridge Univ. Press, Cambridge, 1996.
- [13] Yu. Chekanov. Differential algebras of Legendrian links. preprint 1996.
- [14] C. Conley and E. Zehnder. Morse type index theory for flows and periodic solutions of Hamiltonian equations. *Comm. Pure Appl. Math.*, 37:207–253, 1984.
- [15] C. Conley and E. Zehnder. The Birkhoff–Lewis fixed point theorem and a conjecture of V. I. Arnold. *Invent. Math.*, 73:33–49, 1983.
- [16] S.K. Donaldson. Symplectic submanifolds and almost-complex geometry. *J. Diff. Geom.*, 44:666–705, 1996.
- [17] I. Ekeland. *Convexity methods in Hamiltonian mechanics*. Springer, 1990. *Ergebnisse der Mathematik und ihrer Grenzgebiete*, 3. Folge.
- [18] I. Ekeland and H. Hofer. Symplectic topology and Hamiltonian dynamics. *Math. Zeit.*, 200: 355–378, 1990.
- [19] I. Ekeland. Une théorie de Morse pour les systèmes hamiltoniens convexes. *Ann. Inst. Henri Poincaré, Analyse non linéaires*, 1:19–78, 1984.
- [20] Y. Eliashberg. Classification of overtwisted contact structures on three manifolds. *Inv. Math.*, pages 623–637, 1989.
- [21] Y. Eliashberg. Filling by holomorphic discs and its applications. *London Math. Society Lecture Notes*, pages 45–67, 1991. Series 151.
- [22] Y. Eliashberg. Contact 3-manifolds, twenty year since J. Martinet’s work. *Ann. Inst. Fourier*, 42:165–192, 1992.

- [23] Y. Eliashberg. Classification of contact structures on  $\mathbf{R}^3$ . *Inter. Math. Res. Notices*, 3:87–91, 1993.
- [24] Y. Eliashberg. Contact homology. Lecture at the Park City/IAS summer institute on symplectic geometry.
- [25] A. Floer. Morse theory for Lagrangian intersection theory. *J. Diff. Geom.*, 28:513–547, 1988.
- [26] A. Floer. Symplectic fixed points and holomorphic spheres. *Comm. Math. Physics*, 120:576–611, 1989.
- [27] A. Floer and H. Hofer. Symplectic Homology I: Open sets in  $\mathbf{C}^n$ . *Math. Zeit.*, 215:37–88, 1994.
- [28] A. Floer, Hofer H., and C. Viterbo. The Weinstein conjecture in  $P \times \mathbf{C}^l$ . *Math. Zeit.*, 203:355–378, 1989.
- [29] J. Franks. Geodesics on  $S^2$  and periodic points of annulus homeomorphisms. *Invent. Math.*, 108:403–418, 1992.
- [30] F. Fukaya and K. Ono. Arnold conjecture and Gromov-Witten invariants for general symplectic manifolds. preprint 1996.
- [31] V. L. Ginzburg. An embedding  $S^{2n-1} \rightarrow \mathbf{R}^{2n}$ ,  $2n-1 \geq 7$ , whose Hamiltonian flow has no periodic trajectories. *Inter. Math. Research Notices*, 2:83–97, 1995.
- [32] V. L. Ginzburg. A smooth counterexample to the Hamiltonian Seifert conjecture in  $\mathbf{R}^6$ . *Inter. Math. Research Notices*, 13:641–650, 1997.
- [33] E. Giroux. Convexité en topologie de contact. *Comm. Math. Helv.* 66:637–677, 1991.
- [34] M. Gromov. Pseudoholomorphic curves in symplectic manifolds. *Invent. Math.*, 82:307–347, 1985.
- [35] M. Gromov. Soft and hard symplectic geometry. Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986), 81–98, Amer. Math. Soc., Providence, RI, 1987.
- [36] J. Harrison.  $C^2$ -Counterexamples to the Seifert conjecture. *Topology*, 27:249–278, 1988.
- [37] M.R. Herman. Exemples de flots Hamiltoniens dont aucune perturbation en topologie  $C^\infty$  n’a d’orbites periodiques sur un ouvert de surfaces d’énergies. *Comptes-Rendus-de-l’Academie-des-Sciences. Serie-I.-Mathématique*, 312 (No. 13):989–994, 1991
- [38] M. Herman. Private communication.
- [39] M. Herman. *Examples of compact hypersurfaces in  $\mathbf{R}^{2p}$ ,  $2p \geq 6$  with no periodic orbits.* Manuscript, 1994
- [40] H. Hofer. Pseudoholomorphic curves in symplectisations with application to the Weinstein conjecture in dimension three. *Invent. Math.*, 114:515–563, 1993.
- [41] H. Hofer. Holomorphic curves and dynamics in dimension three. to appear Park City/IAS lecturer notes.

- [42] H. Hofer and M. Kriener. Holomorphic curves in contact geometry. In *Proceedings of the Conference on Differential Equations Marking the 70th Birthday of Peter Lax and Louis Nirenberg*, to appear.
- [43] H. Hofer and D. Salamon. Floer homology and Novikov rings. The Floer Memorial Volume, Progress in Mathematics, 133: 483–524, Birkhäuser, 1995.
- [44] H. Hofer and C. Viterbo. The Weinstein conjecture in cotangent bundles and related results. *Annali Sc. Norm. Sup. Pisa*, 15:411–445, 1988. Serie IV, Fasc III.
- [45] H. Hofer and C. Viterbo. The Weinstein conjecture in the presence of holomorphic spheres. *Comm. Pure Appl. Math.*, 45(5):583–622, 1992.
- [46] H. Hofer, K. Wysocki, and E. Zehnder. A characterisation of the tight three-sphere. *Duke Math. J.*, 81(1):159–226, 1995.
- [47] H. Hofer, K. Wysocki, and E. Zehnder. A characterisation of the tight three-sphere II: Generalisations. preprint.
- [48] H. Hofer, K. Wysocki, and E. Zehnder. The dynamics on three-dimensional strictly convex energy surfaces. to appear in *Annals of Mathematics*.
- [49] H. Hofer, K. Wysocki, and E. Zehnder. Properties of pseudoholomorphic curves in symplectisations III: Fredholm theory. preprint.
- [50] H. Hofer, K. Wysocki, and E. Zehnder. Properties of pseudoholomorphic curves in symplectisations I: Asymptotics. *Ann. Inst. Henri Poincaré*, 13(3):337–379, 1996.
- [51] H. Hofer, K. Wysocki, and E. Zehnder. *Properties of pseudoholomorphic curves in symplectisations IV: Asymptotics with degeneracies*, pages 78–117. Cambridge University Press, 1996.
- [52] H. Hofer, K. Wysocki, and E. Zehnder. Unknotted periodic orbits for reeb flows on the three-sphere. *Topological Methods in Nonlinear Analysis*, 7(2):219–244, 1996.
- [53] H. Hofer, K. Wysocki, and E. Zehnder. Finite energy foliations of tight three-spheres. In preparation.
- [54] H. Hofer and E. Zehnder. Periodic solutions on hypersurfaces and a result by C. Viterbo. *Inv. Math.* 90 (Fasc 1):1–9, 1987.
- [55] H. Hofer and E. Zehnder. *A new capacity for symplectic manifolds*, pages 405–428. Analysis et cetera. Academic press, 1990. Edit: P. Rabinowitz and E. Zehnder.
- [56] H. Hofer and E. Zehnder. *Symplectic invariants and Hamiltonian dynamics*. Birkhäuser, 1994.
- [57] M. Kontsevich. Enumeration of rational curves via torus actions. Preprint 1994.
- [58] P. Kronheimer and T. Mrowka. The genus of embedded surfaces in the projective plane. *Math. Res. Letters*, 1:797–808, 1994.

- [59] K. Kuperberg. A smooth counterexample to Seifert conjecture in dimension three. *Ann. of Math.*, 140:723–732, 1994.
- [60] G. Kuperberg. A volume-preserving counterexample to the Seifert conjecture. Preprint.
- [61] F. Laudenbach. Orbites périodiques et courbes pseudo-holomorphes, application à la conjecture de Weinstein en dimension 3 [d'après H. Hofer et al.]. *Séminaire Bourbaki*, 46, 1993–1994.
- [62] P. Lisca and G. Matic. Tight contact structures and Seiberg-Witten invariants. Preprint 1996.
- [63] J. Li and G. Tian. Virtual moduli cycles and GW-invariants of general symplectic manifolds. Preprint 1996.
- [64] G. Liu and G. Tian. Floer homology and the Arnold conjectures. Preprint 1996.
- [65] G. Liu and G. Tian. Weinstein conjecture and GW-invariants. Preprint 1997.
- [66] J. Mather. Existence of quasiperiodic orbits for twist homeomorphisms of the annulus. *Topology*. 21: 457–467, 1982.
- [67] D. McDuff. The local behavior of  $J$ -holomorphic curves in almost complex 4-manifolds. *J. Diff. Geom.*, 34:143–164, 1991.
- [68] D. McDuff and D. Salamon. *Introduction to symplectic topology*. Oxford University Press, 1995.
- [69] D. McDuff and D. Salamon. *J-holomorphic curves and quantum cohomology*. AMS, 1994.
- [70] M. Micallef and B. White. The structure of branch points in minimal surfaces and in pseudoholomorphic curves. *Ann. of Math.*, 141:35–85, 1994.
- [71] J. Moser. On invariant curves of area preserving mappings of the annulus. *Nachr. Akad. Wiss. Göttingen, Math. Phys.*, 1–20, 1992
- [72] J. Moser. *Stable and random motions in dynamical systems*. Princeton University Press, 1973. In: *Annals of Math. Studies*, Vol. 77.
- [73] T. Parker and J. Wolfson. Pseudoholomorphic maps and bubble trees. *Jour. Geom. Anal.*, 3:63–98, 1993.
- [74] P. Rabinowitz. Periodic solutions of Hamiltonian systems. *Comm. Pure Appl. Math.*, 31:157–184, 1978.
- [75] P. Rabinowitz. Periodic solutions of Hamiltonian systems on a prescribed energy surface. *J. Diff. Equ.*, 33:336–352, 1979.
- [76] C. Robinson. A global approximation theorem for Hamiltonian systems. *Proc. Symposium in Pure Math.*, XIV:233–244, 1970. Global Analysis, AMS.
- [77] P.A. Schweitzer. Counter examples to the Seifert conjecture and opening closed leaves of foliations. *Ann. Math.*, 100:386–400, 1974.
- [78] H. Seifert. Periodische Bewegungen mechanischer Systeme. *Math. Zeit.*, 51:197–216, 1948.

- [79] H. Seifert. Closed integral curves in 3-space and isotopic two-dimensional deformations. *Proc. Amer. Math. Soc.*, 1: 287–302, 1950.
- [80] J.-C. Sikorav. Singularities of J-holomorphic curves. Preprint, 1995.
- [81] M. Struwe. Existence of periodic solutions of Hamiltonian systems on almost every energy surface. . *Bol. Soc. Bras. Mat.*, 20:49-58, 1990.
- [82] C.H. Taubes. From Seiberg-Witten equations to pseudoholomorphic curves, in SW=Gr: The equivalence of the Seiberg-Witten and Gromov Invariants. to appear International Press.
- [83] C.H. Taubes. SW= $\Rightarrow$  Gr:From Seiberg-Witten equations to pseudoholomorphic curves. *J. Amer. Math. Soc.*, 9:845–918, 1996.
- [84] C. Viterbo. A proof of the Weinstein conjecture in  $\mathbf{R}^{2n}$ . *Ann. Inst. H. Poincaré, Anal. non linéaire*, 4:337–357, 1987.
- [85] A. Weinstein. Periodic orbits for convex Hamiltonian systems. *Ann. Math.*, 108:507–518, 1978.
- [86] A. Weinstein. On the hypothesis of Rabinowitz’s periodic orbit theorems. *J. Diff. Equ.*, 33:353–358, 1979.
- [87] F. W. Wilson. On the minimal sets of non-singular vector fields. *Ann. of Math.* 84:529–536, 1966.
- [88] J. Wolfson. Gromov’s compactness of pseudo-holomorphic curves and symplectic geometry. *J. Diff. Geom.*, 28:683–405, 1988.
- [89] R. Ye. Gromov’s compactness theorem for pseudoholomorphic curves, 1994.
- [90] E. Zehnder Homoclinic orbits near elliptic fixed points. *Comm. Pure Appl. Math.* 26: 131–182, 1973.

Helmut Hofer  
Courant Institute  
New York University  
251 Mercer Street  
New York, NY 10012  
USA  
email: hofer@cims.nyu.edu  
web: www.math.nyu.edu/research/hofer

## GEOMETRIC MODEL THEORY

EHUD HRUSHOVSKI

1991 Mathematics Subject Classification: 03C45, 03C60

Keywords and Phrases: Model theory, stability theory, difference algebra, differential algebra, quasi-finite, pseudo-finite, Manin-Mumford, Mordell-Lang

“Contemporary symbolic logic can produce useful tools – though by no means omnipotent ones – for the development of actual mathematics, more particularly for the development of algebra, and it would appear, of algebraic geometry.” This statement (with a reference to still older roots) was made by Abraham Robinson in his 1950 address to the ICM. Instances of such uses of logic include the correction and proof by Ax-Kochen of a  $p$ -adic conjecture of Artin’s ([1]), and the Denef - Van den Dries proof of a  $p$ -adic analytic conjecture of Serre ([13]). The internal development of model theory since the 70’s has led to entirely new techniques, that, combined with the older ones, have begun to find applications to diophantine geometry. It is the purpose of this talk to explain these methods and connections.

The present applications use only the finite-dimensional part of model theory (in a sense to be explained). Shelah and his followers created a theory of much greater generality (superstability, supersimplicity) incorporating many of the features of the finite dimensional case. One hopes that future applications will use this power. This exposition will limit itself to the finite-dimensional heartland (finite Morley rank, S1-rank).

Instead of defining the abstract context for the theory, I will present some of its results in a number of special, and hopefully more familiar, guises: compact complex manifolds, ordinary differential equations, difference equations, highly homogeneous finite structures. Each of these has features of its own, and the transcription of the general results is not routine; they are nonetheless readily recognizable as instances of a single theory. The current applications to diophantine geometry arise by way of the difference and differential “examples”. §2 and §6 will describe the model theory behind these results, and the prospects and difficulties lying ahead.

### 1 EXAMPLE 1: COMPACT ANALYTIC SPACES

A complex manifold is a space obtained by gluing open discs in  $\mathbb{C}^n$ , using complex analytic gluing maps. A *closed analytic subset* of a complex manifold  $M$  is a closed subset, cut out locally by the vanishing of finitely many analytic functions. This defines a topology on  $M$ . An *analytic subvariety* is an irreducible closed analytic



set, i.e. one that is not the union of closed proper subsets. Every closed subset in this topology has dimension strictly less than  $\dim(M)$ , and is the union of finitely many analytic subvarieties. By a (complex analytic) *space* we will mean, in this section, the complement of a closed analytic  $U'$  in a closed analytic subvariety  $V$  of a compact complex manifold. ( Let  $\mathcal{C}$  denote the class of such spaces.) We do not however wish to remember the *construction* of  $V$ , nor the sheaf of analytic functions or even the topology on  $V$ . Instead we are interested in describing the family  $\mathcal{Z}(V)$ ,  $\mathcal{Z}(V^n)$  of analytic subvarieties of  $M$  and of its Cartesian powers; and the interaction of  $V$  with other spaces  $W$  by means of  $\mathcal{Z}(V \times W)$ .

We would like to map out the category of analytic spaces  $X$ , with a view to the internal geometry of the subvarieties of  $X$  and of  $X \times Z$  for other  $Z$ . We will find that this category is not at all homogeneous: some spaces have a very rich internal geometry, others a very poor one; some interact with each other, some do not. The different features can be well differentiated by a close look at products of *minimal* varieties  $X$ , those that have no proper infinite subvarieties. This is the case though it is very far from being true that every variety can be decomposed as such a product.

Among the minimal varieties, we will find very sharp dividing lines. The *algebraic curves* lie in a class of their own. The non-algebraic complex tori fall into another distinct class; their geometry is essentially *linear*. The third class, about which model theory says least, consists of the minimal varieties whose geometry is trivial (at least generically) from our “subvarieties of Cartesian powers” point of view. These three classes exemplify a deep and general trichotomy, and in the present category has decisive influence on the geometry of all varieties (not just on products of minimal ones.)

**ALGEBRAIC VARIETIES** Among the analytic spaces are those with the structure of algebraic varieties. These have a very rich geometry of subvarieties. In particular, in dimension  $> 1$ , they have algebraic *families* of subvarieties, having arbitrarily large dimension.

A general model theoretic principle, to be discussed later, shows that this richness *characterizes* algebraic varieties.

The complex projective space  $\mathbb{P}^n$ , for example, contains the family  $\mathcal{F}_d$  of hypersurfaces cut out by homogeneous polynomials of degree  $d$  in  $n + 1$  variables; this family is parameterized by  $\binom{n+d}{d-1}$ -dimensional projective space.

Intersecting the elements of  $\mathcal{F}_d$  with a projective variety - a subvariety  $V$  of  $\mathbb{P}^n$  - yields large families of subvarieties on  $V$ . We thus see in passing that any projective variety is “rich” ( $V$  or  $V^2$  have many subvarieties.) By the model theoretic characterization alluded to above, it follows that projective varieties are algebraic. This indeed fits in with a classical theorem of Chow’s, asserting in more detail that projective varieties are automatically defined by finitely many homogeneous polynomials.

**1.1 MINIMAL SPACES AND THE SEMI-MINIMAL ANALYSIS**  $M$  is called *minimal* if it has no proper analytic subvarieties, other than points.

Every one-dimensional (connected) complex manifold is minimal, but there are also many others. For example, if  $\Lambda$  is the subgroup of  $\mathbb{C}^n$  generated by a sufficiently general  $\mathbb{R}$ -basis, the *torus*  $T = \mathbb{C}^n / \Lambda$  is minimal.

Given a minimal  $M$ , a subgroup  $G$  of  $Sym(n)$ , one can form the space  $M^n/G$ . Such spaces, as well as subspaces of their finite products, will be called *semi-minimal*. We will later (1.6) obtain a good description of semi-minimal spaces (in terms of minimal ones.)

The following theorem is an instance of Shelah's theory of "regular types" (adapted to minimal types using a contribution of Lascar's.)

**THEOREM 1.1** *Let  $V \in \mathcal{C}$ . There exists a minimal space  $Y \in \mathcal{C}$  and a  $F \in \mathcal{Z}(V \times Y)$ , inducing a morphism from the complement of an analytic subset  $V'$  in  $V$ , onto a subspace of  $Y^{[k]}$ .*

The theorem provides a proper closed subvariety  $V_0$  of  $V$ , and a map  $f : (V \setminus V_0) \rightarrow L_1$  with  $L_1$  semi-minimal. ( $f$  is defined by:  $f(a) = \{b : (a, b) \in F\}$ .) Once  $f$  is found, the theorem can be re-applied to  $V_0$  and to each fiber of  $f$ . This process, "the semi-minimal analysis", terminates after a finite number of steps.

**REMARK 1.1** *There is a largest semi-minimal image  $V_{sm}$  of  $V$  (in the sense of 1.1); it is unique at least up to "birational isomorphism" (or even a constructible bijection).*

**1.2 ORTHOGONALITY** Let  $X, Y$  be a variety. We say that  $X$  *dominates*  $Y$  if there exists a subvariety  $Z$  of  $X \times Y$ , such that the projection of  $Z$  to  $X$  has finite fibers, while the projection to  $Y$  is surjective (or it may miss a proper closed subset.) For algebraic varieties,  $X$  dominates  $Y$  iff  $\dim(X) \geq \dim(Y)$ . However this is far from being true in general.

Two varieties  $X, Y$  are called *orthogonal* if every proper subvariety  $T \subset X^m \times Y^n$  is contained in  $U \times Y^n$  or in  $X^m \times V$  for some closed analytic  $U, V$  of smaller dimension. When  $X, Y$  are minimal, this implies that every closed subvariety of  $X^m \times Y^n$  is a rectangle  $U \times V$ .

**THEOREM 1.2** [*Shelah*]

1. *For minimal  $X, Y$ ,  $X$  dominates  $Y$  iff they are not orthogonal. Domination is an equivalence relation on minimal spaces.*
2. *Each  $X$  dominates a finite number of minimal  $Y$  (up to domination equivalence.) For each such  $Y$ , there exists a maximal integer  $m$  such that  $X$  dominates  $Y^m$ .*
3. *Two varieties are not orthogonal iff they dominate a common minimal.*

1.3 NON-ORTHOGONALITY AND LIAISON GROUPS If a minimal, occurring beyond the first level of the semi-minimal analysis is non-orthogonal to an earlier one, their interaction must be mediated by a group action. For example:

**THEOREM 1.3** *Let  $X$  be a space,  $f : X \rightarrow X_{sm}$  the maximal semi-minimal quotient, and  $a \in X_{sm}$ ,  $X(a) = f^{-1}(a)$ , and let  $g : X(a) \rightarrow X(a)_{sm}$  be the semi-minimal quotient of  $X(a)$ . If  $X(a)_{sm}$  is an algebraic variety, it is a homogeneous space for an algebraic group.*

1.4 DIMENSIONS Each compact complex manifold has a complex analytic dimension, the number of complex parameters needed locally to determine a point. A more intrinsic dimension from our point of view assigns each minimal space dimension 1. More generally, we say inductively that  $X$  has (Morley) dimension  $d + 1$  if it does not have dimension  $\leq d$ , and contains an infinite collection of subvarieties  $X_i$  of dimension  $d$ , with  $\dim(X_i \cap X_j) < d$  for  $i \neq j$ .

It can be shown that for minimal  $X$ , for any  $Y \subset X^n$ ,  $\dim_{Morley}(Y) = e \dim_{\mathbb{C}}(Y)$  where  $e = \dim_{\mathbb{C}}(X)$  does not depend on  $Y$ . (This resembles the relation between complex and real dimension, with  $e = 2$ .) When working systematically with the geometry of  $X^n$  and its subvarieties, the intrinsic dimension is helpful even if one is already aware of the complex analytic dimension. For instance, subspace of dimension one are treated as *curves*; it is useful to know in advance that the intersection of two such curves must be finite (as does not follow directly from the analytic dimension.)

### 1.5 CLASSIFICATION OF MINIMAL SPACES: AMPLENESS VS. MODULARITY

FAMILIES OF VARIETIES Given  $X \in \mathcal{Z}(M \times P)$ , and  $a \in P$ , let

$$X(a) = \{b \in M : (b, a) \in X\}$$

Then  $X(a) \in \mathcal{Z}(M)$ . As  $a$  varies through  $P$ , (or perhaps through the complement in  $P$  of a proper closed analytic subvariety), we will say that the varieties  $X(a)$  form a uniform family of subvarieties of  $M$ . Without changing the family of sets  $X(a)$ , it is possible to replace  $X$  and  $P$  in such a way that the sets  $X(a)$  are distinct for distinct elements  $a \in P$ . The *dimension* of the family is then  $\dim(P)$ .

A space is called *geometrically modular* if, for each  $k$ , there exists an absolute bound to the dimension of any uniform family of subvarieties of  $V^k$ . The significance of this condition will be explained later; for now we view it as an expression of a sharp difference between algebraic curves and the other minimal varieties. For minimal  $V$ , it can be shown that the bound is  $k - l$ , where  $l = \dim(X(a))$ .

The terms “locally modular” and “1-based” are also used in the literature. The first refers to a condition on the lattice of algebraically closed subsets, that we will not enter into here. The latter refers to the following:

**DEFINITION 1.2** *A space  $V$  is 1-based if for any  $k$ , through a sufficiently general point  $a \in V^k$ , there pass only countably many subvarieties of  $V^k$ .*

Equivalently, no uniformly definable family of subvarieties intersects in that point. A dimension - counting argument shows that geometric modularity is equivalent to 1-basedness.

EXAMPLE: NON-ALGEBRAIC TORI Some complex tori can be embedded in projective space; the embedding is then an algebraic subvariety of projective space (defined by the vanishing of finitely many homogeneous polynomials.) These are called Abelian varieties, and have a rich structure of subvarieties; they are not geometrically modular. We will see later however that any minimal complex torus that is not an Abelian variety is geometrically modular. For a sufficiently general torus, the subvarieties of  $T^n$  passing through a point  $a = (a_1, \dots, a_n)$  are not only countable in number but completely explicit: they are defined by equations of the form  $\sum n_i(x_i - a_i) = 0$ .

THEOREM 1.4 *Let  $V \in \mathcal{C}$  be minimal, and not algebraic. Then  $V$  is geometrically modular.*

1.6 CLASSIFICATION OF MINIMAL SPACES: GEOMETRIC TRIVIALITY If  $V$  is a geometrically modular minimal space, through a typical point of  $V^k$  there pass at most countably many curves. There are always at least  $k$  curves through  $a = (a_1, \dots, a_k)$ , namely those “parallel to the axes”:  $(a_1, \dots, a_{k-1}) \times V, \dots, (a_1) \times V \times (a_3, \dots, a_k), V \times (a_2, \dots, a_k)$ .

Call  $V$  *geometrically trivial* if for every  $a \in V^k$ , (except perhaps for a finite union of proper subvarieties), these  $k$  curves are the only ones passing through  $a$ . (This condition implies equally strong constraints on subvarieties of higher dimension passing through a general point.)

A complex torus  $T$  can never be geometrically trivial. For example, for each rational  $\frac{a}{b}$  ( $(a, b) = 1$ ) and any point  $c = (c_1, c_2) \in T^2$ , one has the subvariety

$$\{(y_1, y_2) : ay_1 + by_2 = ac_1 + bc_2\}$$

passing through  $c$ .

It can be shown more generally that a subvariety of a group variety can never be geometrically trivial.

THEOREM 1.5 ([15]) *Let  $V$  be minimal, modular, and not geometrically trivial. Then there exists a minimal  $U$  equivalent to  $V$  and admitting a group structure, whose graph is a subvariety of  $U^3$ .*

Putting together Theorems 1.4, 1.5, we obtain

COROLLARY 1.3 (TRICHOTOMY) *Every minimal variety  $X$  is geometrically trivial, or equivalent to a geometrically modular group variety, or is algebraic.*

It can be shown, from modularity, that a geometrically modular group variety  $U$  must be commutative ([19]). It is very likely that  $U$  must be a complex torus; this requires proof, and provides an example of the kind of work needed to adapt the general theory to a special context.

## 1.7 INTERNAL STRUCTURE OF SEMI-MINIMAL SETS

THEOREM 1.6 *Let  $X$  be a minimal variety. Let  $Y$  be a subvariety of  $X^n$ .*

1. *If  $X$  is algebraic, then  $Y$  is algebraic.*
2. *If  $X$  is a geometrically modular group, then  $Y$  is defined by linear equations  $\sum a_{ij}X_i = b_j$ , with respect to the group structure, and certain analytic endomorphisms  $a_{ij}$ .*
3. *If  $X$  is geometrically trivial, then  $Y$  is a direct product of minimal varieties  $Y_j$*

Item (1) (with  $X = \mathbb{P}^1$  or  $\mathbb{P}^n$ ) is a classical theorem of Chow's. In model theoretic language, the *induced structure* on the complex analytic  $X$  is precisely that given by *algebraic* geometry. Here the result is derived from a general model-theoretic *recognition theorem* for algebraic geometry, ([23]). Having recognized algebraic geometry, the model theory hands the variety over to methods best suited to it.

Item (2) (taken from [19]) shows that the induced structure on complex tori is given by *linear algebra* (over the endomorphism ring.) The linearity is relative to the group structure; it is not comparable within the category we work in to the additive group of  $\mathbb{C}$ .

In (3), each  $Y_j$  is a subvariety of  $X^{l(j)}$ , a certain product of  $l(j)$  of the  $n$  factors of  $X^n$ . The statement is a fairly direct consequence of the definition of geometric triviality. Note that (3) gives no information in the case  $\dim(Y) = 1$ . In this respect the information concerning geometrically trivial varieties is less decisive than in the other cases.

COROLLARY 1.4 (TO (3) ) *Let  $A$  be a geometrically modular group variety, minimal as a group variety. Then  $A$  is a minimal variety.*

Thus if a non-algebraic torus has no proper nontrivial sub-tori ( a condition easily verified), then it has no proper analytic subvarieties of any kind (other than points.)

Combining Theorem 1.6 with the theory of orthogonality, we see that a subvariety of a product of geometrically modular group varieties, geometrically trivial varieties, and algebraic varieties, is itself a product of the same form. Any semi-minimal variety is domination-equivalent to such a product.

1.8 LOCAL-GLOBAL PRINCIPLES The above theory of minimal and semi-minimal varieties is useful to the extent that global properties of arbitrary varieties can be reduced to properties of their minimal components. This happens often; we give just one example here.

THEOREM 1.7 ([5]) *Let  $V \in \mathcal{C}$ , and assume every minimal variety occurring in the semi-minimal decomposition of  $V$  is geometrically modular. Then so is  $V$ .*

In view of 1.4, this expresses the idea that  $\mathcal{Z}(V)$  can be “large” *only* as an effect of algebraic varieties within  $V$ . As a corollary, one can globalize also 1.4(2):

**THEOREM 1.8** *Let  $X$  be a complex torus. Assume  $X$  has a maximal chain  $(0) = V_0 \subset V_1 \subset \dots \subset V_n = X$  of sub-tori, and no quotient  $V_{i+1}/V_i$  is an Abelian variety. Then the conclusion of 1.6 (3) holds for  $X$ .*

Sometimes just one layer in the semi-minimal analysis controls the situation. Shelah’s Theorem 1.2 (3) is an example of this, using the first layer alone. Here is an example where only the *last* layer matters. It is a local-global principle for the notion of geometric triviality.

**THEOREM 1.9** *Let  $g : X \rightarrow Y$  be the last stage of the canonical semi-minimal analysis. Assume the minimal varieties associated with the semi-minimal fibers  $X_b$  ( $b \in Y$ ) are all geometrically trivial, of dimension  $\leq n$  say. Then through any  $a \in X^m$  (outside some proper subvariety) there pass at most  $mn$  distinct curves (one dimensional spaces.)*

## 2 MODEL THEORETIC INPUTS: FINITE MORLEY RANK THEORY

The theory described in the last section was in reality developed in a more general context. We stated it for compact complex manifolds essentially as a device of exposition, hoping to illuminate the general theory without plunging immediately into abstraction. We will now make some comments on the model theoretic setting.

**2.1 QUANTIFIER ELIMINATION** A *first-order structure* in the sense of model theory has many “universes”, called *sorts*. The sorts are assumed to be closed under finite Cartesian products; if a structure with a single universe  $M$  is presented, the other sorts will be the Cartesian powers  $M^n$ ; it is there that the model theory will take place. One is given a family of subsets of the various sorts, the *basic relations*. One considers not only the given subsets, but also others formed from them using the “first-order operations”: pullbacks and pushforwards under projections and diagonal maps, finite unions and intersections, and complements. *Any hope for a useful model theory depends on some control over the outcome of the first-order operations.* The strongest form of this control is:

*Quantifier-elimination:* Every projection of a Boolean combination of basic relations, is itself a basic relation.

(cf.[7]). This must be achieved separately in each application, and is rarely trivial.

In the example presented in §1, the sorts are the complex manifolds; the basic relations are the complex analytic subvarieties. Quantifier elimination was proved by Boris Zil’ber; the main ingredient is the theorem (Remmert, Grauert) that images of analytic subvarieties under proper maps are analytic.

Zil’ber also proved that the structure consisting of compact complex manifolds satisfies the appropriate axioms of dimension theory, so that the general results on structures of finite Morley rank, and on Zariski geometries [23], apply.

2.2 STRUCTURES WITH DIMENSION §1 is a simple transcription of a part of the theory of structures of finite Morley dimension. These are first order structures, with a non-negative integer-valued function on the definable sets, satisfying the condition in §1.3. The same dimension theory will work for differential algebra. For our difference and quasi-finite examples, we will use a modification, S1-dimension, defined in the same way but with  $X_i = X(a_i)$  assumed to be taken from a uniform family.

The theory of semi-minimal reduction, and the theory of orthogonality, are due to Shelah ([37]). They are instances of his much more general theory of regular types in superstable theories. A part of the theory, in the finite dimensional case, appeared in the work of Morley and of Baldwin-Lachlan on categoricity. The books [34], [4],[35] are general references for this section, and contain further references.

*Modularity* is the most important concept of geometric model theory. It appeared first in work of Lachlan's [28] on the  $\aleph_0$ -categorical theories, and of Zilber's in the  $\aleph_1$ -categorical and totally categorical theories ([40]). There are many equivalent definitions of modularity; Lachlan's original definition involved the absence of *pseudo-planes*, structures modeled roughly on plane geometry. The idea is the existence of a sharp dividing line between the combinatorial and linear worlds (modularity), and between nonlinear, geometric complexity, as found in algebraic geometry. This was successfully generalized from the categorical cases to the superstable and general stable frameworks, and beyond that (perhaps not yet in full) to simple theories. It is clear that the idea continues to be meaningful and important in much wider domains, not yet technically developed.

Theorem 1.4 follows from the main theorem of [23]. It states that structures with a dimension theory having the basic properties of the dimension theory of algebraic varieties, and with *large* uniform families of subvarieties, must arise from algebraic geometry. It is not assumed there that the structure arises from analytic geometry or from any other specific geometry. The "basic properties" are here understood to include the "dimension theorem": intersection with a codimension - one variety lowers dimension by at most one, in every component. This is the only general result used in §1 that requires assumptions beyond that of finite Morley rank. This was originally conceived as a foundational result, showing that algebraic geometry is *sui generis*.

The proof of [23] involves geometric constructions in powers  $X^n$ , using the intrinsic dimension. One-dimensional sets are viewed as curves, and one constructs tangent spaces to them synthetically. (Note that this is applied, in §1, to complex analytic spaces, where Morley dimension one translates to higher complex dimension!)

The analogous theorem is now known ([33]) for structures with a dimension theory analogous to that of the reals (called "O-minimal" to recall the ordering; cf. [38].) A similar result may well be true for much more general types of geometries, including in particular  $p$ -adic geometries, and it would be valuable to develop it. The rest of the theory in §1 has not been developed even for the O-minimal context (where "semi-minimality" is in effect built into the assumptions.)

## 3 DIFFERENTIAL EQUATIONS

(General reference: [31]) A theory fully parallel to that of §1 exists for algebraic ordinary differential equations. The most interesting difference is the identification of the nontrivial, geometrically modular objects; the non-algebraic tori of §1 are replaced with certain equations, discovered by Manin and deeply studied by Buium, associated to any algebraic family of Abelian varieties. It is at first surprising that such a preliminary model-theoretic investigation of the basic geography of algebraic differential equations should discover Abelian varieties in a special role.

The results apply more generally to systems of (nonlinear) algebraic partial differential equations whose set of solutions is finite-dimensional in an appropriate sense. (In classical language, “the general solution involves only finitely many arbitrary constants”.) Technically, we fix a field  $k$ , and let  $k\{X\}$  be the ring of differential polynomials over  $k$  in variables  $X = (X_1, \dots, X_m)$ . We use ODE’s or PDE’s; in positive characteristic, we use Hasse-Witt derivatives. We assume the equations generate a differential ideal  $J$  such that for every prime  $p \supset J$ ,  $k\{X\}/p$  has finite transcendence degree over  $k$ . This condition is automatic for a nontrivial ODE in one variable. In characteristic  $p > 0$ , on the other hand, infinitely many equations are required.

An important open problem is the extension of the theory to less constrained systems of PDE’s; Shelah’s theory of superstability is available, but not the required generalization of the trichotomy theorem [23] (analog of 1.6(1)).

The necessary *quantifier elimination* was achieved by A. Robinson in characteristic 0, Delon, Ershov, Wood in positive characteristic; (cf. [12]). Certain verifications concerning the dimension theory, and the identification of the geometrically nontrivial minimal modular sets, are from [20]. (The approach we take here will make both of these essentially immediate, for finite dimensional systems.)

It is here that applications to diophantine geometry first arose, using a connection discovered by Buium, [6]. The model theory handles all characteristics with equal ease. It provides the only known proof of the Mordell-Lang conjecture in characteristic  $p > 0$ ; cf. [17], [18] [2]. We will not go into details here, but will discuss a related result in §4.

There are several possible ways to describe the first order structure associated with such differential equations.

1) The standard model theoretic approach defines a *universal domains* for differential algebra. These are differential fields, in which every consistent, countable set of differential equations has a solution. The *sorts* can be taken to be the solution sets in this universal domain, to given equations; the basic relations, called Kolchin-closed sets, are defined by further equations.

2) One can define the category using the differential equations themselves, disregarding the sets of solutions.

3) The variant we will use will be a purely geometric representation of the differential equations. (It uses points again, but these are related to the points of the sorts of (1) only indirectly, via (2)). We will restrict attention to characteristic 0, and to ODE’s, and work over an algebraically closed base field  $k$  with a trivial derivation.



The sorts will be smooth algebraic varieties endowed with algebraic vector fields; i.e. of pairs  $(V, s)$  where  $V$  is a smooth variety over  $k$ , and  $s : V \rightarrow TV$  is a section of the tangent bundle. The product of two sorts  $(V, s)$  and  $(V', s')$  is naturally defined. The basic relations are now the integral subvarieties, i.e. the algebraic subvarieties  $U$  of  $V$  such that  $s$  restricts to a section of  $TU$ . (Formally or analytically, we can define a flow corresponding to  $s$ ; the integral subvarieties are then those fixed by the flow, and it is not surprising that their Boolean combinations are closed under projections.)

We will be interested in algebraic families  $\{U\}$  of algebraic subvarieties  $V$ , that are left invariant by the flow corresponding to  $s$ . Such a family can be obtained by first taking the product of  $(V, s)$  with another object  $(P, t)$ , fixing an integral subvariety  $R$  of  $(V \times P, (s, t))$ , and then letting

$$\{U\} = \{R(p) : p \in P\}$$

with

$$R(p) = \{a \in V : (a, p) \in R\}$$

Any element of an invariant family will be called  $s$ -coherent.  $\mathcal{Z}(V)$  is the set of  $s$ -coherent subvarieties of  $V$ . Thus every point is  $s$ -coherent, as well as every integral subvariety of  $s$ . We will refer to these as differential-algebraic varieties.

As in §1, we are interested in criteria for the abundance or scarcity of subvarieties of a given flow; the geometry of such subvarieties; and of the reducibility of one vector field to another by algebraic or algebraic differential transformations. The theory of §1 has a perfect analog here. Here,  $\underline{V}$  is *minimal* iff  $V$  has no  $s$ -coherent subvarieties, except for points and all of  $V$ .

In particular, the trichotomy is true in this context. We must however identify the analogs of algebraic varieties, and the geometrically modular groups.

If the vector field is trivial,  $s = 0$ , every subvariety is an integral subvariety, and the geometry on  $V$  is ordinary algebraic geometry. It can be shown conversely (Ph.D. theses of Mesmer, Sokolovic; cf. [2]) that a minimal set, abstractly bi-interpretable with an algebraically closed field, must be isomorphic to a curve  $C$  endowed with the zero vector field. Let us call such minimal differential varieties *algebraic*. The corresponding semi-minimal sets are closely connected to the algebraically integrable flows. Part of the theory will thus take the form, in the present context, of recognition results for algebraically integrable vector fields.

The analog of non-algebraic complex tori is interesting. We are looking for the minimal coherent sets, possessing a group structure, and satisfying the conclusion of 1.4. The right equations were discovered by Manin, [30], and by Buium in a role closer to their status here. (A quick description, essentially following Buium: Let  $A \rightarrow U$  be a family of Abelian varieties. For  $v \in U$ , let  $M_v$  be the maximal extension of  $A_v$  by a vector group. We have  $M \rightarrow A \rightarrow U$ , and now any vector field  $t$  on  $V$  canonically lifts to a vector field  $s$  on  $M$ : we have  $TM \rightarrow TV$ ; the group structure on  $M_v$  can be prolonged to one on  $N_v = (TM)_{(v, t(v))}$ , so that  $N_v$  becomes an extension of  $M_v$  by the vector group  $TM_v$ ; since  $M_v$  is the universal vector extension of  $A$ , there exists a unique section of  $N_v \rightarrow M_v$ . This gives  $s$ .)

**THEOREM 3.1** *There is a 1-1 correspondence between non-isotrivial families of Abelian varieties over  $k$ , up to isogeny, and families of geometrically modular minimal differential varieties. up to equivalence*

“Non-isotrivial” means essentially that the different Abelian varieties in the family are not isomorphic to each other. The equivalence of minimal sets is that of non-orthogonality, §1.2. This recognition theorem ([20]) allows us to state the trichotomy of [23] thus:

**THEOREM 3.2** *Every minimal differential algebraic variety is either geometrically trivial, algebraic, or equivalent to a Manin-Buium variety*

We also obtain a theorem on the internal structure of Manin-Buium varieties similar to 1.6, in particular 1.6 (3). This result was reproved by Buium and Pillay by analytic methods. The trichotomy has no analytic proof at present.

**GEOMETRICALLY TRIVIAL EQUATIONS** Geometric triviality severely limits the possible complexity of the internal geometry on a minimal differential variety  $V$ , but leaves open the question of its precise structure. For ODE’s of differential order one, we have a complete answer. It is essentially the simplest possible one, of no structure at all. A differential variety  $V$  has *trivial internal structure* if the only subvarieties of  $V^m$  are the coordinate subvarieties  $V^l$  (defined by equations  $X_i = a_i$ .) Equations defining such varieties can have only a finite number of algebraic solutions; indeed over a differential field of transcendence degree  $k$ , they can have at most  $k$  solutions. Conversely the condition of finitely many algebraic solutions over a finitely generated field, characterizes geometrically trivial equations, up to equivalence.

**THEOREM 3.3** • *Let  $X$  be a geometrically trivial ODE of order 1. There exists a finite map  $g : X \rightarrow Y$ ,  $Y$  another ODE of order 1, such that  $Y$  has trivial internal structure.*

- $X = \{X_a : a \in T\}$  be a family of geometrically trivial ODE’s of order 1, and assume the generic  $X_a$  is geometrically trivial. Then there exist differential rational maps  $b : T \rightarrow T'$ , another family  $Y$  of order 1 ODE’S, AND  $g : X \rightarrow Y$ , such that (for generic  $a$ , with  $b = b(a)$ )  $X_a$  is equivalent to  $Y_b$ ,  $Y_b$  is trivial, and such that  $Y_b, Y_{b'}$  are equivalent only if  $b = b'$ .

This kind of control over the internal structure and the variation of arbitrary *minimal* ODE’s would make for a much more powerful theory (about arbitrary algebraic ODE’s).

(1) is proved ([26]) by a slight modification of [25], while (2) is proved by a combination of model-theoretic and geometric methods (see [22] for the case of positive genus.) Further results would presumably be proved geometrically, perhaps by extensions of the method of [25]; the model theory may be helpful in suggesting the correct higher dimensional version (the Manin-Buium equations must be taken into account.)

We note that Jouanolou's theorem [25] was used directly by Vojta, to bound the number of rational points on curves over function fields. The model theoretic method uses Buium-Manin equations for similar results applying to subvarieties of Abelian varieties. These results use only one part of the trichotomy, the gap between geometrically modular and algebraic. This state of affairs suggests that the gap between geometrically trivial minimal varieties, and between geometrically modular groups (1.5, here 3.2) may be used for results on rational points on varieties of general type. A higher-dimensional version of 3.3 would be one of the missing ingredients for such an attempt.

Here is a statement of the trichotomy that does not mention minimality. The proof combines the trichotomy and the analogs of 1.9 and 1.3. (The statement of this theorem in the abstract contained an inaccurate mixture of the languages of approaches (2) and (3).)

**THEOREM 3.4** *Assume  $\underline{V} = (V, s)$  is not geometrically trivial. After possibly removing from  $V$  a finite number of lower dimensional integral subvarieties, and possibly pushing forward by an  $s$  - equivariant map with finite fibers, one of the following occurs:*

- a. *There exists a map  $f : V \rightarrow W$ ,  $W$  an algebraic variety of dimension  $\geq 1$ , such that the vector field  $s$  is parallel to the fibers of  $f$ .*
- b. *There exists an equivariant map  $f : V \rightarrow V'$ ,  $V'$  an algebraic variety of smaller dimension carrying a vector field  $s'$ , such that the fibers of  $f$  are principal homogeneous spaces for algebraic groups; and the action respects the vector field.*
- c. *There exists a map  $f : V \rightarrow V'$  as in (3) such that  $s$  is the pullback over  $V'$  of a Buium-Manin family.*

#### 4 DIFFERENCE EQUATIONS

A *difference equation* is analogous to a differential equation, but involves a discrete difference operator  $\sigma$  in place of a differential operator. Classically one thinks of the field of rational or meromorphic functions, and defines  $f^\sigma(z) = f(z + 1)$ , or  $f^\sigma(z) = f(qz)$ . The Leibnitz rule is replaced by the fact that  $\sigma$  is an automorphism :  $\sigma(fg) = \sigma(f)\sigma(g)$ . Thus a *difference domain* is defined to be an integral domain with a distinguished field endomorphism. (See [11]).

There are also arithmetic sources of difference equations: the Galois group of  $\mathbb{Q}$ , and the Frobenius endomorphisms  $x \mapsto x^{p^m}$  in characteristic  $p > 0$ . The latter play a fundamental role among all difference domains; for instance it can be shown that a simple, finitely generated difference domain  $(L, \sigma)$  always has  $\sigma(x) = x^{p^m}$  for some  $p$  and  $m$ . We will not enter here into this story.

The theory described in §1, §2 is available in full, though a great deal more work is needed to access the model theoretic inputs or reprove them in suitable form ([8]). In particular a semi-minimal analysis and a trichotomy theorem exist. Here we will just highlight two of the places where the theory complements rather than merely parallels the differential case.

4.1 FIXED FIELDS It can be shown that the equation  $x^\sigma = x$ , defining the fixed field, is one-dimensional for an appropriate dimension theory; it is an analog of the minimal varieties encountered before. It corresponds to  $Dx = 0$  in the differential case and in characteristic 0, it is the only non-geometrically modular minimal difference variety. (In characteristic  $p > 0$ , one must add equations such as  $x^{\sigma^2} = x^p$ .) The situation is more interesting however in that the fixed field is not algebraically closed, even in a universal domain for difference fields.

For example, in the differential case, it can be shown either by means of differential Lie theory (Phyllis Cassidy) or of model theory (Sokolovic) that every *simple group* defined by differential equations, and finite-dimensional in our sense, is isomorphic to an algebraic group over the field of constants. In the difference case, twisted groups arise. Let  $G$  be a simple algebraic group, and let  $h : G \rightarrow G$  be a graph isomorphism of  $G$ . Then one can use difference equations to define a subgroup of  $G$ :

$$G(h; \sigma) = \{a \in G : h(a) = \sigma(a)\}$$

For instance, if  $G = GL_n$ , and  $h(M) = M^{t-1}$  for a matrix  $M$ , then  $G(h; \sigma)$  is the unitary group  $U_n$  over the fixed field of  $\sigma^2$ , with respect to the conjugation  $\sigma$  of that field.

While the classification up to isomorphism is possible, we will only discuss the classification up to virtual isogeny ( $G_1, G_2$  are virtually isogenous if there exists  $G$  and homomorphisms  $h_i : G \rightarrow G_i$  with finite kernel, and image of finite index.) It can be shown that  $G(h; \sigma)$  defines (in the universal domain) a group virtually isogenous to a simple one.

**THEOREM 4.1** *A simple group definable by difference equations is virtually isogenous to some  $G(h; \sigma)$*

This gives a connection to finite simple groups, more precisely to “horizontal” families of finite simple groups (e.g.  $PSL(n, q)$  with fixed  $n$  and varying  $q$ .) One obtains an infinite family of (almost) simple groups from  $G(h; \sigma)$  by letting  $G(h, q)$  be the solutions to  $G(h; \sigma)$  in the “Frobenius difference field”, the difference field consisting of an algebraically closed field of characteristic  $p > 0$ , and the automorphism  $\sigma(x) = x^q$ . All the families occur (including the Ree and Suzuki groups) making the statement of the classification very natural in this context. See [HP 94], [21]

4.2 GEOMETRICALLY MODULAR, NONTRIVIAL EQUATIONS. In the case of differential algebra, they corresponded to non-isotrivial simple Abelian varieties. In characteristic 0 difference algebra, they still lie on simple Abelian varieties, but precisely on those whose isogeny class is defined over a finite extension of the fixed field (as well as on the multiplicative group  $G_m$ ). They correspond to non-cyclotomic irreducible equations over the endomorphism group. For example, let  $f(T) = \sum a_i T^i$  be a polynomial over  $\mathbb{Z}$ . Let  $E_f$  be the subgroup of the multiplicative group defined by  $X^f(\sigma) = 1$ , or more precisely

$$\prod_{a_i > 0} \sigma^{a_i}(X) = \prod_{a_j < 0} \sigma^{-a_j}(X)$$

**THEOREM 4.2**  *$E_f$  is minimal iff  $f$  is irreducible over  $\mathbb{Z}$ . Whether or not it is minimal,  $E_f$  is geometrically modular iff  $E_f$  has no cyclotomic factors. In this case, every subset of  $(E_f)^n$  defined using difference equations is a Boolean combination of subgroups and their cosets. In particular this is true for the intersection of any algebraic variety with  $(E_f)^n$ .*

A similar result is true for Abelian varieties. For the multiplicative group, at least for the simple equation we will consider below, it is easy to prove directly. The proof in [16] uses the trichotomy, proved for difference equations in [8]: non-linearity inside a group implies non-modularity; this implies the presence of a field; one recognizes the field as a finite extension of the fixed field, thus involving the equation  $\sigma^n(X) = X$ , or  $E_{T^n-1}$ ; the non-orthogonality of  $E_f$  to this equation implies that  $f$  is cyclotomic.

**4.3 FINITENESS FOR TORSION POINTS** In [16], the above was used to give a new proof of the Manin-Mumford conjecture on torsion points on semi-Abelian varieties, proved originally in (for curves on Abelian varieties) in [36]. The conjecture states that the number of torsion points on a curve of genus  $> 1$  is finite; more generally, any variety intersects the torsion points in a finite union of translates of group varieties. The new proof gives effective and indeed explicit (though doubly exponential) bounds; this is automatic from the difference-algebra nature of the proof, more precisely from the fact that one bounds the number of points of a certain difference equation *in any difference field* and not only in number fields.

Here is the proof for the case of curves on powers of the multiplicative group (where the result goes back at least to Lang.) Let  $a$  be an even-order root of unity. Then  $a^3$  is a root of unity of the same order. So there exists an automorphism  $\sigma$  of  $\mathbb{Q}(a)$  with  $\sigma(a) = a^3$ . Similarly if  $a^n = 1$ ,  $n$  odd, there exists an automorphism  $\sigma$  with  $\sigma(a) = a^2$ . Putting these together, and letting  $f(T) = (T-3)(T-2)$ , we can find an automorphism  $\sigma$  such that  $E_f = E_f(\sigma)$  contains all roots of 1. Now by 4.2, the intersection of any curve with  $(E_f)^n$ , in any difference domain, is finite unless the curve is a multiplicative translate of a subgroup of  $(G_m)^n$ , i.e. it is defined by a purely multiplicative equation. A fortiori this holds for the smaller set consisting of the roots of unity.

#### 4.4 TATE-VOLOCH CONJECTURE

**CONJECTURE 4.3 (TATE-VOLOCH)** *Let  $A$  be an Abelian variety over  $\mathbb{C}_p$ , the completion of the algebraic closure of  $\mathbb{Q}_p$ . Let  $C \subset A$  be a curve of genus  $> 1$ , and let  $T$  be the group of torsion points of  $A$ . Then there exists a finite  $F \subset T$  and a  $p$ -adic open neighborhood of  $T \setminus F$ , that meets  $C$  in a finite set.*

Certain cases were proved by Buium, Silverman, Tate-Voloch. When  $A$  is an Abelian variety over  $\mathbb{Q}_p$  with good reduction, and one considers only torsion points  $T_p$  of order prime to  $p$ , the proof of the Manin-Mumford conjecture above – combined with a standard idea of nonstandard analysis – immediately yields a proof of Tate-Voloch. A sketch:

The assumptions are used to find a geometrically modular difference equation  $E_f$ , and an automorphism  $\sigma$  of  $\mathbb{Q}_p$ , such that  $T_p \subset E_f$  in the difference field  $(\mathbb{Q}_p, \sigma)$ .

By 4.2,  $F = C \cap E_f$  is finite in *any* difference field.

Assume  $E_f \setminus F$  has points arbitrarily close to  $C$ . Then, using the compactness theorem of model theory, or nonstandard analysis, one can find a field  $L$  extending  $\mathbb{Q}_p$  with a nonstandard  $p$ -adic valuation, and a point  $a$  on  $E_f$  whose distance to  $C$  is infinitesimal. Modifying the field by identifying sufficiently near elements, we obtain a residue difference field  $\bar{L}$  and a point  $\bar{a}$  on  $E_f \setminus F$ , whose distance to  $C$  is zero. Then  $\bar{a} \in (C \cap E_{\bar{F}}) = F$ , a contradiction.

Note that this proof could not work directly with  $T$  or  $T_p$  in place of  $E_f$ ; a “nonstandard torsion point” is just not torsion, nor has any other immediately obvious properties; whereas  $E_f$  is defined by an equation, so is respected by ultra-products.

This proof was improved by Thomas Scanlon, both in the number theory part (obtaining the automorphism  $f$  under less restrictive conditions) and the model theory (using orthogonality as well as geometric modularity.) He proved:

**THEOREM 4.4** *The Tate-Voloch conjecture is true when  $A$  is over a finite extension of  $\mathbb{Q}_p$ .*

## 5 QUASI-FINITE STRUCTURES

### 5.1 LIE-COORDINATIZED STRUCTURES

In the previous examples, a first-order structure was given; the existence of a dimension theory, a semi-minimal decomposition, and a structure theory for the minimal geometries was proved. Here we will go in the opposite direction. A certain class of linear geometries (“basic Lie geometries”) is explicitly defined, and one considers structures having a semi-minimal analysis in terms of these geometries. (“Lie-coordinatizable structures”.) One then proves the existence of a global dimension theory, global modularity, a structure theory for definable groups, existence of good finite approximations, axiomatizability, and other properties. The results of this section are from [10].

**5.1.1 THE BASIC GEOMETRIES** The full list includes all the “classical geometries” (Weyl): linear, unitary, orthogonal, symplectic; over an arbitrary *finite* field. (There are also some slightly less classical variants.) For definiteness, we take them to be  $\aleph_0$ -dimensional (later finite dimensional ones will be considered too.)

The simplest three examples:

1. A pure set  $X$ . (The only relations on  $X^n$  are the diagonals.)
2. A vector space  $V$  over  $GF(3)$ . (The basic relations:  $\sum a_i X_i = 0$ .)
3. A vector space  $V$  over  $GF(3)$  with a symmetric bilinear form  $V \times V \rightarrow GF(3)$ .

4. A pair  $(V, V^*)$  of vector spaces over  $GF(2)$ . (Basic relations: addition on  $V$  and on  $V^*$ ; a pairing  $(, ) : V \times V^* \rightarrow GF(2)$ .)

We will be interested in these geometries when they are *embedded* in a structure  $M$ . This means (e.g. in case (2) above:)  $V$  coincides with a sort in  $M$ , or with a definable subset of a sort in  $M$ ; and *a subset of  $V^n$  is definable in  $M$  if and only if it is definable in the vector space  $V$* . (In case (2), iff it is a finite Boolean combination of relations  $\sum a_i X_i = 0$ .)

When more than one geometry is involved, say two geometries  $J_1, J_2$ , we will assume they are *jointly embedded*: the disjoint union of  $J_1, J_2$  as structures, is embedded. This is equivalent to an *orthogonality* condition on  $J_1, J_2$  as embedded in  $M$ .

This condition is more complicated when a family of geometries is involved, and we will omit it. If a geometry is embedded in  $M$ , it is automatically minimal in the sense that it has S1-dimension 1 (cf. §2.2)

**5.1.2 DEFINITION OF LIE-COORDINATIZABLE STRUCTURES** Let  $M$  be a first-order structure (§2). We assume a class of basic geometries is jointly embedded in  $M$  (for simplicity, consider a finite class.) We consider the class  $\mathcal{M}$  of basic geometries, and principal homogeneous spaces over groups associated with the basic geometries. (Essentially, affine spaces corresponding to the vector spaces.) *We assume §1.1 - Theorem 1.1 and the remark following it - are true in  $M$  with respect to the class  $\mathcal{M}$ .* Thus for each definable  $D \subset M$ , there exist  $J_1, \dots, J_n \in \mathcal{M}$  and a nontrivial definable map  $f : D \rightarrow (\cup_i J_i)^{[n]}$ .

We also assume that  $M$  is  $\aleph_0$ -categorical, or that  $Aut(M)$  has finitely many orbits on  $M^n$ , for any  $n$ . (Note that this is the case for each of the basic geometries.) It follows that the process of semi-minimal analysis - finding a function on each fiber of  $f$  above into other semi-basic geometries, and iterating - *terminates after finitely many steps*. (Cf. [10] for details.)

**5.1.3 EXAMPLE** Let  $M$  be a free Abelian group of exponent 4.  $M$  contains  $V = 2M = \{x \in M : 2x = 0\}$ . This can be shown to be an embedded geometry (of type (2) on our short list.) The map  $f : M \rightarrow V$  is given by:  $f(x) = 2x$ . For  $a \in V$ ,  $f^{-1}(a)$  is a homogeneous space over  $V$  itself.

The following theorem lifts to a Lie coordinatizable structure, some easy but important properties of the basic geometries themselves.

**THEOREM 5.1** *Let  $M$  be Lie-coordinatizable.*

1.  $M$  has finite S1-dimension.
2.  $M$  is geometrically modular.
3.  $M$  has the finite model property: every finite set of first order sentences true in  $M$ , is true in a finite structure.
4. In fact  $M$  is the union of finite homogeneous substructures: finite substructures  $N$ , such every partial map from  $N$  to  $N$  extending to an automorphism of  $M$ , extends to an automorphism of  $N$ .

5.  $M$  is relatively finitely axiomatizable, over the Lie geometries in  $M$ .

This type of theorem was first proved by Zilber: he showed that a totally categorical structure is Lie-coordinatizable, by a single basic geometry of type (1) or (2), and proceeded to conclude 5.1 (2) and (3). (The assumption of total categoricity was in effect: finite Morley dimension, and a single unknown minimal set, satisfying 5.1 (3). Zilber globalized this last assumption, but his proof went by way of a classification of the geometry involved; no direct proof of a local-global principle for 5.1(3) is known.) [9] extended this to the case of many geometries. It follows from (3), and this was Zilber's original motivation, that totally categorical structures are not finitely axiomatizable. (4) means that a single first order sentence, together with the isomorphism type of the basic geometries embedded in  $M$ , determines the isomorphism type of  $M$ . Now each of the basic geometries is itself determined by a single sentence together with their *dimension*. Thus (4) is equivalent to the statement that  $M$  is axiomatized by finitely many sentences, together with finitely many axiom schemes asserting that certain sets are infinite. It follows in particular that only countably many Lie coordinatizable structures exist.

## 5.2 HIGHLY SYMMETRIC FINITE GRAPHS

Our subject here is the class  $C(\beta)$  of all finite graphs  $M$ , whose automorphism group has  $\leq \beta$  orbits on four-tuples of vertices.

To say that a large graph has a bounded number of orbits on vertices already implies it has some symmetries; but an arbitrary finite graph is easily coded in a (not much larger) graph whose automorphism group is transitive on vertices, or even pairs or triples of vertices. At  $k = 4$  something new happens; the symmetry condition permeates all parts of the graph, and becomes stable under the naming of boundedly many parameters.

The following remark shows the first connection between a single, infinite, Lie-coordinatizable structure, and a *class* of finite, highly homogeneous structures.

REMARK 5.1 *Let  $M$  be a Lie-coordinatizable structure. Let  $\Gamma$  be a definable graph in  $M$ . Let  $\beta$  be the number of orbits of  $\text{Aut}(M)$  on  $\Gamma^4$ . Let  $C(M)$  be the class of finite homogeneous substructures of  $M$ , and*

$$C(M, \Gamma) = \{N \cap \Gamma : N \in C(M)\}$$

*Then  $C(M; \Gamma) \subset C(\beta)$ .*

The proof is immediate from the definition of homogeneous substructure.

If  $M$  has  $k$  Lie geometries (for simplicity),  $J_1, \dots, J_k$  then a homogeneous substructure  $N$  of  $M$  can be assigned  $k$  "dimensions":  $\dim(J_i \cap N), \dots, \dim(J_k \cap N)$ . It can be shown that  $N$  is determined up to isomorphism by these dimensions. The remark thus provides some very orderly subfamilies of  $C(\beta)$ .



EXAMPLE Let  $V(n)$  be an  $n$ -dimensional vector space over a fixed finite field  $F$ , say  $GF(5)$ . As any eight elements of  $V(n)$  are contained in a copy of  $V(8)$ , the automorphism group  $GL(n, F)$  has no more orbits on  $V(n)^8$  than  $GL(8, 5)$  has on  $V(8)^8$ ; this number is bounded by  $5^{64}$ . Let  $\Gamma(n)$  be the graph whose vertices are 2-dimensional subspaces of  $V(n)$ , with an edge between two subspaces contained in the same 3-dimensional space. Then  $GL(n, F)$  acts on  $\Gamma(n)$  by automorphisms, and has  $\leq 5^{64}$  orbits on  $\Gamma(n)^4$ . So  $\Gamma(n) \in C(5^{64})$ . Similarly, any class of graphs formed uniformly out of the  $V(n)$  falls into a single  $C(\beta)$ .

We show that  $C(\beta)$  consists entirely of such graphs:

THEOREM 5.2 *There exist finitely many Lie-coordinatizable structures  $M_1, \dots, M_r$ , such that  $C(\beta) = \cup_{1 \leq i \leq r} C(M_i)$ .*

The entire theory applies to finite structures of any “signature”, e.g. hypergraphs, and not only to graphs (and the “4” remains 4.) The theorem was proved by Lachlan for certain subclasses of  $C(\beta)$ : the graphs (or hypergraphs) that are *homogeneous* in the sense that every partial automorphism extends to an automorphism. In this case, only the trivial geometry (1) occurs in the Lie coordinatized structure.

We will not have time to bring out the power of 5.2, but will list some consequences that can be stated without further definitions, in the language of group theory, combinatorics and complexity, respectively.

COROLLARY 5.2 *There exists a bound  $h = h(\beta)$  such that for any  $M \in C(\beta)$ ,  $Aut(M)$  has at most  $h$  distinct non-Abelian Jordan-Holder components. The isomorphism type of  $M$  is determined by the set of  $\leq h$  simple components of  $Aut(M)$ , up to a bounded number of possibilities.*

Each of these simple components typically occurs unboundedly often in  $Aut(M)$ ; in addition very large Abelian groups occur. The corollary hinges on a correspondence between the basic geometries embedded in a Lie-coordinatizable structure, and the simple components of the finite approximations to the structure.

The next corollary is a version of the global modularity principle. Consider bipartite graphs  $\Gamma = (P, L, I \subset (P \times L))$ . Let  $I(b) = \{a \in P : (a, b) \in I\}$ . Let  $\pi, \lambda, l_b$  denote the sizes of  $P, L, I(b)$  respectively. Let  $l = \min\{l_b : b \in L\}$ .

THEOREM 5.3 *Let  $\Gamma$  vary through a family of bipartite graphs in  $C(\beta)$ . Assume that for  $b \neq b' \in L$ ,  $|I(b) \cap I(b')| = o(l)$ . Then*

$$\lambda l \leq O(p)$$

By contrast, if  $(P, L, I)$  is a projective plane, then  $\pi = \lambda \sim l^2$ , while  $|I(b) \cap I(b')| = 1$ . The theorem thus says that no bipartite graph in  $C(\beta)$  is combinatorially similar to a projective plane; this is rather close to Lachlan’s original formulation in the stable  $\aleph_0$ -categorical framework.

The theorem is obtained from a local-global principle for modularity; the modularity of the basic geometries themselves is a consequence of the classification of

the finite simple groups. It would be interesting to know if the above combinatorial statement can be obtained without the heavy group theory. (In [10] a number of principles of a roughly similar nature are formulated; if all are assumed, one obtains a direct proof of the relevant part of the classification (classification of the large finite simple groups having highly symmetric permutation representations in the above sense, or occurring as components in groups that do.)

Finally,

**COROLLARY 5.3** *Membership of a graph in  $C(k)$  is decidable in polynomial time. So is the problem of deciding isomorphism between two graphs in  $C(k)$*

This is analogous to a famous result of Luks (Proc. 21 FOCS), concerning graphs of bounded valency, but here the graphs are at the opposite extreme (and in particular have bounded diameter.)

**5.3 PROOF OF 5.2** In [27], the primitive permutation groups with few orbits on 4-tuples are analyzed group-theoretically. The conclusion is an almost precise classification of the possibilities. The proof relies massively on the classification of the finite simple groups, and on related methods.

It follows from this result that to each  $\Gamma \in C(\beta)$  one can associate a finite approximation  $M_\Gamma$  to a Lie coordinatized structure, such that  $\Gamma, M_\Gamma$  have the same automorphism group.

A very soft translation into model theory shows that  $M_\Gamma$  and  $\Gamma$  interpret each other;  $\Gamma$  can be viewed as a sort in a structure, built out of  $M_\Gamma$ . A formula  $\phi_\Gamma$  describes the construction of  $\Gamma$  from  $M_\Gamma$ .

The difficulty is that the soft connection between automorphism groups and formulas says nothing of the length of the formula. It may be as large as the finite structure it describes. Take for instance the class  $\{P_n = (V_n, V_n^*)\}$  of dual pairs ( $V_n$  is an  $n$ -dimensional  $GF(2)$ -vector space;  $V_n^*$  is the dual.) The pair  $P_n = (V_n, V_n^*)$  (or a suitable graph formed from it) has the same automorphism group as  $V_n$ . So we may have  $M_{P_n} = V_n$ . Yet there is no formula of bounded length that constructs  $V^*$  from  $V$ . In this case, we were given the wrong basic geometry, and we have to find *another* that does have a construction of bounded length. (In this case, it is just  $P_n$  itself.)

We take an ultraproduct of the structures  $\Gamma$ , and  $M_\Gamma$ , obtaining infinite structures  $\Gamma^*, M^* = (M_\Gamma)^*$ . In a language with formulas of nonstandard size,  $M^*$  interprets  $\Gamma^*$ , so  $\Gamma^*$ , in this rich language, is Lie coordinatizable. *We now prove that the class of Lie coordinatizable structures is closed under interpretations.* This is nontrivial and lengthy; the interpreted structure will no longer have the original coordinatizing geometries, and one must go via more global properties (such as geometric modularity) that are inherited when the language is reduced. We apply this theorem to the reduct  $\Gamma^*$  *in the graph language*, obtaining a new Lie coordinatization. If done appropriately, it can now be shown that the original  $\Gamma$  are homogeneous substructures of  $\Gamma^*$ .

Robinson dreamed of rewriting number theory using nonstandard analysis. The hope is that ultrapowers will smooth out the finite irregularities and help

to bring out the uniform behavior behind the undecidability. Some theorems of number theory (some treated by Robinson, and Robinson - Roquette) are very naturally stated in nonstandard language. The trouble is that when only one road leads from standard to nonstandard territory, a direct nonstandard proof is homotopic to a standard one. Only if two distinct paths lead to the same point can we get a truly new proof. In both uses of nonstandard ideas reported on here, the second road is provided by an axiomatization (difference fields, Lie-coordinatized structures) together with a method of analysis of abstract models of these axioms (In both these cases, finite  $S_1$ -dimension and related concepts of definable groups.) To extend the scope of such results in number theoretic directions, one must develop both new quantifier-elimination results, beyond local fields, and corresponding generalizations of stability capable of dealing with them.

## REFERENCES

- [1] J. Ax and S. Kochen, *Annals of Math.* 83, pp. 437 -456, Diophantine Problems over local fields III.
- [2] E. Bouscaren, ed., *Model Theory and Algebraic Geometry (an introduction)*, North-Holland,  $\infty$
- [3] J.T. Baldwin and A.H. Lachlan *On strongly minimal sets*, *JSL* 36 (1971), 79 - 96.
- [4] S. Buechler, *Essential Stability Theory*, *Perspectives in Mathematical Logic* Springer Verlag, 1996
- [5] S. Buechler, *Locally modular theories of finite rank*, *Annals of Pure and Applied Logic* 30 (1986) no. 1, 83-94
- [6] A. Buium, *Differential algebra and Diophantine geometry*. *Actualités Mathématiques*, Hermann, Paris, 1994. x+182 pp. ISBN: 2-7056-6226-X 12Hxx (11Gxx)
- [7] Chang, and Keisler, J., *Model Theory*, 3rd Edition, North -Holland, Amsterdam - Tokyo 1990
- [8] Z. Chatzidakis and E. Hrushovski, the model theory of difference equations, to appear in *TAMS*
- [9] G. Cherlin, L. Harrington, and A. Lachlan,  $\aleph_0$ -categorical,  $\aleph_0$ -stable structures, *Ann. Pure Appl. Logic* 28 (1985) 103-135.
- [10] G. Cherlin, E. Hrushovski, Quasi-finite structures, available via <http://www.math.rutgers.edu/~cherlin>
- [11] R. Cohn, *Difference Algebra*, Addison-Wesley
- [12] Delon, F., *Ideaux et types sure les corps seperablement clos*, *Supplement au Bulletin de la Société Math. de France* Memoire No. 33, Tome 116 (1988).
- [13] Denef, J.; van den Dries, L., *p*-adic and real subanalytic sets, *Ann. of Math (2)* 128 (1988), no.1,79-138
- [14] E. Hrushovski, PAC structures, MS.

- [15] E. Hrushovski, Locally Modular Regular Types, *Classification Theory: Chicago 1985*, editor J.T. Baldwin, Springer Verlag 1987
- [16] E. Hrushovski, the Manin-Mumford conjecture and the model theory of difference fields, preprint
- [17] E. Hrushovski, E., The Mordell-Lang Conjecture for Function Fields, *Journal of the AMS*
- [18] E. Hrushovski, Stability and its uses, in *Current Development in Mathematics 1996*, World academic 1998
- [19] E. Hrushovski and A. Pillay, Weakly Normal Groups, in *Logic Colloquium 85*, North Holland, Amsterdam 1986
- [HP 94] Hrushovski, E. and Pillay, A., Definable subgroups of algebraic groups over finite fields, *Journal fur die Reine und Angewandte Mathematik* 462 (1995) 69-91
- [20] Hrushovski, E. & Sokolovic, Z., Minimal subsets of differentially closed fields, to appear in *Transactions of the American Mathematical Society*
- [21] Hrushovski, E., The first order theory of the Frobenius automorphisms, preprint
- [22] Hrushovski, E. and Itai M., Superstable differential fields, preprint
- [23] E. Hrushovski and B. Zilber, Zariski Geometries, to appear in *Journal of the AMS*
- [24] E. Hrushovski and B. Zilber, Zariski Geometries, *AMS Bulletin* 28 (1993) no. 2 pp. 315-323
- [25] Jouanolou, J. P.: Hypersurface solutions d'une equation de Pfaff analytique, *Math. Ann.* 232, 239-245 (1978).
- [26] E. Hrushovski, A generalization of a theorem of Jouanolou, preprint.
- [27] W.M. Kantor, M.W. Liebeck, H.D. Macpherson  $\aleph_0$ -categorical structures smoothly approximable by finite substructures, *Proc. London Math. Society* (3) 59 (1989) 439-463
- [28] A.H. Lachlan Two conjectures regarding the stability of  $\aleph_0$ -categorical theories, *Fund. Math.* 81 (1974) 133-145.
- [29] Lachlan, A.H., On countable stable structures which are homogeneous for a finite relational language, *Israel J. Math.* v. 49 (1984) 69-153
- [30] Yu. Manin, Rational points of algebraic curves over function fields, *Izv. Akad. Nauk SSSR Ser Mat* 27 (1963) pp. 1395-1440; English translation, *AMS Translations Ser. II* 59 (1966) pp. 189-234
- [31] D. Marker, M. Mesmer, A. Pillay, *Model Theory of Fields*, Lecture Notes in Logic 5, Springer 1996
- [32] Byunghan Kim, Anand Pillay, from stability to simplicity, *Bulletin of Symbolic logic* 4 (1998), no. 1, 17-36

- [33] Peterzil, Y., Starchenko, S., Geometry, calculus, and Zilber's conjecture, *Bulletin of Symbolic Logic* 2 (1996) no. 1, 72-83
- [34] Anand Pillay, *Geometric Stability Theory*, Oxford Logic Guides No 32, Oxford University Press, 1996
- [35] B. Poizat, *Cours de Théorie de modèles*, Nur al - Mantiq wal Ma'rifah, Lyon 1985.
- [36] Raynaud, M., Around the Mordell conjecture for function fields and a conjecture of Serge Lang, in *Proceedings of Algebraic Geometry of Tokyo, 1982*, Lecture Notes 1016, Springer Verlag
- [37] Saharon Shelah, *Classification Theory*, revised edition, North-Holland Amsterdam-Tokyo 1990
- [38] Lou Van den Dries, *Tame Topology and O-minimal structures*, LMS lecture note series 248, 1998
- [39] van den Dries, Lou, Elimination theory for the ring of algebraic integers. *J. Reine Angew. Math.* 388 (1988), 189–205.
- [40] B.I. Zilber, Strongly minimal countably categorical theories, *Siberian Mathematical Journal* 21 (1980), 219-230, II-III (1984), pp. 396-412, 559-571

Ehud Hrushovski  
Department of Mathematics  
Hebrew University  
Jerusalem, Israel

ehud@math.huji.ac.il

CONSTANT TERM IDENTITIES,  
 ORTHOGONAL POLYNOMIALS,  
 AND AFFINE HECKE ALGEBRAS

I. G. MACDONALD

The main aim of this lecture is to survey a theory of orthogonal polynomials in several variables which has developed over the last ten years or so. We shall concentrate on the purely algebraic aspects of the theory, and for lack of time and competence we shall say nothing about its physical applications (completely integrable systems, *KZ* equations, etc.)

These polynomials include as special cases, on the one hand all the classical orthogonal polynomials in one variable (Legendre, Jacobi, Hermite,  $\dots$ ), and on the other hand polynomials that arise in the representation theory of Lie groups (characters of compact Lie groups, spherical functions on real and  $p$ -adic symmetric spaces and their quantum analogues). The underlying notion is that of a *root system*, to which I shall turn first.

## 1 ROOT SYSTEMS

Root systems and their Weyl groups constitute the combinatorial infrastructure of much of the theory of Lie groups and Lie algebras. Thus a complex semisimple Lie algebra or a compact connected Lie group with trivial centre, is determined up to isomorphism by its root system. Moreover, and quite apart from their Lie-theoretic origin, the geometry and algebra of root systems presents an apparently inexhaustible source of beautiful combinatorics.

It is time for definitions and examples. Let  $V$  be a real vector space of finite dimension, endowed with a positive definite scalar product  $\langle u, v \rangle$ . For each non-zero  $\alpha \in V$  let  $s_\alpha$  denote the orthogonal reflection in the hyperplane  $H_\alpha$  through the origin perpendicular to  $\alpha$ . Explicitly,

$$(1.1) \quad s_\alpha(v) = v - \langle v, \alpha^\vee \rangle \alpha$$

for  $v \in V$ , where  $\alpha^\vee = 2\alpha/\langle \alpha, \alpha \rangle$ .

A *root system*  $R$  in  $V$  is a finite non-empty set of non-zero vectors (called *roots*) that span  $V$  and are such that for each pair  $\alpha, \beta \in R$  we have

$$(1.2) \quad \langle \alpha^\vee, \beta \rangle \in \mathbb{Z},$$

$$(1.3) \quad s_\alpha(\beta) \in R.$$

Thus each reflection  $s_\alpha$  ( $\alpha \in R$ ) permutes  $R$ , and the group of orthogonal transformations of  $V$  generated by the  $s_\alpha$  is a finite group  $W_0$ , called the *Weyl group* of  $R$ .

We may remark straightaway that the integrality condition (1.2) by itself is extremely restrictive. Let  $\alpha, \beta \in R$  and let  $\Theta$  be the angle between the vectors  $\alpha$  and  $\beta$ . Then

$$4 \cos^2 \Theta = \frac{4 \langle \alpha, \beta \rangle^2}{\langle \alpha, \alpha \rangle \langle \beta, \beta \rangle} = \langle \alpha^\vee, \beta \rangle \langle \alpha, \beta^\vee \rangle$$

is an *integer*, hence can only take the values 0, 1, 2, 3, 4. It follows that the only possibilities for  $\Theta$  are  $\pi/m$  or  $\pi - (\pi/m)$ , where  $m = 1, 2, 3, 4$  or 6.

The vectors  $\alpha^\vee$  for  $\alpha \in R$  form a root system  $R^\vee$ , the *dual* of  $R$ . If  $\alpha \in R$ , then also  $-\alpha \in R$  (because  $-\alpha = s_\alpha(\alpha)$ ). The root system  $R$  is said to be *reduced* if the only scalar multiples of  $\alpha$  in  $R$  are  $\pm\alpha$ . Furthermore,  $R$  is said to be *irreducible* if it is not possible to partition  $R$  into two non-empty subsets  $R_1$  and  $R_2$  such that each root in  $R_1$  is orthogonal to each root in  $R_2$  (which would imply that  $R_1$  and  $R_2$  are themselves root systems). We shall assume throughout that  $R$  is both reduced and irreducible.

For those to whom these notions are unfamiliar, some examples to bear in mind are the following. Let  $\varepsilon_1, \dots, \varepsilon_n$  be the standard basis of  $\mathbb{R}^n$  ( $n \geq 2$ ), with the usual scalar product, for which  $\langle \varepsilon_i, \varepsilon_j \rangle = \delta_{ij}$ . Then the vectors

$$(A_{n-1}) \quad \pm \varepsilon_i - \varepsilon_j$$

where  $i \neq j$ , form a root system (and  $V$  is the hyperplane in  $\mathbb{R}^n$  orthogonal to  $\varepsilon_1 + \dots + \varepsilon_n$ ). The Weyl group is the symmetric group  $S_n$ , acting on  $V$  by permuting the  $\varepsilon_i$ .

Moreover, each of the sets of vectors

$$(B_n) \quad \pm \varepsilon_i \quad (1 \leq i \leq n), \quad \pm \varepsilon_i \pm \varepsilon_j \quad (1 \leq i < j \leq n),$$

$$(C_n) \quad \pm 2\varepsilon_i \quad (1 \leq i \leq n), \quad \pm \varepsilon_i \pm \varepsilon_j \quad (1 \leq i < j \leq n),$$

$$(D_n) \quad \varepsilon_i \pm \varepsilon_j \quad (1 \leq i < j \leq n)$$

is a root system. For  $B_n$  and  $C_n$ , the Weyl group is the group of all signed permutations of the  $\varepsilon_i$ , of order  $2^n n!$  (the hyperoctahedral group). For  $D_n$ , it is a subgroup of index 2 in this group. The root systems  $B_n$  and  $C_n$  are duals of each other, and  $A_{n-1}, D_n$  are each self-dual.

In fact, the root systems  $A_n$  ( $n \geq 1$ ),  $B_n$  ( $n \geq 2$ ),  $C_n$  ( $n \geq 3$ ) and  $D_n$  ( $n \geq 4$ ) almost exhaust the catalogue of reduced irreducible root systems (up to isomorphism). Apart from these, there are just five others, the “exceptional” root sys-

tems, denoted by  $E_6, E_7, E_8, F_4$  and  $G_2$ . (In each case the numerical suffix is the dimension of the space  $V$  spanned by  $R$ , which is also called the *rank* of  $R$ .)

Let  $R$  be any (reduced, irreducible) root system in  $V$  and consider the complement

$$X = V - \bigcup_{\alpha \in R} H_\alpha$$

of the union of the reflecting hyperplanes  $H_\alpha, \alpha \in R$ . The connected components of  $X$  are open simplicial cones which are permuted simply transitively by the Weyl group  $W_0$ . Let  $\Gamma$  be one of these components, chosen once and for all; it is bounded by  $n = \dim V$  hyperplanes  $H_{\alpha_i} (1 \leq i \leq n)$ , and

$$\Gamma = \{x \in V : \langle \alpha_i, x \rangle > 0 \quad (1 \leq i \leq n)\}.$$

The  $\alpha_i$  are the *simple roots* determined by  $\Gamma$ , and each root  $\alpha \in R$  is of the form

$$(1.4) \quad \alpha = \sum_1^r r_i \alpha_i$$

with integral coefficients  $r_i$  all of the same sign. A root  $\alpha \in R$  is *positive* (resp. *negative*) relative to  $\Gamma$  if  $\langle \alpha, x \rangle > 0$  (resp.  $< 0$ ) for all  $x \in \Gamma$ . Equivalently,  $\alpha \in R$  is positive (resp. negative) if the coefficients  $r_i$  in (1.4) are all  $\geq 0$  (resp.  $\leq 0$ ). Let  $R^+$  (resp.  $R^-$ ) denote the set of positive (resp. negative) roots. Then  $R^- = -R^+$ , and  $R = R^+ \cup R^-$ . Moreover, there is a unique root  $\varphi \in R^+$ , called the *highest root*, for which the sum of the coefficients  $\sum r_i$  in (1.4) is maximal. In  $A_{n-1}$ , for example, we may take the simple roots to be  $\alpha_i = \varepsilon_i - \varepsilon_{i+1} (1 \leq i \leq n-1)$ ; the positive roots are then  $\varepsilon_i - \varepsilon_j$  with  $i < j$ , and the highest root is  $\varepsilon_1 - \varepsilon_n$ .

The abelian group  $Q$  generated by  $R$ , whose elements are the integral linear combinations of the roots, is a lattice in  $V$  (i. e. a free abelian group of rank  $n = \dim V$ ) called the *root lattice*. Clearly the simple roots  $\alpha_1, \dots, \alpha_n$  form a basis of  $Q$ . We denote by  $Q^+$  the subsemigroup of  $Q$  consisting of all sums  $\sum r_i \alpha_i$  where the coefficients are non negative integers.

Next, the set  $P$  of all  $\lambda \in V$  such that  $\langle \lambda, \alpha^\vee \rangle \in \mathbb{Z}$  for all  $\alpha \in R$  is another lattice, called the *weight lattice*. It has a basis consisting of the *fundamental weights*  $\pi_1, \dots, \pi_n$ , defined by the equations  $\langle \pi_i, \alpha_j^\vee \rangle = \delta_{ij}$ . We denote by  $P^+$  the set of *dominant weights* (i. e.  $\lambda \in P$  such that  $\langle \lambda, \alpha^\vee \rangle \geq 0$  for all  $\alpha \in R^+$ ). We have  $P \supset Q$  (by (1.2)) but  $P^+ \not\supset Q^+$  (unless  $n = 1$ , i. e.  $R = A_1$ ). The quotient  $P/Q$  is a finite group, since both  $P$  and  $Q$  are lattices of the same rank  $n$ . Clearly, both  $P$  and  $Q$  are stable under the action of the Weyl group  $W_0$ . Each  $W_0$ -orbit in  $P$  contains exactly one dominant weight, i. e.  $P^+$  is a fundamental region for the action of  $W_0$  on  $P$ .

Finally, the Weyl group  $W_0$  acts on  $V$  and therefore also on the algebra  $S(V)$  of polynomial functions on  $V$ . It can be shown that the subring  $S(V)^{W_0}$  of  $W_0$ -invariant polynomial functions is generated by  $n = \dim V$  algebraically independent homogeneous polynomial functions, of degrees say  $d_1, \dots, d_n$ . The



functions themselves are not uniquely determined, but their degrees are: they are called the *degrees of  $W_0$* . For example, if  $R$  is  $A_{n-1}$ , so that  $W_0$  is the symmetric group  $S_n$ , we may take as generators of  $S(V)^{W_0}$  the power sums

$$x_1^r + \cdots + x_n^r \quad (2 \leq r \leq n)$$

where  $x_1, \dots, x_n$  are coordinates in  $\mathbb{R}^n$ . Thus in this case the degrees are  $2, 3, \dots, n$ .

## 2 CONSTANT TERM IDENTITIES

Let  $F$  be a field of characteristic zero and let  $A = F[P]$  be the group algebra over  $F$  of the weight lattice  $P$ . Since the group operation in  $P$  is addition, we shall use an exponential notation in  $A$ , and denote by  $e^\lambda$  the element of  $A$  corresponding to  $\lambda \in P$ . These “formal exponentials”  $e^\lambda$  form an  $F$ -basis of  $A$ , such that  $e^\lambda \cdot e^\mu = e^{\lambda+\mu}$  and  $(e^\lambda)^{-1} = e^{-\lambda}$ . In particular,  $e^0 = 1$  is the identity element of  $A$ . The ring  $A$  is an algebra of Laurent polynomials, namely  $A = F[u_1^{\pm 1}, \dots, u_n^{\pm 1}]$  where  $u_i = e^{\pi_i}$  ( $\pi_i$  the fundamental weights).

If

$$f = \sum_{\lambda \in P} f_\lambda e^\lambda$$

is an element of  $A$ , with coefficients  $f_\lambda \in F$ , the *constant term* of  $f$  is  $f_0$ , the coefficient of  $e^0 = 1$  in  $f$ . We can now state two constant term identities that generalize those of Dyson and Andrews described in the abstract to this lecture. As before,  $R$  is a reduced irreducible root system and  $k$  a non negative integer.

(2.1) *The constant term in*

$$\prod_{\alpha \in R} (1 - e^\alpha)^k$$

is equal to

$$\prod_{i=1}^n \binom{kd_i}{k}$$

where  $d_1, \dots, d_n$  are the degrees of the Weyl group of  $R$ .

When  $R$  is  $A_{n-1}$ , the roots are  $\alpha = \varepsilon_i - \varepsilon_j$  where  $i \neq j$ , so that  $e^\alpha = x_i x_j^{-1}$  where  $x_i = e^{\varepsilon_i}$ . Moreover, as we have seen, the degrees of the Weyl group in this case are  $2, 3, \dots, n$ ; and

$$\binom{2k}{k} \binom{3k}{k} \cdots \binom{nk}{k} = \frac{(nk)!}{k!^n}$$

Thus we recover Dyson’s original conjecture [5].

Next, in order to state the generalization of Andrew’s conjecture we introduce the  $q$ -analogue of the binomial coefficient  $\binom{r}{s}$ , namely the *Gaussian polynomial*

$$\begin{bmatrix} r \\ s \end{bmatrix} = \frac{(1-q^r)(1-q^{r-1}) \cdots (1-q^{r-s+1})}{(1-q)(1-q^2) \cdots (1-q^s)}$$

which tends to  $\binom{r}{s}$  as  $q \rightarrow 1$ .

(2.2) The constant term in

$$\prod_{\alpha \in R^+} \prod_{i=0}^{k-1} (1 - q^i e^\alpha) (1 - q^{i+1} e^{-\alpha})$$

is equal to

$$\prod_{i=1}^n \begin{bmatrix} kd_i \\ k \end{bmatrix}.$$

When  $R$  is  $A_{n-1}$ , the positive roots are  $\alpha = \varepsilon_i - \varepsilon_j$  with  $i < j$ , so that we recover Andrews' conjecture. Clearly, also, (2.2) reduces to (2.1) when we let  $q \rightarrow 1$ .

When these conjectures and others like them were first put forward ([12], [18]), they appeared as isolated curiosities, and it was not clear what, if anything, lay behind them. Later [13] it became clear that they could be considered as a special case of a conjectured norm formula for orthogonal polynomials, as we shall explain in the next section.

The identity (2.1) was first proved uniformly for all  $R$  by Opdam [20], using the technique of shift operators developed by Heckman and Opdam in the context of their theory of hypergeometric functions and Jacobi polynomials [8]. The  $q$ -version (2.2) took longer to resolve, and was finally proved in full generality by Cherednik [3], although by that time all the root systems with the exception of  $E_6, E_7$  and  $E_8$  has been dealt with one by one ([2], [9], [6], [7]).

### 3 ORTHOGONAL POLYNOMIALS

As in §2, let  $A$  be the group algebra  $F[P]$  where  $F$  is a field of characteristic 0. The Weyl group  $W_0$  acts on  $P$  and therefore also on  $A$ :  $w(e^\lambda) = e^{w\lambda}$  ( $\lambda \in P, w \in W_0$ ). Let  $A_0$  denote the subalgebra of  $W_0$ -invariants.

Since each  $W_0$ -orbit in  $P$  meets  $P^+$  exactly once, it follows that the *orbit-sums*

$$(3.1) \quad m_\lambda = \sum_{\mu \in W_0\lambda} e^\mu$$

where  $\lambda \in P^+$  and  $W_0\lambda$  is the  $W_0$ -orbit of  $\lambda$ , form an  $F$ -basis of  $A$ . Another basis of  $A_0$  is obtained as follows. Let

$$(3.2) \quad p = \frac{1}{2} \sum_{\alpha \in R^+} \alpha$$

and let

$$(3.3) \quad \delta = \prod_{\alpha \in R^+} (e^{\alpha/2} - e^{-\alpha/2}).$$

In fact,  $p \in P^+$  and  $\delta \in A$  : we have

$$(3.4) \quad \delta = \sum_{w \in W_0} \varepsilon(w) e^{wp}$$

where  $\varepsilon(w) = \det(w) = \pm 1$ . Thus  $\delta$  is skew-symmetric for  $W_0$ , i. e. we have  $w\delta = \varepsilon(w)\delta$  for each  $w \in W_0$ . For each  $\lambda \in P^+$ , the sum

$$\sum_{w \in W_0} \varepsilon(w) e^{w(\lambda+p)}$$

is likewise skew-symmetric, and is divisible by  $\delta$  in  $A$ . The quotient

$$(3.5) \quad \mathcal{X}_\lambda = \delta^{-1} \sum_{w \in W_0} \varepsilon(w) e^{w(\lambda+p)}$$

is an element of  $A_0$  called the *Weyl character* corresponding to  $\lambda$ . In terms of the orbit-sums we have

$$(3.6) \quad \mathcal{X}_\lambda = m_\lambda + \sum_{\mu < \lambda} K_{\lambda\mu} m_\mu$$

where the coefficients  $K_{\lambda\mu}$  are integers (indeed positive integers) and  $\mu < \lambda$  means that  $\lambda - \mu \in Q^+$  and  $\lambda \neq \mu$ .

From (3.6) it follows that the  $\chi_\lambda$  form another  $F$ -basis of  $A_0$ . From now on we shall take  $F$  to be the field  $\mathbb{Q}(q, t)$  of rational functions in two indeterminates  $q, t$ . Let

$$(3.7) \quad \Delta = \Delta(q, t) = \prod_{\alpha \in R^+} \prod_{r=0}^{\infty} \frac{(1 - q^r e^\alpha)(1 - q^{r+1} e^{-\alpha})}{(1 - q^r t e^\alpha)(1 - q^{r+1} t e^{-\alpha})}.$$

Suppose first that  $t = q^k$  where  $k$  is a non-negative integer. Then  $\Delta$  is a finite product, namely the polynomial whose constant term was the subject of (2.2). (In the general case,  $\Delta$  can be expanded as a formal power series in the  $n+1$  variables  $u_0, u_1, \dots, u_n$ , where  $u_i = e^{\alpha_i}$  ( $1 \leq i \leq n$ ) and  $u_0 = qe^{-\varphi}$ ,  $\varphi$  the highest root of  $R$ .)

We shall use  $\Delta$  to define a scalar product on  $A$ , as follows. If  $f \in A$ , say

$$f = \sum_{\lambda \in P} f_\lambda e^\lambda,$$

let

$$(3.8) \quad f^* = \sum_{\lambda \in P} f_\lambda^* e^{-\lambda}$$

where  $f_\lambda^*$  is the image of  $f_\lambda$  under the automorphism  $(q, t) \mapsto (q^{-1}, t^{-1})$  of  $F$ . We now define, for  $f, g \in A$ ,

$$(3.9) \quad (f, g) = \text{constant term in } fg^* \Delta.$$

We can now state

(3.10) *There is a unique  $F$ -basis  $(P_\lambda)_{\lambda \in P^+}$  of  $A_0$  such that*

- (i)  $P_\lambda = m_\lambda + \sum_{\mu < \lambda} u_{\lambda\mu} m_\mu$  with coefficients  $u_{\lambda\mu} \in F$ ;
- (ii)  $(P_\lambda, P_\mu) = 0$  if  $\lambda \neq \mu$ .

It is easy to see that the  $P_\lambda$ , if they exist, are uniquely determined by (i) and (ii). Their existence, however, requires proof. If the partial order  $\lambda > \mu$  on  $P^+$  were a total ordering, existence would follow directly from the Gram-Schmidt orthogonalization process. But it is not a total ordering (unless  $R = A_1$ ) and we should therefore have to extend it to a total ordering before applying the Gram-Schmidt mechanism. Thus the content of (3.10) is that however we extend the partial order  $\lambda > \mu$  to a total order, we always obtain the same basis.

We shall not reproduce the original proof ([13] [16]) of (3.10) here, since it will arise more naturally later in the context of affine Hecke algebras. Instead, let us look at some special cases:

- (1) When  $t = 1$ , we have  $\Delta = 1$  and  $P_\lambda$  is the orbit-sum  $m_\lambda$  (3.1).
- (2) When  $t = q$ ,  $P_\lambda$  is the Weyl character  $\mathcal{X}_\lambda$  (3.5).
- (3) When  $q \rightarrow 0$ ,  $t$  being arbitrary, the  $P_\lambda$  (suitably normalized) occur as the values of spherical functions on a  $p$ -adic symmetric space, when  $t^{-1}$  is a prime power.
- (4) Let  $t = q^k$  and fix  $k$  (which need not be an integer) and let  $q \rightarrow 1$ , so that  $t \rightarrow 1$  also. In the limit we have  $\Delta = \prod_{\alpha \in R} (1 - e^\alpha)^k$ . In this limiting case the polynomials  $P_\lambda$  are the ‘‘Jacobi polynomials’’ of Heckman and Opdam [8]. For particular values of  $k$  these polynomials occur as values of spherical functions, but this time on a *real* symmetric space.
- (5) Finally, when  $R$  is  $A_{n-1}$ , the  $P_\lambda$  are the symmetric functions of ([15], chapter VI), restricted to  $n$  variables  $x_1, \dots, x_n$  such that  $x_1 \cdots x_n = 1$ .

To conclude this section, we shall record some properties of the polynomials  $P_\lambda$ . For simplicity of statement, we shall assume that  $t = q^k$  where  $k$  is a positive integer.

a.) *Norms*

The squared norm of  $P_\lambda$  is given by the formula

$$(3.11) \quad (P_\lambda, P_\lambda) = W_0(t) \prod_{\alpha \in R^+} \prod_{i=0}^{k-1} \frac{1 - q^{\langle \lambda + kp, \alpha^\vee \rangle + i}}{1 - q^{\langle \lambda + kp, \alpha^\vee \rangle - i}}$$

where  $p$  is given by (3.2) and  $W_0(t)$  is the Poincaré polynomial of the Weyl group  $W_0$ :

$$W_0(t) = \sum_{w \in W_0} t^{\ell(w)}$$

where  $l(w)$  is the *length* of  $w$ , i. e. the number of  $\alpha \in R^+$  such that  $w\alpha \in R^-$ .

Notice that when  $\lambda = 0$  we have  $P_\lambda = 1$ , so that in this case (3.11) gives the constant term of  $\Delta$ , i. e. it gives the constant term identity (2.2) (though a little work is required to recast it in that form). The formula (3.11) was originally conjectured in [13], and verified there in some cases. In the limiting case  $q \rightarrow 1$ , it was first proved for all root systems  $R$  by Opdam [20], and then in full generality by Cherednik [3]. We shall indicate a proof later, in §5.

b.) *Specialization*

Let  $P^\vee$  be the weight lattice of the dual root system  $R^\vee$ : it consists of all  $\lambda \in V$  such that  $\langle \lambda, \alpha \rangle \in \mathbb{Z}$  for all  $\alpha \in R$ . It will be convenient to regard each  $f \in A$  as a function on  $P^\vee$ , as follows: if  $\mu \in P^\vee$  and  $f = \sum f_\lambda e^\lambda$ , then

$$f(\mu) = \sum f_\lambda q^{\langle \lambda, \mu \rangle}.$$

Then we have

$$(3.12) \quad P_\lambda(kp^\vee) = q^{-\langle \lambda, kp^\vee \rangle} \prod_{\alpha \in R^+} \prod_{i=0}^{k-1} \frac{1 - q^{\langle \lambda + kp, \alpha^\vee \rangle + i}}{1 - q^{\langle kp, \alpha^\vee \rangle + i}}$$

where

$$p^\vee = \frac{1}{2} \sum_{\alpha \in R^+} \alpha^\vee$$

(warning:  $p^\vee \neq 2p/\langle p, p \rangle$ ).

When  $k = 1$  and  $q \rightarrow 1$ , this reduces to Weyl's formula for the dimension of an irreducible representation of a compact Lie group. The formula (3.12) was originally conjectured in [13]. As with (3.11), it was first proved for all  $R$  in the limiting case  $q \rightarrow 1$  by Opdam [20], and then in full generality by Cherednik [4].

c.) *Symmetry*

For  $\lambda \in P$  let

$$\tilde{P}_\lambda = P_\lambda / P_\lambda(kp^\vee).$$

Then we have

$$(3.13) \quad \tilde{P}_\lambda(\mu + kp^\vee) = \tilde{P}_\mu(\lambda + kp)$$

for all  $\lambda \in P^+$  and  $\mu \in (P^\vee)^+$ , and on the right-hand side of (3.13),  $P_\mu$  is an orthogonal polynomial for  $R^\vee$ , so that  $\tilde{P}_\mu = P_\mu / P_\mu(kp)$ . When  $R$  is of type  $A_{n-1}$ , (3.13) is due to Koornwinder ([15], chapter VI, §6). The general case is due to Cherednik [4].

#### 4 THE AFFINE ROOT SYSTEM AND THE EXTENDED AFFINE WEYL GROUP

The root systems and Weyl groups of §1 have affine counterparts, to which we now turn. As before,  $R$  is a reduced, irreducible root system spanning a real vector

space  $V$  of dimension  $n \geq 1$ . Let  $Q^\vee, P^\vee$  respectively denote the root lattice and the weight lattice of the dual root system  $R^\vee$ .

We shall regard each  $\alpha \in R$  as a linear function on  $V$ :  $\alpha(x) = \langle \alpha, x \rangle$  for  $x \in V$ . Let  $c$  denote the constant function 1 on  $V$ . Then

$$(4.1) \quad S = S(R) = \{\alpha + nc : \alpha \in R, n \in \mathbb{Z}\}$$

is the *affine root system* associated with  $R$ . The elements of  $S$  are affine-linear functions on  $V$ , called *affine roots*, and we shall denote them by italic letters,  $a, b, \dots$

For each  $a \in S$ , let  $H_a$  denote the affine hyperplane in  $V$  on which  $a$  vanishes, and let  $s_a$  denote the orthogonal reflection in this hyperplane. The affine Weyl group  $W_S$  is the group of affine isometries of  $V$  generated by these reflections. For each  $\alpha \in R$ , the mapping  $s_\alpha \circ s_{\alpha+c}$  takes  $x \in V$  to  $x + \alpha^\vee$ , so that

$$\tau(\alpha^\vee) = s_\alpha \circ s_{\alpha+c}$$

is translation by  $\alpha^\vee$ . It follows that  $W_S$  contains a subgroup of translations isomorphic to  $Q^\vee$ , and we have

$$(4.2) \quad W_S = W_0 \ltimes \tau(Q^\vee)$$

(semidirect product).

The *extended affine Weyl group* is

$$(4.3) \quad W = W_0 \ltimes \tau(P^\vee).$$

It acts on  $V$  as a discrete group of isometries, and hence by transposition on functions on  $V$ . As such, it permutes the affine roots  $a \in S$ .

As in §1, let  $R^+$  be a system of positive roots in  $R$  and  $\alpha_1, \dots, \alpha_n$  the simple roots,  $\varphi$  the highest root. Correspondingly, the affine roots  $a_0, a_1, \dots, a_n$ , where  $a_0 = -\varphi + c$  and  $\alpha_i = \alpha_i$  ( $1 \leq i \leq n$ ) form a set of simple roots for  $S$ : each  $a \in S$  is of the form

$$(4.4) \quad a = \sum_{i=0}^n r_i a_i$$

where the  $r_i$  are integers, all of the same sign. Let

$$C = \{x \in V : a_i(x) > 0 \ (0 \leq i \leq n)\}$$

so that  $C$  is an open  $n$ -simplex bounded by the hyperplanes  $H_{a_i}$  ( $0 \leq i \leq n$ ). The group  $W_S$  is generated by the reflections  $s_i = s_{a_i}$  ( $0 \leq i \leq n$ ), subject to the relations

$$(4.5) \quad s_i^2 = 1,$$

$$(4.6) \quad s_i s_j s_i \cdots = s_j s_i s_j \cdots$$

whenever  $i \neq j$  and  $s_i s_j$  has finite order  $m_{ij}$  in  $W_S$ , there being  $m_{ij}$  terms on either side of (4.6). In other words,  $W_S$  is a Coxeter group on the generators  $s_0, s_1, \dots, s_n$ .

The connected components of  $V - \bigcup_{a \in S} H_a$  are open simplexes, each congruent to  $C$ , and each component is of the form  $wC$  for a unique element  $w \in W_S$ . Thus, for example, when  $R$  is of type  $A_2$  we obtain the familiar tessellation of the Euclidean plane by congruent equilateral triangles.

An affine root  $a \in S$  is *positive* (resp. *negative*) relative to  $C$  if  $a(x) > 0$  (resp.  $a(x) < 0$ ) for  $x \in C$ . Equivalently,  $a \in S$  is positive or negative according as the coefficients  $r_i$  in (4.4) are all  $\geq 0$  or all  $\leq 0$ . Let  $S^+$  (resp.  $S^-$ ) denote the set of positive (resp. negative) affine roots. Then  $S^- = -S^+$ , and  $S = S^+ \cup S^-$ .

Explicitly, the positive affine roots are  $\alpha + rc$  where  $r \geq 0$  if  $\alpha \in R^+$ , and  $r \geq 1$  if  $\alpha \in R^-$ . It follows that the product  $\Delta$  (3.7) may be written in the form

$$(4.7) \quad \Delta = \prod_{a \in S^+} \frac{1 - e^a}{1 - te^a}$$

where for  $a = \alpha + rc \in S$ ,  $e^a = e^{\alpha+rc} = q^r e^\alpha$  (i. e. we define  $e^c = q$ ).

We shall now define a length function on the extended group  $W$ . If  $w \in W$ , let

$$\ell(w) = \text{card}(S^+ \cap wS^-),$$

the number of positive affine roots made negative by  $w$ . Equivalently,  $\ell(w)$  is the number of hyperplanes  $H_a, a \in S$ , that separate  $C$  from  $wC$ .

Now  $W$ , unlike  $W_S$ , is not in general a Coxeter group (unless  $P^\vee = Q^\vee$ ) and may contain elements  $\neq 1$  of length zero. Let

$$\Omega = \{w \in W : \ell(w) = 0\}$$

The elements of  $\Omega$  stabilize the simplex  $C$ , and hence permute the simple affine roots. For each  $w \in W$  there is a unique  $w' \in W_S$  such that  $wC = w'C$ , and hence  $w$  factorizes uniquely as  $w = w'v$ , with  $w' \in W_S$  and  $v \in \Omega$ . Consequently we have

$$(4.8) \quad W = W_S \rtimes \Omega$$

(semidirect product). From (4.2), (4.3) and (4.8) it follows that  $\Omega \cong W/W_S \cong P^\vee/Q^\vee$ , hence is a finite abelian group.

Next, the *braid group*  $B$  of  $W$  is the group with generators  $T(w), w \in W$ , and relations

$$T(v)T(w) = T(vw)$$

whenever  $\ell(vw) = \ell(v) + \ell(w)$ . We shall denote  $T(s_i)$  by  $T_i$  ( $0 \leq i \leq n$ ) and  $T(\omega)$  ( $\omega \in \Omega$ ) simply by  $\omega$ . Then  $B$  is generated by  $T_0, T_1, \dots, T_n$  and  $\Omega$  subject to the following relations:

(a) the counterparts of (4.6), namely the *braid relations*

$$(4.9) \quad T_i T_j T_i \cdots = T_j T_i T_j \cdots$$

where  $i \neq j$  and there are  $m_{ij}$  terms on either side;

(b) the relations

$$(4.10) \quad \omega T_i \omega^{-1} = T_j$$

for  $\omega \in \Omega$ , where  $\omega(a_i) = a_j$ .

Let  $\lambda \in (P^\vee)^+$  be a dominant weight for  $R^\vee$ , and define

$$Y^\lambda = T(\tau(\lambda))$$

where  $\tau(\lambda)$  is translation by  $\lambda$ . If  $\lambda$  and  $\mu$  are both dominant, we have

$$(4.11) \quad Y^\lambda \cdot Y^\mu = Y^{\lambda+\mu}$$

in  $B$ . If now  $\lambda$  is any element in  $P^\vee$ , we can write  $\lambda = \mu - \nu$  where  $\mu, \nu$  are both dominant, and we define

$$(4.12) \quad Y^\lambda = Y^\mu (Y^\nu)^{-1}.$$

In view of (4.10), this definition is unambiguous. The elements  $Y^\lambda, \lambda \in P^\vee$ , form a commutative subgroup of  $B$ , isomorphic to  $P^\vee$ .

## 5 THE AFFINE HECKE ALGEBRA

The *Hecke algebra*  $H$  of  $W$  is the quotient of the group algebra  $F[B]$  of the braid group by the ideal generated by the elements  $(T_i - t^{1/2})(T_i + t^{-1/2})$  ( $0 \leq i \leq n$ ). (The field  $F$  should now include  $t^{1/2}$  as well as  $q$  and  $t$ .) For each  $w \in W$ , we denote the image of  $T(w)$  in  $H$  by the same symbol  $T(w)$ : these elements form an  $F$ -basis of  $H$ . Thus  $H$  is generated over  $F$  by  $T_0, T_1, \dots, T_n$  and  $\Omega$  subject to the relations (4.9), (4.10), together with the *Hecke relations*

$$(5.1) \quad (T_i - t^{1/2})(T_i + t^{-1/2}) = 0.$$

When  $t = 1$ ,  $H$  is the group algebra of  $W$ .

The following proposition is due to Cherednik [3].

(5.2) *The Hecke algebra  $H$  acts on  $A = F[P]$  as follows:*

$$\begin{aligned} T_i e^\mu &= t^{1/2} e^{s_i \mu} + \left( t^{1/2} - t^{-1/2} \right) (1 - e^{a_i})^{-1} (e^\mu - e^{s_i \mu}), \\ \omega e^\mu &= e^{\omega \mu}. \end{aligned}$$

where  $0 \leq i \leq n$  and  $\omega \in \Omega$ . Moreover, this representation is faithful.



A proof of (5.2) is sketched in [14]. (In the formulas above, recall that  $e^{a_0} = e^{-\varphi+c} = qe^{-\varphi}$ .)

The elements  $Y^\lambda, \lambda \in P^\vee$ , span a commutative subalgebra of  $H$ , isomorphic to  $A^\vee = F[P^\vee]$ . If  $u \in A^\vee$ , say

$$u = \sum u_\lambda e^\lambda$$

let

$$u(Y) = \sum u_\lambda Y^\lambda \in H.$$

(5.3) For each  $w \in W$ , the adjoint of  $T(w)$  for the scalar product (3.9) on  $A$  is  $T(w)^{-1}$ , i. e., we have

$$(T(w)f, g) = (f, T(w)^{-1}g)$$

for all  $f, g \in A$ . In particular, the adjoint of  $Y^\lambda$  is  $Y^{-\lambda}$ , and the adjoint of  $u(Y)$ , where  $u \in A^\vee$ , is  $u^*(Y)$  (3.8).

It is enough to show that the adjoint of  $T_i$  (resp.  $\omega \in \Omega$ ) is  $T_i^{-1}$  (resp.  $\omega^{-1}$ ), and this may be verified directly from the definitions.

From (5.2) we have an action of  $A^\vee$  on  $A$ , with  $u \in A^\vee$  acting as  $u(Y)$ . One shows that  $A_0 = A^{W_0}$  is stable under the action of  $A_0^\vee = (A^\vee)^{W_0}$ , so that we have an action of  $A_0^\vee$  on  $A_0$ . It turns out (see, e.g. [16] chapter III) that this action is diagonalized by the polynomials  $P_\lambda (\lambda \in P^+)$ , and more precisely that

$$(5.4) \quad u(Y)P_\lambda = u(-\lambda - kp)P_\lambda$$

for all  $u \in A^\vee$ . The pairwise orthogonality of the  $P_\lambda$  then follows immediately from (5.3) and (5.4).

Likewise, the action of  $A^\vee$  on  $A$  can be diagonalized, and this gives rise to a family of non-symmetric orthogonal polynomials:

(5.5) There is a unique  $F$ -basis  $(E_\lambda)_{\lambda \in P}$  of  $A$  such that

$$(i) \quad E_\lambda = e^\lambda + \text{lower terms},$$

$$(ii) \quad (E_\lambda, E_\mu) = 0 \text{ if } \lambda \neq \mu.$$

(By “lower terms” is meant a linear combination of exponentials  $e^\mu$  where  $\mu < \lambda$  in a certain partial ordering on  $P$ .)

The polynomials  $E_\lambda$  are simultaneous eigenfunctions of all operators  $u(Y)$ ,  $u \in A^\vee$ . (See [19] or [16], Ch. III.)

Consider now the operators

$$U^+ = \sum_{w \in W_0} t^{\ell(w)/2} T(w),$$

$$U^- = \sum_{w \in W_0} \varepsilon(w) t^{-\ell(w)/2} T(w),$$

on  $A$ . The operator  $U^+$  maps  $A$  onto  $A_0$ , and in particular if  $\lambda \in P^+$  then  $U^+E_\lambda$  is a scalar multiple of  $P_\lambda$ .

Next consider, again for  $\lambda \in P^+$ ,

$$Q_\lambda = U^-E_\lambda.$$

If  $\lambda$  is not regular (i. e. if  $\langle \lambda, \alpha_i \rangle = 0$  for some  $i$ ) then  $Q_\lambda = 0$ .

Both  $P_\lambda$  and  $Q_\lambda$  are linear combinations of the  $E_\mu, \mu \in W_0\lambda$ , with coefficients that can be computed explicitly. Hence both  $(P_\lambda, P_\lambda)$  and  $(Q_\lambda, Q_\lambda)$  can be expressed in terms of  $(E_\lambda, E_\lambda)$ . In this way we obtain [14]

$$(5.6) \quad \frac{(Q_\lambda, Q_\lambda)}{(P_\lambda, P_\lambda)} = q^{-Nk} \prod_{\alpha \in R^+} \frac{1 - q^{\langle \lambda+kp, \alpha^\vee \rangle + k}}{1 - q^{\langle \lambda+kp, \alpha^\vee \rangle - k}}$$

where as usual  $t = q^k$ , and  $N = \text{card}(R^+)$ .

To conclude, we shall sketch a proof of Cherednik’s norm formula (3.1). The proof will be by induction on  $k$ , the cases  $k = 0$  and  $k = 1$  being trivial. From now on we shall write  $P_{\lambda,k}$  and  $Q_{\lambda,k}$  in place of  $P_\lambda$  and  $Q_\lambda$ , to stress the dependence on the parameter  $k$ , and likewise for the scalar product:  $(f, g)_k$  in place of  $(f, g)$ . Let

$$\pi_k = \prod_{\alpha \in R^+} (e^{\alpha/2} - q^{-k}e^{-\alpha/2}).$$

Then the  $P$ ’s and  $Q$ ’s are related as follows:

(5.7) *For all  $\lambda \in P^+$ , we have*

$$P_{\lambda,k+1} = \pi_k^{-1}Q_{\lambda+p,k}.$$

Taking  $\lambda = 0$ , it follows that  $Q_{p,k} = \pi_k$ . The formula (5.7) may be regarded as a generalization of Weyl’s character formula (3.5), which is the case  $k = 0$ .

From (5.7) we obtain

$$(5.8) \quad \frac{(P_{\lambda,k+1}, P_{\lambda,k+1})_{k+1}}{(Q_{\lambda+p,k}, Q_{\lambda+p,k})_k} = q^{Nk} \frac{W_0(q^{k+1})}{W_0(q^k)}.$$

Coupled with (5.6) (with  $\lambda$  replaced by  $\lambda + p$ ) this gives

$$\frac{(P_{\lambda,k+1}, P_{\lambda,k+1})_{k+1}}{(P_{\lambda+p,k}, P_{\lambda+p,k})_k} = \frac{W_0(q^{k+1})}{W_0(q^k)} \prod_{\alpha \in R^+} \frac{1 - q^{\langle \lambda+(k+1)p, \alpha^\vee \rangle + k}}{1 - q^{\langle \lambda+(k+1)p, \alpha^\vee \rangle - k}}$$

and (3.11) follows by induction on  $k$ .

For simplicity of exposition we have restricted ourselves in this survey to affine root systems of the type  $S(R)$  (4.1). The general picture is that one can attach to any irreducible affine root system  $S$ , reduced or not, families of orthogonal

polynomials  $P_\lambda, Q_\lambda$  and  $E_\lambda$  as above. These depend (apart from  $q$ ) on as many parameters  $t_i$  as there are orbits in  $S$  under the affine Weyl group  $W_S$ , and the whole theory can be developed in this more general context. For an irreducible  $S$ , the maximum number of orbits is 5, and is attained by the (non-reduced) affine root systems denoted by  $C^\vee C_n (n \geq 2)$  in the tables at the end of [11]. Correspondingly, we have orthogonal polynomials  $P_\lambda, Q_\lambda$  and  $E_\lambda$  depending on  $q$  and five parameters  $t_i$ . These  $P_\lambda$  are the orthogonal polynomials defined by Koornwinder [10], which are therefore amenable to the Hecke algebra techniques described here. A full account will (eventually) appear in the book [17].

## REFERENCES

- [1] G. E. Andrews, *Problems and prospects for basic hypergeometric functions*, in *Theory and Applications of Special Functions*, ed R. Askey, Academic Press, New York, 1975.
- [2] D. Bressoud and D. Zeilberger, *A proof of Andrews'  $q$ -Dyson conjecture*, *Discrete Math.* 54 (1985), 201–224.
- [3] I. Cherednik, *Double affine Hecke algebras and Macdonald's conjectures*, *Ann. Math.* 141 (1995), 191–216.
- [4] I. Cherednik, *Macdonald's evaluation conjectures and difference Fourier transform*, *Inv. Math.* 122 (1995), 119–145.
- [5] F. J. Dyson, *Statistical theory of the energy levels of complex systems I*, *J. Math. Phys.* 3 (1962), 140–156.
- [6] F. Garvan and G. Gonnet, *Macdonald's constant term conjectures for exceptional root systems*, *Bull AMS* 24 (1991), 343–347.
- [7] L. Habsieger, *La  $q$ -conjecture de Macdonald-Morris pour  $G_2$* , *C. R. Acad. Sci. Paris, Sér. 1, Math.* 303 (1986), 211–213.
- [8] G. J. Heckman and E. M. Opdam, *Root system and hypergeometric functions I, II*, *Comp. Math.* 64 (1987), 329–373.
- [9] K. Kadell, *A proof of the  $q$ -Macdonald-Morris conjecture for  $BC_n$* , *Memoirs of the AMS* 108 (1994).
- [10] T. H. Koornwinder, *Askey–Wilson polynomials for root systems of type  $BC$* , in *Hypergeometric functions on domains of positivity, Jack polynomials and application*, ed. D. St. P. Richards, *Contemp. Math.* 138, AMS (1992).
- [11] I. G. Macdonald, *Affine root systems and Dedekind's  $\eta$ -function*, *Inv. Math.* 15 (1972), 91–143.
- [12] I. G. Macdonald, *Some conjectures for root system*, *SIAM J. Math. Anal.* 13 (1982), 988–1007.
- [13] I. G. Macdonald, *Orthogonal polynomials associated with root systems*, preprint (1987).
- [14] I. G. Macdonald, *Affine Hecke algebras and orthogonal polynomials*, *Sém. Bourbaki* 797 (1995).
- [15] I. G. Macdonald, *Symmetric functions and Hall polynomials, 2nd edition*, Oxford University Press (1995).

- [16] I. G. Macdonald, *Symmetric functions and orthogonal polynomials*, AMS Univ. Lecture Series, 12 (1998).
- [17] I. G. Macdonald, *Affine root systems and affine Hecke algebras*, in preparation.
- [18] W. G. Morris, *Constant term identities for finite and affine root systems: conjectures and theorems*. Thesis, Madison (1982).
- [19] E. M. Opdam, *Root systems and hypergeometric functions III, IV*, Comp. Math. 67 (1988), 21–49, 191–209.
- [20] E. M. Opdam, *Some applications of hypergeometric shift operators*, Inv. Math. 98 (1989), 1–18.

I. G. Macdonald  
8 Blandford Avenue  
Oxford OX2 8DY  
U. K.



## APPLIED MATHEMATICS MEETS SIGNAL PROCESSING

STÉPHANE MALLAT

1991 Mathematics Subject Classification: Primary 11E16; Secondary 11D09, 11E04, 15A63.

Keywords and Phrases: Image compression, Markov random fields, noise removal, non linear approximations, sparse representations, wavelets.

## 1 BEYOND FOURIER

The Fourier transform has long ruled over signal processing, leaving little space for new challenging mathematics. Until the 70's, signals were mostly speech and other sounds, which were modeled as realizations of Gaussian processes. As a result, linear algorithms were considered optimal over all procedures. With a hypothesis of stationarity, we end-up restricting ourselves to the exclusive class of convolution operators that are diagonalized by the Fourier transform.

The situation has completely changed with the development of image processing in the 1980's. Images are poorly modeled by Gaussian processes, and transient structures such as edges are often more important than stationary properties. Non-linear algorithms were suddenly unavoidable, opening signal processing to modern mathematics. Beyond classical applications to transmission, coding and restoration, signal processing also entered the field of information analysis, whose main branches are speech understanding and computer vision. This interface with perception raised a rich body of new mathematical problems.

The construction of sparse representations for signals (functions), processes, and operators is at the root of many signal and information processing problems. A sparse representation characterizes an approximation with few parameters, that may be obtained from an expansion in a basis or in a more redundant "dictionary". Complex non-linear processings can often be reduced to simpler and faster algorithms over such representations. Sparse representations are also powerful tools which radiate in many branches of mathematics. At ICM'90, Coifman and Meyer gave a harmonic analysis point view, followed at ICM'94 by Daubechies and Donoho who explained the impact of wavelet bases in numerical analysis and statistics. Signal processing is now a driving force that has regrouped a community of mathematicians and engineers sharing representation techniques. Applications to signal compression, noise removal, and stochastic modeling lead us through recent developments in approximation theory, harmonic analysis, operator theory, probability, and statistics.

## 2 SPARSE REPRESENTATIONS

Sparse representations have direct applications to data compression, but are also necessary to reduce the complexity of classification and identification problems for large size signals. This section begins with an approximation theory point of view, and progresses towards signal compression.

## 2.1 IMAGE MODELS

A Bayesian view of the world interprets a signal  $f(x)$  as a realization of a process  $F(x)$  and the error of a processing is measured in expected value with respect to the probability distribution of  $F$ . Natural images are realizations of non-Gaussian processes, and there is yet no stochastic model that incorporates the diversity of complex scenes with edges and textures, such as the Image 1(a). This motivates the use of poorer but more realistic deterministic models that consider signals as functions  $f(x)$  in a subset  $\mathcal{S}$  of  $\mathbf{L}^2[0,1]^d$ , with no prior information on their probability distribution in this set. For a particular processing, one then tries to minimize the maximum error for signals in  $\mathcal{S}$ , which is the *minimax* framework. The discretization of a signal  $f$  with  $N$  samples raises no difficulty since it is equivalent to a projection in a subspace of dimension  $N$ .

Large class of images, including Image 1(a), have bounded total variation. Over  $[0,1]$  the total variation of  $f(x)$  measures the sum of the amplitudes of its oscillations

$$\|f\|_{TV} = \int |f'(x)| dx < +\infty .$$

The total variation of an image over  $[0,1]^2$  is defined by

$$\|f\|_{TV} = \iint |\vec{\nabla} f(x)| dx \leq C .$$

This norm has a simple geometrical interpretation based on the level-sets

$$\Omega_t = \{(x, y) \in \mathbb{R}^2 : f(x, y) > t\} .$$

If  $H^1(\partial\Omega_t)$  is the one-dimensional Hausdorff measure of the boundary of  $\Omega_t$  then

$$\|f\|_{TV} = \int_{-\infty}^{+\infty} H^1(\partial\Omega_t) dt. \quad (1)$$

A bounded variation model for images also incorporates a bounded amplitude

$$\mathcal{S}_{\mathbf{BV}} = \{f : \|f\|_{TV} = \iint |\vec{\nabla} f(x)| dx \leq C, \|f\|_{\infty} = \sup_{x \in [0,1]^2} |f(x)| \leq C\} . \quad (2)$$

Such images typically have level sets and thus “contours” of finite length. Although simple, this model is sufficient to illustrate the central ideas and difficulties of signal representations. More restricted classes of images, such as homogeneous textures, are better represented by Markov random fields over sparse representations, introduced in Section 4.

## 2.2 REPRESENTATIONS ARE APPROXIMATIONS

A sparse representation of  $f \in \mathbf{L}^2[0, 1]^d$  can be obtained by truncating its decomposition in an orthonormal basis  $\mathcal{B} = \{g_m\}_{m \in \mathbb{N}}$

$$f = \sum_{m=0}^{+\infty} \langle f, g_m \rangle g_m.$$

Understanding the performance of sparse representations in a basis is a central topic of approximation theory. A quick overview motivates the use of non-linear representations, but a more complete tutorial is found in [13].

A linear approximation of  $f$  from  $M$  inner products  $\langle f, g_m \rangle$  is an orthogonal projection on a space  $\mathbf{V}_M$  generated from  $M$  vectors of  $\mathcal{B}$ , say the first  $M$

$$f_M = P_{\mathbf{V}_M} f = \sum_{m=0}^{M-1} \langle f, g_m \rangle g_m.$$

The maximum approximation error over a signal set  $\mathcal{S}$  is

$$\epsilon_l(\mathcal{S}, M) = \sup_{f \in \mathcal{S}} \|f - f_M\|^2 = \sup_{f \in \mathcal{S}} \sum_{m=M}^{+\infty} |\langle f, g_m \rangle|^2.$$

Such a representation is efficient if  $\epsilon_l(\mathcal{S}, M)$  has fast decay as  $M$  decreases, and hence if  $|\langle f, g_m \rangle|$  has fast decay as  $m$  increases. This depends upon the choice of  $\mathcal{B}$  relative to  $\mathcal{S}$ . For example, uniformly regular functions are well approximated by  $M$  low-frequency vectors of a Fourier basis  $\{e^{i2\pi mx}\}_{m \in \mathbb{Z}}$  of  $\mathbf{L}^2[0, 1]$ . If  $\mathcal{S}$  is included in a ball of a Sobolev space  $\mathbf{W}^s[0, 1]$  of functions of period 1 then the decay of Fourier coefficients at high frequencies implies that  $\epsilon_l(\mathcal{S}, M) = O(M^{-2s})$  [13]. Bounded variation functions may have discontinuities, and are thus not well approximated in a Fourier basis. Using the concept of  $M$ -width introduced by Kolmogorov, one can prove that for a ball  $\mathcal{S}_{\mathbf{BV}}$  of bounded variation functions, the most rapid error decay in a basis  $\mathcal{B}$  is  $\epsilon_l(\mathcal{S}_{\mathbf{BV}}, M) \sim M^{-1}$  [13].

To improve this result, a more adaptive representation is constructed by projecting  $f$  over  $M$  basis vectors selected depending upon  $f$

$$f_M = \sum_{m \in I_M} \langle f, g_m \rangle g_m. \quad (3)$$

Since  $\|f - f_M\|^2 = \sum_{m \notin I_M} |\langle f, g_m \rangle|^2$ , the best approximation is obtained by selecting in  $I_M$  the  $M$  vectors which yield coefficients  $|\langle f, g_m \rangle|$  of maximum amplitude. This approximation depends upon  $2M$  parameters, the  $M$  indexes in  $I_M$  and the values  $\{\langle f, g_m \rangle\}_{m \in I_M}$ . Let us sort the inner products of  $f$  in decreasing order. We denote  $c_k = \langle f, g_{m_k} \rangle$  such that  $|c_k| \geq |c_{k+1}|$  for  $k \geq 1$ . The non-linear approximation error is

$$\|f - f_M\|^2 = \sum_{k=M+1}^{+\infty} |c_k|^2 \quad \text{and} \quad \epsilon_n(\mathcal{S}, M) = \sup_{f \in \mathcal{S}} \|f - f_M\|^2.$$



It depends upon the decay rate of the sorted amplitudes  $|c_k|$ . In the basis  $\mathcal{B}$ , a  $w\mathbf{P}$  ball of radius  $C$  is defined by

$$\mathcal{S}_{w\mathbf{P}} = \{f : |c_k| = |\langle f, g_{m_k} \rangle| \leq C k^{-1/p}\} . \tag{4}$$

We easily verify that  $\mathcal{S} \subset \mathcal{S}_{w\mathbf{P}}$  for some  $C > 0$  and  $p < 2$  if and only if  $\epsilon_n(\mathcal{S}, M) = O(M^{1-\frac{2}{p}})$ . The main difficulty of non-linear approximations is to find the minimum  $p$  and a corresponding basis  $\mathcal{B}$  such that  $\mathcal{S} \subset \mathcal{S}_{w\mathbf{P}}$ . Such a basis is said to be *optimal* for the non-linear approximation of  $\mathcal{S}$ . Unconditional bases are examples of optimal bases.

An orthonormal basis  $\mathcal{B}$  is an *unconditional* basis of a Banach subspace  $\mathbf{B} \subset \mathbf{L}^2[0, 1]^d$  if there exists  $A$  such that for any sign sequence  $s_m \in \{-1, 1\}$  and  $f \in \mathbf{B}$

$$\left\| \sum_{m=0}^{+\infty} s_m \langle f, g_m \rangle g_m \right\|_{\mathbf{B}} \leq A \left\| \sum_{m=0}^{+\infty} \langle f, g_m \rangle g_m \right\|_{\mathbf{B}} .$$

The fact that  $\|f\|_{\mathbf{B}} < +\infty$  can thus be characterized from the amplitudes  $|\langle f, g_m \rangle|$ , and related to a decay condition of the sorted coefficients. One can prove [13] that if  $\mathcal{B}$  is an unconditional basis of  $\mathbf{B}$  then it is an optimal basis for the non-linear approximation of a ball  $\mathcal{S} = \{f : \|f\|_{\mathbf{B}} \leq C\}$  of  $\mathbf{B}$ .

### 2.3 WAVELET ADAPTIVE GRID

Wavelet bases have important applications in mathematics and signal processing because of their ability to build sparse representations for large classes of functions. The first orthonormal wavelet bases of  $\mathbf{L}^2(\mathbb{R})$  were introduced by Strömberg and Meyer [25]. A multiresolution interpretation of wavelet bases gives a general framework for constructing nearly all wavelets that generate a wavelet basis of  $\mathbf{L}^2(\mathbb{R})$  [19]. It also leads to a fast discrete algorithm that requires  $O(N)$  calculations to compute  $N$  wavelet coefficients [22]. Daubechies [9] discovered wavelets with compact support, and the resulting bases have been adapted to  $\mathbf{L}^2[0, 1]^d$ . Her presentation at ICM'94 [10] introduces the main results, that we quickly summarize.

An orthonormal wavelet basis of  $\mathbf{L}^2[0, 1]$  is a family of functions

$$\mathcal{B} = \left( \{\phi_{l,n}\}_{0 \leq n < 2^l} \cup \{\psi_{j,n}\}_{j \geq l, 0 \leq n < 2^j} \right) .$$

At resolution  $2^l$ , the *scaling functions*  $\{\phi_{l,n}\}_{0 \leq n < 2^l}$  generate a space  $\mathbf{V}_l$  which includes all polynomials of degree  $q$ , for some  $q \geq 0$ . The wavelets  $\psi_{j,n}$  at higher resolutions  $2^j > 2^l$  are thus orthogonal to all polynomials of degree  $q$ . Wavelets  $\psi_{j,n}$  whose support lie inside  $(0, 1)$  are obtained by dilating and translating a single “mother” wavelet  $\psi$

$$\psi_{j,n}(t) = \sqrt{2^j} \psi(2^j t - n) .$$

Boundary wavelets are modified to keep the support inside  $[0, 1]$ .

A linear approximation of  $f$  from  $M = 2^J > 2^l$  wavelets and scaling functions is calculated by keeping all coefficients at resolutions  $2^j < 2^J$ :

$$f_M = \sum_{n=0}^{2^l} \langle f, \phi_{l,n} \rangle \phi_{l,n} + \sum_{j=l}^{J-1} \sum_{n=0}^{2^j} \langle f, \psi_{j,n} \rangle \psi_{j,n} .$$

The first sum provides a coarse approximation of  $f$  at resolution  $2^l$ , and each partial sum  $\sum_{n=0}^{2^j} \langle f, \psi_{j,n} \rangle \psi_{j,n}$  brings “details” that improve this approximation from resolution  $2^j$  to resolution  $2^{j+1}$ . If  $f$  is continuous, this linear approximation at resolution  $2^j$  is essentially equivalent to a uniform grid approximation calculated by interpolating the samples  $\{f(2^{-j}n)\}_{0 \leq n < 2^j}$ . Like a linear Fourier approximation, this uniform grid approximation is efficient only if  $f$  is uniformly regular. It provides poor approximations of functions with singularities, such as bounded variation functions.

A non-linear wavelet approximation keeps the  $M$  wavelet coefficients of largest amplitude. The amplitude of  $|\langle f, \psi_{j,n} \rangle|$  depends upon the local regularity of  $f$ . Suppose that the mother wavelet  $\psi$  is  $\mathbf{C}^{q+1}$  and orthogonal to polynomials of degree  $q$ . One can prove [25] that  $f$  is uniformly Lipschitz  $\alpha < q + 1$  over an interval  $[a, b]$  if and only if there exists  $A > 0$  such that for all  $\psi_{j,n}$  whose support are included in  $[a, b]$  (modulo boundary issues)

$$|\langle f, \psi_{j,n} \rangle| \leq A 2^{-(\alpha+1/2)j} .$$

In the domains where the Lipschitz regularity  $\alpha$  is large,  $|\langle f, \psi_{j,n} \rangle|$  decays quickly as the resolution  $2^j$  increases. At high resolution  $2^j$ , large coefficients appear in the neighborhood of singularities, where  $0 \leq \alpha < 1$ . More wavelet coefficients are kept in the neighborhood of singularities, so a non-linear wavelet approximation is equivalent to an adaptive grid whose resolution is refined in the neighborhood of singularities.

The impact of wavelet bases in functional analysis comes from the fact that they are unconditional bases of a large family of smoothness spaces (Besov spaces) [25], and are thus optimal for non-linear approximations in balls of these spaces. Although the space  $\mathbf{BV}$  of bounded variation functions admits no unconditional basis, it can be embedded in two Besov spaces. This allows one to prove that wavelet bases are optimal to approximate a ball  $\mathcal{S}_{\mathbf{BV}}$  of bounded variation functions. A ball  $\mathcal{S}_{\mathbf{BV}}$  is included in a  $w\mathbf{P}$  ball (4) for  $p = 2/3$  but not for  $p < 2/3$  [12]. Hence  $\epsilon_n(\mathcal{S}_{\mathbf{BV}}, M) = O(M^{1-2/p}) = O(M^{-2})$ . When  $M$  increases, the asymptotic decay of  $\epsilon_n(\mathcal{S}_{\mathbf{BV}}, M)$  is thus faster than any linear approximation using  $M$  parameters, which decays at most like  $M^{-1}$ .

In two dimensions, wavelet bases are constructed with three “mother” wavelets  $\psi^k$  for  $1 \leq k \leq 3$ , which are dilated and translated

$$\psi_{j,n}^k(x_1, x_2) = \psi_{j,n}^k(x) = 2^j \psi^k(2^j x_1 - n_1, 2^j x_2 - n_2) .$$

Appropriate modifications are made at the boundary so that supports stay in  $[0, 1]^2$ . A wavelet  $\psi_{j,n}^k$  has a square support of size proportional to  $2^{-j}$ , and centered near  $2^{-j}n = (2^{-j}n_1, 2^{-j}n_2)$ . An orthonormal wavelet basis of  $\mathbf{L}^2[0, 1]^2$  is obtained by adding orthonormal scaling functions that define a lower resolution space

$$\mathcal{B} = \left( \{\phi_{l,n}\}_{2^{-l}n \in [0,1]^2} \cup \{\psi_{j,n}^k\}_{j \geq l, 2^{-j}n \in [0,1]^2, 1 \leq k \leq 3} \right) . \quad (5)$$

A discrete image is a square array of  $N^2$  points (pixels), with  $N = 512$  in Image 1(a). The wavelet basis (5) can be discretized to define an orthonormal basis

of images of  $N^2$  pixels. The wavelet coefficients of the image 1(a) are shown in 1(b). Each sub-image gives the values of  $\{|\langle f, \psi_{j,n}^k \rangle|\}_{2^{-j}n \in [0,1)^2}$  for a fixed  $j$  and a fixed  $k$ . The number of wavelet coefficients in each sub-image is  $2^{2j}$ . White and black points correspond respectively to nearly zero or large coefficients  $|\langle f, \psi_{j,n}^k \rangle|$ . These sub-images go by triplets corresponding to the index  $1 \leq k \leq 3$ . The wavelets for  $k = 1, 2, 3$  are sensitive to image variations along different orientations. Most points are white, meaning that the majority of wavelet coefficients are nearly zero. The few large ones are located in the domains where the image intensity has a sharp variation due to an “edge” or a “texture”.

(a) (b)

Figure 1: (a): Original image  $f$ . (b): Amplitude of coefficients  $|\langle f, \psi_{j,n}^k \rangle|$  in a wavelet orthonormal basis. Each sub-image corresponds to a different resolution  $2^j$  and different orientation  $k$  (see text).

A linear approximation from  $M = 2^{2J}$  wavelets is calculated by keeping all coefficients at resolutions  $2^j < 2^J$ . This uniform grid approximation is particularly ineffective for images including discontinuities. For a ball of bounded variation images (2), one can prove that  $\epsilon_l(\mathcal{S}_{\mathbf{BV}}, M) = A > 0$ . The maximum approximation error does not decay to zero as  $M$  increases.

Non-linear approximations are much more effective because they keep wavelet coefficients near the singularities and (1) indicates that the lengths of “edges” remains finite. More formally, one can prove that  $\mathcal{S}_{\mathbf{BV}}$  is included in a  $w^1$  ball [4] and as a consequence  $\epsilon_n(\mathcal{S}_{\mathbf{BV}}, M) = O(M^{-1})$ . The wavelet adaptive grid gives much better image approximation than a uniform grid, and no other orthonormal basis can improve the approximation rate of an orthonormal wavelet basis.

## 2.4 SIGNAL COMPRESSION

Economic storage and fast transmission of large signals through channels of limited bandwidth (such as Internet) are major applications of signal compression. Coding efficiently a signal with as few bits as possible requires to build a sparse representation. Signal processing engineers did not wait for a mathematical analysis of non-linear approximations in order to develop compressed audio or image codes in orthonormal bases. The first wavelet image coder was implemented in 1986 [34], before wavelet orthonormal bases had truly been studied in mathematics. The fast

orthogonal wavelet transform is indeed computed with a “filter bank” algorithm, which was initially introduced in signal processing to *multiplex* signals (aggregate several signals into one) [7]. A discrete filter bank theory has been developed in signal processing [33], but only later the connection with wavelet orthonormal bases was established [19]. Although the mathematics came late, analyzing the performance of image coders requires use of recent approximation theory results, and these open directions for potential improvements.

The signals in  $\mathcal{S}$  are now discretized and approximated at resolution  $N$ , which means that they belong to a space of dimension  $N$ . A *transform code* decomposes  $f$  in an orthonormal basis  $\mathcal{B} = \{g_m\}_{0 \leq m < N}$

$$f = \sum_{m=0}^{N-1} \langle f, g_m \rangle g_m,$$

and approximates each coefficient  $\langle f, g_m \rangle$  with a *quantized value*, which is coded with as few bits as possible. A uniform quantizer with *bin size*  $\Delta$  approximates  $x \in \mathbb{R}$  by  $Q(x) = k\Delta$  with  $k \in \mathbb{Z}$  and  $|x - Q(x)| \leq \Delta/2$ . The resulting quantized signal is

$$\tilde{f} = \sum_{m=0}^{N-1} Q(\langle f, g_m \rangle) g_m.$$

The problem is to minimize the maximum *distortion*  $d(\mathcal{S}, R) = \sup_{f \in \mathcal{S}} \|f - \tilde{f}\|^2$  for a maximum number of bits  $R$  allocated to code  $\tilde{f}$ .

(a)

(b)

Figure 2: (a): Image coded with 0.25 bits/pixel, by quantizing the wavelet coefficients of the original image displayed in Figure 1. (b): Image coded with 0.125 bits/pixel.

The distortion of a transform code is first related to a non-linear approximation. Let  $M$  be the number of coefficients above  $\Delta/2$  and  $f_M$  the non-linear approximation of  $f$  from these  $M$  largest coefficients

$$f_M = \sum_{|\langle f, g_m \rangle| > \Delta/2} \langle f, g_m \rangle g_m.$$

Since  $Q(x) = 0$  when  $|x| < \Delta/2$ , and  $|x - Q(x)| \leq \Delta/2$ , the distortion is

$$d(f, R) = \|f - \tilde{f}\|^2 \leq \|f - f_M\|^2 + M \frac{\Delta^2}{4}. \quad (6)$$

This connects us with non-linear approximations. Suppose that  $\mathcal{S}$  is in a  $w\mathbb{P}$  ball  $\mathcal{S}_{w\mathbb{P}}$  (4) of radius  $C$ , with  $p < 2$ . Denote by  $M_0 = C^p(\Delta/2)^{-p}$ . Since  $|c_k| = |\langle f, g_{m_k} \rangle| \leq C k^{-1/p}$ , necessarily  $M \leq M_0$ . We also verify that

$$d(\mathcal{S}, R) = \sup_{f \in \mathcal{S}} d(f, R) \leq \sup_{f \in \mathcal{S}} \|f - f_{M_0}\|^2 + M_0 \frac{\Delta^2}{4} = O(M_0^{-2/p+1}). \quad (7)$$

The total distortion is thus driven by the non-linear approximation error.

To optimize the transform code, we must minimize the maximum number of bits  $R$  required to code the  $N$  values  $\{Q(\langle f, g_m \rangle)\}_{0 \leq m < N}$  for  $f \in \mathcal{S}$ . For high compression rates  $N \gg M_0 \geq M$ , in which case a large proportion  $\frac{N-M}{N}$  of coefficients quantized to zero. An *entropy code* takes advantage of this, by allocating fewer bits to code coefficients that occur more frequently than others. Knowing that  $\mathcal{S} \subset \mathcal{S}_{w\mathbb{P}}$ , one can construct an arithmetic code which requires a maximum number of bits  $R \sim M_0 \log_2 \frac{M_0}{N}$  [22]. We thus derive from (7) that  $d(\mathcal{S}, R) = O(R^{1-2/q})$  for any  $q > p$ .

The decay rate of  $d(\mathcal{S}, R)$  is maximized in a basis  $\mathcal{B}$  which is optimal for non-linear approximations in  $\mathcal{S}$ , because it minimizes the exponent  $p$  such that  $\mathcal{S} \subset \mathcal{S}_{w\mathbb{P}}$ . In particular, wavelet bases are optimal for bounded variation images and the minimum is  $p = 1$ . The Figures 2(a,b) are compressed images  $\tilde{f}$  calculated by quantizing the wavelet coefficients in Figure 1(b). They are coded respectively with  $\frac{R}{N} = 0.25$  bits/pixel and 0.125 bits/pixel, with an optimized coder for zero coefficients [30]. The original image 1(a) is coded with 8 bits/pixel, so this corresponds to compression factors of 32 and 64. For 0.25 bits/pixel, the distortions are hardly visible but become apparent for 0.125 bits/pixel.

Let us emphasize that the choice of basis depends entirely on the nature of the signals in  $\mathcal{S}$ . For sounds, totally different bases must be chosen in order to approximate efficiently complex oscillatory waveforms of varying durations. Figure 3 shows the recording of the word “greasy”. Current compression audio standard for Compact Disk quality, such as the AC-system of Dolby, are calculated in bases that are similar to a local cosine basis. Such a basis is constructed with an even function  $w(t)$ , called a *window*, which has a support  $[-2l, 2l]$  and is translated to cover the real axis uniformly:

$$\sum_{p=-\infty}^{+\infty} |w(t - pl)|^2 = 1.$$

Malvar [23], Coifman and Meyer [5] proved that if further symmetry properties are imposed on  $w(t)$  then multiplications by cosine functions yield an orthonormal basis of  $\mathbf{L}^2(\mathbb{R})$

$$\left\{ g_{p,k}(t) = \frac{1}{\sqrt{l}} w(t - pl) \cos\left(\pi k (l^{-1}t - p)\right) \right\}_{k \in \mathbb{N}, p \in \mathbb{Z}}. \quad (8)$$

As in the image case, the performance of an audio code in this basis depends on being able to approximate the recorded sound with few local cosine vectors. However, the most relevant audio distortions measures are not  $L^2$  norms. Sophisticated masking techniques are used by engineers to introduce quantization errors which are below our hearing sensitivity threshold [22], and above our mathematical understanding.

Figure 3: Speech recording of the word “greasy” sampled at 16kHz.

## 2.5 GEOMETRY AND MORE ADAPTIVITY

Wavelet bases are optimal for representing general bounded variation images, but better approximations can be obtained by taking advantage of the geometrical regularity of most images. The total variation formula (1) shows that the level sets of bounded variation images typically have a finite length. However, this imposes no condition on the regularity of these level sets. In the Image 1(a), the “contours” are mostly piecewise regular geometrical curves in the image plane, with small curvature at most locations. Understanding how to take advantage of this regularity is fundamental for image processing. This has motivated the use of non-linear partial differential equations to modify the curvature of level sets in images [1, 28, 31]. This important new branch of mathematical image processing leads to interesting applications for noise removal and image segmentation. Yet, we shall not follow this line of thought, which is not based on explicit sparse representations.

To understand the importance of geometrical regularity, let us consider a simple “image”  $f = \mathbf{1}_\Omega$ , which is the indicator function of a set  $\Omega$ . The boundary  $\partial\Omega$  of  $\Omega$  is a differentiable curve of finite length with bounded curvature. If the square support of  $\psi_{j,n}^k$  does not intersect  $\partial\Omega$  then  $\langle f, \psi_{j,n}^k \rangle = 0$ . The wavelets  $\psi_{j,n}^k$  are translated on a square grid with step sizes  $2^{-j}$  and have square support proportional to  $2^{-j}$ , as illustrated in Figure 4(a). At resolution  $2^j$ , there are  $O(2^j)$  wavelets  $\psi_{j,n}^k$  whose supports intersect  $\partial\Omega$ . The  $M$  larger amplitude wavelet coefficients selected by a non-linear approximation are at resolutions  $2^j \leq 2^J \sim M$  and the non-selected wavelets produce an error  $\|f - f_M\|^2 \sim M^{-2}$ , like for any bounded variation image.

A better piecewise linear approximation is calculated with an adaptive triangulation of  $[0, 1]^2$  having  $M$  triangles [16]. Since the curvature of  $\partial\Omega$  is bounded, this boundary can be covered by  $M/2$  triangles, which have a narrow width proportional to  $M^{-2}$  along the normal to  $\partial\Omega$ , and which are elongated along the tangent to  $\partial\Omega$ . The interior and exterior of  $\Omega$  are covered by  $M/2$  larger triangles, as illustrated in Figure 4(b). A function  $f_M$  which is linear on each triangle can

(a) (b)

Figure 4: (a): Wavelets  $\psi_{j,n}$  are translated on a square grid of interval  $2^{-j}$ , and have a square support proportional to  $2^{-j}$ . For  $f = \mathbf{1}_\Omega$ , the darker points locate the wavelets  $\psi_{j,n}$  such that  $\langle f, \psi_{j,n} \rangle \neq 0$ . (b): A piecewise linear approximation of  $f = \mathbf{1}_\Omega$  is optimized by choosing narrow triangles that are elongated along the boundary where  $f$  is discontinuous.

approximate  $f = \mathbf{1}_\Omega$  with  $\|f - f_M\|^2 = O(M^{-4})$ . The approximation error is concentrated on the triangles along the border and the small width of these triangles yields a smaller error than with wavelets of square support. The error is reduced because the triangles are adapted to the geometry of  $\partial\Omega$ .

Building a bridge between geometrical constraints and adaptive approximations is a fundamental issue for image processing. The human visual system takes great notice of geometrical “features” such as “corners” or the regularity of “edges” [24, 26]. The Kanizsa illusion shown in Figure 5 illustrates this fact. We perceive a triangular “edge” although the image has no grey level variation in the center. Such illusions are explained by imposing geometrical constraints on the interpretation (models) of images. It is also known [11] that *simple cells* in the visual cortex perform an image decomposition over a family of functions that have close similarities to wavelets, but which is more redundant than a basis and thus offers more flexibility. This indicates that our brain constantly crosses this bridge between functional analysis and geometry.

(a) (b)

Figure 5: The illusory edges of a straight and of a curved triangle are perceived in domains where the images are uniformly white.

Adapting to geometry in images can be interpreted as a particular instance of

a more general adaptive approximation problem. A basis is a complete family in our functional space, but it is often too small to fully utilize all of the structures included in complex signals. More precise approximations are obtained with  $M$  vectors selected from a much larger dictionary  $\mathcal{D} = \{g_\gamma\}_{\gamma \in \Gamma}$ , that may include an infinite number of bases. This follows the same idea that motivates someone to enlarge his vocabulary to build more concise and precise sentences. For recognition, is also often important to construct representations that have invariant properties, with respect to translation or affine transformations. This imposes some further conditions on the dictionary [20]. A dictionary for images can be constructed with wavelets whose supports have a parameterized elongation and an arbitrary orientation. Like the elongated triangles in Figure 4(b), the chosen wavelets can be adapted to the geometry of the level sets in the image. Audio signals are also more efficiently approximated with a dictionary of local cosine vectors such as (8), but where the window length  $l$  may be freely adapted to the duration of waveforms produced by attacks, harmonics or other transient events.

An adaptive representation is constructed from a dictionary  $\mathcal{D}$  by selecting  $M$  vectors  $\{g_{\gamma_k}\}_{1 \leq k \leq M}$  to approximate  $f$  with a partial sum

$$f_M = \sum_{k=1}^M \alpha_k g_{\gamma_k} .$$

In the absence of orthogonality, finding the  $M$  vectors that minimize  $\|f - f_M\|$  leads to a combinatorial explosion. Greedy pursuit algorithms have been developed to avoid this explosion [20], by selecting the vectors  $g_{\gamma_k}$  one by one from the dictionary, but their approximation performance is far from optimal [3, 13]. In structured dictionaries composed of orthonormal bases embedded in a tree, Coifman and Wickerhauser [6] have introduced dynamical programming algorithm that selects  $M$  vectors which define a “reasonable” but non optimal approximation. There is yet no approximation theory that can analyze the performance of these highly non-linear approximations and improve their performance.

Let us finally mention that enlarging the dictionary has a cost. In a larger dictionary, more parameters are needed to characterize the index  $\gamma_k$  of each selected vector. For a fixed approximation error, making the dictionary too large can increase the total number of parameters that characterize the signal approximation  $f_M$ . Finding dictionaries of optimal size is thus another open issue.

### 3 NOISE REMOVAL BY THRESHOLDING

The removal of noise, added when measuring the signal or during its transmission, is an important problem where sparse representations play a crucial role. In a basis that transforms the signal into few large amplitude values plus a small remainder, most of the noise is easily suppressed by a thresholding which sets to zero the smallest coefficients. A similar version of this simple idea has been used to remove noise from television images since the 1960’s. However, it is only recently that Donoho and Johnstone [14] were able to develop the mathematics proving that



thresholding estimators are nearly optimal in sparse representations, which opened new signal processing applications.

A discrete approximation of  $f(x)$  defined over  $[0, 1]^d$  is characterized by  $N$  coefficients, denoted  $f[n]$ , for  $0 \leq n < N$ . The measured noisy data are

$$D[n] = f[n] + W[n], \quad (9)$$

where the noise values  $W[n]$  are modeled by independent Gaussian random variables, and thus define a *white noise*. Figure 6(a) gives an example. An estimator  $F$  of  $f$  is calculated by applying an operator  $L$  on the data,  $F = LD$ . The risk of this estimation is

$$r(L, f) = \mathbb{E}\{\|f - LD\|^2\}.$$

We want to minimize the maximum risk over a signal set  $\mathcal{S}$

$$r(L, \mathcal{S}) = \sup_{f \in \mathcal{S}} r(L, f).$$

The goal is to find an operator  $L$  which approaches the optimal minimax risk

$$r_o(\mathcal{S}) = \inf_{All L} r(L, \mathcal{S}).$$

There is a considerable body of literature in mathematical statistics for evaluation of minimax risk [15].

A new approach to minimax estimation is to separate the representation from the estimation problem. The first step is to construct an appropriate representation by decomposing  $D = f + W$  in an orthogonal basis  $\mathcal{B} = \{g_m\}_{0 \leq m < N}$ :

$$\langle D, g_m \rangle = \langle f, g_m \rangle + \langle W, g_m \rangle.$$

A thresholding estimator is then simply defined by

$$F = L_t D = \sum_{m=0}^{N-1} \theta_T(\langle D, g_m \rangle) g_m, \quad (10)$$

where  $\theta_T(x) = x \mathbf{1}_{|x| > T}$ . It sets to zero all coefficients below  $T$  and keeps the others. The threshold  $T$  is chosen to be just above  $\max_{0 \leq m < N} |\langle W, g_m \rangle|$ , with a high probability, so that  $\theta_T(\langle D, g_m \rangle) = 0$  if  $\langle f, g_m \rangle \approx 0$ .

Since  $W$  is a Gaussian white noise of variance  $\sigma^2$ , in any basis  $\mathcal{B}$ , the noise coefficients  $\langle W, g_m \rangle$  are independent Gaussian random variables of same variance  $\sigma^2$ . Let  $M$  be the number of coefficients such that  $|\langle f, g_m \rangle| \geq \sigma$ , and  $f_M$  be the non-linear approximation (3) of  $f$  from these  $M$  largest vectors. If  $T = \sigma \sqrt{2 \log_e N}$  then Donoho and Johnstone proved [14] that

$$r(L_t, f) \leq (2 \log_e N + 1) \left( \|f - f_M\|^2 + (M + 1) \sigma^2 \right).$$

The right part of the upper bound is similar to the distortion (6) of a transform code. The risk is thus reduced by choosing a basis where there is a small number

(a) (b)

Figure 6: (a): Image contaminated by an additive Gaussian white noise. (b): Thresholding estimation calculated in a wavelet basis.

$M$  of large amplitude coefficients above  $\sigma$ , which yield a small approximation error  $\|f - f_M\|$ . Once more we face the problem of finding a sparse but precise representation. Figure 6(b) is an estimation calculated by thresholding the wavelet coefficients of the noisy image shown in (a).

The asymptotic performance of thresholding estimators is calculated as the resolution  $N$  of the measurements increases to  $+\infty$ . For a given set  $\mathcal{S}_0$  of signals  $f(x)$ , we look for an orthonormal basis  $\mathcal{B}_0$  which is optimal for non-linear approximations. Suppose that  $\mathcal{S}_0$  is a ball of a space  $\mathbf{B}$ , then we can choose  $\mathcal{B}_0$  to be an unconditional basis of  $\mathbf{B}$ . The set  $\mathcal{S}$  of discretized signals is obtained with a projection in dimension  $N$ . These signals are decomposed in the basis  $\mathcal{B}$  derived from  $\mathcal{B}_0$  through the same projection. As  $N$  increases, one can prove [15] that the thresholding estimator is nearly optimal in the sense that

$$r(L_t, \mathcal{S}) \leq O(\log N) r_o(\mathcal{S}) . \quad (11)$$

This result applies to discretized signals from Besov spaces, decomposed in a discrete wavelet basis. It is also valid for a set  $\mathcal{S}_{\mathbf{BV}}$  of bounded variation signals decomposed in a wavelet basis, because  $\mathbf{BV}$  is embedded in two Besov spaces which are close enough. In this case, the thresholding risk has faster asymptotic decay than the risk of any linear estimator as  $N$  increases.

The efficiency of thresholding estimators depends crucially on the approximation performance of the representation. To take advantage of complex signal structures, such as the geometrical regularity of some images, the thresholding must be calculated in more adaptive representations, as explained in Section 2.5. However, the minimax optimality of these highly adaptive estimators remains to be understood.

#### 4 SPARSE INTERACTION PROCESSES

In many classification problems, including speech recognition and visual texture discrimination, the observed signal is modeled as the realization of a process that

we need to characterize. This is difficult because the underlying process is often non Gaussian or non-stationary, and a single realization provides little data to identify it. It is therefore necessary to characterize these processes with few parameters in an appropriate representation, that can be estimated and used for the classification. After studying non stationary Gaussian processes, we consider more general Markov random field models.

#### 4.1 NON STATIONARY GAUSSIAN PROCESSES

Gaussians processes provide resonable models for large class of signals, including speech recordings. A zero-mean Gaussian process  $X(t)$  for  $t \in \mathbb{R}$  is entirely characterized by its covariance  $k(t, s) = \mathbf{E}\{X(t)X(s)\}$ , which is the kernel of the covariance operator  $K$ :

$$Kf(t) = \int_{-\infty}^{+\infty} k(t, s) f(s) ds. \quad (12)$$

To estimate this covariance from few realizations, it is necessary to reduce the number of coefficients describing the kernel. This can be done by finding an orthonormal basis  $\mathcal{B} = \{g_m\}_{m \in \mathbb{Z}}$  in which the matrix coefficients

$$\langle Kg_m, g_n \rangle = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} k(t, s) g_m(s) g_n(t) ds dt \quad (13)$$

have fast off-diagonal decay. These matrix values are the decomposition coefficients of the kernel  $k(t, s)$  in a separable orthonormal basis  $\{g_n(t)g_m(s)\}_{(n,m) \in \mathbb{Z}^2}$  of  $\mathbf{L}^2(\mathbb{R}^2)$ . Finding a sparse matrix representation is thus equivalent to approximating  $k(t, s)$  with few non-zero coefficients in a separable basis. If the matrix coefficients have a sufficiently fast off-diagonal decay, then  $K$  is closely approximated (with a sup or a Hilbert Schmidt norm) by a narrow band matrix  $\tilde{K}$  in  $\mathcal{B}$ , which is the covariance of a Gaussian process  $\tilde{X}$  that approximates  $X$  [21]. Since  $\tilde{K}$  has a band-matrix representation, for each  $m \in \mathbb{N}$  there exists a neighborhood  $\mathcal{N}_m$  which is a finite set of integers such that if  $n \notin \mathcal{N}_m$  then

$$\langle \tilde{K}g_m, g_n \rangle = \mathbf{E}\{\langle \tilde{X}, g_m \rangle \langle \tilde{X}, g_n \rangle\} = 0.$$

Since  $\langle \tilde{X}, g_m \rangle$  and  $\langle \tilde{X}, g_n \rangle$  are jointly Gaussian random variables, they are independent because uncorrelated. The model  $\tilde{X}$  of  $X$  has therefore a representation in  $\mathcal{B}$  with coefficients that are dependent only in small neighborhoods, which is a particular case of Markov random field.

Writing the covariance operator  $K$  as a pseudo-differential operators is a powerful approach to find bases where the matrix coefficients have fast off-diagonal decay [25]. Let  $\hat{f}(\omega) = \int_{-\infty}^{+\infty} f(s) e^{-i\omega s} ds$  be the Fourier transform of  $f$ . The *symbol* of the operator  $K$  is

$$\beta(t, \omega) = p.v. \int_{-\infty}^{+\infty} k(t, t-s) e^{-i\omega s} ds.$$

Applying the Parseval formula to (12) yields

$$Kf(t) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \beta(t, \omega) \hat{f}(\omega) e^{i\omega t} d\omega.$$

For example, if  $\beta(t, \omega) = \sum_{p=0}^P a_p(t) (i\omega)^p$  then  $K = \sum_{p=0}^P a_p(t) (\frac{d}{dt})^p$  is a differential operator with time varying coefficients. The process  $X$  is stationary if  $k(t, s) = k(t - s)$ , in which case  $\beta(t, \omega) = \beta(\omega)$  is the spectrum of  $K$ . The Fourier transform is therefore an ideal tool to characterize stationary Gaussian processes. For non-stationary processes, one needs to relate the properties of  $X(t)$  to the properties of  $\beta(t, \omega)$ , and derive a basis where  $K$  is approximated by a narrow band matrix.

Locally stationary processes  $X(t)$  appear in many physical systems in which the mechanisms that produce random fluctuations change slowly in time or space [29]. Over short time intervals  $l$ , such processes can be approximated by a stationary one. This is the case for many components of speech or audio signals. Over a sufficiently short time interval, the throat behaves like a steady resonator which is excited by a stationary noise source. A simple class of locally stationary processes is obtained by imposing that there exists  $A > 0$  such that for all  $k, j \geq 0$

$$|\partial_t^k \partial_\omega^j \beta(t, \omega)| \leq A l^{j-k}.$$

We derive [21] the existence of a local cosine basis (8) in which the operator  $K$  is closely approximated by a narrow band matrix. The size  $l$  of each window is adapted to the interval of stationarity. When the length  $l(t)$  of the interval of stationarity varies strongly in time, which is the case of audio signals, the resulting covariance operator has more complex properties and often does not belong to a classical family of pseudo-differential operators. Depending upon the regularity of  $l(t)$ , adapted local cosine bases can still provide sparse representations of such operators [21].

Multifractals provide useful models for signals having some self-similarity properties [27]. Among the many examples, let us mention economic records like the Dow Jones industrial average, physiological data including heart records, electromagnetic fluctuations in galactic radiation noise, some image textures, variations of traffic flow... A fractional Brownian motion  $X(t)$  of Hurst exponent  $H$  is a canonical example of fractal Gaussian processes, whose increments are stationary and which is self-similar in the sense that  $s^{-H}X(st)$  has the same probability distribution as  $X(t)$ , for all  $s > 0$ . The symbol of the covariance  $K$  of  $X$  is  $\beta(t, \omega) = \lambda |\omega|^{-2H-1}$ . This corresponds to a Calderón-Zygmund operator of the first generation [25], which is known to have fast off-diagonal decay in a wavelet basis. In signal processing, fractional Brownian motions are often approximated by a process  $\tilde{X}$  whose covariance  $\tilde{K}$  is diagonal in a wavelet basis, which leads to fast synthesis algorithms [27]. General conditions on  $\partial_t^k \partial_\omega^j \beta(t, \omega)$  can be established to guarantee that  $K$  has fast off-diagonal decay in a wavelet basis [2]. Multifractal Brownian motions are examples with Hurst exponents that vary in time:  $\beta(t, \omega) = \beta_0(t) |\omega|^{-2H(t)-1}$ . Accurate estimations of  $\beta_0(t)$  and  $H(t)$  are obtained in wavelet bases.

When the process is uniformly locally stationary or multifractal, the basis which compresses the covariance matrix is known beforehand. For more complex non-stationary processes, this basis must also be estimated, given some prior information. This is an adaptive approximation problem, similar to the ones described in Section 2.5, although we approximate operators as opposed to functions. Best basis search algorithms have been introduced to perform such adaptive approximation of covariance operators [21], but these techniques are still in their infancy, and more work is needed to understand the properties of the resulting statistical estimators.

## 4.2 MARKOV RANDOM FIELDS IN SPARSE REPRESENTATIONS

The characterization and synthesis of visual textures is one of the most challenging low-level vision problem. Homogeneous visual textures such as images of woods, carpets or marbles, can be considered as stationary, but they are not Gaussian. Figure 7 gives two examples. It is necessary to model these processes with few parameters to hope identify them from a single realization. This is feasible since the human visual system can do it. The importance of this problem goes well beyond texture discrimination. Indeed, providing a general framework to model non-Gaussian processes is necessary to analyze the properties of various classes of signals such as financial time series or the velocity of turbulent fluids.

Markov random field models of textures have been proposed by Cross and Jain [8], but such models became computationally and mathematically attractive through the work of Geman and Geman [17], who introduced a stochastic relaxation algorithm for sampling Gibbs distributions. To simplify the presentation, we restrict ourselves to a random vector  $X(n)$ , where  $n \in \mathbb{Z}^d$  varies over a grid  $\mathcal{G}$  of size  $N$ . We define a neighborhood system  $\mathcal{N} = \{\mathcal{N}_n\}_{n \in \mathcal{G}}$  such that  $n \notin \mathcal{N}_n$  and  $m \in \mathcal{N}_n$  if and only if  $n \in \mathcal{N}_m$ . For any  $\mathcal{G}_0 \subset \mathcal{G}$ , let  $X(\mathcal{G}_0)$  denote the set of values taken by  $X$  over  $\mathcal{G}_0$ . We say that  $p(X)$  is a *Markov random field* distribution with respect to  $\mathcal{N}$  if

$$p\left(X(n) \mid X(\mathcal{G} - \{n\})\right) = p\left(X(n) \mid X(\mathcal{N}_n)\right).$$

A subset  $C$  of  $\mathcal{G}$  is called a clique if every pair of elements in  $C$  are neighbors of each other. Let  $\mathcal{C}$  be the set of all cliques. If  $X$  takes its values in a finite alphabet then the Hammersley-Clifford theorem proves that  $p(X)$  is a Markov random field if and only if it can be written as a *Gibbs distribution* with respect to  $\mathcal{N}$

$$p(X) = \frac{1}{Z} \exp\left[-\sum_{C \in \mathcal{C}} \phi_C(X)\right],$$

where  $Z$  is a normalization constant and  $\phi_C$  is a *potential function* which depends only of the values of  $X$  in the clique  $C$ . Markov random field models have interesting applications to texture discrimination and image restoration, but limited success due to the difficulty to incorporate the long range interactions of image pixels. Several approaches have been introduced to circumvent this problem, including renormalization techniques [18].

Mumford and Zhu [35] introduced a different point of view by creating Markov random field models on a sparse representation of  $X$ , rather than on the sample values  $X(n)$ . Let  $\mathcal{D} = \{g_\gamma\}_{\gamma \in \Gamma}$  be a dictionary of vectors, which can be an orthogonal basis or be more redundant. Let  $X_\gamma = \langle X, g_\gamma \rangle$ . A neighborhood system  $\mathcal{N} = \{\mathcal{N}_\gamma\}_{\gamma \in \Gamma}$  is defined over  $\Gamma$ . For example, if  $\mathcal{D} = \{\psi_{j,n}^k\}_{k,j,n}$  is a wavelet basis in two dimensions, the index  $\gamma = (k, j, n)$  specifies the orientation  $k$ , the resolution  $2^j$  and the position  $2^{-j}n$  of the wavelet. The neighborhood  $\mathcal{N}_{(k,j,n)}$  includes wavelets  $\psi_{j',n'}^{k'}$  with  $|j - j'| \leq 1$  and a position  $2^{-j'}n'$  which is close to  $2^{-j}n$ . The multiresolution aspect of wavelet bases allows one to construct Markov random field models that incorporate short range and long range interactions.

To construct a Markov random field model  $X$  from observed signals  $\{X_p^{obs}\}_{0 \leq p < P}$ , we compute average measurements over  $M$  cliques  $\{C_m\}_{0 \leq m < M}$  with potential functions  $\phi_{C_m}$

$$\mu_{C_m}^{obs} = \frac{1}{P} \sum_{p=1}^P \phi_{C_m}(X_p^{obs}) .$$

If  $X$  is stationary then a spatial averaging is done over all  $\phi_{C_m}$  that perform identical calculations but at translated locations. These empirical averages are estimates of  $E\{\phi_{C_m}(X)\}$  for the model  $X$  that we construct. Most often, the cliques have at most two elements  $C = \{\gamma, \gamma'\}$ . Covariance measurements correspond to  $\phi_C(X) = X_\gamma X_{\gamma'}$ . However, different potential functions may be useful such as  $p^{th}$  order moments

$$\phi_C(X) = |X_\gamma|^p |X_{\gamma'}|^p \quad \text{for } p > 0 . \tag{14}$$

(a) (b) (c) (d)

Figure 7: (a): Observation of a uniform texture. (b): Realization of the wavelet Markov random field model calculated from (a). (c): The center shows an example of texture. (d): The center is identical to (c) whereas the periphery is a realization of a wavelet Markov random field model calculated from (c).

The *maximum entropy principle* suggests choosing  $p(X)$  that achieves the maximum entropy

$$p(X) = \arg \max \left\{ - \int p(X) \log p(X) dX \right\} .$$

under the constraints

$$E\{\phi_{C_m}(X)\} = \int \phi_{C_m}(X) p(X) dX = \mu_{C_m}^{obs} \quad \text{for } 1 \leq m \leq M . \tag{15}$$

By maximizing the entropy, the resulting  $p(X)$  is the “most uniform” distribution given the prior knowledge provided by the observation  $\mu_{C_m}^{obs}$ . It thus does not include more “information” than what is available. The solution is calculated with Lagrange multipliers

$$p(X, \Lambda) = \frac{1}{Z(\Lambda)} \exp \left( - \sum_{m=1}^M \lambda_m \phi_{C_m}(X) \right). \quad (16)$$

The parameter vector  $\Lambda = \{\lambda_m\}_{1 \leq m \leq M}$  is uniquely characterized by the constraints (15), if the potential functions satisfy a linear independence property.

If  $\phi_{C_m}(X)$  are covariance measurements then (16) is the probability distribution of a Gaussian process, and if  $\mathcal{D}$  is an orthonormal basis then  $\Lambda$  is calculated by inverting a band covariance matrix. The entropy maximization is a convex problem [17], but for general potential functions  $\phi_{C_m}$  the vector  $\Lambda$  can not be calculated analytically. Numerical procedures compute  $\Lambda$  iteratively by estimating  $E_{p(X, \Lambda)}\{\phi_{C_m}(X)\}$ , while updating  $\Lambda$  with a gradient descent to reach the conditions (15). Let us mention that the estimation of  $E_{p(X, \Lambda)}\{\phi_{C_m}(X)\}$  is performed with a Gibbs sampler or other Markov chain Monte Carlo methods, which are computationally expensive.

Mumford and Zhu [35], as well as Simoncelli and Portilla [32], use such Markov random fields to construct a model from a single observation of a texture. The Markov model of Simoncelli and Portilla is calculated in a wavelet basis, with constraints on covariance values and on moments (14) with  $p = 1$ . The textured image 7(a) is the only observation used to compute the parameters  $\Lambda$  of the model, with a stationarity assumption. The Figure 7(b) shows a realization of the resulting wavelet Markov model. It is remarkably close to the original texture, in the sense that visually it can not be distinguished preattentively, in less than  $10^{-1}$  seconds. A similar wavelet Markov model is calculated from the “text” texture of Figure 7(c). The image 7(d) is obtained by adding a realization of this Markov model at the periphery, which is preattentively not discriminable from the center.

Markov random fields provide a general framework to construct processes with sparse interactions over appropriate representations. The validity of such models depends on the choice of representation and on the potential functions  $\phi_C$ . Understanding how to optimize these two components and analyzing the properties of such Markov random fields over functional spaces is an open problem.

## REFERENCES

- [1] L. Alvarez, F. Guichard, P.L. Lions and J.M. Morel. Axioms and fundamental equations of image processing. *Archieve for Rational Mechanic*, 123:199–257, 1993.
- [2] A. Benassi, S. Jaffard, and D. Roux, Elliptic Gaussian random processes *Revista Mathematica Iberoamericana* 13:19–90, 1997.
- [3] S. Chen and D. Donoho. Atomic decomposition by basis pursuit. In *SPIE International Conference on Wavelets*, San Diego, July 1995.

- [4] A. Cohen, R. DeVore, P. Pertrushev, and H. Xu, Non-linear approximation and the space  $BV(\mathbb{R}^2)$  *American J. of Math.*, to appear 1998.
- [5] R. R. Coifman and Y. Meyer. Remarques sur l'analyse de Fourier a fenêtre. *C.R. Acad. Sci.*, pages 259–261, 1991.
- [6] R. R. Coifman and M. V. Wickerhauser. Entropy-based algorithms for best basis selection. *IEEE Trans. Info. Theory*, 38(2):713–718, March 1992.
- [7] A. Croisier, D. Esteban, and C. Galand. Perfect channel splitting by use of interpolation/decimation/tree decomposition techniques. In *Int. Conf. on Info. Sciences and Systems*, pages 443–446, Patras, Greece, August 1976.
- [8] G. Cross, and A. Jain. Markov random field texture models *IEEE Trans. on PAMI*, 5:25–39, 1983.
- [9] I. Daubechies. *Ten Lectures on Wavelets*. SIAM, Philadelphia, PA, 1992.
- [10] I. Daubechies Wavelets and other phase space localization methods *Proc. of ICM 94*, Birkhäuser Verlag, Switzerland 1995.
- [11] J. G. Daugmann. Two-dimensional spectral analysis of cortical receptive field profile. *Vision Research*, 20:847–856, 1980.
- [12] R. DeVore, B. Jawerth, and V. Popov, Compression of wavelet decompositions *Amer. J. Math.*, 114:737–785, 1992.
- [13] R. DeVore, Nonlinear approximation *Acta Numerica*, 51–150, Cambridge University Press, 1998.
- [14] D. Donoho and I. Johnstone. Ideal spatial adaptation via wavelet shrinkage. *Biometrika*, 81:425–455, December 1994.
- [15] D. Donoho, Abstract statistical estimation and modern harmonic analysis. *Proc. of ICM 94*, Birkhäuser Verlag, Switzerland 1995.
- [16] N. Dyn and S. Rippa. Data-dependent triangulations for scattered data interpolation and finite element approximation. *Applied Num. Math.*, 12:89–105, 1993.
- [17] S. Geman, and D. Geman. Stochastic relaxation, Gibbs distributions, and the Bayesian restoration of images *IEEE Trans. on PAMI*, 6:721-741, November 1984.
- [18] B. Gidas. A renormalization group approach to image processing. *IEEE Trans. on PAMI*, 11:164-180, 1989.
- [19] S. Mallat. Multiresolution approximations and wavelet orthonormal bases of  $\mathbf{L}^2(\mathbb{R})$ . *Trans. Amer. Math. Soc.*, 315:69–87, September 1989.
- [20] S. Mallat and Z. Zhang. Matching pursuits with time-frequency dictionaries. *IEEE Transactions on Signal Processing*, 41(12):3397–3415, December 1993.



- [21] S. Mallat, Z. Zhang, and G. Papanicolaou. Adaptive covariance estimation of locally stationary processes. *Annals of Stat.*, 26(1):1–47, 1997.
- [22] S. Mallat. *A Wavelet Tour of Signal Processing*. Academic Press, Boston, MA, 1998.
- [23] H. S. Malvar. *Signal Processing with Lapped Transforms*. Artech House, Norwood, MA, 1992.
- [24] D. Marr. *Vision*. W.H. Freeman and Co., San Fransisco, 1982.
- [25] Y. Meyer. *Wavelets and Operators*. Advanced Mathematics. Cambridge University Press, 1992.
- [26] D. Mumford. Mathematical Theories of Shape: Do they model perception? *SPIE: Geometric Methods in Computer Vision*, 1570:2–10, 1991.
- [27] J. F. Muzy, E. Bacry, and A. Arneodo. The multifractal formalism revisited with wavelets. *Int. J. of Bifurcation and chaos*, 4:245, 1994.
- [28] S. Osher, and L. Rudin. Feature-oriented image enhancement using shock filters. *SIAM J. on Numerical Analysis*, 27:919–940, 1990.
- [29] M. Priestley, Evolutionary spectra and non-stationary processes. *J. Roy. Stat. Soc. Ser. B*, 27:204–237, 1965.
- [30] J. M. Shapiro. Embedded image coding using zero-trees of wavelet coefficients. *IEEE Trans. Signal Proc.*, 41(12):3445–3462, December 1993.
- [31] G. Shapiro, and A. Tannenbaum. On invariant curve evolution and image analysis. *J. of Functional Analysis*, 119(1):79–120, 1993.
- [32] E. Simoncelli., and J. Portilla. Texture characterization via second-order statistics of wavelet coefficient amplitudes. Proc. of 5<sup>th</sup> IEEE Int. Conf. on Image Proc., Chicago, October 1998.
- [33] M. Vetterli and J. Kovacevic. *Wavelets and Subband Coding*. Prentice-Hall, Englewood Cliffs, NJ, 1995.
- [34] J. W. Woods and S. D. O’Neil. Sub-band coding of images. *IEEE Trans. Acoust., Speech, and Signal Proc.*, 34(5):1278–1288, May 1986.
- [35] S. C. Zhu, and D. Mumford. Prior learning and Gibbs reaction-diffusion. *IEEE Trans. on PAMI*, 19:1236–1250, November 1997.

Stéphane Mallat  
Dept. of Applied Mathematics  
Ecole Polytechnique  
91128 Palaiseau Cedex, France

Courant Institute  
New York University  
215 Mercer Street  
New York, NY 10012, US

## FIBRATIONS IN SYMPLECTIC TOPOLOGY

DUSA MCDUFF<sup>1</sup>

ABSTRACT. Every symplectic form on a  $2n$ -dimensional manifold is locally the Cartesian product of  $n$  area forms. This local product structure has global implications in symplectic topology. After briefly reviewing the most important achievements in symplectic topology of the past 4 years, the talk will discuss several different situations in which one can see this influence: for example, the use of fibered mappings in the construction of efficient symplectic embeddings of fat ellipsoids into small balls, and the theory of Hamiltonian fibrations (work of Lalonde, Polterovich, Salamon and the speaker). The most spectacular example is Donaldson's recent work, showing that every compact symplectic manifold admits a symplectic Lefschetz pencil.

1991 Mathematics Subject Classification: 53 C 15

Keywords and Phrases: symplectic topology, J-holomorphic curves, Hamiltonian fibration, nonsqueezing theorem, symplectic embeddings, Hamiltonian group

## 1 INTRODUCTION

In this talk I will give an overview of what has been achieved in symplectic topology in the past 4 years and then will discuss the relevance of symplectic fibrations. First, I will review some basic facts.

A symplectic manifold  $(M, \omega)$  is a pair consisting of a smooth  $2n$ -dimensional manifold  $M$  together with a closed 2-form  $\omega$  that is nondegenerate, i.e. the top power  $\omega^n$  never vanishes. By Darboux's theorem such a form  $\omega$  can always be expressed locally as the sum

$$\omega = \sum_{i=1}^n dx_i \wedge dy_i.$$

Thus the only invariants of a symplectic manifold are global. The other essential feature of symplectic geometry is its connection with dynamics. Every function  $H : M \rightarrow \mathbf{R}$  has a symplectic gradient  $X_H$ , which is the vector field defined by the equation  $\omega(X_H, \cdot) = dH$ . Because  $\omega$  is closed, the flow of  $X_H$  is a family  $\phi_t^H$  of

---

<sup>1</sup>Partially supported by NSF grant DMS 9704825.

*symplectomorphisms*, i.e. diffeomorphisms that preserve the symplectic structure. Thus  $(\phi_t^H)^*(\omega) = \omega$  for all  $t$ .

One can think that these flows are built into the local structure of a symplectic manifold. Any (local) hypersurface  $Q$  in  $(M, \omega)$  is a regular level set  $H = \text{const}$  of some function  $H$ . Since  $dH(X_H) = \omega(X_H, X_H) = 0$ , the vector field  $X_H$  is tangent to  $Q$  and so induces a flow on it. The corresponding flow lines are independent of the choice of  $H$  and so give rise to a 1-dimensional foliation on  $Q$  called the *characteristic foliation*. As we shall see in §4.1, these foliations give rise to a good theory of symplectic connections on symplectic fibrations.

Another more global consequence is that each symplectic manifold gives rise to an interesting infinite-dimensional group, namely the *group of symplectomorphisms*  $\text{Symp}(M, \omega)$ . Its identity component contains a connected subgroup of finite codimension, called the *Hamiltonian subgroup*  $\text{Ham}(M, \omega)$ . This consists of all symplectomorphisms that are the time-1 map of some Hamiltonian flow  $\phi_t^H$ , where here one allows the Hamiltonian  $H_t : M \rightarrow \mathbf{R}$  to depend on time  $t \in [0, 1]$ . I shall say more about these groups in §2.6 and §4.2 below.

A basic theme in symplectic topology is that properties that hold locally are often valid more globally. One example is Darboux's theorem. Here the local statement is that there is a unique symplectic structure at a point (i.e. on the tangent space), and this extends to the fact that there is a unique structure in a neighborhood of each point. Another example is Arnold's conjecture. The local statement here is that when  $M$  is compact every Hamiltonian symplectomorphism that is sufficiently close to the identity in the  $C^1$ -topology has at least  $\sum_i \dim H^i(M, \mathbf{R})$  distinct fixed points, provided that these are all nondegenerate.<sup>2</sup> The global statement is that this remains true for all elements of  $\text{Ham}(M, \omega)$ . This has now been proved: see §2.2.

One further example of this phenomenon that I want to mention here concerns the fact that a symplectic form  $\omega$  is a local product: by Darboux's theorem  $\omega$  can always be expressed locally as the Cartesian product of  $n$  area forms  $dx \wedge dy$  on  $\mathbf{R}^2$ . Observe that a general symplectomorphism does not preserve this local product structure. For example, the linear map

$$L : (x_1, y_1, x_2, y_2) \mapsto (x_1 + x_2, y_1, x_2, y_2 - y_1)$$

preserves  $\omega$  but neither preserves nor interchanges its individual summands  $dx_i \wedge dy_i, i = 1, 2$ . Nevertheless, I hope to show in this talk that the existence of this local product structure is reflected globally in various important ways, both in the "semi-local" properties that are discussed in §3 and in the theory of symplectic fibrations that is presented in §4. The best evidence is, of course, Donaldson's theorem on the existence of symplectic Lefschetz pencils that is discussed in §2.3 below.

---

<sup>2</sup>A fixed point  $x$  of  $\phi$  is said to be *nondegenerate* if the graph of  $\phi$  in  $M \times M$  intersects the diagonal transversally at the point  $(x, x)$ . There are other versions of Arnold's conjecture that allow degenerate fixed points and/or make homotopy theoretic rather than homological estimates of the number of fixed points, but these have not yet been established in full generality.

## 1.1 ANALYTIC TECHNIQUES IN SYMPLECTIC TOPOLOGY

Until Donaldson's recent work, there were two main sources of analytic techniques in symplectic geometry, variational methods (that relate to the above mentioned flows) and elliptic methods. These have been combined to create powerful tools such as Floer theory. Since Hofer who is one of the main exponents of the variational method is also talking at this I.C.M. I will not say anything more about this here, and will concentrate on more purely elliptic methods that exploit the close relation of symplectic geometry with complex geometry.

One important kind of symplectic manifold is a *Kähler manifold*. This is a complex manifold  $M$  that admits a Riemannian metric  $g$  that is well adapted to the induced almost complex structure  $J$  on the tangent bundle  $TM$ .<sup>3</sup> One way of expressing the Kähler condition is that the bilinear form  $\omega$  defined by

$$\omega(v, w) = g(Jv, w)$$

is skew-symmetric and closed. Since the nondegeneracy of  $g$  implies that of  $\omega$ , the form  $\omega$  is symplectic. As a kind of converse, observe that a symplectic manifold always supports an almost complex structure  $J$  on the tangent bundle  $TM$  that is compatible with  $\omega$  in the sense that the bilinear form  $g$  defined by the above equation is a positive definite inner product. In fact, for any symplectic manifold  $M$  there is a contractible set  $\mathcal{J}(\omega)$  of such almost complex structures. In most cases, these will not be integrable. It was Gromov who first realised (in 1985) how to use these almost complex structures to get information about the underlying symplectic structure: see [G1], [G2].

Gromov's fundamental idea was to look at spaces of *J-holomorphic curves* in  $(M, \omega, J)$ . These are maps  $u$  from a Riemann surface  $(\Sigma, j)$  to the almost complex manifold  $(M, J)$  that satisfy the generalized Cauchy–Riemann equation

$$du \circ j = J \circ du.$$

If  $J$  is integrable,  $u$  is a (parametrized) holomorphic curve of the usual kind. Even if  $J$  is not integrable, these curves behave very much as one would expect, basically because every almost complex structure on a 2-manifold is integrable. In particular, the ellipticity of the Cauchy–Riemann equation implies that the set  $\mathcal{M}(A, J)$  of all such curves that represent the homology class  $A \in H_2(M; \mathbf{Z})$  is a finite-dimensional manifold for generic  $J$  in  $\mathcal{J}(\omega)$ . The other essential ingredient comes from the existence of the symplectic form  $\omega$ . This gives an *a priori* bound to the energy (or  $W^{1,2}$ -norm) of the elements in  $\mathcal{M}(A, J)$ , which in turn implies that this space has a well-behaved compactification. Hence it makes sense to try to count the number of these curves that intersect certain homology classes in  $M$ . In general, one gets a finite number that is independent of  $J$ . This gives rise to symplectic invariants, that in various contexts are called Gromov invariants, Gromov–Witten invariants, or Gromov–Taubes invariants and so on. Many foundational results in symplectic topology can be proved using *J-holomorphic curves*,

<sup>3</sup>An almost complex structure is an automorphism of the tangent bundle  $TM$  with square equal to  $-\text{Id}$ . If it is induced from an underlying complex structure on  $M$  it is said to be *integrable*.

for example the nonsqueezing theorem that we discuss below. They are also an essential ingredient in symplectic versions of Floer homology.

## 2 RECENT ADVANCES

In this section I will list some of the most significant advances in symplectic geometry of the past 4 years. I will be very brief (and in particular do not attempt to give full references) since in many cases other people will be giving talks on these subjects at this I.C.M.

### 2.1 TAUBES–SEIBERG–WITTEN THEORY

A few months after the Seiberg–Witten equations were first formulated in Fall 1993, Taubes realised that the methods used by Witten to calculate the associated invariants for Kähler manifolds could be adapted to the symplectic case. This was the first time that methods of gauge theory were found to interact significantly with symplectic geometry. His first results [T1,2] from Spring 1994 established a structure theorem for the Seiberg–Witten invariants of symplectic 4-manifolds, that implied in particular that they do not vanish. He then wrote a series of deep papers that showed that these invariants coincide with a certain kind of Gromov invariant that counts  $J$ -holomorphic curves in an appropriate way: see [T3–6] and also Ionel–Parker [IP1].

This has opened the door to the construction of many interesting examples of symplectic 4-manifolds as well as to a much better understanding of the relation of smooth 4-manifolds to symplectic ones: cf. the I.C.M. talks of Taubes and Fintushel–Stern. For example, Taubes gave the first examples of manifolds that satisfy the necessary topological preconditions for being symplectic (namely they support an almost complex structure and also have a cohomology class  $a \in H^2(M, \mathbf{R})$  whose top power does not vanish) but nevertheless have no symplectic structure. One such example is the connected sum  $\mathbf{C}P^2 \# \mathbf{C}P^2 \# \mathbf{C}P^2$  of three copies of the projective plane, which cannot be symplectic because its Seiberg–Witten invariants vanish. Another consequence is a proof that there is only one symplectic structure on the complex projective plane (up to rescaling) (see [G1] and [T2]) and a complete classification of symplectic structures on blow-ups of rational and ruled surfaces. This last is a combination of work by Li–Liu [LL1,LL2], Ohta–Ono [OO] and Liu [Liu] on Seiberg–Witten theory for symplectic manifolds with  $b^+ = 1$ , work by Lalonde–McDuff [LM4] classifying symplectic structures on ruled surfaces and work on blow-ups by McDuff [Mc1] and Biran [Bi].

### 2.2 GENERAL GROMOV–WITTEN INVARIANTS

The theory of  $J$ -holomorphic curves outlined above was unsatisfactory for many years because there was a basic technical problem (the “multiply-covered curve problem”) that meant that it worked only in a very restricted class of manifolds. In 1994 Kontsevich suggested a way to get around this difficulty using the concept of stable maps and other ideas from algebraic geometry, and subsequently several teams have made this a reality. Among them are Fukaya–Ono [FO], Li–Tian [LiT],

Liu–Tian [LiuT], Ruan [R], and Siebert [Sieb], who have all completed substantial papers on this subject in the past two years. (See also Hofer–Salamon [HS].) This important foundational work shows that methods that one might think are intrinsically algebraic can be extended to the smooth symplectic context. Another consequence is a proof that the nondegenerate case of Arnold’s conjecture holds on all symplectic manifolds: see [FO], [LiuT].

One of the recent insights that has come from string theory and quantum physics is that Gromov–Witten invariants have very interesting formal properties: for example they give rise to a deformation of the cup product on the cohomology ring of a symplectic manifold. This is known as quantum cohomology: see Ruan–Tian [RT]. These invariants have been also used to solve long-standing problems in enumerative geometry and have many other applications: cf. the I.C.M. talks by Vafa and Ruan.

### 2.3 DONALDSON THEORY

In the past two years Donaldson has developed a completely new way to use the existence of almost complex structures on symplectic manifolds, taking the manifold  $(M, J)$  to be not the target space but rather the domain of the maps considered. He has developed a theory of “almost holomorphic” sections of certain “almost ample” line bundles that imitates the usual theory in the Kähler case so faithfully that he can prove that every closed symplectic manifold admits a symplectic Lefschetz pencil: see [D1, D2] and also the Bourbaki seminar [Sik]. I will state a version of the theorem here because of its relevance to the theme of this talk. For a much fuller discussion, see Donaldson’s I.C.M. talk.

**THEOREM 2.1** *Let  $(M, \omega)$  be a closed symplectic manifold such that the cohomology class  $[\omega]$  is integral. Then for each sufficiently large  $k$  there is a symplectic submanifold  $B_k$  of codimension 4 and a smooth map  $p : M - B_k \rightarrow \mathbf{CP}^1$  that has only finitely many singular points. Each fiber of  $p$  is symplectically embedded except at its singular points, and near these  $p$  has the form  $(z_1, \dots, z_n) \mapsto \sum_i z_i^2$  in suitable local coordinates  $(z_1, \dots, z_n) \in \mathbf{C}^n$ . Finally,  $p$  extends smoothly to the blow-up  $\widetilde{M}$  of  $M$  along  $B_k$ .*

The induced map  $p : \widetilde{M} \rightarrow \mathbf{CP}^1$  is usually called a Lefschetz fibration. It is constructed so that its general fiber  $F_k$  represents the Poincaré dual  $\text{PD}(k[\omega])$  of a suitably large integral multiple of the symplectic cohomology class  $[\omega]$ . Auroux [Au] has shown that for sufficiently large  $k$  the codimension-2 symplectic submanifold  $F_k$  is unique up to isotopy. Similarly, it can be shown that the whole structure of the Lefschetz pencil is unique up to isotopy for sufficiently large  $k$ . Moreover the symplectic form on such a pencil is determined up to deformation<sup>4</sup> by the symplectic form on the fiber  $F_k$ . Hence, in principle, the classification of symplectic  $2n$ -manifolds can be reduced to that of symplectic  $(2n - 2)$ -manifolds, and hence to the complicated world of symplectic 4-manifolds. This, in turn, is

---

<sup>4</sup>Two closed symplectic manifolds  $(V, \omega_V), (W, \omega_W)$  are said to be *deformation equivalent* if there is a diffeomorphism  $\phi : V \rightarrow W$  and a family of not necessarily cohomologous symplectic forms  $\omega_t, t \in [0, 1]$  on  $V$  such that  $\omega_0 = \omega_V, \omega_1 = \phi^*(\omega_W)$ .

reduced to data concerning Riemann surfaces. Many very interesting questions arise here, and I refer you to the I.C.M. talks by Donaldson and Fintushel–Stern for further discussion. One important point is that it is not known whether the classification of symplectic 4-manifolds is more complicated than that of smooth 4-manifolds. For example, I do not know any example of a smooth 4-manifold that supports two symplectic structures which are not deformation equivalent.

## 2.4 CONTACT GEOMETRY

Contact geometry is the odd-dimensional analog of symplectic geometry. It is now particularly well understood in dimension 3 because there are two ways to get geometric information about a contact 3-manifold  $M$ . One can reduce to 2-dimensions by looking at the intersection of the contact structure with families of surfaces in  $M$ , an approach pioneered by Eliashberg [E3] and Giroux [Gi], and one can also use elliptic techniques in the 4-dimensional symplectization  $M \times \mathbf{R}$ . For new developments in this area I refer you to the I.C.M. talks by Eliashberg and Hofer.

## 2.5 HOFER GEOMETRY

Hofer [H] pointed out in 1990 that the group of Hamiltonian symplectomorphisms carries a biinvariant metric, that is now called the Hofer metric. There have been significant advances in understanding the properties of this metric and its geometric and dynamic implications, notably by Bialy–Polterovich [BP], a series of papers by Polterovich (see [P]) and Lalonde–McDuff [LM1–3]. In particular, the papers [LM1–3] develop a new elliptic approach to Hofer geometry, and show that the energy-capacity inequality that is basic to the whole theory is equivalent to the nonsqueezing theorem discussed in §3 below. There also is an interesting connection between the Hofer length of an element in  $\pi_1(\text{Ham}(M))$  and properties of the associated symplectic fibration over  $S^2$  with fiber  $M$ : see [P] §7, and §4.2 below. For further details, see the I.C.M. talk by Polterovich [P].

## 2.6 THE TOPOLOGY OF THE GROUP OF SYMPLECTOMORPHISMS

There has been quite a bit of recent progress in understanding the relations between the groups

$$\text{Ham}(M, \omega) \hookrightarrow \text{Symp}(M, \omega) \hookrightarrow \text{Diff}(M)$$

for closed symplectic manifolds  $(M, \omega)$ . Observe that the inclusion  $\text{Ham}(M, \omega) \rightarrow \text{Symp}(M, \omega)$  induces an isomorphism on all homotopy groups except for  $\pi_0$  and  $\pi_1$ . As far as concerns  $\pi_0$ , the Hamiltonian group is path-connected by definition, while  $\text{Symp}(M, \omega)$  often is not. As for  $\pi_1$ , there is an exact sequence

$$0 \rightarrow \pi_1(\text{Ham}(M, \omega)) \rightarrow \pi_1(\text{Symp}(M, \omega)) \rightarrow \Gamma_\omega \rightarrow 0,$$

where  $\Gamma_\omega$  is a countable subgroup of  $H^1(M, \mathbf{R})$  that is called the *Flux group*: see [MS] or [LMP1]. It is not hard to show that  $\text{Ham}(M, \omega)$  coincides with the

identity component of  $\text{Symp}(M, \omega)$  in the case when  $b_1(M) = \text{rk } H^1(M, \mathbf{R}) = 0$ , in particular if  $M$  itself is simply connected.

Perhaps the most surprising recent result is that of the stability of Hamiltonian loops, i.e if  $\{\phi_t\}_{t \in [0,1]}$  represents an element of  $\pi_1(\text{Ham}(M, \omega))$  then any perturbation  $\{\phi'_t\}$  of the loop  $\{\phi_t\}$  that preserves some nearby symplectic form  $\omega'$  represents an element of  $\pi_1(\text{Symp}(M, \omega'))$  that lies in the image of  $\pi_1(\text{Ham}(M, \omega'))$ : see Lalonde–McDuff–Polterovich [LMP2]. Another way of saying this is that if  $\phi \in \pi_1(\text{Symp}(M, \omega))$  and  $\phi' \in \pi_1(\text{Symp}(M, \omega'))$  map to the same element of  $\pi_1(\text{Diff}(M))$  and if  $\phi$  maps to zero in  $\Gamma_\omega$  then  $\phi'$  must map to zero in  $\Gamma_{\omega'}$ . It follows fairly easily that the Flux subgroup  $\Gamma_\omega$  never has more than  $b_1(M)$  generators. It is still not known whether it is always discrete. This would be the case if and only if the group  $\text{Ham}(M, \omega)$  is closed in  $\text{Symp}(M, \omega)$  with respect to the  $C^1$ -topology: see [LMP1].

Otherwise the theory is at the stage of computing interesting examples. Seidel [Seid1] has found a very nice construction that shows that for many symplectic 4-manifolds that contain a Lagrangian 2-sphere<sup>5</sup> the map  $\pi_0(\text{Symp}(M, \omega)) \rightarrow \pi_0(\text{Diff}(M))$  is not injective. This work is based on an analysis of the Floer homology of the generalized Dehn twists that occur as monodromy in Lefschetz fibrations: see Donaldson’s I.C.M. talk. Seidel has also shown that when  $M$  is the product of two projective spaces  $\mathbf{C}P^m \times \mathbf{C}P^n$ , where  $m \leq n$ , the map  $\pi_k(\text{Symp}(M, \omega)) \rightarrow \pi_k(\text{Diff}(M))$  is not surjective for odd  $k \leq 2n - 1$ . Many of the above results are proved by considering properties of appropriate fibrations: see §4.2 below.

We end this section by mentioning an example where the rational cohomology of the groups  $\text{Symp}(M, \omega)$  has been fully worked out. Here  $(M, \omega)$  is the product  $S^2 \times S^2$  equipped with the symplectic form  $\omega^\lambda = (1 + \lambda)\sigma_0 \oplus \sigma_1$ , where  $\sigma_i, i = 0, 1$ , is an area form on  $S^2$  of total area 1. Let  $G^\lambda, \lambda \geq 0$  denote the corresponding group of symplectomorphisms. Gromov showed in [G1] that, when  $\lambda = 0$ ,  $G^\lambda$  is deformation equivalent to the extension of the Lie group  $\text{SO}(3) \times \text{SO}(3)$  by the involution that interchanges the two factors. Abreu showed in [Ab] that when  $0 < \lambda \leq 1$  the group  $G^\lambda$  no longer has the homotopy type of a Lie group since its rational cohomology ring has an even-dimensional generator. Abreu–McDuff [AM] have completed this calculation, showing that when  $k - 1 < \lambda \leq k$

$$H^*(G^\lambda, \mathbf{Q}) = \Lambda(x_1, x_3, x'_3) \otimes S(x_{4k}),$$

where  $x_i, x'_i$  denote generators in dimension  $i$ ,  $\Lambda$  is an exterior algebra and  $S$  is a polynomial algebra. One can give a meaning to the “limit” of these groups  $G^\lambda$  as  $\lambda \rightarrow \infty$  and show that this is homotopy equivalent to the group  $\mathcal{D}$  of fiberwise orientation-preserving diffeomorphisms of the trivial fibration  $S^2 \times S^2 \rightarrow S^2$ . Since  $\text{Diff}(S^2)$  is homotopy equivalent to the Lie group  $\text{O}(3)$ , the group  $\mathcal{D}$  is homotopy equivalent to a group  $\mathcal{D}'$  that fits in the exact sequence

$$0 \rightarrow \text{Map}(S^2, \text{SO}(3)) \rightarrow \mathcal{D}' \rightarrow \text{SO}(3) \rightarrow 0.$$

The cohomology ring of  $\mathcal{D}$  is isomorphic to  $\Lambda(x_1, x_3, x'_3)$  and restricts onto this part of  $H^*(G^\lambda)$ , while the “jumping generator”  $x_{4k}$  dies in the limit.

<sup>5</sup>i.e. a sphere on which the symplectic form vanishes.



## 2.7 SYMPLECTIC FIBRATIONS

A unifying theme that is relevant to several of the areas mentioned above is that of symplectic fibration. This concept occurs in symplectic topology in several closely related variants, but one essential ingredient is a fibration (possibly local and/or singular) with a family of cohomologous symplectic forms on its fibers. Moreover, these fiberwise forms should be induced by the ambient symplectic form, if there is one. (A precise definition is given in §4.)

I pointed out in various places above that the proofs use properties of symplectic fibrations. It is also worth noting that the use of (local) fibrations is ubiquitous in 4-dimensional symplectic topology. This is obvious in so far as Donaldson's theory goes. However, this remark applies also to the kinds of symplectic surgeries that have been recently developed and explored. For instance, almost all the new examples of symplectic 4-manifolds are constructed using the fiber connect sum (see Gompf [Go], and McCarthy–Wolfson [MW]) which exploits the local fibered structure of a symplectic manifold near a symplectic submanifold with trivial normal bundle. This construction is also known as the symplectic sum. It has good formal properties: see for example Ionel–Parker [IP2] and McDuff–Symington [MSy]. Other symplectic surgeries developed by Luttinger [Lu], Eliashberg and Polterovich [EP] and Symington [Sym] also use the canonical local fibered structure of a symplectic manifold near a symplectic or Lagrangian submanifold.

As another example, observe that the knot surgeries used by Fintushel and Stern in [FS] to construct a family  $X_K$  of homotopy  $K3$ -surfaces are only known to yield symplectic manifolds when the knot  $K$  is fibered. To some extent this is a matter of expedience: the presence of a suitable fibration allows one to construct a symplectic form out of forms on the base and the fibers. However, Donaldson's theorem shows that fibrations are intrinsic to the structure of symplectic manifolds, and it is quite possible that it will eventually be shown that Fintushel and Stern's manifolds  $X_K$  are symplectic if and only if the knot  $K$  is fibered.

## 3 SYMPLECTIC RIGIDITY

In this section we will discuss “semi-local” symplectic topology, which I take to mean properties of open subsets of Euclidean space and of the symplectomorphisms between them. To emphasize that we are dealing with the standard symplectic form here, I will denote it by  $\omega_0 = \sum_i dx_i \wedge dy_i$ . We will begin with a discussion of Gromov's nonsqueezing theorem, which is the basis of all symplectic topology, and then in §3.2 will talk about some more specialised problems concerning symplectic embeddings.

### 3.1 THE NONSQUEEZING THEOREM

Gromov's nonsqueezing theorem [G1] answers the question of when a ball can be symplectically embedded in a cylinder. To emphasize the relation with fibrations we will think of the cylinder

$$Z^{2n}(\lambda) = B^2(\lambda) \times \mathbf{R}^{2n-2}$$

as the inverse image of the 2-disc  $B^2(\lambda)$  of radius  $\lambda$  by the projection

$$p : \mathbf{R}^{2n} \rightarrow \mathbf{R}^2, \quad (x_1, \dots, y_n) \mapsto (x_1, y_1).$$

Then, if  $B^{2n}(r)$  denotes the (closed) standard ball of radius  $r$  in Euclidean space  $\mathbf{R}^{2n}$  the nonsqueezing theorem can be stated as follows.

**THEOREM 3.1** *For all (local) symplectomorphisms  $\phi$  of  $\mathbf{R}^{2n}$*

$$\text{area} (p \circ \phi(B^{2n}(r))) \geq \pi r^2.$$

In other words, it is impossible to embed a standard ball of radius  $r$  into the cylinder  $Z^{2n}(\lambda)$  of radius  $\lambda$  when  $\lambda < r$ .

This property of symplectomorphisms is fundamental. Indeed it characterises symplectomorphisms in the following sense. Suppose that  $\psi$  is a diffeomorphism such that

$$\text{area} (p \circ L \circ \psi(B^{2n}(x; r))) \geq \pi r^2$$

for all linear symplectomorphisms  $L$  and all sufficiently small balls  $B^{2n}(x; r)$  in  $\mathbf{R}^{2n}$ . Then  $\psi^*(\omega_0) = \pm\omega_0$ . If in addition  $\psi$  is orientation preserving we must have the + sign when  $n$  is odd. Applying this to the diffeomorphism  $\psi \times \text{Id}$  of  $\mathbf{R}^{2n} \times \mathbf{R}^2$ , one also can characterize symplectomorphisms in this way when  $n$  is even. This is the essential ingredient of the proof by Eliashberg [E1] (see also Ekeland–Hofer [EH]) that the group of symplectomorphisms is  $C^0$ -closed in the group of diffeomorphisms.<sup>6</sup> As Gromov pointed out in his 1986 ICM talk [G2], without this there would be no interesting theory of symplectic topology. This result is also the foundation of the theory of symplectic measurements such as the Gromov width of sets<sup>7</sup> and the Hofer norm on the group of Hamiltonian symplectomorphisms that is discussed in Polterovich’s talk [P].

I will consider two aspects of this theorem in more detail below. Firstly, if one thinks of it as a statement about symplectic embeddings, the question obviously arises as to what other symplectic embeddings are possible between standard objects such as ellipsoids and polydiscs. Secondly, one can view this theorem as a fact about the trivial fibration

$$p : Z^{2n}(\lambda) \rightarrow B^2(\lambda),$$

and ask whether general symplectic fibrations have similar properties.

To end this section, I’d like to say one more thing concerning the relation of the  $C^0$  (or uniform) topology to the symplectic world. Using the above ideas it is possible to define the notion of a *symplectic homeomorphism* between two smooth symplectic manifolds, though very little is known about the properties of such maps. For example, as in [EH] one can define the notion of a symplectic capacity such as the Gromov width and then say that a homeomorphism is symplectic if it preserves the capacity of sufficiently small open sets. Here I want to mention

<sup>6</sup>The  $C^0$ -topology is the topology of uniform convergence on compact subsets.

<sup>7</sup>The Gromov width  $w_G(U)$  of an open subset  $U$  of  $(M^{2n}, \omega)$  is defined to be the supremum of the numbers  $\pi r^2$  such that the ball  $B^{2n}(r)$  embeds symplectically in  $U$ .

a slightly different question. Colin [C] has recently shown that contact structures are  $C^0$ -stable in dimension 3 though not in higher dimensions. In other words, two plane fields  $\xi, \xi'$  on a closed 3-manifold that are sufficiently  $C^0$ -close and that both satisfy the contact condition are isotopic through a family of contact plane fields.

QUESTION 3.2 *Is there a symplectic analog of this result?*

It is not even clear what is the appropriate notion of “ $C^0$ -close” in this context. In the contact case the condition for a hyperplane field  $\xi$  to be contact involves the first derivative of the defining form  $\alpha$ . In other words, if  $\xi = \ker \alpha$  and the manifold has dimension  $2n+1$  then one requires that  $\alpha \wedge d\alpha^n \neq 0$ . It follows that one can get a sensible  $C^0$ -topology by using the  $C^0$ -topology on the defining forms  $\alpha$  (which is, of course, equivalent to using the  $C^0$ -topology on the plane fields themselves). However, any two symplectic forms  $\omega$  and  $\omega'$  that are cohomologous and sufficiently  $C^0$ -close may be joined by the symplectic isotopy  $t\omega + (1-t)\omega', t \in [0, 1]$ , and so are diffeomorphic by Moser’s theorem. Hence this is not the right analog. The question is whether there is an intrinsic  $C^0$  notion of a symplectic structure for which the above stability result would hold at least in dimension 4. One might, for example, say that two symplectic structures are  $\varepsilon$ -close on a compact domain  $K$  if

$$|w_G(U, \omega) - w_G(U, \omega')| \leq \varepsilon$$

for all open subsets  $U \subset K$ , where  $w_G$  is the Gromov width defined above. It is not known what the consequences of such a definition would be.

This raises the whole question of what a symplectic structure “really is”. I do not think that it is just a structure that allows certain analytic techniques (such as those of Gromov, Taubes and Donaldson) to work. As the nonsqueezing theorem shows there is a geometric flavor to the theory that does not seem to be captured this way. I would argue that one important geometric element is the presence of the local characteristic foliations mentioned in §1 and that another is the local product structure. An idea of what one might expect is suggested by the Eliashberg–Thurston [ET] paper on confoliations, where the authors work out the relation between foliations and contact structures and show that an essential ingredient of a contact structure is a “positive twist” condition.

### 3.2 SYMPLECTIC EMBEDDINGS AND FOLDING

Let us write  $E(a_1, \dots, a_n)$  for the ellipsoid

$$E(a_1, \dots, a_n) = \left\{ z \in \mathbf{R}^{2n} : \sum_i \frac{x_i^2 + y_i^2}{a_i} \leq 1 \right\}.$$

It is well known that every ellipsoid in  $\mathbf{R}^{2n}$  is linearly symplectomorphic to one of the form  $E(a_1, \dots, a_n)$ , where  $a_1 \leq \dots \leq a_n$ . Consider the question of when  $E(a_1, \dots, a_n)$  embeds symplectically into the unit ball  $B^{2n}(1) = E(1, \dots, 1)$ . Floer, Hofer and Wysocki [FHW] looked at the 4-dimensional case and showed using

symplectic homology that when the ellipsoid is “round”, that is when the ratio  $a_2/a_1$  is  $\leq 2$ , there is such an embedding only if the ellipsoid is a subset of the ball. Recently Schlenk [Sch] extended this result to higher dimensions, basing his argument on Ekeland–Hofer capacities.

**THEOREM 3.3** *If  $a_n \leq 2a_1$  then  $E(a_1, \dots, a_n)$  embeds symplectically in  $B^{2n}(1)$  only if  $a_n \leq 1$ .*

He has also shown that this result is sharp in the sense that as soon as  $a_n > 2a_1$  it is possible to construct symplectic embeddings of  $E(a_1, \dots, a_n)$  into a ball with radius  $r$ , where  $r^2 < a_n$ . To be precise, he proved:

**THEOREM 3.4** *Given any  $\nu > \varepsilon > 0$  there is a symplectic embedding*

$$E(1, \dots, 1, 2 + 2\nu) \hookrightarrow E(2 + \nu + \varepsilon, \dots, 2 + \nu + \varepsilon) = B^{2n}(\sqrt{2 + \nu + \varepsilon}).$$

The proof constructs explicit embeddings by a technique known as symplectic folding. This is based on an idea of Traynor [Tr], who realised that in these embedding questions it is useful to think of a ball or ellipsoid as fibered over the 2-disc  $E(a_1)$  via the projection

$$p : E(a_1, \dots, a_n) \rightarrow E(a_1).$$

Observe that the fiber of  $p$  at a point  $x \in E(a_1)$  is simply the ellipsoid  $E(a'_2, \dots, a'_n)$  where  $a'_i = a_i(a_1 - |x|^2)/a_1$ . The idea is to construct embeddings of  $E(a_1, \dots, a_n)$  into  $\mathbf{R}^{2n} = \mathbf{R}^2 \times \mathbf{R}^{2n-2}$  of the form  $f \times g$  where  $f : E(r_1) \rightarrow \mathbf{R}^2$  is area-preserving and  $g : E(a_2, \dots, a_n) \rightarrow \mathbf{R}^{2n-2}$  is symplectic. In doing this one just has to control the image of  $f \times g$  on the “partial product”  $E(a_1, \dots, a_n)$ . This technique was developed further by Lalonde–McDuff [LM1], who incorporated the idea of folding.

For simplicity, we explain this in the case  $n = 2$ . The idea is that what is really important about the fibration  $p : E(a_1, a_2) \rightarrow E(a_1)$  is:

- (i) the fact that the subset  $B_c$  of the base  $E(a_1)$  over which the fiber has area  $\geq c$  is connected;
- (ii) the fact that the fibers are nested, i.e. if we identify the fibers with subsets of  $\mathbf{R}^2$ , then fibers of equal area are identical and lie inside the fibers of greater area; and
- (iii) the precise function  $A(c) = \text{area } B_c$ .

It is shown in [LM2] that any other smoothly triangulable set  $T_Y$  of  $\mathbf{R}^4$  that fibers over a smoothly triangulable set  $Y$  in  $\mathbf{R}^2$  of area  $\pi a_1$  and has properties (i), (ii) and the same function  $A(c)$  is equivalent to the ellipsoid  $E(a_1, a_2)$  in the following sense: for any  $\varepsilon > 0$ , one can symplectically embed  $E(a_1, a_2)$  into an  $\varepsilon$ -neighborhood of  $T$  and also symplectically embed  $T$  into an  $\varepsilon$ -neighborhood of  $E(a_1, a_2)$ . These embeddings are also fibered, i.e. of the form  $(z, w) \mapsto f(z) \times g(w)$ . In particular we can take  $Y$  to be a set consisting of two rectangles of total area  $a_1$  joined by a line segment  $I$ , and then map  $T_Y$  by embeddings into the product space  $\mathbf{R}^2 \times \mathbf{R}^2$  that are fibered over each rectangle and “folded” over the interval

$I$ . The set in  $T_Y$  that lies over  $I$  is a product  $I \times F$  and the folding map has the form

$$I \times F \rightarrow U \times \mathbf{R}^2 \subset \mathbf{R} \times \mathbf{R} \times \mathbf{R}^2, \quad (t, x) \mapsto (t, H(t, x), \phi_t(x)).$$

The minimum amount of room needed to make this fold (i.e. the minimum area of  $U$ ) is closely related to the Hofer norm of the embedding  $\phi_1 \circ \phi_0^{-1} : \phi_0(F) \rightarrow \mathbf{R}^2$ . In this construction one can see the relevance of local symplectic fibrations and the close connection between embedding problems and Hofer geometry that was exhibited in [LM1].

Here is a problem suggested by Schlenk [Sch]. Define  $s(a)$  for  $a \geq 1$  to be the infimum of the numbers  $s$  such that there is a symplectic embedding of the ellipsoid  $E(1, a)$  into the ball  $E(s, s)$ . Schlenk has shown that as  $a \rightarrow \infty$  the image of  $E(1, a)$  fills up an arbitrarily large percentage of the volume of the ball. Thus  $s(a)^2/a$  converges to 1 as  $a \rightarrow \infty$ .

QUESTION 3.5 *Find sharp estimates for  $s(a)$ , in particular as  $a \searrow 2$ .*

By Theorem 3.3  $s(a) = a$  for  $a \leq 2$ , but otherwise this function is unknown. Schlenk has made some computer calculations of the best upper bound for  $s(a)$  that can be obtained by (multiple) folding but it is not clear whether his estimate is even asymptotically sharp as  $a \searrow 2$ . To improve this estimate one would need a new way to construct symplectic embeddings. It would be interesting to know if there is another way to construct such embeddings that is not so closely tied to the local product structure as is the method of folding.

Here is another embedding problem that involves understanding the interaction of an embedded ball with a fibration. The nonsqueezing theorem gives an obstruction for a ball  $B$  to embed in a cylinder. But when this obstruction vanishes we do not yet know much about the space of all symplectic embeddings  $\phi$  of the ball into the cylinder, except that it is path-connected when  $n = 2$ . Consider the slicing of the cylinder  $Z^{2n}(1)$  by the flat discs  $D_x = B^2(1) \times \{x\}$ ,  $x \in \mathbf{R}^{2n-2}$ , that intersect the boundary  $\partial Z^{2n}(1)$  along the leaves of its characteristic foliation. Each disc  $D_x$  has an area form given by the restriction of the standard symplectic form  $\omega_0$ .

QUESTION 3.6 *Find a lower bound for*

$$c_r = \min_{\phi} \max_x \text{area } \phi(B) \cap D_x,$$

where  $\phi$  varies over all symplectic embeddings of the ball  $B$  of radius  $r$ . In particular, does  $\lim_{r \rightarrow 1} c_r / \pi r^2 = 1$ ?

Polterovich pointed out<sup>8</sup> that the ratio  $c_r / \pi r^2 \rightarrow 0$  as  $r \rightarrow 0$ . One can see this by beginning with a slicing (or foliation) of  $\mathbf{R}^{2n}$  by parallel isotropic 2-planes (i.e. planes on which  $\omega_0$  vanishes) and then slightly perturbing it to a slicing by parallel symplectic planes whose intersections with the standard ball  $B = B^{2n}(r)$

<sup>8</sup>Private communication

have  $\omega_0$ -area  $\leq \varepsilon\pi r^2$  for some  $\varepsilon$ . There is a symplectomorphism  $\psi$  of  $\mathbf{R}^{2n}$  that takes the slicing  $\mathbf{R}^2 \times \{x\}$  to this new one, and, provided that  $r$  is sufficiently small, we can arrange that the restriction  $\psi^{-1}|_B$  extends to a symplectomorphism  $\phi$  of  $\mathbf{R}^{2n}$  with support in the cylinder  $Z^{2n}(1)$ . Hence, for these  $r$ , we find  $c_r/\pi r^2 \leq \varepsilon$ . On the other hand, we showed in [LM3] that when  $r = 1$  any embedding  $\phi$  of the unit ball  $B$  into the cylinder  $B^2(1) \times \mathbf{R}^{2n-2}$  must intersect the boundary of the cylinder in a set that contains some flat circle  $\partial B^2(1) \times \{x\}$ . Hence one could say that  $c_1 = \pi$ .

#### 4 SYMPLECTIC FIBRATIONS

We will begin by describing the general theory of (nonsingular) symplectic fibrations that originated in work of Guillemin, Lerman and Sternberg [GLS], and then will discuss some of the recent results about their structure.

##### 4.1 SYMPLECTIC CONNECTIONS AND HAMILTONIAN FIBRATIONS

A (nonsingular) fibration  $p : P \rightarrow B$  is said to be *symplectic* if its fiber is a symplectic manifold  $(M, \omega)$  and the structural group of the fibration is  $\text{Symp}(M, \omega)$ . It follows that every fiber  $M_b = p^{-1}(b)$  carries a well defined symplectic form  $\omega_b$ . However, neither the base  $B$  nor the total space  $P$  need have a symplectic form. (In fact, here we may take the base to be any CW complex.)

There is an especially nice theory when all spaces involved are manifolds and  $p$  is smooth. (In this case we will say that the fibration is smooth.) A 2-form  $\tau$  on  $P$  that restricts to  $\omega_b$  on each fiber  $M_b$  is called a *connection 2-form*. Note that  $\tau$  need not be either closed or nondegenerate. Nevertheless, the fact that it is nondegenerate on the fibers implies that its restriction to the inverse image  $p^{-1}(\gamma)$  of any smooth path  $\gamma : [0, 1] \rightarrow B$  in the base has a one-dimensional kernel<sup>9</sup> that is everywhere transverse to the fibers. Hence the integral lines of this kernel are horizontal lifts of  $\gamma$  that define parallel translation of the fibers along  $\gamma$ . It is easy to see from this description that parallel translation preserves the symplectic forms on the fibers precisely when the restriction of  $\tau$  to any submanifold of the form  $p^{-1}(\gamma)$  is closed. Thus one needs

$$d\tau(v_1, v_2, \cdot) = 0$$

whenever the vectors  $v_1, v_2$  are vertical, i.e. tangent to a fiber. In this case the connection form  $\tau$  is said to be *symplectic*.

It is not hard to see that every symplectic fibration has a symplectic connection  $\tau$ . However, one cannot always choose  $\tau$  to be closed. For example, if  $p : S^3 \rightarrow S^2$  is the Hopf map, the composite map  $S^3 \times S^1 \rightarrow S^3 \xrightarrow{p} S^2$  can be given the structure of a symplectic fibration, but clearly does not support a closed connection 2-form.

---

<sup>9</sup>The kernel is spanned by vectors  $v$  such that  $\tau(v, w) = 0$  for all vectors  $w$  tangent to  $p^{-1}(\gamma)$ . This is a generalization of the characteristic foliation on a hypersurface in the sense that if  $\tau$  were a symplectic form on  $P$  then this kernel would consist precisely of the vectors tangent to the characteristic foliation of  $\tau$  on the hypersurface  $p^{-1}(\gamma)$ .

Thurston showed in [Th] that there is a closed connection form if and only if there is a cohomology class  $a \in H^2(P, \mathbf{R})$  that restricts to the symplectic class  $[\omega_b]$  in each fiber. There are some obvious situations in which such a class  $a$  always exists, for example if  $[\omega_b]$  is the first Chern class of the tangent bundle to the fibers.<sup>10</sup> In [GLS] Guillemin, Lerman and Sternberg prove that if the manifold  $M$  is simply connected every symplectic fibration with fiber  $M$  supports a closed connection 2-form. They give a beautiful construction of this form (that they call the coupling form) from the curvature of a symplectic connection on  $P$ . This result was extended by McDuff–Salamon, who prove the following result in [MS].

**THEOREM 4.1** *Suppose that  $M \rightarrow P \rightarrow B$  is a smooth symplectic fibration with fiber  $(M, \omega)$ . Then the following conditions are equivalent:*

- (i) *The structural group of the fibration can be reduced to  $\text{Ham}(M, \omega)$ ;*
- (ii) *The fibration is symplectically trivial over the 1-skeleton of  $B$  and supports a closed connection 2-form.*

**NOTE** One needs to assume triviality over the 1-skeleton of  $B$  because the group  $\text{Ham}(M, \omega)$  is path-connected. It should be possible to define a subgroup  $H$  of  $\text{Symp}(M, \omega)$  such that fibrations with structural group  $H$  are precisely those with closed connection 2-form: see [LMP3]. This group  $H$  would have to be disconnected and have identity component equal to  $\text{Ham}(M, \omega)$ .

**DEFINITION 4.2** A smooth symplectic fibration  $p : M \rightarrow B$  is said to be *Hamiltonian* if it satisfies one of the equivalent conditions in the above theorem. A symplectic form  $\Omega$  on the total space of a symplectic fibration  $p : P \rightarrow B$  is said to be *compatible with the fibration* if restricts to  $\omega_b$  on each fiber  $M_b$  of  $p$ .

**PROPOSITION 4.3** *Let  $p : P \rightarrow B$  be a Hamiltonian fibration and suppose that  $B$  has a symplectic form  $\sigma_B$ . Then there is a symplectic form  $\Omega$  on  $P$  that is compatible with  $p$  and is unique up to deformation.*

**PROOF:** Take  $\Omega = \tau + \kappa p^*(\sigma_B)$ , where  $\tau$  is some closed connection form and  $\kappa > 0$  is sufficiently large. For more details see [Th] (or [MS]).

## 4.2 THE TOPOLOGY OF SYMPLECTIC FIBRATIONS

One way to construct symplectic fibrations is to start with an element  $\phi \in \pi_k(\text{Symp}(M, \omega))$  and use it as a clutching function to construct a bundle over  $S^{k+1}$ :

$$p : P_\phi = (D_+^{k+1} \times M) \cup_\phi (D_-^{k+1} \times M) \rightarrow S^{k+1}.$$

When  $k > 1$  the resulting fibrations are Hamiltonian, but this may not be so when  $k = 1$  since  $\pi_1(\text{Ham}(M, \omega))$  is often different from  $\pi_1(\text{Symp}(M, \omega))$ : see § 2.6. Since  $S^2$  is symplectic, it follows from Proposition 4.3 above that the loop  $\phi$  is Hamiltonian precisely when the total space  $P_\phi$  carries a symplectic form  $\Omega$  that is compatible with the fibration  $p : P_\phi \rightarrow S^2$ .

<sup>10</sup>Note that this bundle has a well defined complex structure since the space  $\mathcal{J}(\omega_b)$  of fiberwise compatible almost complex structures is contractible for all  $b \in B$ .

Seidel pointed out in [Seid2] that every element of  $\pi_1(\text{Ham}(M, \omega))$  gives rise to an automorphism of the quantum cohomology of  $M$  (cf. § 2.2). By interpreting this automorphism in terms of the geometry of the bundle  $P_\phi \rightarrow S^2$ , Lalonde–McDuff–Polterovich showed in [LMP2] that the Leray spectral sequence for the rational cohomology of the total space  $P_\phi$  degenerates. To do this it is enough to show that every rational homology class  $\alpha \in H_*(M, \mathbf{Q})$  is the intersection with  $[M]$  of a homology class  $\tilde{\alpha} \in H_{*+2}(P)$ . Roughly speaking, one constructs  $\tilde{\alpha}$  as the set of points in  $P$  that lie on a suitable family of  $J$ -holomorphic sections of  $p : P \rightarrow S^2$  that intersect a cycle representing  $\alpha$ .

This argument generalizes significantly, for example to Hamiltonian fibrations over any sphere: see [LMP3].

QUESTION 4.4 *If  $(M, \omega) \rightarrow P \rightarrow B$  is a fibration with structural group  $\text{Ham}(M, \omega)$ , is the rational cohomology  $H^*(P, \mathbf{Q})$  of  $P$  isomorphic as a vector space to  $H^*(B; \mathbf{Q}) \otimes H^*(M, \mathbf{Q})$ ?*

The answer is known to be “yes” when the hard Lefschetz theorem holds for  $H^*(M, \mathbf{Q})$ : see [B]. However, it is “no” if one drops the Hamiltonian condition. For example, the Kodaira–Thurston manifold in [Th] that is symplectic but nonKähler is the total space of a symplectic fibration  $X \rightarrow T^2$  with fiber  $T^2$ . Here

$$X = T^2 \times S^1 \times [0, 1] / \sim, \quad (x, y, s, 0) \sim (x, x + y, s, 1),$$

and it is easily seen that  $b_1(X) = 3$  rather than 4.

The story concerning the multiplicative structure of  $H^*(P, \mathbf{Q})$  is more complicated. Here one can consider both the standard cup product and also versions of the quantum (or deformed) cup product. Seidel exploits properties of the quantum product in his work on  $\text{Symp}(\mathbf{C}P^m \times \mathbf{C}P^n)$  that was mentioned in 2.6 above. He also pointed out<sup>11</sup> that if  $(M, \omega)$  admits no  $J$ -holomorphic spheres at all and if  $P$  is a fibration over  $S^2$  then  $H^*(P, \mathbf{Q})$  is isomorphic as a ring (under cup product) with the product of the rings  $H^*(S^2, \mathbf{Q})$  and  $H^*(M, \mathbf{Q})$ . The following generalization looks very plausible, but the full details of the proof are not yet worked out: see [Mc2]. We say that the quantum product is trivial if it equals the usual cup product.

CLAIM 4.5 *Let  $(M, \omega) \rightarrow P \rightarrow S^2$  be a fibration with structural group  $\text{Ham}(M, \omega)$ , and suppose that the quantum product on  $M$  is trivial. Then  $H^*(P, \mathbf{Q})$  is isomorphic as a ring (under cup product) with the product of the rings  $H^*(S^2, \mathbf{Q})$  and  $H^*(M, \mathbf{Q})$ .*

If the quantum product on  $M$  is nontrivial, no general statement about the ring structure of  $H^*(P)$  has yet been found. Nor is it yet clear what happens with bases other than  $S^2$ .

In view of Donaldson’s work mentioned in §2.3 above, it would be interesting to have an answer to the following question.

---

<sup>11</sup>Private communication



QUESTION 4.6 *To what extent do these results carry over to Lefschetz (i.e. singular) fibrations?*

In the algebraic case there is a good understanding of the cohomology of Lefschetz pencils: see Looijenga [L] for example. However, this is closely related to the fact that the hard Lefschetz theorem holds for algebraic manifolds, and so it is not clear what, if anything, will carry over to the symplectic case.

Finally, we remark that these ideas allow one to decide when the nonsqueezing theorem holds for the fibration  $P \rightarrow S^2$ : see [Mc2]. By this we mean the following. Let  $(P, \Omega)$  be a symplectic  $(2n+2)$ -dimensional manifold such that  $\Omega$  is compatible with the fibration  $P \rightarrow S^2$ , and define the *area* of  $(P, \Omega)$  to be the number  $A$  such that

$$\frac{1}{(n+1)!} \int_P \Omega^{n+1} = \frac{A}{n!} \int_M \omega^n.$$

Thus, if the fibration  $P \rightarrow S^2$  is symplectically trivial so that  $(P, \Omega)$  is the product  $(S^2 \times M, \sigma \oplus \omega)$ ,  $A$  is simply the area of the base  $(S^2, \sigma)$ . Then we will say that *the nonsqueezing theorem holds for the fibration  $p : (P, \Omega) \rightarrow S^2$*  if the area  $A$  constrains the size of the balls that embed into  $(P, \Omega)$ , i.e. if  $\pi r^2 \leq A$  whenever  $B^{2n+2}(r)$  embeds symplectically in  $(P, \Omega)$ . By considering the case when  $P$  is  $\mathbf{C}P^2$  blown up at a point, it is not hard to see that some condition is needed in order for the nonsqueezing theorem to hold. It looks very likely that by studying properties of  $J$ -holomorphic sections one can establish the following claim: see [Mc2].

CLAIM 4.7 *Let  $p : P \rightarrow S^2$  be a symplectic fibration whose fiber  $(M, \omega)$  has trivial quantum product, and let  $\Omega$  be a symplectic form on  $P$  compatible with  $p$ . Then the nonsqueezing theorem holds for the fibration  $p : (P, \Omega) \rightarrow S^2$ .*

## References

- [Ab] M. Abreu, Topology of symplectomorphism groups of  $S^2 \times S^2$ , *Inventiones Mathematicae*, 131 (1998), 1–23.
- [AM] M. Abreu and D. McDuff, Topology of symplectomorphism groups of rational ruled surfaces, in preparation.
- [Au] D. Auroux, Asymptotically holomorphic families of symplectic submanifolds, *Geometric and Functional Analysis*, 7(1997), 971–995.
- [BP] M. Bialy and L. Polterovich, Geodesics of Hofer’s metric on the group of Hamiltonian diffeomorphisms, *Duke Mathematical Journal*, 76 (1994), 273–292.
- [Bi] Biran, P. Symplectic packing in dimension 4 *Geometric and Functional Analysis*, 7 (1997), 420–37.
- [B] A. Blanchard, Sur les variétés analytiques complexes, *Ann. Sci. Ec. Norm. Sup.*, (3) 73, (1956).
- [C] V. Colin, Stabilité topologique des structures de contact en dimension 3, preprint ENS Lyon # 225, (1998).
- [D1] S. K. Donaldson, Symplectic submanifolds and almost-complex geometry, *Journ. of Differential Geometry* 44 (1996), 666–705.

- [D2] S. K. Donaldson, Symplectic submanifolds and topological Lefschetz fibrations, in preparation.
- [EH] I. Ekeland and H. Hofer, Symplectic topology and Hamiltonian dynamics. *Mathematische Zeitschrift*, 200 (1989), 355–78.
- [E1] Y. Eliashberg, The theorem on the structure of wave fronts and its applications in symplectic topology. *Functional Analysis and Applications*, 21 (1987), 65–72.
- [E2] Y. Eliashberg, Topological characterization of Stein manifolds of dimension  $> 2$ . *International Journal of Mathematics*, 1, (1990) 29–47.
- [E3] Y. Eliashberg, Contact manifolds twenty years since J. Martinet’s work. *Annales de l’Institut Fourier*, 42 (1992), 165–92.
- [EP] Y. Eliashberg and L. Polterovich, New Applications of Luttinger’s surgery, *Comment. Math. Helveticae*, 69 (1994), 512–522.
- [ET] Y. Eliashberg and W. Thurston, *Confoliations*, University Lecture Series # 13, American Mathematical Society, Providence (1998).
- [FHW] A. Floer, H. Hofer and K. Wysocki, Applications of symplectic homology I. *Mathematische Zeitschrift* 217 (1994), 577–606.
- [FS] R. Fintushel and R. Stern, Knots, links and 4-manifolds, preprint (1996).
- [FO] K. Fukaya and K. Ono, Arnold conjecture and Gromov–Witten invariants, preprint (1996)
- [Gi] E. Giroux, Structures de contact sur les fibrés aux cercles, Preprint (1994)
- [Go] R. Gompf, A new construction for symplectic 4-manifolds, *Annals of Mathematics*, 142 (1995), 527–595.
- [G1] M. Gromov, Pseudo holomorphic curves in symplectic manifolds, *Inventiones Mathematicae*, 82 (1985), 307–47.
- [G2] M. Gromov, Soft and hard symplectic geometry. In *Proceedings of the ICM at Berkeley 1986*, Vol. 1, pp. 81–98. American Mathematical Society, Providence, RI, (1987).
- [GLS] V. Guillemin, E. Lerman, and S. Sternberg, *Symplectic fibrations and multiplicity diagrams*. Cambridge University Press, (1996).
- [H] H. Hofer, On the topological properties of symplectic maps. *Proceedings of the Royal Society of Edinburgh*, 115 (1990), 25–38.
- [HS] H. Hofer and D. Salamon,  $J$ -holomorphic curves, multi-valued perturbations, and rational Gromov–Witten invariants, in preparation.
- [IP1] E. Ionel and T. Parker, The Gromov invariants of Ruan–Rian and Taubes, preprint (1997).
- [IP2] E. Ionel and T. Parker, Gromov–Witten invariants of symplectic sums, preprint (1998)
- [LM1] F. Lalonde and D. McDuff, The geometry of symplectic energy, *Annals of Mathematics*, 141 (1995), 349–371.
- [LM2] F. Lalonde and D. McDuff, Hofer’s  $L^\infty$  geometry: geodesics and stability, I, II. *Invent. Math.* 122 (1995), 1–33, 35–69.

- [LM3] F. Lalonde and D. McDuff, Local nonsqueezing theorems and stability, *Geometric and Functional Analysis*, 5, (1995) 364–386.
- [LM4] F. Lalonde and D. McDuff, The classification of ruled symplectic 4-manifolds, *Math. Research Letters* 3, (1996), 769–778.
- [LMP1] F. Lalonde, D. McDuff and L. Polterovich, On the Flux conjectures, CRM Proceedings and Lecture Notes vol 15, (1998), 69–85
- [LMP2] F. Lalonde, D. McDuff and L. Polterovich, Topological rigidity of Hamiltonian loops and quantum homology, to appear in *Inventiones Mathematicae*.
- [LMP3] F. Lalonde, D. McDuff and L. Polterovich, On Hamiltonian fibrations, in preparation.
- [LL1] T. J. Li and A. Liu, General wall crossing formula, *Math Research Letters* 2 (1995), 797–810.
- [LL2] T. J. Li and A. Liu, Symplectic structure on ruled surfaces and generalized adjunction formula, *Math Research Letters* 2 (1995), 453–471.
- [LiT] Jun Li and G. Tian, Virtual moduli cycles and Gromov–Witten invariants for general symplectic manifolds, preprint alg-geom 9608032.
- [Liu] A. Liu, Some new applications of general wall crossing formula, *Math Research Letters* 3 (1995), 569–586.
- [LiuT] G. Liu and G. Tian, Floer homology and Arnold conjecture, (1996) to appear in *Journal of Differential Geometry*.
- [L] E. Looijenga, Cohomology and Intersection Homology of Algebraic Varieties, in *Complex Algebraic Geometry* ed. J. Kollar, IAS/Park City Math Series Vol 3, AMS/IAS, (1997)
- [Lu] K. Luttinger, Lagrangian tori in  $\mathbf{R}^4$ , *Journal of Differential Geometry* 42 (1995), 220–228.
- [MW] J. McCarthy and J. Wolfson, Symplectic normal connect sum, *Topology* 33 (1994), 729–764.
- [Mc1] D. McDuff, From symplectic deformation to isotopy, to appear in the Proceedings of the conference at Irvine 1996, ed Stern, International Press.
- [Mc2] D. McDuff, Quantum homology of fibrations over  $S^2$ , in preparation.
- [MS] D. McDuff and D.A. Salamon, *Introduction to Symplectic Topology*, 2nd edition, OUP, Oxford (1998).
- [MSy] D. McDuff and M. Symington, Associativity properties of the symplectic sum, *Math. Research Letters* 3, (1996), 591–608.
- [P] L. Polterovich, Geometry on the group of Hamiltonian diffeomorphisms, *Doc. Math. J. DMV Extra Volume ICM II*, (1998) 401–410.
- [OO] H. Ohta and K. Ono, Notes on symplectic 4-manifolds with  $b_2^+ = 1$ , II, *Internat. Journal of Math* 7, (1996) 755–70.
- [R] Y. Ruan, Virtual neighborhoods and pseudoholomorphic curves, preprint alg-geom 9611021.
- [RT] Y. Ruan and G. Tian, A mathematical theory of quantum cohomology. *Journ Diff Geo* 42 (1995), 259–367.

- [Sch] F. Schlenk, On symplectic folding, in preparation.
- [Seid1] P. Seidel, Floer homology and the symplectic isotopy problem. PhD thesis, Oxford, (1997).
- [Seid2] P. Seidel,  $\pi_1$  of symplectic automorphism groups and invertibles in quantum cohomology rings, *Geometric and Functional Analysis*, 7 (1997), 1046–95.
- [Sied3] P. Seidel, On the group of symplectic automorphisms of  $\mathbf{C}P^m \times \mathbf{C}P^n$ , preprint (1998)
- [Sieb] B. Siebert, Gromov–Witten invariants for general symplectic manifolds, preprint (1997)
- [Sik] J.-C. Sikorav, Construction de sous-variétés symplectiques, Seminaire Bourbaki no 844, (March 1998).
- [Sym] M. Symington, A new symplectic surgery: the 3-fold sum, preprint (1997).
- [T1] C. H. Taubes, The Seiberg–Witten invariants and symplectic forms, *Math. Res. Letters* 1 (1994), 809–822
- [T2] C. H. Taubes, More constraints on symplectic forms from Seiberg–Witten invariants, *Math. Research Letters* 2 (1994), 9–14.
- [T3] C. H. Taubes, The Seiberg–Witten and the Gromov invariants, *Math. Research Letters* 2, (1995), 221–238.
- [T4] C. H. Taubes,  $SW \implies Gr$ : From the Seiberg–Witten equations to pseudo-holomorphic curves, *J. Amer. Math Soc* 9 (1996), 845–918
- [T5] C. H. Taubes, Counting pseudoholomorphic submanifolds in dimension 4, *Journal of Differential Geometry* 44, (1996), 818–893.
- [T6] C. H. Taubes,  $Gr \implies SW$ : From pseudo-holomorphic curves to the Seiberg–Witten equations, preprint, to appear in the Proceedings of the conference at Irvine 1996, ed Stern, International Press.
- [Th] W. Thurston, Some simple examples of symplectic manifolds. *Proceedings of the American Mathematical Society*, 55, (1976) 467–8.
- [Tr] L. Traynor, Symplectic packing constructions, *Journal of Differential Geometry* 42 (1995), 411–429.

Dusa McDuff  
SUNY Stony Brook  
Department of Mathematics  
NY 11794-3651 Stony Brook  
USA



SOLVABLE LATTICE MODELS  
AND  
REPRESENTATION THEORY OF QUANTUM AFFINE ALGEBRAS

TETSUJI MIWA

ABSTRACT. A review on some recent developments in solvable lattice models in connection with the representation theory of the quantum affine algebras is given.

Keywords and Phrases: the XXZ model, the six-vertex model, the quantum affine algebras, the qKZ equation, the corner transfer matrix, the intertwiner

## 1 THE XXZ MODEL: A SOLVABLE SYSTEM OF INFINITE DEGREES OF FREEDOM

The aim of this talk is to review some recent (in 90's) progress in solvable lattice models. I will, in particular, stress the connection with the representation theory of the quantum affine algebras. In this section, I introduce the XXZ model and the six-vertex model, state the problems we wish to solve and give the clue to the solvability of these models. I also give some results in prehistoric ages (i.e., before '85, the birth of Quantum Groups) which led us to this connection.

### 1.1 THE XXZ HAMILTONIAN

Consider the one-dimensional quantum Hamiltonian with a real parameter  $\Delta$ ,

$$H = -\frac{1}{2} \sum_k (\sigma_k^x \sigma_{k+1}^x + \sigma_k^y \sigma_{k+1}^y + \Delta \sigma_k^z \sigma_{k+1}^z). \quad (1)$$

Here  $\sigma^x, \sigma^y, \sigma^z$  are the Pauli matrices, and the index  $k$  signifies the  $k$ -th component of the tensor product  $\otimes_k V_k$  of the two-dimensional spaces  $V_k \simeq V = \mathbf{C}v_0 \oplus \mathbf{C}v_1$ . The Hamiltonian (1) is called the XXZ Hamiltonian.

Here we have not specified the range of the index  $k$ . If the range is finite, e.g., an interval  $0 \leq k \leq N-1$  or a periodic chain  $k \in \mathbf{Z}/N\mathbf{Z}$ , both the space  $\otimes_k V_k$  and the operator  $H$  are well-defined. However, in physics, we are interested in the large volume limit, i.e.,  $N = \infty$ , where the number of degrees of freedom of the system becomes infinite. There is no a priori meaning of these expressions in this limit. In fact, some physical quantities are divergent (e.g., the trace of  $e^{-H/kT}$ ).

We say a model is solved if we can extract finite quantities and give them closed expressions.

The problems we are interested in, in general, are

- (A) the diagonalization of the Hamiltonian; and
- (B) the computation of the matrix elements of the local operators; a particular case of (B) is
- (C) the computation of the correlation functions.

## 1.2 VACUUM STATES AS INFINITE LINEAR COMBINATIONS OF PATHS

Our consideration is restricted to the  $T = 0$  case. In this case, we are interested in the lowest eigenvalue of the Hamiltonian and the corresponding eigenvectors (the vacuum states). We are also interested in those eigenvectors whose eigenvalues have finite differences to the lowest one in the large volume limit (the excited states).

If  $\Delta \rightarrow \pm\infty$ , the Hamiltonian effectively approaches a diagonal one  $H \sim \mp \frac{1}{2} \sum_k \sigma_k^z \sigma_{k+1}^z$ . If  $\Delta = \infty$ , there are two vacuums ( $i = 0, 1$ ),

$$|\bar{p}^{(i)}\rangle = \otimes_k v_{\bar{p}^{(i)}(k)} \quad \text{where } \bar{p}^{(i)}(k) = \frac{1}{2}(1 - (-1)^i). \quad (2)$$

All the spins are equal in the vacuum states. The corresponding eigenvalue is  $-\#\{k\}$ , and therefore divergent in the large volume limit. However, we renormalize the Hamiltonian by replacing  $\sigma_k^z \sigma_{k+1}^z$  by  $\sigma_k^z \sigma_{k+1}^z - 1$  so that its lowest eigenvalue is 0. On the other hand, if  $\Delta = -\infty$ , the vacuums ( $i = 0, 1$ ) are

$$|p^{(i)}\rangle = \otimes_k v_{p^{(i)}(k)} \quad \text{where } p^{(i)}(k) = \frac{1}{2}(1 - (-1)^{k+i}). \quad (3)$$

The spins are alternating in the vacuum states. The renormalization of the Hamiltonian is such that  $\sigma_n^z \sigma_{n+1}^z + 1$ .

If  $\Delta$  is finite we must take account of the interaction terms  $\sigma_k^x \sigma_{k+1}^x + \sigma_k^y \sigma_{k+1}^y$ . These terms are non-diagonal and mix the vectors of the form  $|p\rangle = \otimes_k v_{p(k)}$ . However, they preserve the total spin of the vectors, i.e.,  $\frac{1}{2} \sum_k (1 - 2p(k))$ . Therefore, if  $|\Delta|$  is sufficiently large, it is natural to expect that the vacuum states are contained in the same subspace of total spin as  $|\bar{p}^{(i)}\rangle$  or  $|p^{(i)}\rangle$ . In fact, this is true. For  $\Delta \sim \infty$ , this implies that  $|\bar{p}^{(i)}\rangle$  remains as the vacuum.

The case  $\Delta \sim -\infty$  is more interesting because the vacuum states are linear combinations of (3) and other vectors of total spin 0 (we assume  $N$  is even). If  $N$  is infinite, infinitely many terms appear in the linear combination. Mathematically, this is a serious problem because it is not clear if we can introduce a suitable topology in order to deal with this infinite sum.

One can make a perturbation expansion of the vacuum state in the form

$$|vac\rangle_i = \sum_p c(p) |p\rangle \quad \text{where } |p\rangle = \otimes_{k \in \mathbf{Z}} v_{p(k)}. \quad (4)$$

Note that  $N = \infty$  in this formula. We set  $c(p^{(i)}) = 1$  and the other coefficients are of the form  $c(p) = \sum_{j \geq 1} c_j(p) \varepsilon^j$  with  $\varepsilon = \Delta^{-1}$ . In principle, one can determine

each coefficient  $c_j(p)$  recursively by solving the equation  $H_{re}|vac\rangle_i = 0$ . Here the renormalized Hamiltonian  $H_{re}$  is given in the form

$$H_{re} = -\frac{1}{2} \sum_k \left( \sigma_k^x \sigma_{k+1}^x + \sigma_k^y \sigma_{k+1}^y + \Delta (\sigma_k^z \sigma_{k+1}^z + 1 + \sum_{j \geq 1} r_j \varepsilon^j) \right), \quad (5)$$

in which the coefficients  $r_j$  are determined in each step of the recursion to remove the divergence and to make the eigenvalue 0.

An important feature of this expansion is that  $c(p)$  is zero unless  $p(k) = p^{(i)}(k)$  for all but finite  $k$ . We call such  $p$  a *path* belonging to the  $i$ -th ground-state.

### 1.3 PHASES OF THE XXZ MODEL

If we vary  $\Delta$  from  $-\infty$  to  $\infty$ , the eigenvalues cross each other. The vacuum states change from one region to another when the eigenvalues cross. In the infinite volume limit, it is known that there are three different phases (see, e.g., [1]),

$$(i) \Delta < -1, \quad (ii) -1 \leq \Delta \leq 1, \quad (iii) \Delta > 1. \quad (6)$$

We have already mentioned (i) and (iii). The phase (ii) is such that the vacuum state belongs to the subspace of the total spin 0. In this phase, there is a unique vacuum state, which belongs to the space of total spin 0. Nothing like the path expansion (4) is available because there is no special limit where the Hamiltonian is diagonal. I will discuss that this difference between phase (i) and (ii) causes an essential difference in our treatment of the model in the representation theory. As for the phase (iii), where the vacuum states are trivial, there is nothing to say about from the representation theory, and I will not discuss this phase any further.

### 1.4 EXCITED STATES AND PARTICLES

The method invented by Bethe when he solved the XXX model is called the Bethe Ansatz. It starts with finite periodic  $N$ , and consider the infinite volume limit in the second step. The key idea in this method is to introduce the notion of quasi-particles borrowed from the quantum field theory.

For finite  $N$ , there exist only finitely many eigenvectors of the Hamiltonian. It has only discrete eigenvalues. However, in the infinite volume limit, continuous spectra appear. To parametrize the eigenvectors belonging to the continuous spectra we need continuous parameters. The Bethe Ansatz uses a set of continuous parameters  $\beta_1, \dots, \beta_n$ , called the rapidity variables, to parametrize the eigenvectors in the finite volume. An eigenstate parametrized by  $n$  continuous parameters is called an  $n$  quasi-particle state. Since there are only finitely many eigenvectors, only some discrete values of the quasi-momenta are allowed to give actual eigenvectors.

The vector  $|p^{(0)}\rangle = \otimes_k v_0$  is the 0 quasi-particle state. One quasi-particle state is a linear combination of  $|p\rangle$  such that  $p(k) = 1$  for one and only one  $k$ , and so on for two and more quasi-particle states. This picture is not appropriate in



the phases (i) and (ii), and, in particular, in the large volume limit, because the vacuum states in this terminology are  $\frac{N}{2}$  particle states. In these phases,  $n(> 0)$  quasi-particle states may have lower ‘energies’ (=eigenvalues of the Hamiltonian) than the 0 quasi-particle state. There is a trick to reparametrize the vacuum and the excited states in such a way that the vacuum states are the 0 particle states and the excited states are the  $n(> 0)$  particle states. This is possible only in the infinite volume limit. I stress this point because in many cases something good happens only in the infinite volume limit. The remarkable thing in this parametrization is that the renormalized energy of an  $n$ -particle state with the rapidities  $\beta_j(1 \leq j \leq n)$  is given by an additive formula  $\sum_j \varepsilon(\beta_j)$ . The function  $\varepsilon(\beta)$  is a simple function, e.g., if  $\Delta = -1$ , we have  $\varepsilon(\beta) = \frac{\pi}{\text{ch } \beta}$ . Each particle with the rapidity  $\beta_j$  carries the energy  $\varepsilon(\beta_j)$ . This is the reason why these states are called the  $n$ -particle states.

Note that, if  $\Delta = -1$  the above formula tells that there is no energy gap between the vacuum and the excited states: The energy difference  $\varepsilon(\beta)$  approaches 0 if  $|\beta| \rightarrow \infty$ . This property is called ‘massless’ by using the language of quantum field theory. In statistical mechanics, this is called ‘critical’. In the phase (ii) the particles are massless, while in the phase (i) they are massive.

A further remarkable fact about the particle structure, valid both in the massive and the massless phases, is the degeneracy of the  $n$ -particle states ([15, 6]). A clear view of this fact was given in [6] for  $\Delta = -1$ . I write their formula in the form adapted to our notation. Denote the space of the eigenvectors of the Hamiltonian by  $\mathcal{F}$ . We call it the physical space. We have the decomposition

$$\mathcal{F} = \bigoplus_{n \geq 0, \text{even}} \prod_{j=1}^n \int_{-\infty}^{\infty} \frac{d\beta_j}{2\pi} [\otimes_{j=1}^n (\mathbf{C}^2)_{\beta_j}]_{\text{sym}} \tag{7}$$

It means that the  $n$ -particle states with a fixed set of rapidities  $(\beta_1, \dots, \beta_n)$  have  $2^n$ -fold degeneracy. This degeneracy is identified with the tensor product  $\otimes^n \mathbf{C}^2$ .

Here is a key to the connection with the representation theory. The Hamiltonian (1) with  $\Delta = -1$  has a global  $sl_2$  symmetry, i.e., there exists an  $sl_2$  action on  $\otimes_k V_k$  which commutes with the Hamiltonian. The formula (7) claims that the vector space of the  $n$ -particle states with rapidities  $(\beta_1, \dots, \beta_n)$  is isomorphic to

$$\otimes^n \mathbf{C}^2 = \bigoplus_{\varepsilon_1, \dots, \varepsilon_n = 0, 1} \mathbf{C}v_{\varepsilon_1} \otimes \dots \otimes \mathbf{C}v_{\varepsilon_n}. \tag{8}$$

as  $sl_2$ -module. In other words, we have a complete parameterization of the excited states by the rapidities  $(\beta_1, \dots, \beta_n)$  and the isospins  $(\varepsilon_1, \dots, \varepsilon_n)$ . Let us denote this state by  $|\beta_n, \dots, \beta_1\rangle_{\varepsilon_n, \dots, \varepsilon_1}$ .

There is a further symmetry of the  $n$ -particle states that is indicated by the symbol  $\left[ \right]_{\text{sym}}$  in (7): There exists a matrix  $S(\beta)$  depending on the rapidity variable  $\beta$ , which acts on  $\mathbf{C}^2 \otimes \mathbf{C}^2$ . This is called the  $S$ -matrix. The  $S$ -matrix exchanges the rapidities of  $n$ -particle states.

$$\begin{aligned} & |\beta_n, \dots, \beta_j, \beta_{j+1}, \dots, \beta_1\rangle_{\varepsilon_n, \dots, \varepsilon_j, \varepsilon_{j+1}, \dots, \varepsilon_1} \tag{9} \\ &= \sum_{\varepsilon'_j, \varepsilon'_{j+1}} S(\beta_j - \beta_{j+1})_{\varepsilon_j, \varepsilon_{j+1}}^{\varepsilon'_j, \varepsilon'_{j+1}} |\beta_n, \dots, \beta_{j+1}, \beta_j, \dots, \beta_1\rangle_{\varepsilon_n, \dots, \varepsilon'_{j+1}, \varepsilon'_j, \dots, \varepsilon_1}. \end{aligned}$$

I will give the explicit formula of the  $S$ -matrix only later when I discuss the sine-Gordon theory.

The meaning of the rapidity variables in the representation theory is unclear at this stage because a larger symmetry is still hidden behind. In Section 2, I will show that the hidden symmetry distinguishes the rapidities. The particles with different rapidities correspond to different (i.e., non-isomorphic) representations.

### 1.5 CORRELATION FUNCTIONS

Now, I will explain what (B) and (C) mean. We call a linear operator acting on  $\otimes_{k \in \mathbf{Z}} V_k$  local if its action is restricted to a finite interval of the one-dimensional lattice  $\mathbf{Z}$  where the index  $k$  runs. The Hamiltonian is not local though each summand in (1) is local.

The correlation functions are the vacuum-to-vacuum matrix element of local operators. If we take a local operator acting on  $n$  sites of the lattice, its correlation function is called an  $n$ -point function. Quantities of physical interest are often given in terms of the correlation functions. For example, the one point function

$$P^{(i)}(k) = \frac{i \langle vac | \sigma_k^z | vac \rangle_i}{i \langle vac | vac \rangle_i} \quad (10)$$

gives the magnetization.

Introduce a new parameter  $q$  by  $\Delta = \frac{1}{2}(q + q^{-1})$ . The massive phase is  $-1 < q < 0$  and, the massless phase is  $|q| = 1$ . Here we are considering the one-point function in the massive phase.

By obvious reasons, the one-point function satisfies  $P^{(1-i)}(k+1) = P^{(i)}(k)$  and  $P^{(0)}(0) + P^{(1)}(0) = 0$ . The function  $P^{(0)}(0)$  was computed by Baxter ([2]):

$$P^{(0)}(0) = \prod_{k=1}^{\infty} \left( \frac{1 - q^{2k}}{1 + q^{2k}} \right)^2. \quad (11)$$

The above  $q$  is identified with the  $q$  in the affine quantum algebra  $U_q(\widehat{sl}_2)$ . The representation theory of  $U_q(\widehat{sl}_2)$  provides us with the scheme for computing the general correlation functions, and the general matrix elements of local operators with respect to the excited states. I will explain this in Section 4.

## 2 QUANTUM AFFINE ALGEBRAS: THE STRUCTURE UNDERLYING THE SOLVABILITY

An operator which commutes with the Hamiltonian is called its symmetry. In this section I discuss the symmetries of the XXZ Hamiltonian. There are two kinds of symmetries, abelian and non-abelian. The latter is the symmetry of the quantum affine algebra  $U_q(\widehat{sl}_2)$ . This algebra underlies the solvability of the XXZ Hamiltonian.

## 2.1 INTEGRABILITY AND THE TRANSFER MATRIX

What I have described in the previous section is heavily dependent on the special choice of the Hamiltonian (1). In the infinite volume limit, in general, Hamiltonians have infinitely degenerate eigenvalues. This is an obstacle for the diagonalization. In the XXZ case, this infinite degeneracy is decomposed into finite degeneracy in the particle structure: If the number of particles and their rapidities are fixed, the degeneracy reduces to finite. The decomposition is explained as follows.

The XXZ Hamiltonian on the finite  $N$ -periodic lattice has an abelian (i.e., mutually commuting) family of symmetries. The simultaneous eigenspaces of this commuting family of operators give rise to the decomposition into the particles in the infinite volume limit.

Let us discuss the commuting family. There exists a family of operators  $T(\zeta)$  parametrized by a complex parameter  $\zeta$

$$T(\zeta)(\otimes_k v_{\varepsilon_k}) = \sum_{\{\varepsilon'_k\}_{k \in \mathbf{Z}/N\mathbf{Z}}} T(\zeta)_{\{\varepsilon'_k\}}^{\{\varepsilon_k\}} (\otimes_k v_{\varepsilon'_k}). \quad (12)$$

We have

$$[T(\zeta_1), T(\zeta_2)] = 0, \quad (13)$$

$$T(1) \text{ is the shift operator, i.e., } T(1)_{\{\varepsilon'_k\}}^{\{\varepsilon_k\}} = \prod_k \delta_{\varepsilon_{k+1}, \varepsilon'_k}, \quad (14)$$

$$T(1)^{-1}T(\zeta) = 1 + (c_1 H + c_2)(\zeta - 1) + O((\zeta - 1)^2). \quad (15)$$

This operator naturally appears in the study of a statistical mechanical model of a different kind, which I will explain in the next section.

## 2.2 THE SIX-VERTEX MODEL

The operator  $T(\zeta)$  appears in the six-vertex model, a model in classical statistical mechanics on the two dimensional lattice. Consider a 'lattice' consisting of lines in the two dimensional plane. The lines are either horizontal or vertical. We call an intersection of two lines a *vertex*. We associate a local variable  $\varepsilon_k$  to each edge  $k$ , which is a line segment between two neighboring vertices. The variable  $\varepsilon_k$  takes values 0 or 1.

A configuration  $\mathcal{C}$  is an assignment of values 0 or 1 to all the local variables. Consider a vertex  $v$ , and a local configuration around the vertex, say  $\varepsilon'_1$  and  $\varepsilon_1$  for the upper and the lower edges on the vertical line, and  $\varepsilon'_2$  and  $\varepsilon_2$  for the right and the left edges on the horizontal line. We associate a local weight,  $R_{\varepsilon'_1, \varepsilon'_2}^{\varepsilon_1, \varepsilon_2}$ , called the Boltzmann weight, to each local configuration. We consider these weights as the matrix elements of an matrix  $R$  acting on  $V \otimes V$ :

$$R(v_{\varepsilon_1} \otimes v_{\varepsilon_2}) = \sum_{\varepsilon'_1, \varepsilon'_2} R_{\varepsilon'_1, \varepsilon'_2}^{\varepsilon_1, \varepsilon_2} v_{\varepsilon'_1} \otimes v_{\varepsilon'_2}. \quad (16)$$

The most basic quantity in classical statistical mechanics is the partition function  $Z$ . This is the sum of the product of the local Boltzmann weights; the

sum is taken over all the configurations and the product is taken over all the vertices.

$$Z = \sum_{\mathcal{C}} \prod_v R_{\varepsilon'_1(v,\mathcal{C}),\varepsilon'_2(v,\mathcal{C})}^{\varepsilon_1(v,\mathcal{C}),\varepsilon_2(v,\mathcal{C})}. \tag{17}$$

Sometimes it is necessary to consider similar configuration sums for a different arrangement of lines, e.g., by introducing lines with different angles.

Now, consider a vertical slice of the whole lattice, i.e., a vertical line and the two sets of horizontal edges in the right and left sides of the vertical line. Let us denote the local variables on the right edges by  $\{\varepsilon'_k\}$  and those on the left by  $\{\varepsilon_k\}$ . One can associate a matrix  $T$  acting on  $\otimes_k V_k$ . This is called the transfer matrix:

$$T_{\{\varepsilon'_k\}}^{\{\varepsilon_k\}} = \sum_{\mathcal{C}_s} \prod_{v_s} R_{\varepsilon'_1(v_s,\mathcal{C}_s),\varepsilon'_2(v_s,\mathcal{C}_s)}^{\varepsilon_1(v_s,\mathcal{C}_s),\varepsilon_2(v_s,\mathcal{C}_s)}. \tag{18}$$

Here the subscript  $s$  is put to indicate the restriction to the slice. The configuration  $\mathcal{C}_s$  is fixed to  $\{\varepsilon'_k\}$  and  $\{\varepsilon_k\}$  on the horizontal edges.

The transfer matrix is convenient in the calculation of the partition function. For a finite lattice on the torus  $Z = \text{tr } T^N$  where  $N$  is the number of the vertical lines on the torus.

So far, I have discussed general setting for a type of models called *vertex models*. Now, I introduce the six-vertex model whose transfer matrix gives the commuting family of operators satisfying (13-15).

We associate a rapidity variable  $\beta_j$  to each line  $j$  in the lattice. We set  $\zeta_j = e^{\frac{\pi\beta_j}{\xi}}$ , where  $\xi$  and  $q$  are related by  $q = -e^{-\frac{\pi^2 i}{\xi}}$ . In the massive phase,  $\xi$  is purely imaginary ( $\text{Im } \xi < 0$ ), and in the massless phase,  $\xi > 0$ .

Consider the following  $\bar{R}$  depending on the parameters  $q$  and  $\zeta$ .

$$\bar{R}_{\varepsilon,\varepsilon}^{\varepsilon,\varepsilon} = 1, \bar{R}_{\varepsilon,1-\varepsilon}^{\varepsilon,1-\varepsilon} = \frac{q(1-\zeta^2)}{1-q^2\zeta^2}, \bar{R}_{1-\varepsilon,\varepsilon}^{\varepsilon,1-\varepsilon} = \frac{\zeta(1-q^2)}{1-q^2\zeta^2} \quad (\varepsilon = 0, 1), \tag{19}$$

all the other weights are zero.

The vertex model given by this  $R$ -matrix is called the six-vertex model. Note that only 6 out of 16 local configurations have a non-zero weight.

In general, we choose the Boltzmann weights at a vertex  $v$  to be  $\bar{R}(\zeta_1/\zeta_2)$  if the vertical line passing thorough  $v$  carries the parameter  $\beta_1$  and the horizontal line  $\beta_2$ . With this special choice of the Boltzmann weights, the partition function has a large symmetry, i.e., it is invariant under deformation of the arrangement of the lines. This is called the  $Z$ -invariance. General  $Z$ -invariance is a straightforward consequence of the simplest case where only three lines are involved. The equation of the  $Z$ -invariance in this case is called the Yang-Baxter equation.

Suppose we define the transfer matrix  $T$  by choosing the parameter  $\zeta$  for the vertical line, and 1 commonly for the horizontal lines. With this choice the transfer matrix  $T(\zeta)$  satisfies (13-15). Note, in particular, that (13) follows from the  $Z$ -invariance.

The origin of the  $Z$ -invariance, or the Yang-Baxter equation, is clarified in the theory of quantum groups. I will explain this in the particular context of the six-vertex model.

2.3  $R$ -MATRICES AS INTERTWINERS [5, 9]

The quantum affine algebra  $U_q(\widehat{sl}_2)$  is a  $q$ -deformation of the universal enveloping algebra  $U(\widehat{sl}_2)$  of the affine Lie algebra  $\widehat{sl}_2$ . The structure and the representation theory of the former for a generic value of  $q$  is not very far from those of the latter which I will recall partly.

The Lie algebra  $\widehat{sl}_2$  is a central extension of the infinite dimensional Lie algebra  $sl_2 \otimes \mathbf{C}[t, t^{-1}]$ . The last one contains two subalgebras that are isomorphic to  $sl_2$ :  $(sl_2)_i = \mathbf{C}e_i \oplus \mathbf{C}f_i \oplus \mathbf{C}h_i$  ( $i = 0, 1$ ) where

$$\begin{aligned} e_0 &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \otimes t, f_0 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \otimes t^{-1}, h_0 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \otimes 1 + c, \\ e_1 &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \otimes 1, f_1 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \otimes 1, h_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes 1. \end{aligned} \quad (20)$$

Here,  $c$  is the central element.

There are two important categories of representations of  $\widehat{sl}_2$ :

$$\text{the affinization of finite dimensional representations;} \quad (21)$$

and

$$\text{the integrable highest weight representations (IHWR).} \quad (22)$$

There exists one-parameter family of automorphisms  $A_\zeta : U(\widehat{sl}_2) \rightarrow U(\widehat{sl}_2)$  sending the generators  $e_i, f_i, h_i$  to  $\zeta e_i, \zeta^{-1} f_i, h_i$ . Given a finite dimensional representation  $M$ , i.e., an algebra map  $\rho : U(\widehat{sl}_2) \rightarrow \text{End}(M)$ , one can define a new representation by  $\rho \circ A_\zeta$ . This representation is called the affinization of  $M$ . For example, there is a natural action of  $\widehat{sl}_2$  on  $V \simeq \mathbf{C}^2$  given by the matrix part of (20). The affinization of  $V$  is denoted by  $V_\zeta$ .

The value of  $c$  is called the level of representation. The level of  $V_\zeta$ , as well as the affinizations of all the finite dimensional representations, is zero.

I will say a few words on IHWR. A representation of  $\widehat{sl}_2$  is called integrable if  $M$  is decomposed into a direct sum of finite dimensional modules by the action of each subalgebra  $(sl_2)_i$ . Let  $\lambda \in (\mathbf{C}h_0 \oplus \mathbf{C}h_1)^*$  be an  $\widehat{sl}_2$ -weight. A vector  $u_\lambda$  is called a highest weight vector with the highest weight  $\lambda$  if  $e_i u_\lambda = 0$ ,  $h_i u_\lambda = \lambda(h_i) u_\lambda$  ( $i = 0, 1$ ). A representation  $M$  is called a highest weight representation if it is generated by a highest weight vector:  $M = U(\widehat{sl}_2) u_\lambda$ . There exists (and, in fact, uniquely exists) an integrable highest weight representation with the highest weight  $\lambda$  if and only if  $\lambda_i = \lambda(h_i)$  is non-negative integer for each  $i$ . We denote it by  $V(\lambda)$ . The level of this representation is equal to  $l = \lambda_0 + \lambda_1$ .

The above story of the representation theory of  $\widehat{sl}_2$  is 'deformed' to that of  $U_q(\widehat{sl}_2)$ . There is, however, one significant difference in the two theories. The tensor product of two representations is defined in both theories. The action is given by the canonical algebra map  $\Delta : U \rightarrow U \otimes U$  ( $U = U(\widehat{sl}_2)$  or  $U = U_q(\widehat{sl}_2)$ ). This map (unfortunately, there is a conflict in the notation ' $\Delta$ ') is called the coproduct. For  $U = U(\widehat{sl}_2)$  the coproduct is given by  $\Delta(X) = X \otimes 1 + 1 \otimes X$  for

$X \in \mathfrak{sl}_2$ . It is invariant with respect to the transposition  $\sigma : U \otimes U \rightarrow U \otimes U$ ,  $\sigma(x \otimes y) = y \otimes x$ . Namely, we have  $\sigma \circ \Delta = \Delta$ . This is no longer true after the deformation:  $\Delta$  and  $\Delta' = \sigma \circ \Delta$  are different.

A question arises. Are the two actions on the tensor product, one given by  $\Delta$  and the other given by  $\Delta'$ , isomorphic? The answer is ‘no’ in general. However, it is ‘yes’ in certain situation including the tensor product of two representations from the union of the categories (21) and (22).

I recall the notion of intertwiner, which plays the central role in the following story. Consider two actions of an algebra  $A$ ,  $M_i$  with the action given by  $\rho_i$  ( $i = 1, 2$ ). A map  $F : M_1 \rightarrow M_2$  is called an intertwiner if the following diagram commutes:

$$\begin{array}{ccc} M_1 & \xrightarrow{F} & M_2 \\ \rho_1(a) \downarrow & & \rho_2(a) \downarrow \quad (x \in A). \\ M_1 & \xrightarrow{F} & M_2 \end{array} \tag{23}$$

Consider the tensor product of two affinizations  $V_{\zeta_i}$  ( $i = 1, 2$ ) of the two dimensional representation  $V$  of  $U_q(\widehat{\mathfrak{sl}}_2)$ . The  $R$ -matrix  $\bar{R}(\zeta_1/\zeta_2) \in \text{End}(V_{\zeta_1} \otimes V_{\zeta_2})$ , which gives the Boltzmann weights of the six-vertex model, is the intertwiner of the two representations, one given by  $\Delta$  and the other given by  $\Delta'$ . Namely, we have an equality  $\bar{R}(\zeta_1/\zeta_2)\Delta(x) = \Delta'(x)\bar{R}(\zeta_1/\zeta_2)$  for all  $x \in U_q(\widehat{\mathfrak{sl}}_2)$ .

### 2.4 $U_q(\widehat{\mathfrak{sl}}_2)$ SYMMETRY OF THE XXZ MODEL

After these preparation from the representation theory, it is high time that I told the main idea of this talk: the  $U_q(\widehat{\mathfrak{sl}}_2)$  symmetry of the XXZ Hamiltonian and the transfer matrix of the six-vertex model. It exists only for the massive phase and only in the infinite volume limit. This limitation makes a clear distinction of this symmetry from the abelian symmetry given by the transfer matrix itself.

Formally speaking, the space on which these operators act is the infinite tensor product  $\otimes_{k \in \mathbf{Z}} V_k$  of the two dimensional spaces  $V_k \simeq \mathbf{C}^2$ . We consider these spaces as the two dimensional  $U_q(\widehat{\mathfrak{sl}}_2)$  module with the following actions of the generators.

$$e_0 = f_1 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, e_1 = f_0 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, t_0^{-1} = t_1 = \begin{pmatrix} q & 0 \\ 0 & q^{-1} \end{pmatrix}. \tag{24}$$

Formally speaking again, an action  $\rho_\infty$  on  $\otimes_{k \in \mathbf{Z}} V_k$  is given by the coproduct,  $\Delta(e_i) = e_i \otimes 1 + t_i \otimes e_i$ ,  $\Delta(f_i) = f_i \otimes t_i^{-1} + 1 \otimes f_i$ ,  $\Delta(t_i) = t_i \otimes t_i$ . Namely, we have,

$$\begin{aligned} \Delta_\infty(e_0) &= \sum_k \cdots \otimes \begin{pmatrix} q^{-1} & 0 \\ 0 & q \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots, \\ \Delta_\infty(f_0) &= \sum_k \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} q & 0 \\ 0 & q^{-1} \end{pmatrix} \otimes \cdots, \\ \Delta_\infty(e_1) &= \sum_k \cdots \otimes \begin{pmatrix} q & 0 \\ 0 & q^{-1} \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots, \end{aligned} \tag{25}$$

$$\Delta_\infty(f_1) = \sum_k \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} q^{-1} & 0 \\ 0 & q \end{pmatrix} \otimes \cdots,$$

$$\Delta_\infty(t_0^{-1}) = \Delta_\infty(t_1) = \cdots \otimes \begin{pmatrix} q & 0 \\ 0 & q^{-1} \end{pmatrix} \otimes \begin{pmatrix} q & 0 \\ 0 & q^{-1} \end{pmatrix} \otimes \cdots.$$

This action is obviously not well-defined on arbitrary vectors of the form  $\otimes_{k \in \mathbf{Z}} v_{\varepsilon_k}$  because  $\Delta_\infty(t_1)$  counts the total spin  $q^{\sum_{k \in \mathbf{Z}} \frac{1}{2}(1+(-1)^{\varepsilon_k})}$ . The total spin is finite if we restrict to the vectors  $|p\rangle$  considered in Section 1. Hopefully, if  $-1 < q < 0$ , the formal expressions (25) define actions on certain vectors of the form (4). One can check this idea in the small  $q$  expansion. For example, one can seek for a singlet, i.e., a vector annihilated by all  $\rho_\infty(e_i)$  and  $\rho_\infty(f_i)$  ( $i = 0, 1$ ) starting from the ground state vector  $|p^{(0)}\rangle$  of (3). The result is remarkable. We get the same expansion as the vector  $|vac\rangle_0$ .

Denote the physical space corresponding to the  $i$ -th ground state by  $\mathcal{F}_i$ . We postulate that there is an action  $\rho^{(i)}$  of  $U_q(\widehat{sl}_2)$  on  $\mathcal{F}_i$ , and that the transfer matrix  $T(\zeta)$  intertwines  $\rho^{(0)}$  with  $\rho^{(1)}$ . In other words, the transfer matrix, and in particular, the XXZ hamiltonian, has the  $U_q(\widehat{sl}_2)$  symmetry. If this is true, the  $U_q(\widehat{sl}_2)$  module  $\mathcal{F}_i$  must be highly reducible because the space of the intertwiners, containing all  $T(\zeta)$ , is infinite dimensional. Recall the decomposition (7) for  $\Delta = -1$ . This result suggests how the space  $\mathcal{F}_i$  for  $\Delta < -1$  decomposes with respect to the  $U_q(\widehat{sl}_2)$  action. The rapidity variables  $\beta_j$  in (7) should be the parameters of the affinization  $\zeta_j = e^{\frac{\pi\beta_j}{\varepsilon}}$ .

This is a nice picture. However, its mathematical content is still unclear because we have no means to make a rigorous meaning of the infinite tensor product. In the following sections, I will give a different picture to the space  $\mathcal{F}_i$  which enables us to formulate everything in the representation theory without using the infinite tensor product.

### 3 CFT AND THE SG MODEL:INTEGRABLE QUANTUM FIELD THEORIES

Quantum field theory and statistical mechanics are twins. They share similar ideas in many aspects. Integrable QFT and solvable lattice models, in particular, have a common algebraic structure. In this section, I review a few results of the former, from which we learn how to solve the models by using the symmetry algebras.

#### 3.1 LATTICE THEORY AND CONTINUUM LIMIT

In Section 1, I have described the structure of the eigenvectors of the XXZ model by using the language of QFT. This is possible because of the similarity between QFT and statistical mechanics. In fact, the connection between these two theories is more than a mere analogy because in the continuum limit, lattice theories are described by QFT. The correlation functions of local variables in the former are scaled to those of local fields in the latter. For example, take the two dimensional Ising model. This is a model in classical statistical mechanics on the two

dimensional lattice. We have the scaling identity (see [21, 18])

$$\langle \varphi(0)\varphi(x) \rangle = \lim_{\substack{\varepsilon \rightarrow 0, m, n \rightarrow \infty \\ x=(m\varepsilon, n\varepsilon)}} \langle \sigma_{0,0}\sigma_{m,n} \rangle. \quad (26)$$

Here,  $\varepsilon$  is a parameter in the Ising model such that the system becomes massless at  $\varepsilon = 0$ . This identity along with the  $n$  point generalization defines a massive QFT with the local field  $\varphi(x)$ .

In general, it is rather difficult to carry out the computation in the right hand side. Instead one can study the left hand side by using some other principle, and then identify it with the continuum limit of some statistical mechanical system. This idea was fully developed and extremely successful in the two dimensional conformal field theory, which deals with the short distance behavior of massive QFT.

The success of CFT came from the principle of conformal invariance. The conformal invariance forces the theory to be massless. Therefore, it has no power to say something about the scaling limit of off-critical (massive) models except in the short distance limit. My interest in CFT in this talk lies not in taking the scaling limit like (26) for critical models but in seeking for an algebraic machinery applicable to off-critical models.

### 3.2 PRIMARY FIELDS AND VERTEX OPERATORS [3, 16, 20]

The local fields in CFT have the conformal invariance. This is a symmetry of the Virasoro algebra, which is a central extension of the Lie algebra of vector fields on the unit circle. (I restrict the discussion to the so-called chiral CFT.) This symmetry is a little bit different from the symmetry of the XXZ Hamiltonian discussed in Section 2. The action of  $U_q(\widehat{sl}_2)$  commutes with the XXZ Hamiltonian. The action of Virasoro algebra does not commute with the local fields. However, it induces an adjoint action on the set of local fields, and this action is identified with a highest weight representation.

The operators serving as a highest weight vector in this representation are called the primary fields. It is important to know the primary fields as an operator acting on the physical space of the conformal field theory. The operators in this context is called the vertex operators.

Let us consider the conformal field theory with the symmetry of the affine Lie algebra  $\widehat{sl}_2$ . We fix a positive integer  $l$ . The physical space of this theory is the direct sum of the level  $l$  integrable highest weight representations:  $\mathcal{F}_{\text{CFT},l} = \bigoplus_{\lambda} V(\lambda)$ .

Let  $V_{\zeta}^{(j)}$  be the affinization of the  $2j + 1$  dimensional representation of  $\widehat{sl}_2$ . We considered a special case,  $j = \frac{1}{2}$  in Section 2. The intertwiner of the form

$$\phi^{(j)}(\zeta) : \mathcal{F}_{\text{CFT},l} \rightarrow \mathcal{F}_{\text{CFT},l} \otimes V_{\zeta}^{(j)} \quad (27)$$

exists if and only if  $0 \leq j \leq \frac{l}{2}$ . It is called the vertex operator of level  $l$  and spin  $j$ . This is identified with the primary field which generates the highest weight module with the highest weight  $\lambda$  such that  $\lambda(h_1) = 2j$ .



## 3.3 THE KZ EQUATION

The two-point scaling function of the Ising model (26) is expressed in a closed form by using a solution of the non-linear ordinary differential equation called the Painleve equation. No such result is known for other solvable lattice models that are essentially different from the Ising model. In CFT, the correlation functions satisfy a system of linear partial equations which is a generalization of the hypergeometric differential equation.

Let us consider a particular example, the operator  $\phi^{(\frac{1}{2})}(\zeta)$  in (27). For simplicity we denote it by  $\phi(\zeta)$ . This operator has two components  $\phi_0(\zeta), \phi_1(\zeta)$  corresponding to  $v_0, v_1 \in V_\zeta$ , each of which acts on  $\mathcal{F}_{\text{CFT}, l}$ . Denote by  $|0\rangle$  the highest weight vector in the spin 0 highest weight module. Set

$$f(\zeta_1, \dots, \zeta_n) = \sum_{\varepsilon_1, \dots, \varepsilon_n} f_{\varepsilon_1, \dots, \varepsilon_n}(\zeta_1, \dots, \zeta_n) v_{\varepsilon_1} \otimes \dots \otimes v_{\varepsilon_n} \in V_{\zeta_1} \otimes \dots \otimes V_{\zeta_n} \quad (28)$$

where

$$f_{\varepsilon_1, \dots, \varepsilon_n}(\zeta_1, \dots, \zeta_n) = \langle 0 | \phi_{\varepsilon_1}(\zeta_1) \dots \phi_{\varepsilon_n}(\zeta_n) | 0 \rangle. \quad (29)$$

Let  $P_{jk}$  be the transposition of the  $j$ -th and the  $k$ -th components in the tensor product  $V_{\zeta_1} \otimes \dots \otimes V_{\zeta_n}$ . After some trivial modification the function  $f$  satisfy the following system of linear partial differential equations called the Knizhnik-Zamolodchikov equation.

$$\frac{\partial}{\partial \zeta_j} f(\zeta_1, \dots, \zeta_n) = \frac{1}{l+2} \sum_{k \neq j} \frac{P_{jk}}{\zeta_j - \zeta_k} f(\zeta_1, \dots, \zeta_n). \quad (30)$$

## 3.4 FORM FACTORS OF THE SG MODEL [19]

The two-point functions in CFT are simple power functions. This is clearly seen from the equation (30). The quantum field theory in the scaling limit of the Ising model is not conformally invariant. The two-point function is already highly non-trivial. There are a variety of quantum field theories obtained as the scaling limit of the off-critical solvable lattice models. These are massive field theories. Their correlation functions are, in general, not known. However, these theories have the integrability inherited from the lattice models. They have the factorized  $S$ -matrix and their form factors satisfy the  $q$ -deformation of the KZ equation. I will explain these points in the sine-Gordon model which are the scaling limit of the eight-vertex model (a generalization of the six-vertex model).

One way to compute the two-point function is to put a complete set of intermediate states.

$$\begin{aligned} \langle vac | \phi(0) \phi(x) | vac \rangle &= \sum_{n \geq 0, \text{even}} \prod_{j=1}^n \int_{-\infty}^{\infty} \frac{d\beta_j}{2\pi} \frac{1}{n!} \sum_{\varepsilon_1, \dots, \varepsilon_n} \\ &\times \langle vac | \phi(0) | \beta_n, \dots, \beta_1 \rangle_{\varepsilon_n, \dots, \varepsilon_1} \langle \beta_1, \dots, \beta_n | \phi(x) | vac \rangle. \end{aligned} \quad (31)$$

The matrix elements  $\langle vac|\phi(0)|\beta_n, \dots, \beta_1\rangle_{\varepsilon_n, \dots, \varepsilon_1}$  are called the form factors. For the Ising model, the form factors are given by the Pfaffian of the two-particle one, which is  $\tanh \frac{\beta_1 - \beta_2}{2}$ .

There is a redundancy of the vectors  $\langle vac|\phi(0)|\beta_n, \dots, \beta_1\rangle_{\varepsilon_n, \dots, \varepsilon_1}$ . Only those with the restriction  $\beta_1 < \dots < \beta_n$  are independent. The assumption of the factorized  $S$ -matrix is such that the linear relations among the vectors are given by the two-particle  $S$ -matrix in the form (9). For example, the two-particle  $S$ -matrix of the Ising model is  $-1$ .

The  $S$ -matrix of the sine-Gordon theory is given by (19) with a real parameter  $\xi$ , as  $S = S_0 \bar{R}$ . The scalar factor  $S_0$  is given by

$$S_0 = -e^{-i \int \frac{\sin \kappa \beta \operatorname{sh} \frac{\pi - \xi}{2} \kappa}{\operatorname{ch} \frac{\pi}{2} \kappa \operatorname{sh} \frac{\xi}{2} \kappa} d\kappa} \tag{32}$$

This function is expressed by means of the double gamma functions ([22, 13]). Note that  $S_0$  depends on  $\beta, \xi$  in such a way that it is not single-valued in  $\zeta, q$  as opposed to the matrix part  $\bar{R}$ .

In the limit  $\xi \rightarrow \infty$ , the double gamma function reduces to the usual gamma function, and the  $S_0$  is given by

$$S_0(\beta) = \frac{\Gamma(\frac{1}{2} + \frac{\beta}{2\pi i})\Gamma(-\frac{\beta}{2\pi i})}{\Gamma(\frac{1}{2} - \frac{\beta}{2\pi i})\Gamma(\frac{\beta}{2\pi i})} \tag{33}$$

The  $\bar{R}$  reduces to  $\frac{\beta - \pi i P}{\beta - \pi i}$  where  $P$  is the transposition.

The  $S$ -matrix of the SG theory is identical with the  $S$ -matrix of the six-vertex model in the massless phase. This is because the SG theory is the continuum limit of the eight-vertex model as I have already mentioned. The continuum limit is taken at the critical region of the eight-vertex model. This is nothing but the six-vertex model in the massless phase. The case discussed in Section 1 is a special case of this story where  $\xi = \infty$ .

Set

$$F_{\varepsilon_1, \dots, \varepsilon_n}(\beta_1, \dots, \beta_n) = \langle vac|\phi(0)|\beta_n, \dots, \beta_1\rangle_{\varepsilon_n, \dots, \varepsilon_1} \tag{34}$$

Because of (9) it satisfies

$$F_{\varepsilon_1, \dots, \varepsilon_{j+1}, \varepsilon_j, \dots, \varepsilon_n}(\beta_1, \dots, \beta_{j+1}, \beta_j, \dots, \beta_n) = \sum_{\varepsilon'_j, \varepsilon'_{j+1}} S(\beta_j - \beta_{j+1})_{\varepsilon_j, \varepsilon_{j+1}}^{\varepsilon'_j, \varepsilon'_{j+1}} F_{\varepsilon_1, \dots, \varepsilon'_j, \varepsilon'_{j+1}, \dots, \varepsilon_n}(\beta_1, \dots, \beta_j, \beta_{j+1}, \dots, \beta_n) \tag{35}$$

There is another equation for the form factor. It gives the analytic continuation of the form factor in the last variable  $\beta_n$ :

$$F_{\varepsilon_1, \dots, \varepsilon_n}(\beta_1, \dots, \beta_n + 2\pi i) = F_{\varepsilon_n, \varepsilon_1, \dots, \varepsilon_{n-1}}(\beta_n, \beta_1, \dots, \beta_{n-1}) \tag{36}$$

I will not explain why this is valid. In Section 4, however, its origin in the representation theory is given in the case of the XXZ model with  $\Delta < -1$ .

## 3.5 THE QUANTUM KZ EQUATION [8]

Set

$$F(\beta_1, \dots, \beta_n) = \sum_{\varepsilon_1, \dots, \varepsilon_n} F_{\varepsilon_1, \dots, \varepsilon_n}(\beta_1, \dots, \beta_n) v_{\varepsilon_1} \otimes \cdots \otimes v_{\varepsilon_n}. \quad (37)$$

Combination of (9) and (36) gives the following difference equation for the form factor.

$$F(\beta_1, \dots, \beta_j + 2\pi i, \dots, \beta_n) = S_{j+1, j}(\beta_{j+1} - \beta_j - 2\pi i) \cdots S_{n, j}(\beta_n - \beta_j - 2\pi i) \\ \times S_{1, j}(\beta_1 - \beta_j) \cdots S_{j-1, j}(\beta_{j-1} - \beta_j) F(\beta_1, \dots, \beta_j, \dots, \beta_n). \quad (38)$$

Here, I denote by  $S_{j, k}$  the action of  $S$  on the  $j$ -th and  $k$ -th components. In the limit where  $\xi, \beta_1, \dots, \beta_n \rightarrow \infty$ , this equation scales to the differential equation (30) with the level  $l$  equal to 0.

One can repeat the story in 3.2 and 3.3 for  $U_q(\widehat{sl}_2)$ . Vertex operators are defined as the intertwiners between the highest weight representations with and without the tensor product by the affinization of a finite dimensional representation. The matrix elements of the product of vertex operators between the highest weight vectors satisfy a system of difference equation. This is called the quantum KZ equation. The above equation is a special case with level 0.

A question arises: Are these matrix elements representing the correlation functions of some integrable models? The answer is NO BUT. I will come back to this question later.

## 4 CTM AND HTM: THE KEY WORDS IN THE DICTIONARY

I present the algebraic structure of the XXZ and the six-vertex models in the language of representation theory. Two kinds of transfer matrices, that are acting on the half-infinite tensor product, play the central roles in the symmetry of  $U_q(\widehat{sl}_2)$ . I will explain how to identify these operators in the representation theory. This identification brings us the solutions to the problems mentioned before: the diagonalization of the XXZ Hamiltonian, and the computation of the form factors and the correlation functions.

## 4.1 CTM [1]

Our goal is to understand the infinite tensor product  $\otimes_{k \in \mathbf{Z}} V_k$  as a  $U_q(\widehat{sl}_2)$  module. It is rather a big representation, of course not irreducible. The half infinite tensor product is also a representation space of  $U_q(\widehat{sl}_2)$ . It is much smaller than the infinite tensor product in both directions. The idea is to study the content of this representation first, There are two operators which naturally act on this space. They are the corner transfer matrix (CTM) and the half transfer matrix (HTM).

I start from the CTM. Recall the Boltzmann weights given by (19). There are three different ones. Let us call them the  $a$ ,  $b$  and  $c$  weights, respectively, from the left to the right. We restrict to the region

$$-1 < q < 0, \quad 1 < \zeta < -q^{-1}. \quad (39)$$

In this region, the  $c$  weight dominates the others.

The XXZ Hamiltonian and the transfer matrix of the six-vertex model act formally on the vectors parametrized by the paths, which satisfy certain boundary conditions. We consider similar boundary conditions for the configurations on the two-dimensional lattice. A configuration is called the ground state if it consists of the  $c$  weight only. There are two such configurations. The local variables take constant values 0 or 1 along the NE-to-SW diagonal lines, and these values alternate over the diagonal lines. Choose two vertical lines, and consider the set of horizontal edges between these two lines. We number these edges by  $\mathbf{Z}$  (increasingly from S to N). The configuration of a ground state on these edges is equal to  $p^{(0)}$  or  $p^{(1)}$ . Accordingly, we call it the  $i$ -th ground state.

Consider the half infinite tensor product  $\otimes_{k=1}^{\infty} V_k$ . We denote by  $\mathcal{H}_i$  the space spanned by the vector of the form  $\otimes_{k=1}^{\infty} v_{p(k)}$  where the half infinite path  $p$  satisfies  $p(k) = \frac{1}{2}(1 - (-1)^{k+i})$  for sufficiently large  $k$ . The corner transfer matrix  $A(\zeta)$  formally acts on the space  $\mathcal{H}_i$ . Its matrix element is given as follows.

Consider the center of the plaquet in the lattice between the edges 0 and 1. Divide the whole lattice into four quadrants at this point making cuts in the N,E,W,S directions. Take the NW quadrant. Fix the local variables of the edges on the N-cut to  $\{p'(k)\}_{k \in \mathbf{Z}_{\geq 1}}$ , and those on the W-cut to  $\{p(k)\}_{k \in \mathbf{Z}_{\geq 1}}$ . Consider the configuration sum for this quadrant with this restriction on the N and W boundaries. We also restrict the sum to those configurations which belong to the  $i$ -th ground state, i.e., different from the  $i$ -th ground state at finitely many places. We define the matrix element  $A(\zeta)_{\{p(k)\}}^{\{p'(k)\}}$  to be the configuration sum under these restrictions.

This is only a formal definition, and it is divergent. In the region (39), the CTM can be renormalized to a 'finite' operator with discrete (and, in fact, equally spaced) eigenvalues, while if  $|q| = 1$ , the renormalized operator has a continuum spectrum. This difference comes from the difference in the analytic structure of the free energy.

Consider a finite lattice with  $N$  sites (i.e.,  $N = \#\{\text{vertex}\}$ ). The limit  $\kappa = \lim_{N \rightarrow \infty} Z^{\frac{1}{N}}$  is called the partition function per site. (The free energy is given by its logarithm.) In the massive region, it is given by

$$\kappa = \zeta \frac{(q^4 \zeta^2; q^4)_{\infty} (q^2 \zeta^{-2}; q^4)_{\infty}}{(q^4 \zeta^{-2}; q^4)_{\infty} (q^2 \zeta^2; q^4)_{\infty}} \quad (40)$$

where  $(z; p)_{\infty} = \prod_{n=0}^{\infty} (1 - p^n z)$ .

The above  $\kappa$  is a single-valued meromorphic function in  $\zeta$ . It has a natural boundary at  $|q| = 1$ . If  $|q| = 1$ , the partition function per site has an different expression: it is given by  $-S_0^{-1}$  (see (32)) with a real value of  $\xi$  and an imaginary value of  $\beta$ . (Note that in the sine-Gordon theory,  $\beta$  is real.) This is not single-valued in  $\zeta$ , nor in  $q$ .

Physical intuition tells that the renormalization of CTM and HTM is done by choosing the overall factor of the Boltzmann weight in such a way that the partition function per site is 1. Therefore, the structure of the physical space and the renormalized operators acting on it differs in the massive and the massless phases.

In the region (39), we have

$$A_{\text{re}}(\zeta) = \zeta^{-D}. \tag{41}$$

The operator  $D$  is independent of  $\zeta$  and has the spectrum  $\{0, 1, 2, \dots\}$ . This remarkable (however, no rigorous proof is available) property is a consequence of the single-valuedness of  $\kappa$ .

Let  $\Lambda_i$  be the affine  $sl_2$  weight such that  $\langle \Lambda_i, h_j \rangle = \delta_{ij}$  ( $i, j = 0, 1$ ). I state the main postulate:

*the space of the eigenvectors of the CTM in the  $i$ -th ground state is isomorphic to the integrable and irreducible highest weight representation  $V(\Lambda_i)$  of  $U_q(\widehat{sl_2})$ .*

Namely, the half infinite tensor product  $\mathcal{H}_i$  is interpreted as the highest weight module ([7])

$$\mathcal{H}_i \simeq V(\Lambda_i). \tag{42}$$

I give the evidence for this statement: The character of the space  $\mathcal{H}_i$  and that of  $V(\Lambda_i)$  are equal. The former can be computed in the the crystal limit  $q \rightarrow 0$  because we have

$$D = -\frac{1}{2} \sum_{k=1}^{\infty} k(\sigma_k^x \sigma_{k+1}^x + \sigma_k^y \sigma_{k+1}^y + \Delta \sigma_k^z \sigma_{k+1}^z), \tag{43}$$

and this is diagonal in the limit. The equality of the characters is equivalent to the combinatorial identity

$$\sum_{p \in \mathcal{H}_{i,m}} q^{\sum_{k=1}^{\infty} p(k)} \left( (-1)^{p(k)+p(k+1)} - (-1)^{p^{(i)}(k)+p^{(i)}(k+1)} \right) = \frac{q^{(m-i)(m-i+1)}}{(q^2; q^2)_{\infty}}, \tag{44}$$

where  $\mathcal{H}_{i,m} = \{p \in \mathcal{H}_i; 2 \sum_{k=1}^{\infty} (p(k) - p^{(i)}(k)) = m\}$ .

#### 4.2 HTM [4, 14, 13]

The matrix element of the transfer matrix is formally given by the configuration sum (18) for a slice of the lattice consisting of one vertical line and horizontal lines indexed by  $k \in \mathbf{Z}$  which intersect the vertical one. Cut the vertical edge between the  $k = 0, 1$  horizontal lines. The matrix element of the half transfer matrix  $\Phi_{\varepsilon}^{(i)}(\zeta)$  ( $\varepsilon = 0, 1$ ) is given by the configuration sum for the upper half of the slice where the local variables on the right and left edges are fixed to  $\{\varepsilon'_k\}$  and  $\{\varepsilon_k\}$ , and the one on the cut edge is fixed to  $\varepsilon$ . The superscript  $i$  indicates the restriction of the sum to those configurations which belong to the  $i$ -th ground state.

The half transfer matrix acts as

$$\dots \otimes V \otimes V \otimes V \rightarrow (\dots \otimes V \otimes V) \otimes V_{\zeta}. \tag{45}$$

The components described by  $V$  corresponds to the horizontal lines and the one denoted by  $V_{\zeta}$  corresponds to the vertical line.

In the dictionary, the half transfer matrix (45) is translated into the unique (up to the normalization) intertwiner

$$\Phi^{(i)}(\zeta) = \sum_{\varepsilon=0,1} \Phi_{\varepsilon}^{(i)}(\zeta) \otimes v_{\varepsilon} : V(\Lambda_i) \rightarrow V(\Lambda_{1-i}) \otimes V_{\zeta}. \tag{46}$$

If  $\zeta = 1$  in (45), the mapping is nothing but the identity operator. However, its translation (46) is a highly non-trivial operator even if  $\zeta = 1$ .

I list some properties of the intertwiners.

$$\zeta^D \Phi_{\varepsilon}^{(i)}(\zeta) = \Phi_{\varepsilon}^{(i)}(\zeta \zeta^D), \tag{47}$$

$$\Phi_{\varepsilon_2}^{(1-i)}(\zeta_2) \Phi_{\varepsilon_1}^{(i)}(\zeta_1) = \sum_{\varepsilon'_1, \varepsilon'_2=0,1} R_{\varepsilon_1 \varepsilon_2}^{\varepsilon'_1 \varepsilon'_2}(\zeta_1 / \zeta_2) \Phi_{\varepsilon'_1}^{(1-i)}(\zeta_1) \Phi_{\varepsilon'_2}^{(i)}(\zeta_2), \tag{48}$$

$$\sum_{\varepsilon} \Phi_{1-\varepsilon}^{(1-i)}(-q^{-1}\zeta) \Phi_{\varepsilon}^{(i)}(\zeta) = \text{id}_{\mathcal{H}_i} \tag{49}$$

The  $R$ -matrix in (48) is normalized as  $R(\zeta) = \frac{1}{\kappa(\zeta)} \bar{R}(\zeta)$  (see (40)).

### 4.3 SPACE OF THE PHYSICAL STATES

The identification of the physical space follows from (42) by a simple functorial argument.

Consider the inner product of  $V$ ,  $\langle v_i, v_j \rangle = \delta_{i+j,1}$ . The  $U_q(\widehat{sl}_2)$  action (24) on  $V$  satisfies  $\langle xv, v' \rangle = \langle v, b(x)v' \rangle$  where  $b$  is the anti-automorphism of  $U_q(\widehat{sl}_2)$  given by  $b(e_i) = qt_i e_i$ ,  $b(f_i) = qt_i^{-1} f_i$ ,  $b(t_i) = t_i^{-1}$ . Since the left half  $\dots \otimes V \otimes V \otimes V$  is equal to  $\oplus_{i=0,1} V(\Lambda_i)$ , the right half  $V \otimes V \otimes V \otimes \dots$  is equal to the dual space  $\oplus_{i=0,1} V(\Lambda_i)^*$ . The action on the dual space is given by the transposed action  $b(x)^t$ . The infinite tensor product  $\mathcal{F}$  is identified with  $\text{End}(\mathcal{H}) = \mathcal{H} \otimes \mathcal{H}^*$ . The action on  $\mathcal{F}$  is given by the adjoint action.

$$\mathcal{F} = \text{End}(\mathcal{H}) = \oplus_{i,j=0,1} \text{Hom}(V(\Lambda_i), V(\Lambda_j)), \tag{50}$$

$$x.f = \sum x_{(1)} \circ f \circ b(x_{(2)}) \quad \text{for } x \in U_q(\widehat{sl}_2), f \in \text{End}(\mathcal{H}). \tag{51}$$

Here  $\Delta(x) = \sum x_{(1)} \otimes x_{(2)}$  is the coproduct of  $x$ .

The inner product on  $\mathcal{F}$  is given by

$$\langle f, g \rangle = \text{trace}_{\mathcal{H}} f \circ g \quad \text{for } f, g \in \text{End}(\mathcal{H}). \tag{52}$$

The transfer matrix in the dictionary reads as

$$T(\zeta)f = \sum_{\varepsilon} \Phi_{\varepsilon}(\zeta) \circ f \circ \Phi_{1-\varepsilon}(\zeta). \tag{53}$$

Now, I will diagonalize this operator.

4.4 VACUUM AND EXCITED STATES

The vacuum state (4) is given by the iteration of the transfer matrix, because it is the largest eigenvector. Namely, the coefficient  $c(p)$  in (4) is (up to a divergent scalar) written as  $c(p) \sim \lim_{N \rightarrow \infty} \langle p | T(\zeta)^N | p^{(N+i)} \rangle$  where  $p^{(i)} = p^{(i+2)}$  is the ground state path.

The right hand side is nothing but the partition function for the one half of the lattice, or equivalently, is equal to the matrix element  $(A(\zeta)B(\zeta))_{\{p^{(k)}\}_{k \geq 1}}^{\{1-p^{(1-k)}\}_{k \geq 1}}$  of the product of the CTMs corresponding to the NW and the SW quadrants. Using the symmetry property of  $R(\zeta)$ ,  $R_{\varepsilon_2 \varepsilon'_1}^{\varepsilon_1 \varepsilon'_2}(\zeta_2/\zeta_1) = R_{1-\varepsilon_1, \varepsilon_2}^{1-\varepsilon'_1, \varepsilon'_2}(-q^{-1}\zeta_1/\zeta_2)$ , we obtain  $B_{re}(\zeta) = A_{re}(-q^{-1}\zeta^{-1})$ , and therefore  $A_{re}(\zeta)B_{re}(\zeta) = (-q)^D$ .

We reached the conclusion.

$$|vac\rangle_i = \chi^{-\frac{1}{2}}(-q)^D \in \text{End}(\mathcal{H}_i). \tag{54}$$

Here  $\chi = \text{trace}_{\mathcal{H}_i} q^{2D} = \prod_{n=1}^{\infty} \frac{1}{1-q^{2n}}$  is the normalization factor such that  ${}_i\langle vac|vac\rangle_i = 1$ . One can easily check  $T(\zeta)|vac\rangle_i = |vac\rangle_{1-i}$  by using (48) and (49).

To find particles in  $\mathcal{F}$  is equivalent to find submodules isomorphic to  $V_{\xi_n} \otimes \dots \otimes V_{\xi_1}$  in  $\text{End}(\mathcal{H})$ . This problem is also solved by using intertwiners, but of a different kind:

$$\Psi^{*(i)}(\xi) : V_{\xi} \otimes V(\Lambda_i) \rightarrow V(\Lambda_{1-i}). \tag{55}$$

The essential difference of this intertwiner from  $\Phi^{(i)}(\zeta)$  is that  $V_{\xi}$  is placed in the left of  $V(\Lambda_i)$ . In the CFT case, there are no such difference because the coproduct is symmetric.

We have

$$\xi^D \Psi_{\varepsilon}^{*(i)}(\zeta) = \Psi_{\varepsilon}^{*(i)}(\xi \zeta) \xi^D, \tag{56}$$

$$\Psi_{\varepsilon_1}^{*(1-i)}(\xi_1) \Psi_{\varepsilon_2}^{*(i)}(\xi_2) = - \sum_{\varepsilon'_1, \varepsilon'_2} R_{\varepsilon'_1, \varepsilon'_2}^{\varepsilon_1, \varepsilon_2}(\xi_1/\xi_2) \Psi_{\varepsilon'_2}^{*(1-i)}(\xi_2) \Psi_{\varepsilon'_1}^{*(i)}(\xi_1), \tag{57}$$

$$\Phi_{\varepsilon_1}^{(1-i)}(\zeta) \Psi_{\varepsilon_2}^{*(i)}(\xi) = \tau(\zeta/\xi) \Psi_{\varepsilon_2}^{*(1-i)}(\xi) \Phi_{\varepsilon_1}^{(i)}(\zeta). \tag{58}$$

Here, we set

$$\tau(\zeta) = \zeta^{-1} \frac{(q\zeta^2; q^4)_{\infty} (q^3\zeta^{-2}; q^4)_{\infty}}{(q\zeta^{-2}; q^4)_{\infty} (q^3\zeta^2; q^4)_{\infty}}. \tag{59}$$

Using these relations, one can show that the  $n$ -particle states is given by

$$|\xi_n, \dots, \xi_1\rangle_{\varepsilon_n, \dots, \varepsilon_1, i} = \Psi_{\varepsilon_n}^{*(n-1+i)}(\xi_n) \dots \Psi_{\varepsilon_1}^{*(i)}(\xi_1) (-q)^D. \tag{60}$$

The eigenvalue of the transfer matrix on this states is given by  $\prod_{j=1}^n \tau(\zeta/\xi_j)$ .

4.5 CORRELATION FUNCTIONS AND FORM FACTORS [11]

The correlation functions of the XXZ model are by definition  ${}_i\langle vac|\mathcal{O}|vac\rangle_i$  where  $\mathcal{O}$  is some local operators. This expression is immediately written as the trace  $\chi^{-1}\text{trace}_{\mathcal{H}_i} q^{2D}\mathcal{O}$ .

For example, let us consider the simplest case  $\sigma_1^z \in \text{End}(\mathcal{F}) = \text{End}(\mathcal{H} \otimes \mathcal{H}^*)$ . This operator, in fact, acts only on  $\mathcal{H}$ . Recall the half transfer matrix (we now abbreviate the notation by dropping the superscript  $i$ )

$$\Phi(1) = \Phi_0(1) \otimes v_0 + \Phi_1(1) \otimes v_1 : \cdots \otimes V \otimes V \otimes V \xrightarrow{\sim} (\cdots \otimes V \otimes V) \otimes V. \tag{61}$$

The relation (49) gives the inverse map

$$\Phi_1(-q^{-1}) \otimes v_0^* + \Phi_0(-q^{-1}) \otimes v_1^* : (\cdots \otimes V \otimes V) \otimes V \xrightarrow{\sim} \cdots \otimes V \otimes V \otimes V, \tag{62}$$

where  $v_0^*, v_1^*$  are the dual basis of  $v_0, v_1$ . Therefore, we have

$$\sigma_1^z = \Phi_1(-q^{-1})\Phi_0(1) - \Phi_0(-q^{-1})\Phi_1(1). \tag{63}$$

In general, the correlation functions belong to the family of functions of the form

$$\text{trace}_{\mathcal{H}_i} q^{2D} \Phi_{\varepsilon_1}(\zeta_1) \cdots, \Phi_{\varepsilon_n}(\zeta_n). \tag{64}$$

In CFT, the correlation functions are the matrix elements of the product of vertex operators between the highest weight vectors. The  $q$ -analogues of such matrix elements do not contain the lattice correlation functions. Instead, the trace functions (64) give the lattice correlation functions. The trace functions also contain the form factors of the local operators in the form

$$\text{trace}_{\mathcal{H}_i} q^{2D} \Phi_{\varepsilon_1}(\zeta_1) \cdots, \Phi_{\varepsilon_n}(\zeta_n) \Psi_{\kappa_m}^*(\xi_m) \cdots, \Psi_{\kappa_1}^*(\xi_1). \tag{65}$$

This is because the excited states are given by (60).

I finish this talk with several remarks on the formula (65).

A direct computation of the trace is not practical because the trace is taken on the infinite dimensional space  $\mathcal{H}_i$ . However, it is possible to realize  $\mathcal{H}_i$  as the Fock space of free bosons. In this realization, the operators  $\Phi(\zeta)$  and  $\Psi^*(\xi)$  are explicitly expressed in terms of bosonic currents. The integral formula for the trace functions follows from this.

The exchange relations (47-49) for the half transfer matrices induce a set of equations similar to (35) and (36) for the trace functions (64). Solving these equations under a certain analyticity condition which follows from the integral formula, we have

$$\frac{\text{trace}_{\mathcal{H}_0} q^{2D} (\Phi_0(\zeta_1)\Phi_1(\zeta_2) + \Phi_1(\zeta_1)\Phi_0(\zeta_2))}{\text{trace}_{\mathcal{H}_0} q^{2D} (\Phi_0(\zeta_1)\Phi_1(\zeta_2) - \Phi_1(\zeta_1)\Phi_0(\zeta_2))} = \frac{(-q^3\zeta^{-1}; q^2)_\infty (-q\zeta; q^2)_\infty}{(q^3\zeta^{-1}; q^2)_\infty (q\zeta; q^2)_\infty} \tag{66}$$

where  $\zeta = \zeta_2/\zeta_1$ . Baxter's result (11) follows from this.

Suppose that an operator  $\mathcal{O}$  commutes with  $\Psi^*(\xi)$  (in fact, the local operators, e.g., (63), do commute), then the trace functions  $\text{trace}_{\mathcal{H}_i} \mathcal{O} \Psi_{\kappa_m}^*(\xi_m) \cdots, \Psi_{\kappa_1}^*(\xi_1)$



satisfy exactly the same equations as (35) and (36) with pure imaginary  $\xi$ . Note, in particular, that the shift  $\beta \rightarrow \beta + 2\pi i$  corresponds to the shift  $\zeta \rightarrow q^2\zeta$ . The relation (36) follows from  $q^{2D}\Psi^*(\xi) = \Psi^*(q^2\xi)q^{2D}$  and the cyclicity of the trace. The relation (58) tells that the operators  $\Phi(\zeta)$  and  $\Psi^*(\xi)$  commute up to a simple factor  $\tau(\zeta/\xi)$ . With a suitable modification to cancel the factors  $\tau(\zeta_i/\xi_j)$ , the trace function (65), in general, gives a solution of the qKZ equation with level 0.

The connection between the XXZ model and the representation theory of  $U_q(\widehat{sl}_2)$  fails in the massless phase. The reason for this is that the latter is singular when  $|q| = 1$ . The product of the intertwiners exhibit singularities there. However, the bosonic construction of the vertex operators satisfying the relevant exchange relations is possible ([17, 13, 10]). The integral formulas for the correlation functions and the form factors are, thus, available (so far, without a firm basis of the representation theory).

#### REFERENCES

- [1] R. J. Baxter. *Exactly Solved Models in Statistical Mechanics*. Academic, London, 1982.
- [2] R. J. Baxter. Spontaneous staggered polarization of the F model. *J. Stat. Phys.*, 9:145–182, 1973.
- [3] A. A. Belavin, A. N. Polyakov and A. N. Zamolodchikov . Infinite conformal symmetries in two dimensional quantum field theory. *Nucl. Phys.*, B 241:333–380, 1984.
- [4] B. Davies, O. Foda, M. Jimbo, T. Miwa, and A. Nakayashiki. Diagonalization of the XXZ Hamiltonian by vertex operators. *Comm. Math. Phys.*, 151:89–153, 1993.
- [5] V. G. Drinfeld. Quantum Groups. In *Proceedings of the International Congress of Mathematicians*. 798–820, Berkeley, 1987.
- [6] L. D. Faddeev and L. A. Takhtajan. Spectrum and scattering of excitations in the one-dimensional isotropic Heisenberg model. *J. Soviet Math.* 24: 241–267, 1984.
- [7] O. Foda and T. Miwa. Corner Transfer Matrices and Quantum Affine Algebras. *Int. J. Mod. Phys.*, A7 supplement 1A:279, 1992.
- [8] I. B. Frenkel and N. Yu. Reshetikhin. Quantum affine algebras and holonomic difference equations. *Comm. Math. Phys.*, 146: 1-60, 1992.
- [9] M. Jimbo. A  $q$  analogue of  $U(\mathfrak{gl}(N+1))$ , Hecke algebra, and the Yang-Baxter equation. *Lett. Math. Phys.*, 11: 247–252, 1986.
- [10] M. Jimbo, H. Konno and T. Miwa Massless XXZ model and degeneration of the elliptic algebra  $A_{q,p}(\widehat{sl}_2)$  In the proceedings for Ascona meetings, 1996.

- [11] M. Jimbo, K. Miki, T. Miwa and A. Nakayashiki. Correlation functions of the  $XXZ$  model for  $\Delta < -1$ . *Phys. Lett. A* 168: 256–263, 1992.
- [12] M. Jimbo and T. Miwa. *Algebraic Analysis of Solvable Lattice Models*. CBMS Regional Conference Series in Mathematics vol. 85, AMS, 1994.
- [13] M. Jimbo and T. Miwa. Quantum KZ equation with  $|q| = 1$  and correlation functions of the  $XXZ$  model in the gapless regime. *J. Phys.*, A 29: 2923–2958, 1996.
- [14] M. Jimbo, T. Miwa, and A. Nakayashiki. Difference equations for the correlation functions of the eight-vertex model. *J. Phys.*, A26:2199–2209, 1993.
- [15] J. D. Johnson, S. Krinsky and B. M. McCoy Vertical-arrow correlation length in the eight-vertex model and the low-lying excitations of the X-Y-Z Hamiltonian. *Phys. Rev.*, A8:2526–2547, 1973.
- [16] V. G. Knizhnik and A. B. Zamolodchikov. Current algebra and Wess-Zumino models in two dimensions. *Nucl. Phys.*, B247: 83–103, 1984.
- [17] S. Lukyanov. Free field representation for massive integrable models. *Comm. Math. Phys.*, 167: 183–226, 1995.
- [18] M. Sato, T. Miwa and M. Jimbo. Studies on holonomic quantum fields I. *Proc. Japan Acad.*, 53 A: 6–10. 1977.
- [19] F. A. Smirnov. *Form Factors in Completely Integrable Models in Quantum Field Theory*. World Scientific, Singapore, 1992.
- [20] A. Tsuchiya and Y. Kanie. Vertex operators in conformal field theory on  $\mathbf{P}^1$  and monodromy representation of braid group. *Advanced Studies in Pure Mathematics*, 16: 297–372, 1988.
- [21] T. T. Wu, B. M. McCoy, C. Tracy and E. Barouch. Spin-spin correlation functions for the two-dimensional Ising model: Exact results in the scaling region. *Phys. Rev.*, B13: 316–374, 1976.
- [22] A. B. Zamolodchikov and Al. B. Zamolodchikov. *Annal. Phys.*, 120: 253–291, 1979.

Tetsuji Miwa  
Research Institute  
for Mathematical Sciences  
Kyoto University  
Kyoto 606, JAPAN



## DYNAMICAL SYSTEMS – PAST AND PRESENT

JÜRGEN MOSER

## INTRODUCTION

It is a great honor for me to be invited to present a lecture at this International Congress of Mathematicians here in Berlin. This town (and its Academy) brings to mind a distinguished mathematical tradition in the last century, and I want to mention the names of Jacobi, Dirichlet and Weierstraß; they all contributed to the beginning of the topic of this lecture.

It was 94 years ago that the last ICM took place in Germany. This was in 1904 in Heidelberg (where, incidentally, the anniversary of Jacobi's 100th birthday was celebrated).

This long hiatus is, of course, not an accident, if one remembers that Germany was the scene of World War I, World War II and the Nazi terror. It was the time when Germany spread devastation and fear over the world. It was the time when – in the words of my friend Stefan Hildebrandt – Germany stepped out of the community of civilized countries. Even though these events lie more than half a century back I feel compelled to recall these terrible times since I myself lived through this dark period, having been born in this country.

During these times also science was trampled, and many eminent scientists were kicked out of their positions which caused irreparable damage. More than one third of the faculty of German universities was dismissed between 1933 and 1938! This reminds me of the Hilbert story, which I learned from my teacher Franz Rellich in Göttingen: When Hilbert – who was old and retired – was asked at a party by the newly appointed Nazi-minister of education: “Herr Geheimrat, how is mathematics in Göttingen, now that it has been freed of the Jewish influences” he replied: “Mathematics in Göttingen? That does not *exist* anymore!”

We must never forget this low point of German history – yet we also must put it behind us and look ahead. It is gratifying to see so many mathematicians who have come to Berlin to partake in this Congress. Let us celebrate this occasion as a new beginning at the end of this century.

\* \* \* \* \*

In this lecture I will present what I consider significant advances in the field of dynamical systems during the last 50 years. This field had a tremendous expansion in this time and my task would be impossible without severe restrictions. I will restrict myself to Hamiltonian systems – just as Birkhoff understood the concept

in his book “Dynamical Systems” in 1927! Even there I will not attempt a survey, but rather select some topics, which in my view illustrate the dramatic changes that occurred during the past half century in this field. Clearly this lecture is not meant for experts, but for a wide audience.

As guide line I will use the stability problem for Hamiltonian systems, which still holds many fascinating problems. After some historical remarks I will discuss some applications of Kolmogorov’s theorem on invariant tori (1954), then in Section 3 Xia’s solution of the Painlevé problem, in Section 4 completely integrable systems, and, if time permits, in Section 5 the role of minimizers in the Aubry–Mather theory. Because of the limited time, I will omit many related topics, even some of great interest. The activity in symplectic geometry, which grew partially out of the Poincaré–Birkhoff fixed point theorem and led to most remarkable results will be discussed in other lectures at this meeting. Also ergodic theory and hyperbolic systems are active fields which I will not touch at all.

### I HISTORICAL REMARKS

a) The stability problem for Hamiltonian systems is an old unsolved problem which fascinated many mathematicians in the past. It was motivated by celestial mechanics and the stability problem for the planetary system. This is modeled by the  $N$ -body problem where  $N$  masspoints (of positive masses  $m_j$ ) move in Euclidean space  $\mathbf{R}^2$  or  $\mathbf{R}^3$ . One asks for bounded orbits avoiding collisions. More precisely, if  $r_{ij}$  is the distance between the  $i^{\text{th}}$  and  $j^{\text{th}}$  masspoints we require that along the orbits the expression

$$\Delta = \max_{1 \leq i < j \leq N} \left\{ r_{ij}, \frac{1}{r_{ij}} \right\}$$

is bounded *for all times!*

The simplest solutions of this kind are the periodic solutions, represented by closed curves in the phase space. Therefore there was a great interest in establishing the existence of periodic solutions, and Poincaré devised perturbation methods as well as topological arguments for this purpose. However, the periodic solutions forms an exceptional set in phase space and therefore are of limited interest for the understanding of the dynamical behavior – unless one can prove their stability.

The question of stability requires not only finding single orbits with bounded  $\Delta$  but an open set in phase space of such solutions, accounting for the imprecise knowledge of the initial values. In other words, one is interested in an open set in phase space in which  $\Delta$  is bounded and to which the orbits are confined for all times!

In spite of the modern advances in this field this is still an *open problem!* It is conceivable that (for  $N \geq 3$ ) the complement of all orbits which exist for all time and with  $\Delta$  bounded forms a dense set in phase space. This would mean that by arbitrary small changes of the initial states one would find orbits which ultimately escape or end up in collisions!

In this connection it is interesting to read a statement of Charlier from the year 1907 about the question of the stability of the planetary system: “It still has to be considered as an open problem, although one would hardly be considered as a phantastic prophet if one expresses the conjecture that one does not have to wait for many decades for its solution.” So much for prediction about open problems!

b) To proceed more constructively one replaced the quest for periodic solutions by that for quasi-periodic ones. These are given by generalized Fourier series of the form

$$(*) \quad x(t) = \operatorname{Re}\left(\sum_{j \in \mathbf{Z}^d} c_j e^{i(j, \omega)t}\right), \quad \omega = (\omega_1, \omega_2, \dots, \omega_d)$$

where the frequencies  $\omega_1, \omega_2, \dots, \omega_d$  are rationally independent real numbers. Perturbation theory of classical mechanics led to such series expansions for the solutions already in the last century. However, the convergence of these series became a notorious problem. The difficulty is due to the so-called small divisors – powers of terms of the form  $(j, \omega), j \in \mathbf{Z}^d \setminus \{0\}$  – entering the coefficients. Since the frequencies are rationally independent these expressions are not zero, but they become arbitrarily small. This convergence problem – which would lead to the existence of quasi-periodic solutions – has been of central interest at the end of the last century, particularly to Dirichlet, Weierstraß (here in Berlin), Poincaré and others.

c) This problem *has* been solved half a century later! We turn to the fundamental theorem of Kolmogorov, which assures precisely the existence of such solutions, for Hamiltonian systems:

$$\dot{q}_k = H_{p_k}, \dot{p}_k = -H_{q_k}, \quad (k = 1, 2, \dots, n)$$

or, combining  $q, p$  to a vector  $x \in \Omega \subseteq \mathbf{R}^{2n}$  we write this in the form

$$\dot{x} = JH_x, \quad J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}, \quad x \in \Omega.$$

The corresponding flow will be denoted by  $\varphi^t$ .

A more geometrical formulation for quasi-periodic solutions is given by an embedding of a torus  $T^d = \mathbf{R}^d / \mathbf{Z}^d$ ,

$$u : T^d \rightarrow \Omega$$

such that the “Kronecker flow”  $\kappa^t : \theta \rightarrow \theta + \omega t$  on  $T^d$  is mapped into the flow  $\varphi^t$  restricted to the torus  $u(T^d)$ , i. e.

$$u \circ \kappa^t = \varphi^t \circ u.$$

## Torus embedding

Then  $u(T^d)$  is an invariant torus of the flow, and the orbits on it are indeed quasi-periodic. Moreover, by Kronecker's theorem, each of these orbits is dense on this torus; that means that this torus is a minimal set for the flow  $\varphi^t$ .

At the International Congress ICM 1954 in Amsterdam Kolmogorov announced the remarkable theorem: For a Hamiltonian system with Hamiltonian  $H$  of  $n$  degrees of freedom, close to an "integrable" one with Hamiltonian  $H_0$  and compact energy surfaces, there exists a set of such invariant tori of dimension  $d = n$ . Moreover, they form a set of positive measure in phase space.

We will come to the concept of integrable systems in Section 4; here it is sufficient to know that these are Hamiltonian systems with sufficiently many integrals whose level sets are (if they are compact) invariant tori carrying quasi-periodic orbits. The theorem asserts that under small perturbations many of these quasi-periodic orbits persist.

Here is not the place to give the precise formulation of this basic result. But we want to point out some important consequences:

1) The union of these tori, generally, does not form an open set. Since it forms a set of positive measure, these tori are not exceptional!

2) The union of these tori is generally nowhere dense, so that a nearby orbit may not be bounded and may escape if  $n \geq 3$ , while for  $n = 2$  the 2-dimensional tori can be used as boundaries of a domain on the three-dimensional energy surface, providing genuine stability results (some of which we will mention below).

Since the set of the constructed invariant tori have a relatively large measure one is led to a modified concept of stability: Instead of requiring that *all* orbits of a certain neighborhood are bounded for all times, one asks that most (in measure) orbits are bounded. This could be called “stability in measure”, a concept which in applications is often sufficient, and which can be assured also for systems of three or more degrees of freedom.

3) This theorem provides a proof of the convergence of the series (\*) provided the frequencies  $\omega$  satisfy some Diophantine condition, thus answering the question of the last century.

The proof of Kolmogorov’s theorem was published in 1963 by V. I. Arnold. The proof of a related theorem in a simpler situation, namely about the existence of invariant curves of area-preserving mappings in the plane had been published in 1962 by the speaker. It has become customary to refer to this technique as KAM theory.

For the plane three body problem the existence of a set of positive measure of quasi-periodic orbits has been established (Arnold 1963) but even for this problem in  $\mathbb{R}^3$  one encounters difficulties which have not yet been overcome.

d) To return to the exciting history of this problem, we want to mention that Weierstraß had a keen interest in this topic. In the Wintersemester 1880/81 he taught a course “Über die Störungen in der Astronomie” hier in Berlin. In his correspondence with S. Kovalevskaya (1878) (Acta Math. 35, 30) he asserts that he found a series expansion for the solutions of the 3-body-problem, and tried, though in vain, to prove its convergence. He was aware of a remark made by Dirichlet to Kronecker in 1858 that he had found a method to approximate solutions of the  $N$ -body problem successively. Dirichlet died soon afterwards, and no written records were found. Later Weierstraß suggested this problem to Mittag-Leffler as a prize question. This prize, sponsored by the Swedish king, was awarded to Poincaré, although actually he did not solve this problem. But his famous prize-paper contained so many new ideas that there was unanimity in awarding the prize to him. This story can be read in many places now; here I wanted to point out the little known connection of this problem with the mathematicians in Berlin of the last century!

## II APPLICATIONS, MAPPINGS

a) There are many applications of KAM theory to old problems of celestial mechanics. Most interesting are the stability results for systems of two degrees of freedom. We want to single out the stability proof of the periodic solutions in Hill’s lunar theory.



These problems have more historical interest, and nowadays are at most of academic interest to astronomers. However, since many physical phenomena can be described by Hamiltonian systems it is not surprising that the stability theory has a multitude of other applications. I want to mention just two.

b) The early 1950's was the time of the construction of high energy accelerators in the USA, Europe at CERN and other places. In these machines charged particles are accelerated in a huge circular tube to tremendous velocities. This tube is brought to near vacuum state, so as to avoid any slow-down of the particles by the gas. For the successful working of the acceleration process one has to keep the (majority of the) particles from hitting the wall of the vacuum chamber for a long time. This is to be achieved by an appropriate magnetic field which allows to the particles to be trapped in the interior of the vacuum chamber. Since the motion of charged particles in a magnetic field is governed by Hamiltonian systems we are dealing with the stability in question.

At that time a new principle was introduced to improve this stability behavior, which led to the "Alternating Gradient Synchrotron" (AGS) which was built in Brookhaven, NY. This was a "true" application, since the stability behavior was one essential factor for the decision whether such a machine could be built.

Since the theory was not yet so well developed, one resorted to numerical experiments. If I may include some personal experiences: When I first visited the Courant Institute in 1953, there was a lot of activity in calculating the iterates of section maps to decide about the stability of the fixed points. This was done in connection with the AGS machine. These computations were carried out on a UNIVAC still using punch cards! Nowadays everybody can do the same thing on a PC using MATLAB in a few minutes. Let me illustrate to you what such computer pictures yielded: At least in the two-dimensional case the calculations showed much more optimistic results than could be true!

c) By a standard procedure one can reduce the study of a flow to that of a mapping, the so-called "Poincaré mapping". In particular one is interested in studying the stability of a fixed point of an area-preserving mapping, say  $\varphi$ , in the plane.

### Poincaré section map

A necessary condition for stability under iteration of  $\varphi$  is that the linearized mapping is similar to a rotation. One speaks of an elliptic fixed point. In the following I show you some pictures of some 1000 iterates of points under a nonlinear area-preserving map. Near the fixed point the iterates of a point seem to organize themselves on a smooth curve, if one is close enough to the fixed point, indicating stability. The mapping chosen is a simple polynomial mapping, but the output is typical for such mappings.

The computations show that the iterates of a point fall on curves, surrounding the fixed point, making its stability evident. At some distance this curve patterns breaks up, leaving a certain stability region. The problem at the time was: Find a method to construct these curves and the stability region!

What one should have known even then was that there could not be a family of closed curves, and that the calculations were oversimplifying. If one uses more accurate computations and applies a microscope to them one will discover that between such curves there are regions with complicated dynamics (regions of instability in the terminology of G. D. Birkhoff).

Nevertheless, the set of invariant curves form a set of relatively large measure, as follows from KAM theory, so that stability of the fixed point is guaranteed. The orbit structure is amazingly complex for such simple mappings, as here for a polynomial map! Incidentally the region of instability contains “Mather sets” and complicated motions which nowadays would be called “chaotic”. That these phenomena really occur for the typical area-preserving mapping, even in the case of real analytic mappings, has been established by Zehnder (1973) and in a sharper form by Genecand (1990).

Thus in this case the early calculations gave a misleading simplification of the situation. Still they were of great importance for stimulating this activity.

#### d) THE STÖRMER PROBLEM.

Another large scale confinement region is known in the magnetic field of the earth. With the advent in 1957 of satellites it was soon discovered that the earth was surrounded by (two) belts of charged particles caused by its magnetic field. Since the beginning of the century it was known that such charged particles were present above the atmosphere and were responsible for the aurora borealis (and australis). It was Störmer (incidentally president of the ICM 1936 in Oslo) who made calculations of the orbits of these charged particles moving in the magnetic field of the earth, which he modelled as a magnetic dipole field. This is an interesting nonlinear Hamiltonian system.

The satellite measurements led to the discovery of two regions surrounding the earth, the so-called van Allan belts, in which the charged particles were trapped. It turns out that it is an example of a magnetic bottle to which the stability theory is applicable (M. Braun 1970).

It is interesting to realize the dimensions involved: For electrons the “cyclotron radius” is of the order of a few kilometers and the corresponding period of oscillation about one millionth of a second! The “bounce period” of travel from the north pole to the south pole and back is a fraction of a second.

In addition to the natural van Allan belts several artificial radiation belts have been made by the explosion of high-altitude nuclear bombs since 1958. Some of these so created belts had a life time up to several years – which shows the long stability of these experiments as well as the irresponsibility for carrying them out! Some 30 years ago these tests have been stopped.

Störmer problem

Van Allan belt

e) HILL'S LUNAR PROBLEM.

In 1878 Hill developed a theory for the motion of the moon, which attracted great attention and impressed also Poincaré deeply. Later G. D. Birkhoff wrote: "A highly important chapter in theoretical dynamics began to unfold with the appearance in 1878 of G. H. Hill's researches on the lunar theory". He established the existence of 2 periodic solutions on the energy surface

$$\frac{1}{2}(\dot{u}^2 + \dot{v}^2) - \frac{1}{r} - \frac{3}{2}u^2 = \text{const} < 0$$

of the model equation of the equations of the moon:

$$\begin{cases} \ddot{u} - 2\dot{v} = -\frac{u}{r^3} + 3u \\ \ddot{v} + 2\dot{u} = -\frac{v}{r^3} \end{cases}$$

where  $r = \sqrt{u^2 + v^2}$ . Nowadays this result has, of course, been derived in much simpler ways. But it took nearly a century till it was possible to prove the stability of Hill's orbits. This is an application of KAM theory in a rather singular situation. (see Conley, Kummer).

### III PAINLEVÉ PROBLEM

a) Besides the stable behavior we find, of course, unstable motions in Hamiltonian systems, in particular, in the  $N$ -body problem. Here we want to discuss a recently discovered, most extreme form of instability, namely a motion of the  $N$ -body problem in which the greatest mutual distance became unbounded in finite time! This is rather unexpected and hard to visualize, and seems to contradict (naive) energy considerations!

b) Actually this is related to an old problem raised by Painlevé in his lectures on celestial mechanics in 1895. (Incidentally, later in 1904, Painlevé was one of the four plenary speakers at the ICM in Heidelberg). What led to the quest for such strange solutions? Originally Painlevé was interested in the study of *all* possible singularities of the solutions of the  $N$ -body. It is obvious that collisions of two or more masspoints give rise to singularities, the so-called "collision singularities". They can be characterized by the property that the positions of the masspoint approach a definite position in configuration space. Such singularities, especially double and triple collisions have been studied extensively (Levi-Civita, C. L. Siegel et al).

Painlevé asked whether also other noncollision singularities could possibly exist, and the title of this Section refers to this question. Obviously they do not exist for the Kepler problem, and it was known to Painlevé that also for the three-body problem such singularities can not occur. So the problem referred to the  $N$ -body problem for  $N \geq 4$  only.

To describe the situation briefly we denote by  $q_j \in \mathbf{R}^3, j = 1, 2, \dots, N$  the position of the masspoints of mass  $m_j$ , and by  $r_{ij} = |q_i - q_j| > 0$  their distances. The Newton potential is given by

$$-U = \sum_{i < j} \frac{m_i m_j}{r_{ij}}.$$

If at  $t = T$  a singularity occurs then one has  $U \rightarrow -\infty$ , hence  $\min r_{ij} \rightarrow 0$  as  $t \rightarrow T - 0$ . In 1908 von Zeipel discovered that a noncollision singularity can occur only if in addition also

$$\max_{i < j} r_{ij} \rightarrow \infty \text{ for } t \rightarrow T;$$

as a matter of fact this property characterizes a noncollision singularity! Thus the quest for noncollision singularities is the same as that for the extreme form of instability we started with!

c) This makes the situation clearly very unlikely! Nevertheless, J. Xia was able to construct such a weird solution for the 5-body problem in  $\mathbf{R}^3$ . Here is a schematic view of the solution discovered by Jeff Xia in 1992: We consider two doublestars  $(P_1, P_2)$  and  $(Q_1, Q_2)$ , both of equal masses, moving symmetrically on two planes perpendicularly to the  $z$ -axis. These approximately elliptical orbits are chosen so that the angular momentum is zero. Now we add a fifth masspoint, a “shuttle”, traveling back and forth on the  $z$ -axis between these double stars.

Xia's model

Choosing the parameters appropriately one can achieve that the shuttle experiences a huge acceleration at each near-encounter (near triple collision!) so that the return times decrease so fast that they add up to a finite number.

d) Now the history of this solution is not so straight-forward; it came from quite independent investigations, based on work of Conley, McGehee and Mather some 25 years ago. It originated in the investigation of the neighborhood of triple collisions by Conley and McGehee around 1974, which revealed hyperbolic behavior near such a triple collision, which for an individual solution had already been observed by Siegel. Using this hyperbolic behavior Mather and McGehee succeeded (1974) in constructing a noncollision singularity even for the colinear four body problem! However, their solution had a shortcoming: It involved infinitely many double collisions, which were unavoidable in the one-dimensional situation. Nevertheless, it was the first breakthrough for this problem. To find a solution free from this blemish took 18 more years! In 1992 Jeff Xia succeeded in constructing a noncollision solution for the five-body problem, thus solving the almost 100 year old problem! The proof is very intricate and subtle, but the underlying principle is to pass close to a sequence of triple collisions, and to use their instability at each step to reverse the shuttle with tremendous acceleration. It is an extra difficulty to verify that one can avoid collisions on the way.

An earlier attempt is due to Gerver (1984), who constructed another configuration for the five-body problem leading to non-collision singularity, but the details for a complete proof have not yet published.

Clearly this solution is not of any astronomical significance. Why do I present it: It shows, in one example, the progress gained from the study of hyperbolic dynamical systems which provided the understanding and the tools for the solution of this problem. It also reminds us of the efforts that go in the studies of singularities in partial differential equations, e. g. of the Navier-Stokes equation, provided they exist! One usually thinks of singularities as a local phenomenon, but even this (simple!) classical example of ordinary differential equations exhibits such complicated singularities of nonlocal type, whose existence was doubted for a long time.

#### IV INTEGRABLE SYSTEMS

a) All stability results for Hamiltonian systems – aside from trivial exceptions – depend on how well a given system can be approximated by an integrable one! Since these integrable systems are very rare this seems a hopeless proposition.

In the last 30 years, this topic has received immense attention from mathematicians and physicists alike. Its rapid development has affected many branches of mathematics, such as PDE, scattering theory, differential geometry, even algebraic geometry and others. Moreover, it has led to technical applications, as for example in transmission of optical pulses in fibers.

It is one of the fields which attained a certain popularity. Most scientists have heard the catch words “solitons”, “Korteweg-de Vries equations”.

This is all the more surprising as this subject is a very old one having its origin in the last century! At the time of Euler and Jacobi integrable systems were of great interest since they could be solved “by quadrature”, i. e. more or less explicitly which was of great importance, since existence theorems were not available then. Roughly speaking a Hamiltonian system of  $n$  degrees of freedom is called “completely integrable” if it possesses  $n$  integrals of the motion, whose mutual Poisson brackets vanish. In view of E. Noether’s theorem this means that the systems admit an  $n$ -dimensional commutative group action (via symplectic transformations). In the compact case this would be a torus action. In short, these are particularly simple systems, and the structure of the flow can be described fairly easily. For 2 degrees of freedom rotational symmetric systems are completely integrable since they admit the angular momentum and the energy as integrals. In this case the “integrability” is obvious.

Now there are a number of integrable systems whose integrals and whose symmetries are not at all obvious and one speaks loosely of “hidden symmetries”. Who would expect the geodesic flow on an ellipsoid with different axes to be integrable! This was discovered by Jacobi in 1838. He wrote to Bessel: “Yesterday I solved the equations for the geodesic lines on an ellipsoid with three different axes by quadrature. These are the simplest formulae of the world, Abelian integrals, which turn into elliptic integrals if two of the axes become equal”. Today we would say that the solutions lie on a 2-dimensional torus, which is the real part of the Jacobian variety of a hyperelliptic curve of genus 2. They are with the exceptions of the geodesics passing through the focal points quasi-periodic. This statement can be generalized to ellipsoids of any dimension, which was done already in Jacobi’s lectures. There are many other such examples, such as Euler’s two fixed center problem, where one studies the motion of a masspoint under the Newton attraction of two fixed mass points, or the Kovalevskaya top.

Geodesics on an ellipsoid

Lift to the unit tangent bundle

The symmetry in these examples certainly is “hidden”. It was revealed only by analytical methods, namely by solving the Hamilton–Jacobi equation by separation of variables. Later this became a favorite topic for tricky exercises in mechanics.



No wonder that the topic became dormant.

The interest in integrable systems waned when Poincaré showed that, generically, Hamiltonian systems do not possess integrals besides the Hamiltonian itself. The field became obsolete.

b) The revival, or rediscovery, of this dormant field is most surprising. It is no exaggeration to say that this subject was initiated by a computer experiment! In 1965 Kruskal and Zabusky investigated a partial differential equation obtained by replacing the viscosity term in the Burgers equation by a third order derivative (dispersion)-term to see what it does to the shock solutions:

$$u_t + uu_x + u_{xxx} = 0$$

The equation was known in the literature as the Korteweg–de Vries equation, and it played a role in the theory of water waves, but the discoveries of Kruskal et al was absolutely new and totally unexpected. They found a strange phenomenon about the interaction of wave solutions:

The equation admits a family of wave solutions of different velocities, and the interaction between them appeared to be absolutely clean, so that after the interaction the waves reappeared in the same form and shape as before.<sup>1</sup>

In general, for other evolution equations, one would expect a scattering and a loss of the waves after the interaction. Kruskal coined the term “soliton” for these waves because they seemed to retain their identity.

After this observation, based on the numerical calculations, the search for an explanation of this extraordinary phenomenon began. I can not describe here the dramatic development that ensued. Here just some stages: The first guess was that the equation must possess more conserved quantities than the standard 3 (energy, mass and momentum), and after some efforts of a group some 10 integrals were found by laborious hand calculation. Ultimately one could extend these to an infinite number, and a method for solving these equations by inverse scattering methods was devised by Kruskal and his coworkers (1968).

It did not take long until C. Gardner discovered a Poisson bracket in function space, with respect to which the Korteweg–de Vries equation is Hamiltonian. Moreover the Poisson bracket of the integrals vanished, in short the KdV turned out to be the first example of an integrable Hamiltonian system of infinite degrees of freedom! This was the start of an intense activity. One was the discovery that the integrals, in fluid dynamics called conservation laws, could be viewed

---

<sup>1</sup> A video demonstrating this was presented at the lecture. It can be seen in the abstract of this manuscript in the electronic version of these Proceedings.

as eigenvalues of a simple operator, the one-dimensional Schrödinger operator  $L = -D^2 + q(x)$ , with  $q = -u/6$ , in which the solution of the KdV figures as the potential. In other words the flow defined by the KdV defines a deformation of this operator which leaves the spectrum unchanged. The observation of the iso-spectral deformations by P. D. Lax fruitfully led to many other discoveries, in particular, of several other integrable partial differential equations, as well as to further new insights.

c) By analogy with the finite-dimensional case one would expect that this partial differential equation can be solved explicitly! What are the (hidden) symmetries. Here are some highpoints which I want to single out:

i) If one subjects the KdV to the periodic boundary condition  $u(x + 1, t) = u(x, t)$ , i. e. if one considers the solutions on the circle, then all the solutions are almost periodic in  $t$ . (McKean and Trubowitz 1976) This is a most unexpected property for a nonlinear partial differential equation. It is the reflection of the integrability of the equation. For the geodesics on an ellipsoid, for example, all solutions are quasi-periodic, with the exception of the orbits through the focal points. In the case of the KdV such exceptions do not exist! The proof is based on the fact that the isospectral manifolds are infinite-dimensional tori, which can be interpreted as the real part of the Jacobian variety of a Riemann surface (complex curve) of infinite genus, on which the flow is linear. This curve is obtained as follows. It has been known for a long time that the spectrum of the one-dimensional Schrödinger operator with periodic potential has a “band” spectrum, that is, it consists, in general, of infinitely many intervals clustering at  $+\infty$ . Now consider the double covering of the complex plane and glue the 2 sheets along these intervals, in the customary fashion. This gives the desired complex hyperelliptic curve whose genus is equal to the number of intervals — if it is finite.

ii) Inverse spectral theory: In spectral theory it is an old question to construct the potential of an operator from the spectrum, which is the inverse of the usual question of spectral theory. The answer is usually too hard, or the solution not unique. But the question for all the potentials having a “finite gap” potential has been answered by S. Novikov and his coworkers in 1976:

Given a set of finitely many disjoint intervals, one of which is half-infinite stretching to  $+\infty$ , find all potentials having these intervals as spectrum. The answer is given in terms of the hyperelliptic functions on the above mentioned hyperelliptic curve. In case of a single (half-infinite) interval the potential is a constant, for 2 intervals (genus 1) the potentials is an elliptic function (Lamé equation) etc.

d) It is another startling fact that the soliton theory has down-to-earth applications to communication theory. Here the underlying equation is not the KdV but the nonlinear Schrödinger equation

$$iu_t + u_{xx} + |u|^2 u = 0$$

which also was recognized as an integrable system (Zakharov, Shabat 1971) using ideas of P. Lax. This equation also possesses “solitons” with extraordinary stability

properties. This fact was used by physicists (Hasegawa (1973), Mollenauer (1980)) for signal transmission in optical fibres. Here the solitons describe the envelope of a wave train.

This approach has been used with success to transmit ultrashort pulses over large distance ( $\sim 10^4$  km) with less loss than one encounters with standard methods.

e) It is impossible to even touch on the many ramifications that have evolved from the study of integrable system. The question why iso-spectral deformation gives rise to systems respecting a symplectic form has led to interesting applications of Kac–Moody algebras. The old Schottky problem asks for the characterization of those Abelian tori which are Jacobian varieties of an algebraic curve. In 1986 Shiota found an answer in terms of the solutions of the “KP-equation”, a partial differential equation, generalizing the Korteweg-de Vries equation, thus connecting this problem of algebraic geometry with integrable partial differential equations.

On the side of analysis the question has been raised and answered whether the KAM technique can be applied to partial differential equations, e. g. can one establish the existence of quasi-periodic solutions for the perturbed KdV:  $u_t + uu_x + u_{xxx} = \epsilon(g(x, u))_x$  where  $g$  is a real analytic function, periodic in  $x$ . For small values one finds indeed quasi-periodic solutions of this equation. The necessary theory is highly technical. It has been developed by Kuksin, and subsequently by Pöschel, Craig and Wayne and Bourgain. However, one has to point that in this case the solutions so obtained form a “small” subset in the phase space.

## V BREAKDOWN OF STABILITY

a) What happens when the perturbation from the integrable system gets larger and larger? It turns out that the structure of the invariant tori and the stability of the system breaks down! However, the invariant tori degenerate into some invariant sets, generally Cantor sets, the so-called Aubry–Mather sets. This is the object of a theory discovered independently by the physicist Aubry and by John Mather. They were motivated by entirely different questions: Aubry by stable states in a simple model for one-dimensional crystals in solid state physics, while Mather studied invariant sets for area-preserving mappings. Both theories were ultimately recognized to be the same. This (Aubry–Mather) theory (1982) brought a significant advance to dynamical systems, but is also related to an interesting development in differential geometry.

The underlying idea of this theory can be illustrated with the simple model problem of the geodesic flow on a two-dimensional torus  $T^2 = \mathbf{R}^2/\mathbf{Z}^2$ . We give a  $\mathbf{Z}^2$ -periodic metric, say  $g$  on  $\mathbf{R}^2$ . The corresponding geodesic flow gives rise to a Hamiltonian system on the cotangent bundle  $T^*(T^2)$  and the unit-cotangent bundle  $\mathcal{E} = T^*(T^2_1)$  as three-dimensional energy surface. For the flat metric, denoted by  $g_0$ , all geodesics are straight lines, and a family of parallel lines lift to an invariant torus on  $\mathcal{E}$ . According to the KAM theory many of these tori persist under perturbation, namely those for which the slope is an irrational number which

is badly approximable by rationals. In particular, the orbits between two such tori are trapped, and the flow on  $\mathcal{E}$  is certainly not ergodic.

On the other hand, about 10 years ago V. Donnay found smooth metrics, say  $g_1$  on the 2-torus for which the geodesic flow is ergodic. Consequently the structure of invariant tori must break down if we deform  $g_0$  to  $g_1$ .

b) To understand the situation we project the flow on such an invariant torus into the configuration space, i. e.  $\mathbf{R}^2$ . One finds that the orbits on such an invariant torus project into a  $\mathbf{Z}^2$ -invariant foliation made up of geodesics.

In the terminology of the Calculus of Variations this is a “field of extremals”. It is classical result, going back to Weierstraß, that the geodesics belonging to an extremal field are “minimizers”, i. e. any segment of such a geodesic minimizes the length between its endpoints. In other words, all orbits belonging to an invariant torus project into minimizers. This is — or can be taken as — the clue to the Aubry-Mather theory. The goal then is to study the minimizers among all geodesics. This is generally a strict subset of the set of all geodesics. As a matter of fact, by a classical theorem of E. Hopf, a metric for which all geodesics are minimizers, is necessarily flat ( $K = 0$ ). The minimizers on a torus had already been studied by Hedlund, after earlier work by his teacher M. Morse (1924), who called them “geodesics of class A”.

#### Projection of an invariant torus into a minimal foliation

c) These minimizers (or geodesics of class A) intersect each other at most once, as do straight lines. Moreover, they have the crucial property that they are trapped in a strip bounded by two straight lines whose distance  $D$  depends only on the metric, not on the individual minimizer.

## “Trapping” of minimizers

In particular, one can associate with any minimizer a direction, say  $\theta(\text{mod}2\pi)$ . Moreover, for each value of  $\alpha = \theta/2\pi(\text{mod}2\pi)$  the set of these minimizers,  $\mathcal{M}_\alpha$  can be shown to be non-empty. Now at least if  $\alpha$  is irrational one can put together the corresponding extremal field from these not intersecting minimizers of  $\mathcal{M}_\alpha$  to obtain a minimal foliation, provided these minimizers are dense on the torus, and the lift of this foliation recovers the invariant torus. However, it is possible, as simple examples of “bumpy” metrics show, that these minimizers may not be dense, if projects on the torus. In that case these minimizers provide only a “lamination”, covering only a part of the torus.

## Bumpy metric (after Bangart)

In this case these recurrent elements of  $\mathcal{M}_\alpha$  lift to an invariant set, in fact, a unique invariant set, which turns out to be a minimal set associated with any value

of  $\alpha$ . This is the Mather set in question, to which the invariant torus deteriorate under deformation of the metric.

I want to show with this indication, that Mather sets are obtained in a very natural way by selecting out of all orbits only those which are minimizers (and not just stationary).

d) This selection principle of minimizers out of the class of all solutions of the Euler equations is a very useful principle, also for elliptic partial differential equation derived from a variational problem, satisfying a Legendre condition. It has proved useful in differential geometry. It is possible to extend the Mather theory to minimal foliations on a higher dimensional torus, where the orbits are replaced by minimal surfaces of codimension 1. It is even more interesting to study such minimizers of codimension 1 on manifolds where the reference metric has negative curvature. The crucial trapping property mentioned above holds also in this situation and leads to most interesting new results. This development is due to Gromov, who introduced the term “trapping”. I can not and need not enter into this field since it has been presented in an ICM 1994 lecture by V. Bangert. Since then he and Urs Lang have obtained very general results about the so-called asymptotic Plateau problem.

#### VI CONCLUDING REMARKS

I hope to have shown to you that the subject of dynamical systems holds a vast number of connections to other fields — even with the restrictions I imposed on myself.

Most striking to me is the development of integrable systems (some 30 years ago) which did not grow out of any given problem, but out of a phenomenon which was discovered by numerical experiments in a problem of fluid dynamics. Intelligent studies and deep insight opened up to a novel field impinging on differential geometry, algebraic geometry and mathematical physics, including applications in communication of fiber optics. This illustrates that one is ill-advised to try to direct or predict the development of mathematics. In a time of dangerous specialization we should feel free to use all tools available to us, and use them with proper taste. To me, it seems idle to argue whether to prefer solving of challenging problems, building abstract structures, or working on applications. Rather we should keep an open mind when we approach new problems, and not forget the unity of mathematics. In the words of Birkhoff: “It is fortunate that the world of mathematics is as large as it is”.

#### ACKNOWLEDGEMENTS

For the help in preparing the computer pictures I want to express my thanks to the friends and colleagues at the Geometry Center in Minneapolis, whose director, R. McGehee provided me with generous support. Eduardo Tabacman helped with most of the figures and Jeff Schaefer with those concerning the geodesics on an ellipsoid. The MATLAB program for the interacting solitons I owe to David Sattinger from the University of Minnesota.

To Paul Rabinowitz and E. Zehnder I am grateful for their encouragement and patience. My best thanks to all of them.

## REFERENCES

## INTRODUCTION

- 1) Die Elite der Nation im Dritten Reich, Leopoldina-Symposium, Acta Historica Leopoldina 22, Hrsg. C. S. Scriba, Halle (Saale) 1995, [in particular, p.16].
- 2) C. JACOBI, "Vorlesungen über Integration der Differentialgleichungen" WS 1842/43, published by Clebsch as "Vorlesungen über Dynamik" in 1866.
- 3) H. PIEPER, Carl Gustav Jacob Jacobi (1804–1851). Die Albertus-Universität zu Königsberg und ihre Professoren, Hrsg. D. Rauschnig, D. v. Nerée, Dunker & Humblot, Berlin 1995, 473–488.
- 4) G. D. BIRKHOFF, Dynamical Systems, Coll. Lectures, AMS, 1927

## I HISTORICAL REMARKS

- 1) C. L. CHARLIER, Die Mechanik des Himmels, Verlag von Veit & Comp., Leipzig 1907 [especially Band 2 p. vi].
- 2) LEJEUNE DIRICHLET, Werke, vol. 2 Berlin, 1897.
- 3) J. BARROW-GREENE, Poincaré and the three body problem, History of Mathematics, Am. Math. Soc., Providence, R. I.; London Math. Society, London, 1997.
- 4) A. N. KOLMOGOROV, Théorie générale des systèmes dynamiques et mécanique classique. Proc. Int. Congress of Math. 1954, vol. 1 315–333, North Holland, Amsterdam 1957 [Russian].
- 5) V. I. ARNOLD, Small denominators III. Small denominators and problems of stability of motions in classical and celestial mechanics, Russ. Math. Surveys 18, 1963, 213–284.
- 6) C. L. SIEGEL, Iterations of analytic functions, Ann. Math. 43, 1942, 607–612.

## II APPLICATIONS, MAPPINGS

- 1) Proceedings CERN SYMPOSIUM vol.1: High energy accelerators (ed. Regenstein), CERN, Genève 1956 [in particular p.254].
- 2) E. ZEHNDER, Homoclinic points near elliptic fixed points, Comm. Pure Appl. Math. 26, 1973, 131–182.
- 3) C. GENECAUD, Transversal homoclinic points near fixed points of area preserving diffeomorphisms of the plane, Dynamics reports, 1–30, Dynamics Report. Expositions Dynamical Systems (N. S.) 2, Springer Berlin 1993.
- 4) C. STÖRMER, The Polar Aurora, Clarendon Press, Oxford 1955.
- 5) A. J. DRAGT, Trapped orbits in a magnetic dipole field, Reviews of Geophysics 3, 1965, 255–298.
- 6) W. N. HESS, G. D. MEAD and M. P. NAKADA, Advances in Particles and Field Research in the Satellite Era, Reviews of Geophysics vol.3, No. 4, Nov. 1965, 521–570.
- 7) M. BRAUN, Particle Motion in a Magnetic field, Journ. Diff. Equations 8, 1970 294–332.
- 8) E. G. STASSINOPOULOS and J. P. RAYMOND, The space radiation environment for electronics, Prod. IEEE, Nov. 1988, 1423–1442.

9) M. KUMMER, On the stability of Hill's solutions of the plane restricted three-body problem, *Am. Journ. Math.* 101, 1979, 1333–1354.

10) J. C. YOCOZ, Travaux de Herman sur les tores invariants, *Séminaire Bourbaki*, no.754, 1992, *Astérisque* 206, 1992, 311–345.

### III PAINLEVÉ PROBLEM

1) P. PAINLEVÉ, *Leçons sur la Théorie Analytique des Équations Différentielles*. A. Hermann, Paris 1897.

2) J. MATHER and R. MCGEHEE, Solutions of the collinear four body problem which become unbounded in finite time, *Lecture Notes in Physics* 38, Springer Verlag, 1975, 573–597.

3) J. GERVER, A possible model for a singularity without collisions in the five body problem, *Journ. Differential Equations* 52, 1984, 76–90.

4) J. GERVER, The existence of pseudocollisions in the plane, *Journ. Differential Equations* 89, 1991, 1–68.

5) R. NCGEHEE, van Zeipel's theorem on Singularities in celestial mechanics. *Expos. Math.* 4, 1986, 335–345.

6) J. XIA, The existence of noncollision singularities in newtonian systems, *Ann. Math.* 135, 1992, 411–468.

7) A. CHENCINER, À l'infini en temps fini, *Astérisque* 245 1997, *Séminaire Bourbaki*, 1996/97, *Expos.* 832, 5, 323–353.

### IV INTEGRABLE SYSTEMS

1) M. O. KRUSKAL and N. J. ZABUSKY, Interaction of solutions in collisionless plasma and the recurrence of initial states, *Phys. Review Letters* 15, 1965, 240–243.

2) P. D. LAX, Integrals of Nonlinear equations of evolution and solitary waves, *Comm. Pure Appl. Math.* 21, 1968, 467–499.

3) C. S. GARDNER, Korteweg-de Vries equation as a Hamiltonian systems, *Journ. Math. Phys.* 12, 1971, 1548–1557.

3) L. FADDEEV and L. D. ZAKHAROV, Korteweg-de Vries equation as completely integrable Hamiltonian system, *Anal. i Prilizenia* 5, 1971, 18–27.

4) P. D. LAX, Nonlinear Differential Equations of Evolution, *Actes Congress Int. Math.* 1970, vol. 2, 831–870, Gauthies-Villars, Paris 1971.

5) V. E. ZAKHAROV and A. B. SHABAT, *Sov. Phys. JETP* 34, 1972, 62–69.

6) C. S. GARDNER ET AL, Korteweg-de Vries equation and generalizations VI, *Methods of exact solutions*, *Comm. Pure Appl. Math.* 27, 1974, 97–133.

7) H. P. MC KEAN and E. TRUBOWITZ, Hill's Operator and Hyperelliptic function theory in the presence of infinitely many branch points, *Comm. Pure Appl. Math.* 29, 1976, 143–226.

8) DUBROVIN ET AL, Nonlinear equations of Korteweg-de Vries type, finite zone linear operators and Abelian varieties, *Russian Math. Surveys* 31, 1976, 59–146.

9) AKIRA HASEGAWA, *Optical Solitons in Fibers*, Springer-Verlag 1989.

10) *Optical solitons – theory and experiments*, *Cambridge Studies in Modern Optics* 10, (ed. J. R. Taylor), Cambridge Univ. Press 1992.

11) T. SHIOTA, Characterization of Jacobian varieties in terms of soliton equations. *Inv. math.* 83, 333–382 (1986).



- 12) ARBARELLO -DE CONCINI Another proof of a conjecture of S. P. Novikov on periods of abelian integrals on Riemann surfaces. *Duke Math. J.* 54, 163–178 (1987).
- 13) W. CRAIG, C. E. WAYNE, Newton's method and periodic solutions of nonlinear wave equations, *Comm. Pure Appl. Math.* 49, 1990, 1409–1498.
- 14) S. KUKSIN and J. PÖSCHEL, Invariant Cantor Manifolds of Quasi-Periodic Oscillations for a Nonlinear Schrödinger Equation, *Ann. Math.* 143, 1996, 149–179.

#### V BREAKDOWN OF STABILITY

- 1) S. AUBRY and P. Y. LEDAERON, The discrete Frenkel-Kontorova model and its extensions I: exact results for ground states, *Physica* 8D, 1983, 381–422.
- 2) J. N. MATHER, Existence of quasi-periodic orbits for twist homeomorphisms of the annulus, *Topology* 21, 1982, 457–467.
- 3) J. N. MATHER and J. FORNI, Action minimizing orbits in Hamiltonian systems, *Lecture Notes in Mathematics* 1589, Springer Verlag 1991, 92–186. [contains further references].
- 4) J. MOSER, Minimal solutions of variational problems on a torus, *Ann. Inst. Henri Poincaré, Anal. nonlinéaire*, vol 3, 1986, 229–272.
- 5) M. GROMOV Foliated Plateau Problem, Part I, *Minimal Varieties*, *Geom. Functional Analysis*, 1991, 14–79.
- 6) V. BANGERT, Minimal Foliations and Laminations, *Proc. ICM 1994*, vol.1, Birkhäuser Verlag 1995, 453–464.
- 7) V. BANGERT and U. LANG, Trapping quasi-minimizing submanifolds in spaces of negative curvatures, *Commentarii Math. Helv.* 71, 1996, 122–143.

Jürgen Moser  
ETH Zürich  
Department of Mathematics  
CH-8092 Zürich  
Switzerland  
moser@math.ethz.ch

MATHEMATICAL PROBLEMS  
IN GEOPHYSICAL WAVE PROPAGATION

GEORGE PAPANICOLAOU

ABSTRACT. We review several aspects of the mathematical theory of wave propagation in random media with particular emphasis on topics of geophysical interest.

CONTENTS

1	INTRODUCTION	404
1.1	Why geophysical wave propagation . . . . .	404
1.2	Random media or environments in general . . . . .	404
1.3	Acknowledgements . . . . .	406
2	GENERAL NOTIONS ABOUT WAVES IN RANDOM MEDIA	406
2.1	Scales . . . . .	406
2.2	Types of waves . . . . .	407
2.3	Coherent and incoherent fields . . . . .	407
2.4	Localization and transport . . . . .	407
2.5	Nonlinearity and randomness . . . . .	408
2.6	Numerical simulations . . . . .	408
2.7	Parameter estimation and imaging . . . . .	409
3	THE TRANSPORT REGIME	409
3.1	Waves to transport . . . . .	411
3.2	Transport for electromagnetic and elastic waves . . . . .	414
3.3	Boundary conditions . . . . .	415
3.4	The diffusive regime . . . . .	415
3.5	Parameter identification and inverse problems . . . . .	415
4	THE LOCALIZATION REGIME	416
4.1	Pulse reflection from randomly layered media . . . . .	416
4.2	Scale separation . . . . .	417
4.3	Localization regime asymptotics . . . . .	418
4.4	Time domain localization . . . . .	420
4.5	Statistical inverse problems . . . . .	421
4.6	Reflection and transmission of time harmonic plane elastic waves . . . . .	423
4.7	Pulse stabilization and imaging . . . . .	423

## 1 INTRODUCTION

### 1.1 WHY GEOPHYSICAL WAVE PROPAGATION

In deciding what to present as a plenary lecture in applied mathematics and probability at ICM-98, I considered several areas with which I am familiar and decided to focus on geophysical wave propagation for a couple of reasons. One, a technical one, is that inhomogeneities are strong and highly anisotropic so that the modeling and analysis of wave propagation in the earth's crust is mathematically interesting and quite difficult. The other reason is closely related to what my view of modern applied mathematics is: the creation and development of a mathematical environment for physical, economic, biological or other phenomena. This involves active participation of the mathematician in the quantitative modeling, in the analysis, in the computations, as well as in the interpretation of results and assessment of the effectiveness of the modeling.

The resulting mathematical methodology will be uneven, from routine off-the-shelf toolbox applications to entirely uncharted problems that need new ideas and techniques, and it is up to the mathematician to decide what the right mix of mathematical sophistication and rough heuristics should be. An overly mathematical approach will impede communication with nonmathematical specialists who value results and do not care much for mathematical generality. Accepting the conventional wisdom in a field, and concentrating on technical mathematical issues, is not a good idea either. Geophysical wave propagation is a case in point. It is fair to say that wave localization is virtually unknown to geophysicists. But, as I will try to explain in this lecture, wave localization is quite important in exploration geophysics because, among other things, it influences the resolution of seismic imaging and the effective depth penetration of seismic probes. What is the best way to approach these problems mathematically?

A few years ago, K. Aki, a distinguished seismologist whose ideas about the role of crustal inhomogeneities in seismic wave propagation have been very influential, heard a seminar that I gave on wave localization and asked this question: How can one tell from seismic observations that wave localization has taken place? Electronic wave localization in semiconductors goes back forty years [1], with the strong participation of mathematicians during the last twenty years, so we should be able to say quite a bit, as I will try to explain in this lecture. But Aki's question is a profound one that leads to the most complex and least understood issue in geophysical wave propagation, the localization-transport transition. It is a pragmatic, operational question which reminds us that great intellectual challenges can have humble, unpretentious origins. I think that it takes a mathematician to answer Aki's question and perhaps it will be one that does it.

### 1.2 RANDOM MEDIA OR ENVIRONMENTS IN GENERAL

I will treat the earth's crust as a random medium, that is, as an elastic medium with density and Lamé parameters that are random functions of space. The equations of linear elastic wave propagation become now stochastic partial differential equations. Initial and boundary conditions must also be specified and they could

bring in additional randomness, from modeling the rough surface of the earth. At this level of generality the randomness is nothing more than variable coefficients and non-flat boundaries, so general linear PDE methods can deal with everything (symmetric hyperbolic systems). If dissipation is important, and it is in some contexts, it can be put into the equations in different ways. There is no general agreement on how to best model dissipation analytically and this is an interesting issue that I will not address here.

But even this much is somewhat grudgingly accepted by geophysicists. I regularly hear comments like: there is only one earth and it is not changing all that fast, so where is the statistical ensemble of realizations coming from? If stochastic modeling is to be criticized along such lines then why are we modeling the Dow Jones Industrial Average, or some other index or asset price, as a stochastic process? There is only one realization of the DJIA just as there is only one realization of the earth. What the stochastic processes model is uncertainty, lack of information and its consequences when only imperfect and sparse observations or measurements are available, and even desirable. The notion of ‘effective’ medium is very much part of the mathematical physics of the 19th century, of Maxwell, Rayleigh and others, which is why equations with constant coefficients have any relevance at all in modeling. The conceptual barrier seems to come up when one thinks of fluctuations.

It is not an accident, therefore, that in one of the first instances of wave propagation in random media, natural light propagation through a turbulent atmosphere, astrophysicists at the turn of the 20th century did not go to Maxwell’s equations (or the wave equation if the vector nature of light waves can be neglected) but developed a new, phenomenological theory, the radiative transport theory, to interpret observed phenomena. There are a few isolated attempts to consider random media, with fluctuations, during the first half of the 20th century but it is with the advent of radar and sonar during in the forties that random waves emerge as a subject. Keller’s papers in the sixties [2] were very influential because they were the first ones written by a mathematician, who thought about the conceptual foundations and separated heuristics from legitimate calculations. It was also in the sixties that the connection between radiative transport theory and stochastic wave equations was clarified, as I will discuss in section 3.1.

Atmospheric wave propagation, from radio to radar to optical frequencies, and underwater sound propagation, from 20 hertz to kilohertz, were the main applications driving the theory of wave propagation in random media in the seventies and are discussed in Ishimaru’s book [3]. It is interesting to note that the notion of wave localization is nowhere to be found in this book. Random media in seismology appeared first in the mid eighties in a simple version of radiative transport [4]. Transport theory is now just beginning to become mainstream in seismology as is seen from the recent book of Fehler and Sato [5]. But wave localization is not discussed in this book either. A treatment of waves in random media that deals extensively with wave localization is given by Ping Sheng [6].

What is wave localization anyway? I will explain it in some detail in section 4.3 but, roughly, it is when random inhomogeneities trap wave energy in a finite region and do not allow it to spread as it would normally. Random media behave

then like periodic media that have band-gap spectra, allowing wave propagation in some frequency ranges but not in others. It is remarkable that this happens for random media that are not close to periodic ones at all. Mathematically, it is shown that wave or wave-like operators with stationary (translation invariant) random coefficients in unbounded regions have discrete spectra [7]. Discrete spectra means that the wave energy in each mode initially will remain there for ever, oscillating in time but not propagating out to infinity. In three dimensional wave propagation this can happen only when parameter fluctuations are very large. This is not the case for electromagnetic waves in the atmosphere or sound waves in the ocean. The fluctuations are weak, a few percent, and when they are important they lead to radiative transport, which allows spreading of wave energy in diffusive rather than wave-like manner.

Where then do we see wave localization in classical wave propagation? We see it when wave energy is channeled, by a waveguide, by a transmission line, by an optical fiber, by strong anisotropy due to layering in the lithosphere, etc. We also see it in nearly periodic structures. Waves in an one dimensional random medium will localize, even if the fluctuations in the medium parameters are weak. In geophysical wave propagation and elsewhere (in optical localization) a key issue is the identification of structures, more complicated than simple channeling or periodicity, that tend to enhance the onset of wave localization by random fluctuations. This is the localization-transport transition problem.

### 1.3 ACKNOWLEDGEMENTS

I would like to thank several friends and colleagues with whom I worked in the past: R. Burridge, J.B. Keller, W. Kohler and B.S. White with whom I have been associated for a long time, and my more recent collaborators: M. Asch, G. Bal, J. Berryman, J. Bronski, O. Dorn, J.P. Fouque, F. Herrmann, R. Knapp, P. Lewicki, A. Nachbin, M. Postel, L. Ryzhik, Y. Samuelides, P. Sheng, K. Solna and S. Weinryb.

## 2 GENERAL NOTIONS ABOUT WAVES IN RANDOM MEDIA

### 2.1 SCALES

There are three basic length scales in wave propagation phenomena:

- The typical wavelength  $\lambda$
- The typical propagation distance  $L$
- The typical size of the inhomogeneities  $l$

In geophysical wave propagation it is difficult to associate a ‘typical’ scale that is characteristic of the inhomogeneities. The density and local speed of propagation of waves vary on many scales. We may think of  $l$  as a typical correlation length. When the standard deviation of the fluctuations is small then the most effective interaction of the waves with the random medium will occur when  $l \sim \lambda$ , that

is, the wavelength is comparable to the correlation length. And this interaction will not be observable unless the propagation distance is large ( $L \gg \lambda$ ). If propagation distances are short, a few wavelengths or correlation lengths, then effective medium theories will work fine. There will be a deterministic propagation speed (for scalar waves), the effective speed, with which energy will propagate as if the medium were deterministic. The effective medium theory will be valid also when the wavelength is long compared to propagation distances, even if the correlation length is short ( $l \ll L$ ) and the fluctuations have a large standard deviation. This is the homogenization limit.

Of course this rough way of thinking with scales does not capture the effect of a waveguide geometry, or the effective dimension of the propagation phenomenon. But thinking with scales is very useful and, with some experience, it can become a very good heuristic tool.

## 2.2 TYPES OF WAVES

It is classical waves, solutions of the wave equation or more general symmetric hyperbolic systems, that we want consider, rather than electronic waves which are solutions of the Schrödinger equation. The waves are vector fields in general, as with electromagnetic waves which are solutions of Maxwell's equations or elastic waves where the elastic displacement field is a solution of the elastic wave equations. Mode conversion, the transfer of energy from compression to shear waves for example, is an important effect in random media. So is polarization, which is associated with vector waves all of whose components travel with the same speed. Polarization tends to get lost in a random medium and the way this happens is an important way to make inferences about the nature of the propagation environment.

## 2.3 COHERENT AND INCOHERENT FIELDS

When the random fluctuations of the medium parameters are small then the random fluctuations in the solutions will be small, if the propagation distances are not too big. The mean solution, the coherent field, will carry most of the energy. As the waves propagate their fluctuating component, the incoherent field, gets more energy. The total energy is conserved, if there is no dissipation, but the coherent field loses energy and slows down. This behavior of the coherent field is something that can be calculated easily and is well established in the engineering literature.

## 2.4 LOCALIZATION AND TRANSPORT

If fluctuations are weak and propagation distances large, most of the wave energy will be incoherent. In seismology, for example, after the first arrival from a disturbance far away the seismogram is dominated by strong fluctuations from multiple scattering. The later part, the coda of a seismogram is mostly incoherent field measurement. It is in this regime that radiative transport is a good approximation. It allows accurate calculation of the envelopes of the seismograms without resolving the detailed fluctuations. A new scale enters the description of

propagation phenomena: the mean free path. This is a length scale that gives an indication of the importance of multiple scattering and is much more relevant than the correlation length of the inhomogeneities.

Wave localization is total trapping of the wave energy by scattering from the random inhomogeneities. It is the regime where fluctuation phenomena dominate so we have little intuition for what should happen. For one thing the random fluctuations must be very strong and the structure of the propagating medium must be special (a channeling medium or an ordered, periodic structure). In the lithosphere fluctuations in the speeds of propagation of elastic waves can be as large as 15% and they can be highly anisotropic, with horizontal correlation lengths much larger than vertical ones. Localization manifests itself in fat codas of seismograms, or codas with envelopes that decay slowly. This is a clear indication that there is a lot of multiple scattering going on. Moreover, radiative transport would tend to underestimate the size of the codas indicating that a different analytical theory is needed. What is missing at present is a robust and effective criterion for discriminating between these two situations.

## 2.5 NONLINEARITY AND RANDOMNESS

Nonlinearity and randomness interact significantly only in very special situations, as in soliton propagation in optical fibers or when high intensity laser beams interact with material inhomogeneities. Nonlinearity is rarely an issue in seismic wave propagation except very near sources. In one dimensional wave propagation both nonlinearity and randomness are strongly felt and a long-standing problem is the analysis of their interaction. Is there, for example, wave localization when we have nonlinearities? This is a very difficult question that cannot be answered by a yes or no. The phenomena depend sensitively on the exact setup of the problem: the form of the nonlinearity, the various scales associated with the inhomogeneities and the propagation phenomenon, and the form of the excitation [8, 9, 10, 11, 12, 13].

## 2.6 NUMERICAL SIMULATIONS

At the dawn of the 21st century, when computational power is doubling every two years or so, and computational cost is dropping to the point where a good laptop computer today is more powerful than the Cray I supercomputer of the late seventies, why is anybody interested in analytical methods? We have the computational power to simulate anything we want and we have the ability to make detailed and extensive measurements, which in seismology result in huge data sets. What could mathematical analysis contribute in this context?

Being skeptical about the utility of mathematical analysis and believing that we can compute or simulate everything we need may appear naive to a mathematician but it is increasingly the dominant view in many fields, in geophysical wave propagation for example.

The fact is that if we want to understand the behavior of seismic codas we cannot rely on direct numerical simulations. If the typical wavelength is of the order of 3-5 km and we want to calculate a synthetic seismogram 1000 km from

the source we need a spatial grid that has at least five points per wavelength, and more if we want to simulate accurately random fluctuations in the parameters. In a realistic three dimensional setup it is impossible to generate numerical solutions that will yield a 3 second synthetic seismogram with millisecond resolution. What is even more important to realize is that we should not really want to do this because with radiative transport theory seismic coda envelopes can be calculated. What is holding up realistic numerical computations is not computing power but analysis: we do not have good enough transport theoretic boundary conditions on the earth's surface and at interfaces. The mean free path may be as large as 20-30 km and Monte Carlo methods can give reasonably accurate solutions using a high-end workstation. Transport theory does what is called 'sub-grid' modeling in computational fluid dynamics. We do not have to resolve the small scale inhomogeneities if we can do some analysis, which is in fact difficult but doable.

## 2.7 PARAMETER ESTIMATION AND IMAGING

Imaging of the earth's interior is a challenge that will be with us for a very long time because the inhomogeneities are so strong. In exploration seismology, where seismic probing can generate huge data sets, the issue is not so much good algorithms for imaging but low complexity algorithms. Efficient compression of geophysical data sets is perhaps the most urgent problem that exploration seismology faces at present.

It appears at first that this has nothing to do with waves. Wavelets or other tools for compression from signal processing come to mind, and they are being used. If noise effects are ignored and if the typical wave length of a probing pulse is 100-150 m (for shorter wavelengths dissipation effects are much stronger), we cannot expect image resolution better than 25 m or so at a depth of a few kilometers. And if noise and multiple scattering are to be taken into consideration it is not at all clear what the achievable resolutions are without some compensation. Noise reducing methods (stacking) that are used in imaging are not so effective. Much more needs to be done analytically here. Imaging itself, without noise, is based on variants of a backward wave propagation method (migration) that has now a substantial theoretical basis [14, 15, 16].

The best compression method is to go from the seismic data to the image itself, of course, so good compression has to be adapted to the specific data set and its structure. But there must be interesting algorithms, yet to be found, that are somewhere between know-nothing methods like wavelet decomposition and thresholding, and know-all full imaging.

## 3 THE TRANSPORT REGIME

Radiative transport is a phenomenological theory that was introduced to describe the propagation of light intensity through the Earth's atmosphere. It has been applied successfully to many other problems of wave propagation in a complex medium. In its simplest form, let  $a(t, \mathbf{x}, \mathbf{k})$  denote the angularly resolved energy



density defined for all wave vectors  $\mathbf{k}$ , position  $\mathbf{x}$  and time  $t$ . Because of interaction with the inhomogeneous medium through which it propagates, a wave with wave vector  $\mathbf{k}$  may be scattered into any other direction  $\hat{\mathbf{k}}'$ , where  $\hat{\mathbf{k}} = \frac{\mathbf{k}}{|\mathbf{k}|}$ . The transport equation gives the energy balance

$$\begin{aligned} \frac{\partial a(t, \mathbf{x}, \mathbf{k})}{\partial t} + \nabla_{\mathbf{k}} \omega(\mathbf{x}, \mathbf{k}) \cdot \nabla_{\mathbf{x}} a(t, \mathbf{x}, \mathbf{k}) - \nabla_{\mathbf{x}} \omega(\mathbf{x}, \mathbf{k}) \cdot \nabla_{\mathbf{k}} a(t, \mathbf{x}, \mathbf{k}) \\ = \int_{R^n} \sigma(\mathbf{x}, \mathbf{k}, \mathbf{k}') a(t, \mathbf{x}, \mathbf{k}') d\mathbf{k}' - \Sigma(\mathbf{x}, \mathbf{k}) a(t, \mathbf{x}, \mathbf{k}). \end{aligned} \quad (1)$$

Here  $n$  is the dimension of space ( $n = 2$  or  $3$ ),  $\omega(\mathbf{x}, \mathbf{k})$  is the local frequency at position  $\mathbf{x}$  of the wave with wave vector  $\mathbf{k}$ , the differential scattering cross-section  $\sigma(\mathbf{x}, \mathbf{k}, \mathbf{k}')$  is the rate at which energy with wave vector  $\mathbf{k}'$  is converted to wave energy with wave vector  $\mathbf{k}$  at position  $\mathbf{x}$ , and

$$\int \sigma(\mathbf{x}, \mathbf{k}', \mathbf{k}) d\mathbf{k}' = \Sigma(\mathbf{x}, \mathbf{k}) \quad (2)$$

is the total scattering cross-section. The function  $\sigma(\mathbf{x}, \mathbf{k}, \mathbf{k}')$  is nonnegative and usually symmetric in  $\mathbf{k}$  and  $\mathbf{k}'$ . The left side of (1) is the total time derivative of  $a(t, \mathbf{x}, \mathbf{k})$  at a point moving along a trajectory in phase space  $(\mathbf{x}, \mathbf{k})$  and may be written as a Liouville equation

$$\frac{\partial a}{\partial t} = \{\omega, a\}, \quad (3)$$

where  $\{f, g\} = \sum_{i=1}^n \left( \frac{\partial f}{\partial x_i} \frac{\partial g}{\partial k_i} - \frac{\partial f}{\partial k_i} \frac{\partial g}{\partial x_i} \right)$  is the Poisson bracket. The right side of (1) represents the effects of scattering.

The transport equation (1) is conservative when (2) holds because then

$$\iint a(t, \mathbf{x}, \mathbf{k}) d\mathbf{x} d\mathbf{k} = \text{const}$$

independent of time. Absorption may be accounted for easily by letting the total scattering cross-section be the sum of two terms

$$\Sigma(\mathbf{x}, \mathbf{k}) = \Sigma_{sc}(\mathbf{x}, \mathbf{k}) + \Sigma_{ab}(\mathbf{x}, \mathbf{k})$$

where  $\Sigma_{sc}(\mathbf{x}, \mathbf{k})$  is the total scattering cross-section given by (2) and  $\Sigma_{ab}(\mathbf{x}, \mathbf{k})$  is the absorption rate.

The radiative transport equation (1) was derived from the microscopic equations in the sixties and seventies by many authors (see [17] for references). A nice overview of these methods and results is presented in a recent review [18]. We have recently considered scattering of high frequency waves in a random medium [17] and established validity of the radiative transport theory for scalar and vector waves, including mode conversion and polarization in the following regime:

- Distances of propagation  $L$  are much larger than the wave length  $\lambda$ ,

- The medium parameters vary on the scale comparable to the wave length,
- The mismatch between the inhomogeneities and the background medium is small,
- Absorption is small.

This regime arises in many physically important situations. In seismic wave propagation, teleseismic events can be modeled by radiative transport equations [4, 5].

### 3.1 WAVES TO TRANSPORT

Transport equations for the phase space wave energy densities are constructed [17, 19, 20] as follows. We assume here that the space domain is  $R^3$  ( $n = 3$ ) and deal with acoustic waves. The acoustic equations for the velocity  $\mathbf{v}$  and pressure  $p$  are

$$\begin{aligned} \rho \frac{\partial \mathbf{v}}{\partial t} + \nabla p &= 0 \\ \kappa \frac{\partial p}{\partial t} + \nabla \cdot \mathbf{v} &= 0. \end{aligned} \tag{4}$$

This system may be written in a general form of a symmetric hyperbolic system (with convention of summation over repeated indices):

$$A(\mathbf{x}) \frac{\partial \mathbf{u}}{\partial t} + D^j \frac{\partial \mathbf{u}}{\partial x^j} = 0, \tag{5}$$

where  $\mathbf{u} = (\mathbf{v}, p)$ , and  $\mathbf{x} \in R^n$ . The matrix  $A(\mathbf{x}) = \text{diag}(\rho, \rho, \rho, \kappa)$  is symmetric and positive definite and the matrices  $D^j$  are symmetric and independent of  $\mathbf{x}$  and  $t$ . We consider high frequency solutions of (5). Physically this means that the typical wave length  $\lambda$  of the initial data is much smaller than the overall propagation distance  $L$  with  $\varepsilon = \frac{\lambda}{L} \ll 1$ . The spatial energy density for the solutions of (5) is given by

$$\mathcal{E}(t, \mathbf{x}) = \frac{\rho \mathbf{v}^2}{2} + \frac{\kappa p^2}{2} = \frac{1}{2} (A(\mathbf{x}) \mathbf{u}(t, \mathbf{x}) \cdot \mathbf{u}(t, \mathbf{x})) = \frac{1}{2} A_{ij}(\mathbf{x}) u_i(t, \mathbf{x}) \bar{u}_j(t, \mathbf{x}) \tag{6}$$

and the flux  $\mathcal{F}(\mathbf{x})$  by

$$\mathcal{F}_i(t, \mathbf{x}) = p \mathbf{v} = \frac{1}{2} (D^i \mathbf{u}(t, \mathbf{x}) \cdot \mathbf{u}(t, \mathbf{x})). \tag{7}$$

We have the energy conservation law

$$\frac{\partial \mathcal{E}}{\partial t} + \nabla \cdot \mathcal{F} = 0. \tag{8}$$

and thus the total energy is conserved:

$$\frac{d}{dt} \int \mathcal{E}(t, \mathbf{x}) d\mathbf{x} = 0. \tag{9}$$

The high frequency limit  $\varepsilon \rightarrow 0$  of the energy density  $\mathcal{E}(t, \mathbf{x})$  is described in terms of the Wigner transform, which is defined by

$$W_\varepsilon(t, \mathbf{x}, \mathbf{k}) = \left(\frac{1}{2\pi}\right)^n \int e^{i\mathbf{k}\cdot\mathbf{y}} \mathbf{u}_\varepsilon(t, \mathbf{x} - \varepsilon\mathbf{y}/2) \mathbf{u}_\varepsilon^*(\mathbf{x} + \varepsilon\mathbf{y}/2) d\mathbf{y}, \quad (10)$$

where  $\mathbf{u}_\varepsilon(t, \mathbf{x})$  is the solution of (5). The Wigner transform  $W_\varepsilon$  is a  $4 \times 4$  Hermitian matrix. Its limit as  $\varepsilon \rightarrow 0$  is called the Wigner distribution and is denoted by  $W(t, \mathbf{x}, \mathbf{k})$ . The limit Wigner matrix is not only Hermitian but also positive definite. The limit energy density and flux are expressed in terms of  $W(t, \mathbf{x}, \mathbf{k})$  by

$$\mathcal{E}(t, \mathbf{x}) = \frac{1}{2} \int \text{Tr}(A(\mathbf{x})W(t, \mathbf{x}, \mathbf{k})) d\mathbf{k}$$

and

$$\mathcal{F}_i(t, \mathbf{x}, \mathbf{k}) = \frac{1}{2} \int \text{Tr}(D^i W(t, \mathbf{x}, \mathbf{k})) d\mathbf{k}.$$

The limit Wigner distribution may be decomposed over different wave modes in a way that generalizes the plane wave decomposition in a homogeneous medium. The dispersion matrix of the system (5) is defined by

$$L(\mathbf{x}, \mathbf{k}) = A^{-1}(\mathbf{x})k_i D^i = \begin{pmatrix} 0 & 0 & 0 & k_1/\rho \\ 0 & 0 & 0 & k_2/\rho \\ 0 & 0 & 0 & k_3/\rho \\ k_1/\kappa & k_2/\kappa & k_3/\kappa & 0 \end{pmatrix}. \quad (11)$$

It has one double eigenvalue  $\omega_1 = \omega_2 = 0$  and two simple eigenvalues

$$\omega_f = v|\mathbf{k}|, \quad \omega_b = -v|\mathbf{k}|, \quad (12)$$

where  $|\mathbf{k}| = \sqrt{k_1^2 + k_2^2 + k_3^2}$  and  $v$  is the sound speed

$$v = \frac{1}{\sqrt{\kappa\rho}}. \quad (13)$$

The corresponding basis of eigenvectors is

$$\begin{aligned} \mathbf{b}_1 &= \frac{1}{\sqrt{\rho}}(\mathbf{z}^{(1)}(\mathbf{k}), 0)^t, & \mathbf{b}_2 &= \frac{1}{\sqrt{\rho}}(\mathbf{z}^{(2)}(\mathbf{k}), 0)^t, \\ \mathbf{b}_f &= \left(\frac{\hat{\mathbf{k}}}{\sqrt{2\rho}}, \frac{1}{\sqrt{2\kappa}}\right)^t, & \mathbf{b}_b &= \left(\frac{\hat{\mathbf{k}}}{\sqrt{2\rho}}, -\frac{1}{\sqrt{2\kappa}}\right)^t, \end{aligned} \quad (14)$$

where the vectors  $\hat{\mathbf{k}}$ ,  $\mathbf{z}^{(1)}(\mathbf{k})$  and  $\mathbf{z}^{(2)}(\mathbf{k})$  form an orthonormal triplet. The eigenvectors  $\mathbf{b}_1(\mathbf{k})$  and  $\mathbf{b}_2(\mathbf{k})$  correspond to transverse advection modes, orthogonal to the direction of propagation. These modes do not propagate because  $\omega_{1,2} = 0$ . The eigenvectors  $\mathbf{b}_f(\mathbf{k})$  and  $\mathbf{b}_b(\mathbf{k})$  represent forward and backward acoustic waves, which are longitudinal, and which propagate with the sound speed  $v$  given by (13).

The limit Wigner distribution matrix  $W(t, \mathbf{x}, \mathbf{k})$  has the form [17]:

$$W(t, \mathbf{x}, \mathbf{k}) = \sum_{\tau=1}^2 W_{ij}^{\tau}(t, \mathbf{x}, \mathbf{k}) \mathbf{b}^i(\mathbf{k}) \mathbf{b}^{j*}(\mathbf{k}) + a_f(t, \mathbf{x}, \mathbf{k}) \mathbf{b}_f(\mathbf{k}) \mathbf{b}_f^*(\mathbf{k}) + a_b(t, \mathbf{x}, \mathbf{k}) \mathbf{b}_b(\mathbf{k}) \mathbf{b}_b^*(\mathbf{k}). \tag{15}$$

The first term corresponds to the non-propagating modes and may be set to zero here without any loss of generality. The last two terms correspond to forward and backward propagating sound waves. The scalar functions  $a_{f,b}$  are related by  $a_f(t, \mathbf{x}, \mathbf{k}) = a_b(t, \mathbf{x}, -\mathbf{k})$ , and  $a_f$  satisfies the Liouville equation

$$\frac{\partial a}{\partial t} + \nabla_{\mathbf{k}} \omega \cdot \nabla_{\mathbf{x}} a - \nabla_{\mathbf{x}} \omega \cdot \nabla_{\mathbf{k}} a = 0. \tag{16}$$

They may be interpreted as phase space energy densities since they are non-negative (because the matrix  $W(t, \mathbf{x}, \mathbf{k})$  is non-negative) and

$$\mathcal{E}(\mathbf{x}) = \frac{1}{2} \int d\mathbf{k} [a_f(t, \mathbf{x}, \mathbf{k}) + a_b(t, \mathbf{x}, \mathbf{k})] = \int d\mathbf{k} a_f(t, \mathbf{x}, \mathbf{k}).$$

The flux is given by

$$\mathcal{F} = \frac{v}{2} \int d\mathbf{k} [\hat{\mathbf{k}} a_f(t, \mathbf{x}, \mathbf{k}) - \hat{\mathbf{k}} a_b(t, \mathbf{x}, \mathbf{k})] = v \int d\mathbf{k} \hat{\mathbf{k}} a_f(t, \mathbf{x}, \mathbf{k}). \tag{17}$$

The radiative transport equation (1) arises when the density  $\rho$  and compressibility  $\kappa$  are random and oscillating on the scale of the wave length, so we assume they have the form

$$\rho \rightarrow \rho(1 + \sqrt{\varepsilon} \rho_1(\frac{\mathbf{x}}{\varepsilon})), \quad \kappa \rightarrow \kappa(1 + \sqrt{\varepsilon} \kappa_1(\frac{\mathbf{x}}{\varepsilon})).$$

The random processes  $\rho_1$  and  $\kappa_1$  are mean zero space homogeneous with power spectral densities  $\hat{R}_{\rho\rho}$ ,  $\hat{R}_{\kappa\kappa}$ , and cross spectral density  $\hat{R}_{\rho\kappa}$ . The limit  $\varepsilon \rightarrow 0$  is the high frequency limit since the parameter  $\varepsilon$  is the ratio of wave length to propagation distance. In (3.1) we take the ratio of correlation length to propagation distance to be of order  $\varepsilon$  also, and we take the standard deviation of the fluctuations to be of order  $\sqrt{\varepsilon}$ . It is in this scaled limit that radiative transport theory emerges. The radiative transport equation for  $a(t, \mathbf{x}, \mathbf{k}) = a_f(t, \mathbf{x}, \mathbf{k})$  is

$$\frac{\partial a}{\partial t} + v \hat{\mathbf{k}} \cdot \nabla_{\mathbf{x}} a - |\mathbf{k}| \nabla_{\mathbf{x}} v \cdot \nabla_{\mathbf{k}} a = \frac{\pi v^2 |\mathbf{k}|^2}{2} \int \delta(v|\mathbf{k}| - v|\mathbf{k}'|) [a(\mathbf{k}') - a(\mathbf{k})] \cdot \left\{ (\hat{\mathbf{k}} \cdot \hat{\mathbf{k}}')^2 \hat{R}_{\rho\rho}(\mathbf{k} - \mathbf{k}') + 2(\hat{\mathbf{k}} \cdot \hat{\mathbf{k}}') \hat{R}_{\rho\kappa}(\mathbf{k} - \mathbf{k}') + \hat{R}_{\kappa\kappa}(\mathbf{k} - \mathbf{k}') \right\} d\mathbf{k}'. \tag{18}$$

This equation is of the form (1). The *mean free path* is a typical value of the ratio  $\frac{v}{\Sigma}$ , the speed over the total scattering cross-section. It can be thought of as the distance over which scattering by the inhomogeneities is effective. It is a length scale that can be estimated from seismic data while correlation lengths and standard deviations of parameter fluctuations are usually not observable.

The radiative transport equation (1) has been derived from equations governing particular wave motions by various authors, such as Stott [21], Watson et.al. [22], [23], [24], Barabanenkov et.al. [25], Besieris and Tappert [26], Howe [27], Ishimaru [3] and Besieris et. al. [28] with a recent survey presented in [29]. These derivations also determine the functions  $\omega(\mathbf{x}, \mathbf{k})$  and  $\sigma(\mathbf{x}, \mathbf{k}, \mathbf{k}')$  and show how  $a$  is related to the wave field. In [17], (1) and these functions are derived as a special case of a more general theory using the Wigner distribution and symmetric hyperbolic systems.

There is not a lot of mathematical work on the wave-to-transport limit, and most of it is for the Schrödinger equation with random potential. We cite here the work of Martin and Emch [30], of Spohn [31], of Dell'Antonio [32] and the recent extensive study of Ho, Landau and Wilkins [33] as well as [34]. They treat only spatially homogeneous problems but it is known how to extend the analysis to the spatially inhomogeneous case (slow  $x$ -dependent initial data and potential) [35]. A really satisfactory mathematical treatment of radiative transport asymptotics from random wave equations is lacking at present.

### 3.2 TRANSPORT FOR ELECTROMAGNETIC AND ELASTIC WAVES

Transport theory for electromagnetic and elastic waves is interesting because of wave polarization. This is important in astrophysics and is analyzed in great detail in Chandrasekhar's treatise [36]. Coherence of polarized light persists and must be tracked, leading to a *system* of transport equations for the Stokes parameters that fix the state of polarization. The derivation of this system from Maxwell's equations was first done in the early seventies, and using symmetric hyperbolic systems and Wigner distributions in [17], where the earlier papers are cited.

The main reason we wanted a general derivation of transport equations for general waves was so that we could deal with elastic waves. One can, of course, write down phenomenological equations for the transport of elastic wave energy and this was done often in the last 10-15 years [5]. The problem is that shear waves were treated like acoustic waves and the role of polarization was not accounted for correctly in the geophysics literature, even though the similarity with electromagnetic waves (Chandrasekhar's work) should be clear. In [17] it is shown that elastic wave transport is like E&M for shear and like acoustics for compressional waves, and the two wave modes are coupled.

A simple but interesting consequence of the general derivation is the symmetry (self-adjointness) of the transport equations. This implies immediately that the only equilibrium phase space energy densities are the uniform ones (over the support of the energy surface). The spatial energy densities for the compressional P waves and the shear S waves must be in a fixed ratio to each other, which turns out to be

$$\mathcal{E}_P = \frac{v_S^3}{2v_P^3} \mathcal{E}_S$$

Here  $v_S$  is the shear speed (about 3km/sec) and  $v_P$  is the compressional speed (about 5km/sec). This makes the P wave energy about one tenth of the S wave energy deep in the coda of seismograms, assuming surface effects are not important

so that the free space theory can be used. This is independent of what the source is and of the details of the scattering medium, as long as there is effective scattering. The asymptotic energy law is well known empirically but it did not have an explanation from first principles so we presented it in detail and related it to the seismological literature in [37]. It turns out that this kind of long time P-to-S energy equilibrium was known in connection with remote sensing with ultrasound [41].

### 3.3 BOUNDARY CONDITIONS

Finding appropriate transport theoretic boundary conditions for wave propagation in the transport regime is perhaps the most pressing issue both theoretically and for the applications, in geophysics, in electromagnetics, in ultrasound and elsewhere. The problems are analytically difficult as can be seen from [20] where the relatively simple case of inhomogeneous, slowly varying deterministic media with a flat interface is considered and transport theoretic boundary conditions are derived in the high frequency limit.

There is a lot of physical and applied literature on scattering from random rough surfaces [38, 39]. The issue is to determine what is appropriate as a boundary or interface condition for radiative transport equations. As with polarization, interfaces are a source of coherence in an otherwise incoherent scattering process. So they must be treated carefully to avoid oversimplifications. In [40] we consider acoustic reflection and transmission by a flat interface and derive transport theoretic boundary conditions, but a lot more has to be done here, including the derivation of boundary conditions for E&M and elastic wave transport.

### 3.4 THE DIFFUSIVE REGIME

It is well known, primarily from studies that originated in neutron scattering and reactor theory, that when the propagation distance in the transport regime is large compared to the mean free path a simpler diffusion theory emerges. In some seismic propagation problems the mean free path is 20-30 km but propagation is over 1000 km and more. So it is quite clear that a diffusion approximation for the transport equations is called for. We know how to do this when there are no boundaries present [17], even with polarization for E&M and elastic waves.

The problem is that the crustal wave guide is 30-40 km deep and it is not clear how to use the diffusion approximation, or even how to decide if it should be used at all. But the mathematical problem of finding asymptotic boundary and interface conditions in the diffusive regime is interesting, quite delicate analytically and potentially very useful [42]. In radar scattering from clutter, the diffusive transport theory is very likely the most appropriate one to use for wavelengths in the 10 cm to 1 m range, for example.

### 3.5 PARAMETER IDENTIFICATION AND INVERSE PROBLEMS

Parameter identification for radiative transport has received relatively little attention in geophysics [5]. In light propagation through the atmosphere the situation

is, of course, very different if only because the measurements that can be made are very different. The recent activity in diffusive tomography [43] should eventually find applications in geophysics as well, but there are many difficult problems that must be settled along the way, such as getting the right transport theoretic boundary conditions.

#### 4 THE LOCALIZATION REGIME

I will review briefly reflection of acoustic plane wave pulses normally incident on a randomly layered half space,  $z < 0$ , with  $z$  the direction of the layering [45, 46]. A good reference for deterministic wave propagation in layered media is Brekhovskikh's book [44]. It is in randomly layered media that wave localization is dominant. I will describe it in the time domain, for pulses, because this is the most interesting case in geophysical wave propagation, in reflection seismology and elsewhere. It is also not treated much in the mathematical or physical literature specialized to localization problems, and the simple intuition that most specialists have for time harmonic, one dimensional wave localization is not quite adequate for pulses. This was pointed out some time ago [50].

Radiative transport theory is not, of course, valid for randomly layered media. This was also considered long ago in connection with wave guides and optical fibers [47]. But it is not well understood in applied fields, even today, and papers appear occasionally that attempt to 'derive' radiative transport equations for propagation in layered media. I do not mean here three dimensional radiative transport in plane parallel structures. I mean random layering. If radiative transport were valid in this case, then the differential scattering cross-section would be singular, concentrated in only two (in the simplest case) directions, up and down or forwards and backwards propagation.

In the long paper [48] we deal in detail with the point source case, that is, the propagation of an acoustic pulse generated by a point source over a layered random medium. Here I will describe only the reflection of acoustic plane wave pulses.

##### 4.1 PULSE REFLECTION FROM RANDOMLY LAYERED MEDIA

The acoustic pressure  $p(t, z)$  and velocity  $u(t, z)$  satisfy the continuity and momentum equations

$$\begin{aligned} \frac{1}{K}p_t + u_z &= 0 \\ \rho u_t + p_z &= 0 \end{aligned} \tag{19}$$

Here  $\rho$  is the material density and  $K$  the bulk modulus. As in [48] we assume for simplicity that the density has no random variation

$$\rho(z) = \begin{cases} \rho_0, & z > 0, \\ \rho_1, & z < 0 \end{cases} \tag{20}$$

with  $\rho_0$  and  $\rho_1$  constants. For the bulk modulus we assume that

$$K^{-1}(z) = \begin{cases} K_0^{-1}, & z > 0, \\ K_1^{-1}(z) (1 + \nu(\frac{z}{\epsilon^2})), & z < 0 \end{cases} \quad (21)$$

with  $K_0$  a constant,  $K_1(z)$  a smooth deterministic function of  $z$  and  $\nu(s)$  a bounded stationary random function with mean zero, representing the fluctuations in  $K^{-1}$ . Note that they vary on the scale  $\epsilon^2$ , where  $\epsilon$  is a small parameter. If  $z$  is measured in kilometers and the fluctuations vary on the scale of a few meters then a value of  $\epsilon$  around 0.05 captures the scale separation we wish to model. We assume that the random function  $\nu(s)$  has a correlation length of order one so that the correlation length of  $\nu(z/\epsilon^2)$  is of order  $\epsilon^2$  in kilometers (about 2.5 meters for  $\epsilon = 0.05$ ). The mean sound speed  $c$  is given by

$$c(z) = \begin{cases} c_0 = \sqrt{\frac{K_0}{\rho_0}}, & z > 0 \\ \bar{c}(z) = \sqrt{\frac{K_1(z)}{\rho_1}}, & z < 0 \end{cases} \quad (22)$$

Note that the fluctuations in the sound speed are not assumed to be small. The estimation of the vertical correlation length of the inhomogeneities in the lithosphere from well-log data is considered in [51]. They found that 2-3 m is a reasonable estimate of the correlation length of the fluctuations in sound speed.

For  $t < 0$  a normally incident plane wave solution in  $z > 0$  has the form

$$\begin{aligned} u(t, z) &= \frac{1}{\sqrt{\epsilon}} \frac{1}{\sqrt{\rho_0 c_0}} f\left(\frac{t + z/c_0}{\epsilon}\right) \\ p(t, z) &= -\frac{1}{\sqrt{\epsilon}} \sqrt{\rho_0 c_0} f\left(\frac{t + z/c_0}{\epsilon}\right) \end{aligned} \quad (23)$$

Here  $f$  is the pulse shape function which is assumed to vanish for negative arguments and to have support that is of order one in the macroscopic  $t$  units that are seconds. With  $\epsilon = 0.05$ , the pulse width is about 50 msec or, with a speed of 3 km/sec, 150 meters. The multiplicative factor  $1/\sqrt{\epsilon}$  in (23) makes the total energy of the incident plane wave pulse independent of  $\epsilon$ . Continuity of  $p$  and  $u$  at the interface  $z = 0$  makes (19) and (23) a complete problem. We are interested in  $p(t, 0)$  or  $u(t, 0)$  for  $t > 0$ , the pressure or velocity at the interface, and this involves the solution of a complicated random scattering problem because of the form (21) of  $K^{-1}$ .

## 4.2 SCALE SEPARATION

The scaling that we have chosen, and the asymptotic limit  $\epsilon \rightarrow 0$  that we will consider, models well problems in reflection seismology and is quite different from transport theoretic scaling. The main differences are that the fluctuations are not assumed to be small and the typical wavelength of the probing pulse (150 m) is small with respect to the probing depth (5 km, say) but large compared to the correlation length (2-3 m). The parameter  $\epsilon$  is then the ratio of the (typical) wave



length to propagation depth, as well as the ratio of correlation length to wave length. This is a particularly interesting scaling limit mathematically because it is a high frequency limit with respect to the large scale variations of the medium that we want to detect, but it is a low frequency limit with respect to the fluctuations, whose effect acquires a canonical form independent of details.

Is this model realistic and can it be used effectively? One argument that can be made against it is this: There is no real scale separation in sound speed fluctuations, as one can see from well-logs [52], so this neat way of dealing with fluctuations, background and probing pulse cannot possibly be right, even if it can handle large fluctuations. Another is that perfectly layered random media are an unacceptable idealization.

Regarding scale separation, it is fair to say that the scope of the analytical theory that has been developed, and is described briefly here, is well beyond anything that could be expected from any theory that deals with strong fluctuations in a serious way. Radiative transport theory is more robust because the fluctuations are assumed to be small, and then it is not necessary to have scale separation (correlation lengths and wave lengths are comparable). Moreover, the analytical tools that emerge from the asymptotic scale separation theory are far more flexible and robust than the crude thinking with scales implies. Discontinuities and imperfections that are comparable to the pulse width can be handled by the theory and do not make it unusable. The problem is that the theory is not easy to follow, it is analytically difficult to implement and not nearly enough has been done to test it in situations that push against the scale separation assumptions. The statistical analysis of well-log data that was done in [51], that produced the estimate of 2-3 m for the correlation length of the sound speed fluctuations, is quite thorough, but perhaps more can be done here also.

The modifications to the theory that are needed to account for imperfect layering are far more important than anything missed by scale separation asymptotics. This goes back to the localization-delocalization transition that I have mentioned several times already. It remains a big gap in our understanding of wave propagation in random media.

### 4.3 LOCALIZATION REGIME ASYMPTOTICS

We will consider the reflected pressure  $p_{refl}(t, 0)$ , at  $z = 0$  and  $t > 0$ , which is the total pressure minus the incident pressure (23). After a time of order  $\epsilon$ , the duration of the incident pulse, the two are the same. Of particular interest is the two-time reflected average pressure intensity.

$$I(t, \bar{t}) = \frac{1}{\rho_0 c_0} \langle p_{refl}(t + \frac{\epsilon \bar{t}}{2}, 0) p_{refl}(t - \frac{\epsilon \bar{t}}{2}, 0) \rangle \quad (24)$$

with the angular brackets denoting statistical average. The factor  $1/\rho_0 c_0$  is a normalization.

For simplicity, we will assume in the sequel that there is no macroscopic discontinuity at  $z = 0$  so that  $\rho_0 = \rho_1$  and  $K_0^{-1} = K_1^{-1}(0)$ .

Note that the time offset in (24) is proportional to the pulse width  $\epsilon$ . The reason for this is that for time offsets of more than a few pulse widths the reflected signals are essentially uncorrelated. Moreover, in the absence of discontinuities in the medium,  $\langle p_{refl}(t, 0) \rangle$  is essentially zero except for a time of order  $\epsilon$  near  $t = 0$  when the reflection from the interface  $z = 0$  is felt.

That is, there is no coherent backscattering. We formulated a scattering problem where the quantity of interest is as directly related to the medium fluctuations as is possible.

Fix a  $t > 0$ , not close to zero, and a small  $\epsilon$ . Since  $I(t, \bar{t})$  is essentially zero for large  $\bar{t}$  we can introduce its (essentially local) Fourier transform

$$\Lambda(t, \omega) |\hat{f}(\omega)|^2 = \int e^{i\omega\bar{t}} I(t, \bar{t}) d\bar{t} \tag{25}$$

in which  $\Lambda$  is the normalized local power spectral density. The normalization is  $|\hat{f}(\omega)|^2$  with  $\hat{f}(\omega)$  the Fourier transform of the pulse shape function  $f(t)$ . The two-time intensity function can be written as

$$I(t, \bar{t}) = \frac{1}{2\pi} \int |\hat{f}(\omega)|^2 \Lambda(t, \omega) e^{-i\omega\bar{t}} d\omega \tag{26}$$

The main thrust of our theoretical work in [45, 48, 46] is that in the limit  $\epsilon \rightarrow 0$  the local power spectral density can be calculated by solving a system of partial differential equations where

$$\Lambda(t, \omega) = W^1(0, t, \omega) \tag{27}$$

and the  $W^N(z, t, \omega)$ ,  $N \geq 0$  satisfy the equations

$$\frac{\partial W^N}{\partial z} + \frac{2N}{\bar{c}(z)} \frac{\partial W^N}{\partial t} - \frac{2\alpha\omega^2 N^2}{\bar{c}^2(z)} \{W^{N+1} - 2W^N + W^{N-1}\} = 0 \tag{28}$$

for  $-L < z \leq 0$ , with

$$W^N(-L, t, \omega) = \delta(t)\delta_{N,0} \tag{29}$$

Here the mean sound speed  $\bar{c}(z)$  is given by (22) and  $\alpha > 0$  is the noise intensity level of the fluctuations

$$\alpha = \frac{1}{4} \int_0^\infty \langle \nu(s)\nu(0) \rangle ds \tag{30}$$

The length  $L$  is arbitrary, provided that for any given  $t > 0$  for which we want to calculate  $\Lambda(t, \omega)$  it satisfies

$$L > c_{max} \frac{t}{2} \tag{31}$$

with  $c_{max}$  the maximum speed  $\bar{c}(z)$  in  $z \leq 0$ . Because of the hyperbolic nature of the equations (28) it is easy to see (and explained in the references) that the choice of  $L$  satisfying (31) does not affect  $\Lambda(t, \omega)$  given by (27).

## 4.4 TIME DOMAIN LOCALIZATION

There is no quick and simple way to explain the result (27)-(31) that relates the local power spectral density  $\Lambda(t, \omega; \bar{c}(\cdot))$ , the mean sound speed profile  $\bar{c}(z)$  and the noise intensity level  $\alpha$ . But we will now make several remarks that will help explain the nature of this relationship.

From the definition (24) and (25) it is clear that  $\Lambda(t, \omega)$  is a local Fourier transform but it is not necessarily positive as it would have to be if  $p_{refl}(t, 0)$ , the reflected pressure, were a stationary process in  $t$  so that  $I(t, \bar{t})$  were independent of  $t$ . However, in the limit  $\epsilon \rightarrow 0$ , and hence when  $\epsilon$  is small,  $\Lambda(t, \omega)$  given by (27)-(31) is indeed positive. For a general profile  $\bar{c}(z)$  it cannot be computed explicitly but for  $\bar{c}(z) = \bar{c}$ , a constant, it has the form

$$\Lambda(t, \omega) = \frac{\frac{\alpha\omega^2}{\bar{c}}}{\left(1 + \frac{\alpha\omega^2}{\bar{c}}t\right)^2} \quad (32)$$

In terms of the localization length [49] at frequency  $\omega$

$$l(\omega) = \frac{\bar{c}^2}{2\alpha\omega^2} \quad (33)$$

we can write (32) in the form

$$\Lambda(t, \omega) = \frac{1}{2} \frac{\bar{c}l(\omega)}{\left(l(\omega) + \frac{\bar{c}t}{2}\right)^2} \quad (34)$$

As shown in [49] and the many references cited there, the localization length at frequency  $\omega$  is a measure of the depth of penetration of a time harmonic wave with this frequency into a randomly layered medium with uniform sound speed  $\bar{c}$  and noise level  $\alpha$  for the fluctuations. Wave energy does not penetrate much below this length. If  $T(L, \omega)$  is the time harmonic transmission coefficient for a randomly layered medium of width  $L$ , with  $\omega$  the frequency of the incident plane wave, then

$$\lim_{L \rightarrow \infty} \frac{1}{L} \log |T(L, \omega)| = \frac{-1}{l(\omega)}$$

with probability one. This defines the localization length  $l(\omega) > 0$ , which is always positive for a large class of random media. It cannot be computed explicitly but in the low frequency limit it has the form (33). The lower the frequency the deeper the penetration of the waves into the randomly layered medium.

In the time domain, the normalized local power spectral density of the reflected signal at a fixed time  $t$ ,  $\Lambda(t, \omega)$  in (34), has a maximum  $\omega_{max} = \omega_{max}(t)$  that depends on time. From (34) the maximum is calculated to be

$$\omega_{max} = \sqrt{\frac{\bar{c}}{\alpha t}} \quad (35)$$

In a more physical way [49] we can say that the maximum of the local power spectral density at time  $t$  occurs for that  $\omega = \omega_{max}$  for which

$$l(\omega_{max}) = \frac{\bar{c}t}{2} \quad (36)$$

Thus, for the frequency for which the localization length equals the mean distance traveled into the medium, we have the maximum contribution to the noise spectrum of the reflected signal. This is a stochastic resonance relation that identifies precisely the main source of noise in the reflected signals.

It is because of wave localization and its manifestations in the time domain described above that signals reflected by randomly layered media are so noisy. From (32) we find, by integrating over  $\omega$ , that the envelope of the root mean square of the reflected pulse is of the form constant  $\times t^{-3/4}$ . Thus, the fluctuations in the reflected signal decay very slowly, indicating that a great deal of multiple scattering is taking place and that wave localization is dominant.

We can interpret (28) as a hierarchy of equations for moments associated with the scattering problem [48]. The infinite hierarchy ( $N \geq 0$  in (28)) indicates that the second moment that we are interested in ( $I$  of (24) or  $\Lambda$  of (25)) cannot be computed separately from all higher moments (the  $W^N$ ,  $N > 2$  in (28)). This is another manifestation of localization.

When we use the parameters of section 4.2 that are typical in reflection seismology we find that the minimum localization length occurs in the 20-30 Hz regime and is about 15-20 km [51]. This means that random inhomogeneities will effectively prevent probing below this depth because all the wave energy is reflected to the surface by multiple scattering.

What is missing at present is a more general theory that allows us to compute the changes in the one dimensional theory that occur when small three dimensional inhomogeneities are introduced into the model. We need a more general theory that lets us go from localization to transport as the random layering is reduced and isotropic inhomogeneities replace it.

#### 4.5 STATISTICAL INVERSE PROBLEMS

I will describe briefly how the mean sound speed profile  $\bar{c}(z)$  can be estimated from observations of  $p_{refl}(t, 0)$  or

$$R_f(t) = \frac{1}{\sqrt{\rho_0 c_0}} p_{refl}(t, 0) \tag{37}$$

in which dependence of the pulse shape function  $f$  is indicated. The inversion strategy is based on one more fact about the reflected signal  $R_f(t)$ , in addition to (27)-(31). It is that as  $\epsilon$  tends to zero  $R_f(t)$  becomes approximately a Gaussian process. It has not been possible to prove this so far but there are some good heuristic indications that it is true [45] and extensive numerical simulations corroborate it very well [48]. From the Gaussian property of  $R_f(t)$  we conclude that

$$\frac{1}{|\hat{f}(\omega)|^2} \int e^{i\omega\bar{t}} R_f\left(t + \frac{\epsilon\bar{t}}{2}\right) R_f\left(t - \frac{\epsilon\bar{t}}{2}\right) d\bar{t} = \hat{\Lambda}(t, \omega) \tag{38}$$

is approximately, when  $\epsilon$  is small, an exponential random variable with mean  $\Lambda(t, \omega)$  given by (27)-(31), when  $\bar{c}(z)$  is known. Moreover, for distinct  $0 < t_1 < t_2 < \dots < t_{N_t}$  and  $0 < \omega_1 < \omega_2 < \dots < \omega_{N_f}$ , where  $N_t$  and  $N_f$  are integers,

the random variables  $\{\hat{\Lambda}(t_j, \omega_l)\}$  are independent with exponential distribution having mean  $\{\Lambda(t_j, \omega_l)\}$ .

The inversion strategy is now this: Depending on the available data, fix a set of time points  $\{t_j\}$  and frequencies points  $\{\omega_l\}$  as above. For each realization of  $R_f(t)$  that is available, estimate  $\hat{\Lambda}(t_j, \omega_l)$  from (38). This is actually a very delicate step that must be done carefully as we discuss in [48], Appendix E. Then form

$$O(\bar{c}) = \prod_{\text{realiz}} \prod_{j=1}^{N_t} \prod_{l=1}^{N_f} \frac{e^{-\hat{\Lambda}(t_j, \omega_l)/\Lambda(t_j, \omega_l; \bar{c}(\cdot))}}{\Lambda(t_j, \omega_l; \bar{c}(\cdot))} \quad (39)$$

where the first product is over different independent realizations. This is the likelihood functional for the estimates  $\hat{\Lambda}$ , given a known mean speed profile  $\bar{c}(z)$ . We now choose  $\bar{c}(z)$  in order to maximize this functional. This is a rather usual maximum likelihood estimation *except* that now the maximization must be done over the profiles  $\bar{c}(\cdot)$  which in turn determine  $\Lambda(t, \omega; \bar{c}(\cdot))$  in (39) via the partial differential equations (28)-(29) and the relation (27).

The most convenient way to solve the maximization problem for (39), and thus estimate  $\bar{c}(z)$ , is to assume that it is piece-wise linear over a few macroscopically large layers and then maximize  $O$  over a finite set of speeds  $\bar{c}^1, \bar{c}^2, \dots, \bar{c}^{N_z}$ . These speeds are approximations of  $\bar{c}(z)$  at successively larger depths numbered from 1 to  $N_z$ . Moreover, because of the hyperbolic nature of (28)-(29) the maximization can be done one layer at a time with increasing depth. This avoids the difficult problem of finding the maximum of a complicated function of several variables. Physically this layer peeling process makes sense because there is a direct relation between the sound speed profile up to a certain depth and the smallest time before which the rest of the medium is not felt in the reflected signal  $R_f(t)$ .

Of course we need a lot of independent realizations to get reasonable results and this is unrealistic in a geophysical context. But it is important in principle to make this strategy work and amazingly enough it does [50], [48]). It is amazing because we are trying to determine the smooth, mean speed profile from the reflected signals that are swamped by fluctuations due to multiple scattering. The computational and other implementation details are described in [48]).

Could we do this kind of inversion from extremely noisy reflections if we only had one realization? Yes, if we have reflection measurements at different offsets (distances from the source) on the interface, generated by a point source over a randomly layered medium [53]. This is a very difficult problem that requires a great deal of numerical computation. The inversion is not as good as in the plane wave case (with many realizations) but it is reasonably good and, in any case, it shows that the strategy does work. But improving the results requires very careful attention to a host of implementation issues that can be settled only empirically, by trial and adjustment, at present.

An interesting discussion of reflections from time reversed reflections, their statistical properties and their relation in turn to the hierarchy of moments equations (28) is given by Clouet and Fouque [54]. This work should have important applications in statistical inverse problems of geophysical interest.

Another application of time domain localization asymptotics is to surface water waves over a rough bottom [55].

#### 4.6 REFLECTION AND TRANSMISSION OF TIME HARMONIC PLANE ELASTIC WAVES

We have described a variety of results for *acoustic* pulse reflection from randomly layered media, emphasizing time domain effects. For geophysical applications we must also consider *elastic* waves in randomly layered media. The analytical difficulties in extending the theory that we briefly described above to the elastic case are enormous, mainly because there are two wave modes, P and S waves, that are coupled by the inhomogeneities. In [56] we extended the scale-separation asymptotic theory to time harmonic, obliquely incident elastic plane waves. We calculate in detail mode coupling in reflection and transmission, with various kinds of interfacial discontinuities. It is surprising that so many things can be calculated analytically and in such detail, given the complexity of the problem.

However, despite considerable efforts we have not been able to extend the results to the time domain. The hierarchy of moment equations that we used in the analysis of acoustic pulse reflection does not seem to work for elastic wave pulse reflection. The analysis of reflections for elastic wave pulses generated by a point source, the analog of the analysis carried out in [48] for acoustic waves, seems to be out of reach at present.

#### 4.7 PULSE STABILIZATION AND IMAGING

We have focused mostly on reflection in the time domain because the bulk of the measurements that can be made in geophysics, in nondestructive testing with ultrasound and elsewhere are surface measurements. However, transmission is also important as is the analysis of reflections from imbedded discontinuities in a randomly layered medium. The vicinity of the front of the pulse, or the vicinity of first arrival from the discontinuity, has an interesting structure that can be analyzed in considerable detail. This is called the O'Doherty-Anstey theory because it was first discussed by these two geophysicists in the early seventies [57]. The main point is that if the fluctuations are weak and the pulse is followed with its random speed, then it will appear to stabilize (not fluctuate) and become broader as it advances into the medium. This is discussed in detail in [48] where many other papers are cited.

What if the fluctuations are not weak, and we have scale separation as described above? Do we have an O'Doherty-Anstey theory? This question was answered in [58, 59] by overcoming what was the main obstacle before: finding the right random speed with which to center the advancing pulse. The fact that the advancing pulse spreads and loses energy (to fluctuations in its coda) is not so surprising and is true for general random media, not only layered media, although the fluctuations must be weak. What is surprising, and not generally known or anticipated in the geophysics literature, is that in the case of large fluctuations the centering speed is not the local random speed but a function of it, and the

centered pulse stabilizes with probability one with minimal spreading (relative to other centerings).

In [60], Solna shows how this theory can be used to improve the resolution of discontinuity identification in a random medium. He also extends the O'Doherty-Anstey theory to a class of locally layered random media, that is, he allows for slow horizontal variations.

#### REFERENCES

- [1] P.W. Anderson, *Absence of diffusion in certain random lattices*, Phys. Rev., 109 (1958), pp. 1492-1505.
- [2] J.B. Keller, *Stochastic Equations and Wave Propagation in Random Media*, Proc. Symp. Appl. Math., 16, 145-170, Am. Math. Soc., McGraw-Hill, New York, 1964.
- [3] A.Ishimaru, *Wave propagation and scattering in random media*, vol. I,II, Academic Press, New York, 1978.
- [4] K.Aki and R.S.Wu, Multiple scattering and energy transfer of seismic waves – separation of scattering effect from intrinsic attenuation –II. Application of the theory to Hindu Kush region, in *Seismic wave scattering and attenuation*, vol. I (R.S.Wu and K.Aki, eds), pp. 49-80, 1988.
- [5] M.C. Fehler and H. Sato, *Seismic Wave Propagation and Scattering in the Heterogeneous Earth*, AIP Press, 1998.
- [6] P. Sheng, *Introduction to wave scattering, localization, and mesoscopic phenomena*, Academic Press, 1995.
- [7] A. Figotin and L.A. Pastur, *Spectra of Random and Almost-Periodic Operators*, Springer-Verlag, 1992.
- [8] R. Knapp, G. Papanicolaou and B.S. White, *Transmission of waves by a nonlinear random medium*, J. Stat. Physics, 63, pp. 567-584, 1991.
- [9] J.C. Bronski, *Nonlinear Wave Propagation in a Disordered Medium* J. Stat. Phys., 92, 5/6, 1998.
- [10] J.C. Bronski *Nonlinear Scattering and the Analyticity Properties of Solitons*, Journal of Nonlinear Science, 8, pp. 161-182, 1998.
- [11] J.C. Bronski, D.W. McLaughlin and M.J. Shelley, *Stability of Time-Harmonic Localized Solutions in a One Dimensional Disordered Nonlinear Medium*, J. Stat. Phys., 88, 1997.
- [12] J. Garnier, *Transmission of solitons through random media*, to appear in SIAM, J. Appl. Math.
- [13] J. Garnier, PhD Thesis, Ecole Polytechnique, 1996.

- [14] J.F. Claerbout, *Imaging the Earth's Interior*, Blackwell, Boston, 1985.
- [15] N. Bleistein, J.K. Cohen and J.W. Stockwell Jr., *Mathematics of Multidimensional Seismic Inversion*, pp. 1-260, Colorado School of Mines, 1998.
- [16] W.W. Symes, *Mathematics of Reflection Seismology*, pp. 1-85, Rice University, 1995.
- [17] L.Ryzhik, G.Papanicolaou and J.Keller, Transport Equations for Elastic and Other Waves in Random Media, *Wave Motion* 24, pp. 327-370, 1996.
- [18] M.C.W. van Rossum and Th.M.Nieuwenhuizen, Multiple scattering of classical waves: from microscopy to mesoscopy and diffusion, to appear in *Phys. Rev. E*.
- [19] P.Gérard, P.Markowich, N.Mauser and F.Poupaud, Homogenization limits and Wigner transforms, *Comm. Pure Appl. Math.*, 50, pp. 323-380, 1996.
- [20] L.Ryzhik, G.Papanicolaou and J.Keller, Transport equations in a half space, *Comm. PDE's*, 22, pp. 1869-1911, 1997.
- [21] P.Stott, A transport equation for the multiple scattering of electromagnetic waves by a turbulent plasma, *Jour. Phys. A*, 1, pp. 675-689, 1968.
- [22] K.Watson and J.L.Peacher, Doppler shift in frequency in the transport of electromagnetic waves in an underdense plasma, *Jour. Math. Phys.*, 11, pp. 1496-1504, 1970.
- [23] K.Watson, Multiple scattering of electromagnetic waves in an underdense plasma, *Jour. Math. Phys.*, 10, pp. 688-702, 1969.
- [24] C.W.Law and K.Watson, Radiation transport along curved ray paths, *Jour. Math. Phys.*, 11, pp. 3125-3137, 1970.
- [25] Yu.Barabanenkov, A.Vinogradov, Yu.Kravtsov and V.Tatarskii, Application of the theory of multiple scattering of waves to the derivation of the radiative transfer equation for a statistically inhomogeneous medium, *Radiofizika*, 15, pp. 1852-1860, 1972. English translation pp. 1420-1425.
- [26] I.M.Besieris and F.D.Tappert, Propagation of frequency modulated pulses in a randomly stratified plasma, *Jour. Math. Phys.*, 14, pp. 704-707, 1973.
- [27] M.S.Howe, On the kinetic theory of wave propagation in random media, *Phil. Trans. Roy. Soc. Lond.*, 274, pp. 523-549, 1973.
- [28] I.M. Besieris, W. Kohler and H. Freese, A transport-theoretic analysis of pulse propagation through ocean sediments, *J. Acoust. Soc. Am.*, 72, pp. 937-946, 1982.
- [29] Yu.Barabanenkov, Yu.Kravtsov, V.Ozrin and A.Saichev, Enhanced backscattering in optics, *Progress in Optics*, 29, pp. 67-190, 1991.



- [30] P. Martin and G. Emch, A rigorous model sustaining van Hove's phenomenon, *Helv. Phys. Acta*, 48, p. 59, 1967.
- [31] H. Spohn, Derivation of the transport equation for electrons moving through random impurities, *Jour. Stat. Phys.*, 17, pp. 385-412, 1977.
- [32] G.Dell'Antonio, Large time small coupling behavior of a quantum particle in a random potential, *Annals of Inst. H. Poincare*, section A, 39, p. 339, 1983.
- [33] T. Ho, L. Landau and A. Wilkins, On the weak coupling limit for a Fermi gas in a random potential, *Rev. Math. Phys.*, 5, pp. 209-298, 1993.
- [34] L. Erdos and H.T. Yau, preprint, 1997.
- [35] A.Fannjiang, unpublished notes, 1991.
- [36] S.Chandrasekhar, *Radiative transfer*, Dover, New York, 1960.
- [37] G.Papanicolaou, L.Ryzhik and J.Keller, *On the stability of the P to S energy ratio in the diffusive regime*, *Bulletin of the Seismological Society of America*, 86, pp. 1107-1115, 1996.
- [38] J.A. DeSanto and G.S. Brown, *Analytical techniques for multiple scattering from rough surfaces*, in *Progress in Optics XXIII* (E. Wolf, ed.), pp. 1-62, Elsevier, Amsterdam, 1986.
- [39] A.Voronovich, *Wave Scattering from Rough Surfaces*, Springer Verlag, 1991.
- [40] G. Bal, J.B. Keller, G. Papanicolaou and L. Ryzhik, *Transport Theory for Acoustic Waves with Reflection and Transmission at Interfaces*, preprint, 1998.
- [41] R.L.Weaver, *On diffuse waves in solid media*, *Jour.Acoust.Soc.Am.*, 71, pp. 1608-1609, 1982.
- [42] G. Bal, PhD Thesis, University of Paris VI, 1997.
- [43] O. Dorn, *Diffuse tomography*, PhD Thesis, University of Münster, 1997.
- [44] L.Brekhovskikh, *Waves in Layered Media*, Academic Press, 1980.
- [45] R. Burridge, G. Papanicolaou, P. Sheng, and B. White, *Probing a random medium with a pulse*, *SIAM J. Appl. Math.*, 49, pp. 582-607, 1989.
- [46] G. Papanicolaou and S. Weinryb, *A functional limit theorem for waves reflected by a random medium*, *Applied Mathematics and Optimization*, 30, pp. 307-334, 1994.
- [47] W. Kohler and G. Papanicolaou, *Power statistics for wave propagation in one dimension and comparison with radiative transport theory I,II*, *J. Math. Phys.*, 14, pp. 1733-1745, 1973, and 15, pp. 2186-2197, 1974.

- [48] M. Asch, W. Kohler, G. Papanicolaou, M. Postel and B. White, *Frequency Content of Randomly Scattered Signals*, SIAM Review, 33, pp. 526-629, 1991.
- [49] P. Sheng, B. White, Z.Q. Zhang and G.Papanicolaou, *Wave localization and multiple scattering in randomly-layered media*, in ‘Scattering and Localization of Classical Waves in Random Media,’ Ping Sheng, editor, World Scientific, pp. 563-619, 1990.
- [50] B. White, P. Sheng, M. Postel, and G. Papanicolaou, *Probing through cloudiness: Theory of statistical inversion for multiply scattered data*, Phys. Rev. Lett., 63, pp. 2228-2231, 1989.
- [51] B. White, P. Sheng, and B. Nair, *Localization and backscattering spectrum of seismic waves in stratified lithology*, Geophysics, 55, pp. 1158-1165, 1990.
- [52] F. Herrmann, *A scaling medium representation, a discussion of well-logs, fractals and waves*, PhD Thesis, Delft University, 1997.
- [53] M. Asch, W. Kohler, G. Papanicolaou, M. Postel and B. White, *Statistical inversion from reflections of spherical waves by a randomly layered medium*, Waves in Random Media, 6, pp. 293-334, 1996.
- [54] J.F. Clouet and J.P. Fouque, *A time-reversal method for an acoustical pulse propagating in randomly layered media*, Wave Motion, 25, pp. 361-368, 1997.
- [55] A. Nachbin and G. Papanicolaou, *Water waves in shallow channels of rapidly varying depth*, JFM, 241, pp. 311-332, 1992.
- [56] W. Kohler, G. Papanicolaou and B. White, *Localization and mode conversion for elastic waves in randomly layered media I,II*, Wave Motion, 23, pp. 1-22 and 181-201, 1996.
- [57] R.F. O’Doherty and N.A. Anstey, *Reflections on amplitudes*, Geophysical Prospecting, 19, pp. 430-458, 1971.
- [58] J.F. Clouet and J.P. Fouque, *Spreading of a pulse traveling in random media*, Annals of Applied Probability, 4, pp. 1083-1097, 1994.
- [59] R. Burridge, P. Lewicki and G. Papanicolaou, *Pulse stabilization in a strongly heterogeneous layered medium*, Wave Motion, 20, pp. 177-195, 1994.
- [60] K. Solna, PhD Thesis, Stanford University, 1997.

George Papanicolaou  
 Department of Mathematics  
 Stanford University  
 Stanford CA 94305  
 papanico@math.stanford.edu  
 URL: <http://georgep.stanford.edu>



## OPERATOR SPACES AND SIMILARITY PROBLEMS

GILLES PISIER

ABSTRACT. We present an overview of the theory of “Operator Spaces” (sometimes called “non-commutative Banach spaces”), recently developed by Effros, Ruan, Blecher, Paulsen and others. We describe several applications of this new ideology to operator algebras and to various similarity problems.

1991 Mathematics Subject Classification: 46L05, 47D15, 46M05, 46B70

Keywords and Phrases: Operator space, operator algebra, completely bounded, similar to a contraction, uniform algebra, amenable group

## 1 THE THEORY OF OPERATOR SPACES

The notion of “operator space” is intermediate between “Banach space” and “ $C^*$ -algebra”. An operator space (o.s. in short) is simply a Banach space  $E$  (or a normed space before completion) given with an isometric embedding  $j: E \rightarrow B(H)$  into the space  $B(H)$  of bounded operators on some Hilbert space  $H$ . By a slight abuse, we will often identify  $E$  with  $j(E)$ . We can then say that an o.s. is simply a (closed) subspace of  $B(H)$ , or equivalently a (closed) subspace of a  $C^*$ -algebra (since, by Gelfand’s theorem,  $C^*$ -algebras are themselves embedded into some  $B(H)$ ).

Although this notion had appeared earlier, the theory itself really took off only after Z.J. Ruan’s thesis [Ru1] circulated. His “abstract” characterization of operator spaces (see below) plays a crucial rôle to construct new operator spaces from known ones. In particular, immediately after this, Blecher-Paulsen [BP1] and Effros-Ruan [ER3] independently discovered that the latter characterization allows to introduce a duality in the category of operator spaces (see §1.4 below) and they developed the theory much further (cf. [ER2]–[ER6], [B1, B3, P2]).

The definition of operator spaces is a bit disappointing: every Banach space  $E$  embeds isometrically into  $B(H)$  for a suitable  $H$ , hence every such space can be viewed (in at least one way, and actually in many) as an operator space. But the novelty is in the morphisms (or the isomorphisms) which are no longer those of the category of Banach spaces: instead of bounded linear maps, we use completely bounded (in short c.b.) ones, defined in §1.1 below. Those emerged as a powerful tool in the early 80’s in works of Haagerup, Wittstock, Paulsen (see [P1]). Their definition was somewhat implicit in the earlier works of Stinespring (1955) and Arveson (1969) on completely positive maps.

Actually, the theory has been also considerably influenced by several contributions made before Ruan's thesis, as will be seen below. We should also mention that operator spaces were preceded by "operator systems" (these are self-adjoint operator spaces containing the unit): inspired by Kadison's ideas on "function systems" and by Arveson's extension theorem (1969), Choi and Effros developed in the 70's an extensive program to study operator systems with unital completely positive maps as morphisms. In particular, the ideas of duality and quotient spaces already appeared in this context (see [CE]). There, the additional order structure dims the parallelism with Banach spaces, but the overall influence of this program can still be seen throughout the theory.

One of the great advantages of operator spaces over  $C^*$ -algebras is that they allow the use of finite dimensional tools and isomorphic invariants (as in the so-called "local theory" of Banach spaces) in operator algebra theory (see §1.9 below): we can work with a distance  $d_{cb}(E, F)$  which measures the degree of isomorphism of two isomorphic operator spaces  $E, F$  (see §1.1 below). In sharp contrast,  $C^*$ -algebras are much more rigid: there, all morphisms are *automatically* contractive, all isomorphisms are *isometric* and  $C^*$ -algebras have *unique*  $C^*$ -norms. As illustrated below, operator space theory has opened the door to a massive transfer of technology coming from Banach space theory. This process (the "quantization" of Banach space theory, according to the terminology in [E]) is bound to find applications for Banach spaces too. Up to now however, this has mostly benefited operator algebra theory by leading to the solutions of some old problems (for instance, the Halmos similarity problem for polynomially bounded operators, see Example 2.1) while opening broad new directions of research, making many points of contact with other fields.

The main motivation for operator space theory is roughly this: very often, a  $C^*$ -algebra  $A$  comes equipped with a distinguished system of generators, sometimes finite. Call  $E$  the *linear* span of these generators. Then, while the normed space structure of  $E$  reveals little about  $A$ , it turns out that the operator space structure of  $E$  carries a lot of information about  $A$ , and the specific morphisms of o.s. theory allow to keep track of the correspondence  $E \leftrightarrow A$ . However, many constructions which are natural within operator spaces (such as duality or interpolation) do not make sense for  $C^*$ -algebras, yet the systematic investigation of properties of  $E$  leads to a "new" frame of mind, say a new intuition which ultimately can be applied to  $A$ . A good illustration of the fruitfulness of this approach is furnished by the main result in [JP]: by producing an uncountable collection of finite dimensional operator spaces  $(E_i)$  which are mutually separated, *i.e.* such that  $\inf\{d_{cb}(E_i, E_j) \mid i \neq j\} > 1$ , one obtains as a corollary that the tensor product  $B(\ell_2) \otimes B(\ell_2)$  admits more than one  $C^*$ -norm, thus answering a long standing open question (see §1.10). This is a good case study: an investigation that the "new ideology" would surely pursue *for its own sake* (whether the set of finite dimensional operator spaces is separable), for which the best estimates turn out to depend on deep results of number theory ("Ramanujan graphs") and which happens to lead to the solution of a well known  $C^*$ -algebraic problem, a priori not involving operator spaces. Of course, it is the firm belief that more situations like this one will come up which keeps the field blooming.

Much of the research from the intensive development of the last ten years is surveyed below. However, we found the directions currently being explored too diverse to be all duly recorded here, for lack of space. For instance, the reader should consult other sources for an account of Effros and Ruan's work on quantum groups (see [ER8]) and Ruan's work on amenability and Kac algebras ([Ru3, Ru4]).

NOTATION. We denote by  $\ell_2^n$  the  $n$ -dimensional complex Hilbert space. The space  $B(\ell_2^n)$  can be identified with the space  $M_n$  of all  $n \times n$  matrices with complex entries. Let  $H_1, H_2$  be two Hilbert spaces. We denote by  $H_1 \otimes_2 H_2$  their Hilbertian tensor product. We denote by  $B(H_1, H_2)$  the space of all bounded operators  $T: H_1 \rightarrow H_2$ , equipped with its usual norm. When  $H_1 = H_2 = H$  we denote it simply by  $B(H)$ . The same notation is used below when  $H_1, H_2$  or  $H$  are Banach spaces. When  $T$  has  $\|T\| \leq 1$ , we call it "contractive" and refer to it as "a contraction". Given two vector spaces  $V_1, V_2$ , we denote by  $V_1 \otimes V_2$  their algebraic tensor product. All the vector spaces considered here are over the *complex* scalars. We will denote by  $\bar{H}$  the complex conjugate of a (complex) Hilbert space  $H$  and by  $h \rightarrow \bar{h}$  the canonical antilinear isometry from  $H$  to  $\bar{H}$ . We will use the abbreviation o.s. either for "operator space" or for "operator spaces" depending on the context.

### 1.1 THE "NORM" OF AN OPERATOR SPACE. COMPLETE BOUNDEDNESS

Let  $E \subset B(H)$  be an operator space. Then  $M_n \otimes E$  can be identified with the space of all  $n \times n$  matrices with entries in  $E$ , which we will denote by  $M_n(E)$ . Clearly  $M_n(E)$  can be viewed as an operator space naturally embedded into  $B(H^n)$ , where  $H^n = H \oplus \cdots \oplus H$  ( $n$  times). Let us denote by  $\| \cdot \|_n$  the norm of  $M_n(E)$  (*i.e.* the norm induced by  $B(H^n)$ ). Of course, when  $n = 1$ , we recover the ordinary norm of  $E$ . We have a natural embedding  $M_n(E) \rightarrow M_{n+1}(E)$  taking  $x$  to  $\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$ , with which we can view  $M_n(E)$  as included in  $M_{n+1}(E)$ , and  $\| \cdot \|_n$  as induced by  $\| \cdot \|_{n+1}$ . Thus, we may consider the union  $\bigcup_n M_n(E)$  as a normed space equipped with its natural norm denoted by  $\| \cdot \|_\infty$  and we denote by  $\mathcal{K}[E]$  its completion. We also denote  $\mathcal{K}_0 = \bigcup M_n$ . Our notation here is motivated by the fact that if  $E = \mathbb{C}$ , the completion of  $\mathcal{K}_0 = \bigcup M_n$  coincides isometrically with the  $C^*$ -algebra  $\mathcal{K}$  of all compact operators on the Hilbert space  $\ell_2$ . It is easy to check that the union  $\bigcup_n M_n(E)$  can be identified isometrically with  $\mathcal{K}_0 \otimes E$ , and if we denote by  $\{e_{ij}\}$  the classical system of matrix units in  $\mathcal{K}$ , then any matrix  $x = (x_{ij})$  in  $M_n(E)$  can be identified with  $\sum_{i,j=1}^n e_{ij} \otimes x_{ij} \in \mathcal{K} \otimes E \subset \mathcal{K}[E]$ . The basic idea of o.s. theory is that the Banach space norm on  $E$  should be replaced by the sequence of norms  $(\| \cdot \|_n)$  on the spaces  $(M_n(E))$ , or better by the single norm  $\| \cdot \|_\infty$  on the space  $\mathcal{K}[E]$  (we sometimes refer to the latter as the o.s.-norm of  $E$ ), so that the unit ball of  $E$  should be replaced by that of  $\mathcal{K}[E]$ , as illustrated in the following.

DEFINITION. Let  $E_1 \subset B(H_1)$  and  $E_2 \subset B(H_2)$  be operator spaces, let  $u: E_1 \rightarrow E_2$  be a linear map, and let  $u_n: M_n(E_1) \rightarrow M_n(E_2)$  be the mapping taking  $(x_{ij})$  to  $(u(x_{ij}))$ . Then  $u$  is called completely bounded (c.b. in short) if  $\sup_n \|u_n\| < \infty$  and we define  $\|u\|_{cb} = \sup_n \|u_n\|$ . Equivalently,  $u$  is c.b. iff the mappings  $u_n$  extend to a single bounded map  $u_\infty: \mathcal{K}[E_1] \rightarrow \mathcal{K}[E_2]$  and we have  $\|u\|_{cb} = \|u_\infty\|$ . We denote by  $cb(E_1, E_2)$  the space of all c.b. maps  $u: E_1 \rightarrow E_2$ , equipped with

the cb-norm. Thus, the o.s. analog of the identity  $\|u\| = \sup\{\|u(x)\| \mid \|x\| \leq 1\}$  can be written as

$$\|u\|_{cb} = \sup\{\|u_\infty(x)\| \mid x \in \mathcal{K}[E], \|x\| \leq 1\}.$$

Now that we have the “right” morphisms, of course we also have the isomorphisms: we say that two operator spaces  $E_1, E_2$  are completely isomorphic (resp. completely isometric) if there is an isomorphism  $u: E_1 \rightarrow E_2$  which is c.b. as well as its inverse (resp. and moreover such that  $\|u\|_{cb} = \|u^{-1}\|_{cb} = 1$ ). We say that an isometry  $u: E_1 \rightarrow E_2$  is a complete isometry if  $\|u\|_{cb} = \|u|_{u^{-1}(E)}\|_{cb} = 1$ . We say that  $u$  is a complete contraction (or is completely contractive) if  $\|u\|_{cb} \leq 1$ . Note that the preceding properties correspond respectively to the cases when  $u_\infty$  is an isomorphism, an isometry or a contraction.

Let  $E_1, E_2$  be two completely isomorphic operator spaces, we define

$$d_{cb}(E_1, E_2) = \inf\{\|u\|_{cb} \|u^{-1}\|_{cb}\}$$

where the infimum runs over all possible complete isomorphisms  $u: E_1 \rightarrow E_2$ . This is of course analogous to the “Banach-Mazur distance” between two Banach spaces  $E_1, E_2$  defined classically by  $d(E_1, E_2) = \inf\{\|u\| \|u^{-1}\|\}$ , the infimum being this time over all isomorphisms  $u: E_1 \rightarrow E_2$ . By convention, we set  $d(E_1, E_2) = \infty$  (or  $d_{cb}(E_1, E_2) = \infty$ ) when no (complete) isomorphism exists.

We take this opportunity to correct a slight abuse in the definition of an operator space: consider two (isometric) embeddings  $j_1: E \rightarrow B(H_1)$  and  $j_2: E \rightarrow B(H_2)$  of the same Banach space into some  $B(H)$ . We will say (actually we rarely use this) that these are “equivalent” (or define “equivalent o.s. structures”) if  $j_2(j_1)^{-1}: j_1(E) \rightarrow j_2(E)$  is a complete isometry. Then, by an o.s. structure on a Banach space  $B$  what we really mean is an equivalence class with respect to this relation. As often, we will frequently abusively identify an equivalence class with one of its representative, *i.e.* with a “concrete” operator subspace  $E \subset B(H)$ .

Consider for instance a  $C^*$ -algebra  $A$ . Then any two isometric  $*$ -representations  $j_1: A \rightarrow B(H_1)$  and  $j_2: A \rightarrow B(H_2)$  are necessarily “equivalent” in the above sense. (Recall that  $C^*$ -algebras such as  $A$  and  $M_n(A)$  have *unique*  $C^*$ -norms). We will call the resulting operator space structure on  $A$  the “natural” one, (this applies a fortiori to von Neumann algebras). Note that, throughout this text, whenever a  $C^*$ -algebra is viewed as an o.s., it *always* means in the “natural” way (unless explicitly stated otherwise).

We end this section by a brief review of the factorization properties of c.b. (or c.p.) maps. The following statement (due to Wittstock, Haagerup and Paulsen independently) plays a very important role throughout the theory.

FUNDAMENTAL FACTORIZATION THEOREM OF C.B. MAPS. *For any c.b. map  $u: E_1 \rightarrow E_2$  ( $E_i \subset B(H_i), i = 1, 2$ ) between operator spaces, there are a Hilbert space  $H$ , a  $*$ -representation  $\pi: B(H_1) \rightarrow B(H)$  and operators  $V: H \rightarrow H_2$  and  $W: H_2 \rightarrow H$  with  $\|V\| \|W\| \leq \|u\|_{cb}$  such that, for any  $x$  in  $E_1$ , we have  $u(x) = V\pi(x)W$ .*

We say that  $u: E_1 \rightarrow E_2$  is completely positive (c.p. in short) if for any  $n$  and any  $x$  in  $M_n(E_1) \cap M_n(B(H_1))_+$  we have  $u_n(x) \in M_n(E_2) \cap M_n(B(H_2))_+$ . (Here

$M_n(B(H))_+$  denotes the positive cone of the  $C^*$ -algebra  $M_n(B(H))$ .) Actually, c.p. maps are of interest only when  $E_1$  is a  $C^*$ -algebra or an operator system. When, say,  $E_1$  is a  $C^*$ -algebra,  $E_2 = B(H_2)$ , then  $u$  is c.p. iff the above factorization actually holds with  $V = W^*$  (Stinespring). In that case, it is known (Hadwin-Wittstock) that a map  $u: E_1 \rightarrow B(H_2)$  is c.b. iff it is a linear combination of c.p. maps. Moreover, when  $E_2 = B(H_2)$ , any c.b. map  $u: E_1 \rightarrow E_2$ , defined on an arbitrary o.s.  $E_1 \subset B(H_1)$ , extends with the same c.b. norm to the whole of  $B(H_1)$ . This property of  $B(H)$  plays the same role for o.s. as the Hahn-Banach extension theorem for Banach spaces. The o.s. which possess this extension property (like  $E_2 = B(H_2)$  above) are called *injective*, they are all of the form  $E = pAq$ , where  $A$  is an injective  $C^*$ -algebra and  $p, q$  are two projections in  $A$  ([Ru2]), moreover (R. Smith, unpublished) when  $E$  is finite dimensional,  $A$  also can be chosen finite dimensional. In the isomorphic theory of Banach spaces, the separable injectivity of  $c_0$  is classical (Sobczyk), and Zippin proved the deep fact that this characterizes  $c_0$  up to *isomorphism*; the analogous o.s. questions are studied in [Ro]. Of course, there is a parallel notion of *projective* o.s. in terms of lifting property, see [B2, ER9] for more on this theme.

We refer the reader to [P1] for more information and for precise references on c.b. maps. See the last chapter in [Pi7] for the notion of  $p$ -complete boundedness in the case when  $H_1, H_2$  are replaced by two Banach spaces; see also [LM1] for the multilinear case.

## 1.2 MINIMAL TENSOR PRODUCT. EXAMPLES

Let  $E_1 \subset B(H_1)$  and  $E_2 \subset B(H_2)$  be two operator spaces. There is an obvious embedding  $j: E_1 \otimes E_2 \rightarrow B(H_1 \otimes H_2)$  characterized by the identity  $j(x_1 \otimes x_2)(h_1 \otimes h_2) = x_1(h_1) \otimes x_2(h_2)$ . We denote by  $E_1 \otimes_{\min} E_2$  the completion of  $E_1 \otimes E_2$  for the norm  $x \rightarrow \|j(x)\|$ . Clearly  $j$  extends to an isometric embedding, which allows us to view  $E_1 \otimes_{\min} E_2$  as an operator space embedded into  $B(H_1 \otimes H_2)$ . This is called the minimal (= spatial) tensor product of  $E_1$  and  $E_2$ . For example, let  $E \subset B(H)$  be an operator space. Then  $M_n \otimes_{\min} E$  can be identified with the space  $M_n(E)$ , and  $\mathcal{K}[E]$  can be identified isometrically with  $\mathcal{K} \otimes_{\min} E$ . Thus, for any linear map  $u: E_1 \rightarrow E_2$ , we have  $\|u\|_{cb} = \|I \otimes u: \mathcal{K} \otimes_{\min} E_1 \rightarrow \mathcal{K} \otimes_{\min} E_2\| = \|I \otimes u: \mathcal{K} \otimes_{\min} E_1 \rightarrow \mathcal{K} \otimes_{\min} E_2\|_{cb}$ . More generally, it can be shown that, for any operator space  $F \subset B(K)$  ( $K$  Hilbert), we have  $\|I_F \otimes u: F \otimes_{\min} E_1 \rightarrow F \otimes_{\min} E_2\| \leq \|u\|_{cb}$ . Consequently, if  $v: F_1 \rightarrow F_2$  is another c.b. map between operator spaces, we have  $\|v \otimes u: F_1 \otimes_{\min} E_1 \rightarrow F_2 \otimes_{\min} E_2\|_{cb} \leq \|v\|_{cb} \|u\|_{cb}$ . Thus c.b. maps can also be characterized as the ones which “tensorize” with respect to the minimal tensor product.

*Remark.* When  $E_1, E_2$  are  $C^*$ -subalgebras in  $B(H_1)$  and  $B(H_2)$ , then  $E_1 \otimes_{\min} E_2$  is a  $C^*$ -subalgebra of  $B(H_1 \otimes H_2)$ . By a classical theorem of Takesaki (see also §1.10 below), the norm  $\|\cdot\|_{\min}$  is the smallest  $C^*$ -norm on the tensor product of two  $C^*$ -algebras (and it does not depend on the particular realizations  $E_i \subset B(H_i)$ ,  $i = 1, 2$ ). For Banach spaces, Grothendieck [G] showed that the injective tensor product of two Banach spaces corresponds to the smallest reasonable tensor norm on  $B_1 \otimes B_2$ . The analogous result for operator spaces is proved in [BP1]:  $E_1 \otimes_{\min} E_2$



is indeed characterized by a certain minimality among the “reasonable” operator space structures on  $E_1 \otimes E_2$ .

Just like in the  $C^*$ -case, the minimal tensor product is “*injective*” in the o.s. category: this means that, given o.s.  $E_1, E_2$ , if  $F_i \subset E_i$  ( $i = 1, 2$ ) are further closed subspaces, then  $F_1 \otimes_{\min} F_2$  can be identified with a closed subspace of  $E_1 \otimes_{\min} E_2$ . Moreover, this tensor product is “*commutative*” (this means that  $E_1 \otimes_{\min} E_2$  can be identified with  $E_2 \otimes_{\min} E_1$ ) and “*associative*” (this means that given  $E_i$   $i = 1, 2, 3$ , we have

$$(E_1 \otimes_{\min} E_2) \otimes_{\min} E_3 \simeq E_1 \otimes_{\min} (E_2 \otimes_{\min} E_3).$$

We will meet below several other tensor products enjoying these properties.

### 1.3 RUAN’S THEOREM. EXAMPLES

It is customary to describe a Banach space before completion, simply as a vector space equipped with a norm. Ruan’s theorem allows to take a similar viewpoint for operator spaces. Let  $V$  be a (complex) vector space and, for each  $n \geq 1$ , let  $\|\cdot\|_n$  be a norm on  $M_n(V) = M_n \otimes V$ . For convenience, if  $x \in M_n(V)$ ,  $a, b \in M_n$  we denote by  $a \cdot x \cdot b$  the “matrix product” defined in the obvious way. Consider the following two properties:

$$(R_1) \quad \forall n \geq 1 \quad \forall a, b \in M_n \quad \forall x \in M_n(V) \quad \|a \cdot x \cdot b\|_n \leq \|a\|_{M_n} \|x\|_n \|b\|_{M_n}$$

$$(R_2) \quad \forall n, m \geq 1 \quad \forall x \in M_n(V) \quad \forall y \in M_m(V) \quad \left\| \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \right\|_{n+m} = \max\{\|x\|_n, \|y\|_m\}.$$

It is easy to check that the sequence of norms associated to any operator space structure on  $V$  does satisfy this. We can now state Ruan’s theorem, which is precisely the converse (a simplified proof appears in [ER5]).

**THEOREM ([RU1]).** *Let  $V$  be a complex vector space equipped with a sequence of norms  $(\|\cdot\|_n)_{n \geq 1}$ , where, for each  $n \geq 1$ ,  $\|\cdot\|_n$  is a norm on  $M_n(V)$ . Then this sequence of norms satisfies  $(R_1)$  and  $(R_2)$  iff there is a Hilbert space  $H$  and a linear embedding  $j: V \rightarrow B(H)$  such that, for each  $n \geq 1$ , the map  $I_{M_n} \otimes j: M_n(V) \rightarrow M_n(B(H))$  is isometric, in other words, iff the sequence  $(\|\cdot\|_n)$  “comes” from an operator space structure on  $V$ .*

**SOME EXAMPLES.** Let  $C \subset B(\ell_2)$  and  $R \subset B(\ell_2)$  be the “column” and “row” Hilbert spaces defined by  $C = \overline{\text{span}}[e_{i1} \mid i \geq 1]$  and  $R = \text{span}[e_{1j} \mid j \geq 1]$ . Then, we have (completely isometrically)  $\mathcal{K} \simeq C \otimes_{\min} R$ . Moreover, the o.s.-norm for these two examples can be easily computed as follows: for any finitely supported sequence  $(a_i)_{i \geq 1}$  of elements of  $\mathcal{K}$  we have:

$$\left\| \sum a_i \otimes e_{i1} \right\|_{\mathcal{K}[C]} = \left\| \sum a_i^* a_i \right\|_{\mathcal{K}}^{1/2} \quad \text{and} \quad \left\| \sum a_j \otimes e_{1j} \right\|_{\mathcal{K}[R]} = \left\| \sum a_j a_j^* \right\|_{\mathcal{K}}^{1/2}.$$

Thus even though these spaces are clearly isometric (as Banach spaces) to  $\ell_2$ , their (o.s. sense)-norm is quite different, and actually it can be shown that  $R$  and  $C$  are not completely isomorphic. More precisely, let  $C_n = \text{span}[e_{i1} \mid 1 \leq i \leq n]$

and  $R_n = \text{span}[e_{1j} \mid 1 \leq j \leq n]$ . Then it can be shown that  $d_{cb}(R_n, C_n) = n$ , which is the maximum value of  $d_{cb}(E, F)$  over all pairs  $E, F$  of  $n$ -dimensional operator spaces (see §1.9 below). Thus  $R_n, C_n$  (although they are mutually isometric and isometric to  $\ell_2^n$ ) are “extremally” far apart as operator spaces. Some simple questions about them can be quite tricky. For instance, consider the direct sum  $R \oplus C \subset B(\ell_2 \oplus \ell_2)$  (with the induced o.s. structure) and an operator subspace  $E \subset R \oplus C$  such that there is a c.b. projection from  $R \oplus C$  onto  $E$ . By [Oi], we have then  $E \simeq E_1 \oplus E_2$  (completely isomorphically) with  $E_1 \subset R$  and  $E_2 \subset C$ .

Another source of basic but very useful examples is given by the operator spaces  $\min(B)$  and  $\max(B)$  associated to a given Banach space  $B$  (cf. [BP1, P3]). These can be described as follows: consider the set of all norms  $\alpha$  on  $\mathcal{K}_0 \otimes B$  satisfying  $(R_1)$  and  $(R_2)$  and respecting the norm of  $B$ , i.e. such that  $\alpha(e_{11} \otimes x) = \|x\| \forall x \in B$ . Then this set admits a minimal element  $\alpha_{\min}$  and a maximal one  $\alpha_{\max}$ , corresponding to the two o.s.  $\min(B)$  and  $\max(B)$ . If  $B$  is given to us as an operator space, then  $\min(B)$  or  $\max(B)$  is the same Banach space but in general a different o.s. The space  $\min(B)$  can be realized completely isometrically by any isometric embedding of  $B$  into a commutative  $C^*$ -algebra. While the spaces  $\min(B)$  are rather simple, they explain why operator spaces are viewed as “non-commutative Banach spaces”.

#### 1.4 DUALITY. QUOTIENT. INTERPOLATION

Let  $E \subset B(H)$  be an operator space. The dual  $E^*$  is a quotient of  $B(H)^*$ , so, a priori, it does not seem to be an o.s. However, it admits a very fruitful o.s. structure introduced (independently) in [BP1] and [ER3] as follows.

Let  $F$  be another operator space and let  $V = cb(E, F)$ . By identifying  $M_n(V)$  with  $cb(E, M_n(F))$  equipped with its c.b. norm, we obtain a sequence of norms satisfying  $(R_1)$  and  $(R_2)$ . Therefore there is a specific operator space structure on  $cb(E, F)$  for which the identification  $M_n(cb(E, F)) = cb(E, M_n(F))$  becomes isometric for all  $n \geq 1$ . We call this the “natural” o.s. structure on  $cb(E, F)$ . In particular, when  $F = \mathbb{C}$  we obtain an operator space structure on  $E^* = cb(E, \mathbb{C})$  (it is easy to see that for any linear form  $\xi \in E^*$  we have  $\|\xi\| = \|\xi\|_{cb}$  and as mentioned above there is only *one* reasonable way to equip  $\mathbb{C}$  with an operator space structure). Thus, the dual Banach space  $E^*$  is now equipped with an o.s. structure which we call the “dual o.s. structure” (the resulting o.s. is called the standard dual in [BP1]). It is characterized by the property that for any o.s.  $F$ , the natural mapping  $u \rightarrow \tilde{u}$  from  $F \otimes E^*$  (resp.  $E^* \otimes F$ ) into  $cb(E, F)$  defines an isometry from  $F \otimes_{\min} E^*$  (resp.  $E^* \otimes_{\min} F$ ) into  $cb(E, F)$ . When  $\dim(F) < \infty$ , this is onto, whence an isometric identity  $F \otimes_{\min} E^* = cb(E, F) (= E^* \otimes_{\min} F)$ . Note that, for any o.s.  $F$  and any  $u: E \rightarrow F$  we have  $\|u\|_{cb} = \|u^*\|_{cb}$ . Moreover, the inclusion  $E \subset E^{**} = (E^*)^*$  is completely isometric ([B2]) and  $E$  is the o.s. dual of an o.s. iff it admits a completely isometric “realization” as a weak- $*$  closed subspace of  $B(H)$  (cf. [ER2, B2]). To illustrate this with some examples, we have completely isometric identities (cf. [BP1, ER4, B2])  $R^* \simeq C$ ,  $C^* \simeq R$  and  $\min(B)^* \simeq \max(B^*)$ ,  $\max(B)^* \simeq \min(B^*)$  for any Banach space  $B$ .

Let  $M$  be a von Neumann algebra with predual  $M_*$ . The “natural” o.s. struc-

ture just defined on  $M^*$  induces a fortiori an o.s. structure on  $M_* \subset M^*$  which, once more, we call the “natural” one. At this point, a problem of “coherence” of the various duals of  $M_*$  arises, but (fortunately) Blecher [B2] showed that everything “ticks”: if we equip  $M_*$  with the o.s. structure just defined, its o.s. dual coincides completely isometrically with  $M$  equipped with its natural o.s. structure. In sharp contrast, this is no longer true for general operator spaces: Le Merdy (cf. [LM1]) has shown that there is an o.s. structure on  $B(H)^*$  which is not the dual of any o.s. structure on  $B(H)$ .

The principle we just used to define the o.s. duality is valid in numerous other situations, such as quotients ([Ru1]) or interpolation spaces [Pi1]. Let  $E_2 \subset E_1 \subset B(H)$  be operator spaces and let  $\|\cdot\|_n$  be the norm on  $M_n(E_1/E_2)$  naturally associated to  $M_n(E_1)/M_n(E_2)$  equipped with the quotient norm. Again it turns out that these norms verify  $(R_1)$  and  $(R_2)$ , whence they yield an o.s. structure on  $E_1/E_2$ , characterized by the isometric identity  $\mathcal{K}[E_1/E_2] = \mathcal{K}[E_1]/\mathcal{K}[E_2]$ . We thus obtain a notion of quotient of operator spaces satisfying the usual rules of the Banach space duality, namely  $(E_1/E_2)^* \simeq E_2^\perp$  and  $E_2^* \simeq E_1^*/E_2^\perp$  (completely isometrically). We will say that a surjective linear map  $u: E \rightarrow F$  is a complete surjection (resp. a complete metric surjection) if the associated map  $E/\ker(u) \rightarrow F$  is a complete (resp. a completely isometric) isomorphism. Equivalently, that means that  $u^*$  is a completely isomorphic (resp. completely isometric) embedding of  $F^*$  into  $E^*$ .

We now turn briefly to the complex interpolation method, introduced for Banach spaces around 1960 by A. Calderón and J. L. Lions independently, cf. [BL]. Assume given a pair of operator spaces  $E_0, E_1$  together with continuous linear injections  $E_0 \rightarrow \mathcal{X}$ ,  $E_1 \rightarrow \mathcal{X}$  into a topological vector space (actually a Banach space if we wish). Then, for any  $0 < \theta < 1$ , the complex interpolation method produces an “intermediate Banach space”  $(E_0, E_1)_\theta$ . Then again Ruan’s theorem allows us to equip  $(E_0, E_1)_\theta$  with an o.s. structure characterized by the isometric identity  $\mathcal{K}[(E_0, E_1)_\theta] = (\mathcal{K}[E_0], \mathcal{K}[E_1])_\theta$ . The fact that the functor of interpolation essentially commutes with duality, which is well known for Banach spaces, is extended to o.s. in [Pi1], but the proof requires rather delicate factorization properties of operator valued analytic functions.

## 1.5 PROJECTIVE TENSOR PRODUCT. APPROXIMATION PROPERTY (OAP)

Since the minimal tensor product is the o.s. analog of Grothendieck’s injective tensor product, it is tempting to look for the o.s. analog of the projective tensor product. This question is treated independently in [BP1] and [ER3]. Effros and Ruan pursued further: they introduced analogs of Grothendieck’s approximation property ([ER2]), of integral or nuclear operators, of the Dvoretzky-Rogers theorem (characterizing finite dimensional spaces by the coincidence of unconditional and absolute convergence of series) and more. Their program meets several interesting obstacles (due mainly to the lack of local reflexivity, see §1.11 below), but roughly goes through (see [ER6, ER7]). For related work, see also [EWi] on “non-commutative convexity” and a paper by E. Effros and C. Webster in [Ka] devoted to “Operator analogues of locally convex spaces”.

For lack of space, we refer to the original papers for precise definitions, and merely summarize the main results. Let us denote by  $E_1 \otimes^\wedge E_2$  the o.s. version of the projective tensor product. Note that the norm of this o.s. is *different* from Grothendieck’s projective tensor norm  $\|\cdot\|_\wedge$  and the Banach space projective tensor product  $E_1 \widehat{\otimes} E_2$  is *not* the underlying Banach space to  $E_1 \otimes^\wedge E_2$ . Nevertheless, it is shown in [BP1] that, in some sense, this corresponds to the largest o.s.-norm on  $\mathcal{K}_0 \otimes E_1 \otimes E_2$ .

The projective operator space tensor product  $E_1 \otimes^\wedge E_2$  is characterized by the isometric (actually completely isometric) identities  $(E_1 \otimes^\wedge E_2)^* \simeq cb(E_1, E_2^*) \simeq cb(E_2, E_1^*)$ . Moreover, the natural map  $E_1 \otimes^\wedge E_2 \rightarrow E_1 \otimes_{\min} E_2$  is a complete contraction. The projective tensor product is commutative and associative, but in general not injective. However, it is, of course “projective”, *i.e.* if  $u_1: E_1 \rightarrow F_1$  and  $u_2: E_2 \rightarrow F_2$  are complete metric surjections then  $u_1 \otimes u_2$  also defines a complete metric surjection from  $E_1 \otimes^\wedge E_2$  onto  $F_1 \otimes^\wedge F_2$ . Another important property from [ER2] is as follows: let  $M, N$  be two von Neumann algebras with preduals  $M_*, N_*$ . Let  $M \widehat{\otimes} N$  denote their von Neumann algebra tensor product. Then we have a completely isometric identity  $(M \widehat{\otimes} N)_* \simeq M_* \otimes^\wedge N_*$ . This is a non-commutative analog of Grothendieck’s classical isometric identity  $L_1(\mu') \widehat{\otimes} L_1(\mu'') \simeq L_1(\mu' \times \mu'')$  relative to a pair of measure spaces  $(\Omega', \mu'), (\Omega'', \mu'')$ .

Following [ER2], an o.s.  $E$  is said to have the OAP if there is a net of finite rank (c.b.) maps  $u_i: E \rightarrow E$  such that the net  $I \otimes u_i$  converges pointwise to the identity on  $\mathcal{K}[E]$ . This is the o.s. analog of Grothendieck’s approximation property (AP) for Banach spaces. When the net  $(u_i)$  is bounded in  $cb(E, E)$ , we say that  $E$  has the CBAP (this is analogous to the BAP for Banach spaces). To quote a sample result from [ER2]:  $E$  has the OAP iff the natural map  $E^* \otimes^\wedge E \rightarrow E^* \otimes_{\min} E$  is injective. The class of groups  $G$  for which the reduced  $C^*$ -algebra of  $G$  has the OAP is studied in [HK] (see also §9 in [Ki1]). The ideas revolving around the OAP or the CBAP are likely to lead to a simpler and more conceptual proof of the main result of [Sz], but unfortunately this challenge has resisted all attempts so far.

### 1.6 THE HAAGERUP TENSOR PRODUCT

Curiously, the category of operator spaces admits a tensor product which (at least in the author’s opinion) has no true counterpart for Banach spaces, namely the Haagerup tensor product introduced by Effros and Kishimoto (inspired by some unpublished work of Haagerup). But, while these authors originally considered only the resulting Banach space, it is the operator space case which turned out to be the most fruitful, through the fundamental works of Christensen and Sinclair [CS1] (see also [CS2]) and its extension by Paulsen and Smith [PS]. See also [BS] for the “weak- $*$  Haagerup tensor product” of dual o.s.

Let  $E_1, E_2$  be two operator spaces. Consider  $x_i \in \mathcal{K} \otimes E_i$  ( $i = 1, 2$ ). We denote by  $(x_1, x_2) \rightarrow x_1 \odot x_2$  the bilinear form from  $\mathcal{K} \otimes E_1 \times \mathcal{K} \otimes E_2$  to  $\mathcal{K} \otimes (E_1 \otimes E_2)$  defined on elementary tensors by setting  $(k_1 \otimes e_1) \odot (k_2 \otimes e_2) = (k_1 k_2) \otimes (e_1 \otimes e_2)$ . We set  $\alpha_i(x_i) = \|x_i\|_{\mathcal{K} \otimes_{\min} E_i}$  ( $i = 1, 2$ ). Then, for any  $x \in \mathcal{K} \otimes E_1 \otimes E_2$ , we define  $\alpha_h(x) = \inf\{\alpha_1(x_1)\alpha_2(x_2)\}$ , where the infimum runs over all possible decompositions of  $x$  of the form  $x = x_1 \odot x_2$  with  $x_1 \in \mathcal{K} \otimes E_1, x_2 \in \mathcal{K} \otimes E_2$ . Once again it can be

shown (by Ruan's theorem) that this defines an o.s. structure on  $E_1 \otimes E_2$ , so that we obtain, after completion, an operator space denoted by  $E_1 \otimes_h E_2$  and called the Haagerup tensor product.

This definition can be extended to an arbitrary number of factors  $E_1, E_2, \dots, E_N$  and the result is denoted by  $E_1 \otimes_h \dots \otimes_h E_N$ . In [CES], the following very useful "realization" of  $E_1 \otimes_h \dots \otimes_h E_N$  is presented: assume  $E_i$  given as a subspace of a  $C^*$ -algebra  $A_i$ , then  $E_1 \otimes_h \dots \otimes_h E_N$  can be identified with a subspace of the ( $C^*$ -algebraic) "free product"  $A_1 * A_2 * \dots * A_N$ . More precisely the linear mapping  $j: E_1 \otimes_h \dots \otimes_h E_N \rightarrow A_1 * \dots * A_N$  defined by  $j(x_1 \otimes \dots \otimes x_N) = x_1 x_2 \dots x_N$  is a completely isometric embedding. This is closely related to the fundamental factorization of c.b. multilinear maps, obtained in [CS1] for  $C^*$ -algebras and in [PS] in full generality, as follows:

*An  $N$ -linear map  $\varphi: E_1 \times E_2 \times \dots \times E_N \rightarrow B(H)$  defines a complete contraction from  $E_1 \otimes_h \dots \otimes_h E_N$  to  $B(H)$  iff there are a Hilbert space  $\widehat{H}$ , completely contractive maps  $\sigma_i: E_i \rightarrow B(\widehat{H})$  and operators  $V: \widehat{H} \rightarrow H$  and  $W: H \rightarrow \widehat{H}$  with  $\|V\| \|W\| \leq 1$  such that  $\varphi(x_1, \dots, x_N) = V\sigma_1(x_1) \dots \sigma_N(x_N)W$ .*

The preceding result has many important applications notably to the Hochschild cohomology of operator algebras (see [E] [CES] and [SSm]).

The Haagerup tensor product enjoys unusually nice properties: it is associative, and *both* injective and projective (which is quite rare!), but it is *not* commutative: the spaces  $E_1 \otimes_h E_2$  and  $E_2 \otimes_h E_1$  can be very different. However, there is a symmetrized version of the Haagerup tensor product, introduced recently in [OiP] and denoted there by  $E_1 \otimes_\mu E_2$ , which has proved fruitful. For instance, in the situation of the preceding theorem, the paper [OiP] contains a characterization (up to a numerical factor when  $N > 2$ ) of the  $N$ -linear maps  $\varphi: E_1 \times \dots \times E_N \rightarrow B(H)$  which admit a factorization as above but with the additional condition that the ranges of  $\sigma_1, \dots, \sigma_N$  mutually commute.

Another very striking property of the Haagerup tensor product is its *self-duality* (which explains of course its being both injective and projective), for which we refer to [ER4] (according to [ER4], the first point below is due to Blecher):

*Let  $E_1, E_2$  be operator spaces. Then if  $E_1$  and  $E_2$  are finite dimensional we have  $(E_1 \otimes_h E_2)^* \simeq E_1^* \otimes_h E_2^*$  completely isometrically. Moreover, in the general case we have a completely isometric embedding  $E_1^* \otimes_h E_2^* \subset (E_1 \otimes_h E_2)^*$ .*

Here are sample results from [ER4] or [B1]. For every operator space  $E$ , we have a completely isometric isomorphism  $M_n(E) \simeq C_n \otimes_h E \otimes_h R_n$  taking  $(x_{ij})$  to  $\sum e_{i1} \otimes x_{ij} \otimes e_{1j}$ . In particular  $C_n \otimes_h R_n \simeq M_n$  and  $C \otimes_h R \simeq \mathcal{K}$ ,  $R \otimes_h C \simeq \mathcal{K}^*$ . If  $H$  is an arbitrary Hilbert space, let  $H_r$  and  $H_c$  be the o.s. defined by setting  $H_r = B(\overline{H}, \mathbb{C})$  and  $H_c = B(\mathbb{C}, H)$ . Then if  $K$  is another Hilbert space, we have (completely isometrically)  $H_c \otimes_h K_c = (H \otimes_2 K)_c$  and  $H_r \otimes_h K_r = (H \otimes_2 K)_r$ .

## 1.7 CHARACTERIZATIONS OF OPERATOR ALGEBRAS AND OPERATOR MODULES

In the Banach algebra literature, an operator algebra is defined as a closed subalgebra of  $B(H)$ , for some Hilbert space  $H$ , or equivalently a closed subalgebra of a  $C^*$ -algebra  $C \subset B(H)$ . When  $C$  is commutative,  $A$  is called a uniform algebra. Now consider an operator algebra  $A \subset B(H)$  and let  $I \subset A$  be a closed (two-

sided) ideal. Then, curiously, the quotient  $A/I$  is still an operator algebra (due to B. Cole for uniform algebras and to G. Lumer and A. Bernard in general): there is (for some suitable  $\mathcal{H}$ ) an isometric homomorphism  $j: A/I \rightarrow B(\mathcal{H})$ . In the 70's several authors (Craw, Davie, Varopoulos, Charpentier, Tonge, Carne) tried to characterize operator algebras by certain continuity properties of the product map  $p: A \otimes A \rightarrow A$ . Although this chain of thoughts lead to a negative result (see [Ca]), it turns out that, in the operator space framework, the same things work! More precisely:

**THEOREM ([BRS]).** *Let  $A$  be a Banach algebra with a normalized unit element and equipped with an o.s. structure. Then the product map  $p: A \otimes A \rightarrow A$  extends completely contractively to  $A \otimes_h A$  iff there exists, for  $H$  suitable, a unital and completely isometric homomorphism  $j: A \rightarrow B(H)$ . Equivalently, this holds iff the natural matrix product  $f.g$  of any two elements  $f, g$  in  $\mathcal{K}[A]$  satisfies  $\|f.g\| \leq \|f\|\|g\|$ . In other words,  $A$  is an operator algebra (completely isometrically) iff  $\mathcal{K}[A]$  is a Banach algebra.*

Of course it is natural to wonder whether the mere complete *boundedness* of the product  $p: A \otimes_h A \rightarrow A$  characterizes operator algebras up to complete *isomorphism*. This resisted for a few years, until Blecher [B3] proved that indeed this is true. The original proofs of [BRS, B3] did not use the earlier Cole-Lumer-Bernard results (and actually obtained them as corollaries), but it is also possible to go in the converse direction, with some extra work (see [Pi5]). We refer the reader to [LM2] for an extension of the Cole-Lumer-Bernard theorem to quotients of subalgebras of  $B(X)$  when  $X$  is a Banach space, and to [BLM] and [LM5] for a detailed study of the operator algebra structures on  $\ell_p$ , or the Schatten  $p$ -classes. See also [LM6] for a version of the above theorem adapted to dual operator algebras.

Operator spaces which are also modules over an operator algebra (in other words “operator modules”) can also be characterized in a similar way (see [CES] and [ER1], see also [Ma] for dual modules) and suitably modified versions of the Haagerup tensor product are available for them. Operator modules play a central rôle in [BMP] where the foundations of a Morita theory for non self-adjoint operator algebras are laid. There Blecher, Muhly and Paulsen show that operator modules are an appropriate “metric” context for the  $C^*$ -algebraic theory of strong Morita equivalence, and the related theory of  $C^*$ -modules. For example, Rieffel's  $C^*$ -module tensor product is exactly the Haagerup module tensor product of the  $C^*$ -modules with their natural operator space structures. See [BMP], [B4], Blecher's survey in [Ka] and references contained therein for more on this.

## 1.8 THE OPERATOR HILBERT SPACE OH AND NON-COMMUTATIVE $L_p$ -SPACES

Let us say that an operator space is Hilbertian if the underlying Banach space is isometric to a Hilbert space. Examples of this are in abundance, but apparently none of them is self-dual, which induces one to believe that operator spaces do not admit a true analog of Hilbert spaces. Therefore, the next result which contradicts this impression, comes somewhat as a surprise. (Notation: if  $E$  is an operator

space, say  $E \subset B(H)$ , then  $\overline{E}$  is the complex conjugate of  $E$  equipped with the o.s. structure corresponding to the embedding  $\overline{E} \subset \overline{B(H)} = B(\overline{H})$ .

THEOREM ([Pi1]). *Let  $H$  be an arbitrary Hilbert space. There exists, for a suitable  $\mathcal{H}$ , a Hilbertian operator space  $E_H \subset B(\mathcal{H})$  such that the canonical identification (derived from the scalar product)  $E_H^* \rightarrow \overline{E}_H$  is completely isometric. Moreover, the space  $E_H$  is unique up to complete isometry. Let  $(T_i)_{i \in I}$  be an orthonormal basis in  $E_H$ . Then, for any finitely supported family  $(a_i)_{i \in I}$  in  $\mathcal{K}$ , we have*

$$\left\| \sum a_i \otimes T_i \right\|_{\mathcal{K}[E_H]} = \left\| \sum a_i \otimes \bar{a}_i \right\|_{\min}^{1/2}.$$

When  $H = \ell_2$ , we denote the space  $E_H$  by  $OH$  and we call it the “operator Hilbert space”. Similarly, we denote it by  $OH_n$  when  $H = \ell_2^n$  and by  $OH(I)$  when  $H = \ell_2(I)$ . The preceding result suggests to systematically explore all the situations of Banach space theory where Hilbert space plays a central rôle (there are many!) and to investigate their analog for operator spaces. This program is pursued in [Pi1, Pi6]. The space  $OH$  has rather striking complex interpolation properties (see [Pi1]). For instance, we have completely isometric identities  $(\min(\ell_2), \max(\ell_2))_{\frac{1}{2}} \simeq OH$  and  $(R, C)_{\frac{1}{2}} \simeq OH$ . (In the latter case, we should mention that the pair  $(R, C)$  is viewed as “compatible” using the transposition map  $x \rightarrow {}^t x$  from  $R$  to  $C$  which allows to view both  $R$  and  $C$  as continuously injected into  $\mathcal{X} = C$ .) Concerning the Haagerup tensor product, for any sets  $I$  and  $J$ , we have a completely isometric identity  $OH(I) \otimes_h OH(J) \simeq OH(I \times J)$ .

Finally, we should mention that  $OH$  is “homogeneous” (an o.s.  $E$  is called homogeneous if any linear map  $u: E \rightarrow E$  satisfies  $\|u\| = \|u\|_{cb}$ ). While  $OH$  is unique, the class of homogeneous Hilbertian operator spaces (which also includes  $R, C, \min(\ell_2)$  and  $\max(\ell_2)$ ) is very rich and provides a very fruitful source of examples (see e.g. [Pi1, Pi6, Oi, Z]).

Since operator spaces behave well under interpolation (see §1.4), it is natural to investigate what happens to  $L_p$ -spaces, either scalar or vector valued. While in classical Lebesgue-Bochner theory, the Banach space valued  $L_p$ -spaces have been around for a long time, in the non-commutative case there seemed to be no systematic analogous “vector valued” theory. It turns out that operator spaces provide apparently the “right” framework for such a theory and a large part of [Pi2] tries to demonstrate it. Note however that the space of “values”  $E$  has to be an operator space, (not “only” a Banach space) and moreover we need to assume  $M$  hyperfinite for this theory to run “smoothly”.

Many natural questions arise when one tries to “transfer” the Banach space theory of  $L_p$ -spaces to the o.s. framework. For instance, it is open whether  $OH$  embeds completely isomorphically into the predual of a von Neumann algebra (i.e. into a so-called “non-commutative  $L_1$ -space”). The natural candidates (either Gaussian variables, Rademacher functions or free semi-circular systems in Voiculescu’s sense) span in  $L_1$  (commutative or not) an operator space denoted by  $R + C$  in [Pi1, Pi2] and extensively studied there. Note that, in sharp contrast to the Banach analogue, the o.s. spanned by the Rademacher functions in  $L_p([0, 1])$  (meaning classical  $L_p$  with the “interpolated” o.s. structure) depends on  $p$  and it coincides with  $OH$  only when  $p = 2$ . Its dependence on  $p$  is entirely elucidated by F. Lust-Piquard’s non-commutative Khintchine inequalities (see [Pi2]).

In another direction, very recently Marius Junge found a notion of “non-commutative  $p$ -stable process”, which allowed him to prove that if  $1 < p < 2$  any space  $L_p(\varphi)$  (relative to a von Neumann algebra  $M$  equipped with a faithful normal semi-finite trace  $\varphi$ ) embeds isometrically into a non-commutative  $L_1$ -space. This striking result was clearly inspired by o.s. considerations, even though the completely isomorphic version is still unclear.

### 1.9 LOCAL THEORY. EXACTNESS. FINITE DIMENSIONAL OPERATOR SPACES

Let  $E, F$  be two Banach (resp. operator) spaces. Recall that their “distance”  $d(E, F)$  (resp.  $d_{cb}(E, F)$ ) has been defined in §1.1. These are not really distances in the usual sense, but we can replace them if we wish by  $\delta(E, F) = \text{Log } d(E, F)$  (resp.  $\delta_{cb}(E, F) = \text{Log } d_{cb}(E, F)$ ). Still however it is customary to use  $d$  and  $d_{cb}$  instead of  $\delta$  and  $\delta_{cb}$ . Let  $n \geq 1$ . Let  $OS_n$  (resp.  $B_n$ ) be the set of all  $n$ -dimensional operator (resp. Banach) spaces, in which we agree to identify two spaces whenever they are completely isometric (resp. isometric). Then, it is an exercise to check that  $OS_n$  (resp.  $B_n$ ) equipped with the distance  $\delta_{cb}$  (resp.  $\delta$ ) is a complete metric space. In the Banach (= normed) space case,  $(B_n, \delta)$  is even compact, this is the celebrated “Banach-Mazur compactum”! However,  $(OS_n, \delta_{cb})$  is not compact, and furthermore (in answer to a question of Kirchberg, see [Ki2]) it was proved in [JP] that it is *not separable* if  $n > 2$  ( $n = 2$  remains open). The paper [JP] actually gives three different approaches to this fact. The best asymptotic estimate uses Lubotzky-Phillips-Sarnak’s work (see [Lu]) on “Ramanujan graphs”. (This improvement over our two other approaches was pointed out by A. Valette, see his paper [Va] for more on this theme.) To state this estimate precisely, we need the following notation: let  $\delta(n)$  be the infimum of the numbers  $\varepsilon > 0$  such that  $(OS_n, \delta_{cb})$  admits a countable  $\text{Log}(\varepsilon)$ -net. Then, the non-separability of  $OS_3$  means that  $\delta(3) > 1$ . Moreover, if  $n = p + 1$  with  $p$  prime  $\geq 3$  (or  $p$  equal to a prime power, see [Va]), we have  $\delta(n) \geq n(2\sqrt{n-1})^{-1} \geq \sqrt{n}/2$ . On the other hand we have  $\delta(n) \leq \sqrt{n}$  for all  $n$ . Indeed, it can be shown (see [Pil]) that for any  $E$  in  $OS_n$  we have  $d_{cb}(E, OH_n) \leq \sqrt{n}$ , from which  $\delta(n) \leq \sqrt{n}$  follows trivially. Note that the space  $OH_n$  appears thus as a “center” for  $(OS_n, \delta_{cb})$ , in analogy with  $\ell_2^n$  in the Banach space case. As a consequence we can estimate the “diameter” of  $OS_n$ : for any pair  $(E, F)$  in  $OS_n$ , we have  $d_{cb}(E, F) \leq d_{cb}(E, OH_n)d_{cb}(OH_n, F) \leq n$ . These estimates are optimal since  $d_{cb}(R_n, OH_n) = d_{cb}(C_n, OH_n) = n^{1/2}$  and  $d_{cb}(C_n, R_n) = n$ . As in the “local theory” of Banach spaces (see e.g. [DJT]), these ideas can be used to study an infinite dimensional  $C^*$ -algebra through the collection of its finite dimensional subspaces. To illustrate this, let  $X$  be an o.s. For any (finite dimensional) operator space  $E$ , we define  $d_{SX}(E) = \inf\{d_{cb}(E, F)\}$  where the infimum runs over all the subspaces  $F \subset X$  isomorphic to  $E$  (and  $d_{SX}(E) = \infty$ , say, if there is no such  $F$ ). In the Banach space case, if we take  $X = c_0$  and replace  $d_{cb}$  by  $d$ , then the resulting number is equal to 1 for any  $E$  in  $\bigcup_n B_n$ . In sharp contrast, there is no *separable* o.s.  $X$  such that  $d_{SX}(E) = 1$  for any  $E$  in  $OS_3$ , since this would contradict the non-separability of  $OS_3$ .

Various choices of  $X$  lead to interesting estimates of the “growth” of  $d_{SX}(E)$ . For instance, taking  $X = \mathcal{K}$  we find, for any  $E$  in  $OS_n$ ,  $d_{S\mathcal{K}}(E) \leq \sqrt{n}$  (see Th.



9.6 in [Pi1]), but on the other hand if  $E = \ell_1^n$  ( $=$  o.s. dual of  $\ell_\infty^n$ ) equipped with its “natural” structure, we have  $d_{SK}(\ell_1^n) \geq a_n$  where  $a_n = n(2\sqrt{n-1})^{-1/2} \geq \sqrt{n}/2$ . We also have  $n^{1/4} \geq d_{SK}(OH_n) \geq (a_n)^{1/2}$ , for all  $n > 1$ . Inspired by Kirchberg’s results on the  $C^*$ -case (cf. [Ki1, Wa]), we study in [Pi4] the notion of “exact operator space”: an o.s.  $Y \subset B(H)$  is called exact if  $\sup\{d_{SK}(E) \mid E \subset Y, \dim(E) < \infty\} < \infty$ . A  $C^*$ -algebra is exact in Kirchberg’s sense iff it is exact in the preceding sense, so the reader can use this as the definition of an “exact  $C^*$ -algebra” (but actually Kirchberg proved that a  $C^*$ -algebra is exact iff it embeds into a nuclear one, see [Ki1]). Exact o.s. have surprisingly strong properties:

*if  $E, F$  are both exact, then any c.b. map  $u: E \rightarrow F^*$  factors boundedly through a Hilbert space* ([JP]). Although this is reminiscent of Grothendieck’s classical factorization theorem, actually such a result has no Banach space counterpart!

Another very useful choice is  $X = C^*(\mathbb{F}_\infty)$  the “full”  $C^*$ -algebra of the free group on countably infinitely many generators; for lack of space, we refer the reader to [JP] for more information on  $d_{SX}(\cdot)$  in this case.

### 1.10 APPLICATION TO TENSOR PRODUCTS OF $C^*$ -ALGEBRAS

Let  $A_1, A_2$  be  $C^*$ -algebras. By classical results due respectively to Takesaki (1958) and Guichardet (1965), there is a minimal  $C^*$ -norm and a maximal one, denoted respectively by  $\|\cdot\|_{\min}$  and  $\|\cdot\|_{\max}$  on  $A_1 \otimes A_2$ . The resulting  $C^*$ -algebras (after completion) are denoted respectively by  $A_1 \otimes_{\min} A_2$  and  $A_1 \otimes_{\max} A_2$ . Thus, the tensor product  $A_1 \otimes A_2$  admits a unique  $C^*$ -norm iff  $A_1 \otimes_{\min} A_2 = A_1 \otimes_{\max} A_2$ . (Note: this holds for all  $A_2$  iff  $A_1$  is nuclear, or iff  $A_1^*$  is injective, see [CE] for precise references.) Kirchberg’s work [Ki2] highlights pairs  $A_1, A_2$  satisfying this unicity. In particular, he proved this holds if  $A_1 = B(\ell_2)$  and  $A_2 = C^*(\mathbb{F}_\infty)$  (see [Pi3] for a simple proof using o.s. theory). However, the results of the preceding section imply that this does *not* hold when  $A_1 = A_2 = B(\ell_2)$  (see [JP]), thus answering a long standing open question. Here is a brief sketch: let  $(E_i)_{i \in I}$  be a family of  $n$ -dimensional operator spaces and let  $u_i \in E_i^* \otimes E_i$  be associated to the identity map  $I_i$  on  $E_i$ . Using the dual o.s. structure on  $E_i^*$ , we have embeddings  $E_i \subset B(\ell_2)$ ,  $E_i^* \subset B(\ell_2)$  so that we may consider  $u_i$  as an element of  $B(\ell_2) \otimes B(\ell_2)$  and (by definition of the o.s. structure of  $E_i^*$ ) we have  $\|u_i\|_{\min} = \|I_i\|_{cb} = 1 \forall i \in I$ . Then, (see [JP] for a proof) if  $\|u_i\|_{\max} = \|u_i\|_{\min} \forall i \in I$ , the family  $\{E_i \mid i \in I\}$  is necessarily separable in  $(OS_n, \delta_{cb})$ . Thus the non-separability of (say)  $OS_3$  (see the preceding section) implies  $B(\ell_2) \otimes_{\min} B(\ell_2) \neq B(\ell_2) \otimes_{\max} B(\ell_2)$ . More precisely, let  $\lambda(n) = \sup\{\|u\|_{\max}\}$  where the supremum runs over all  $u \in B(\ell_2) \otimes B(\ell_2)$  with  $\|u\|_{\min} = 1$  and  $\text{rank} \leq n$ . Then, the same idea (see [JP]) leads to  $\delta(n) \leq \lambda(n) \leq \sqrt{n}$  for all  $n \geq 1$ , hence, by the estimates of  $\delta(n)$  given in §1.9,  $\lambda(n)$  grows like  $\sqrt{n}$  (up to a constant factor) when  $n \rightarrow \infty$ .

In sharp contrast, the question whether there is a unique  $C^*$ -norm on  $A_1 \otimes A_2$  when  $A_1 = A_2 = C^*(\mathbb{F}_\infty)$  remains an outstanding open problem, equivalent to a number of fundamental questions, for instance this holds iff every separable  $II_1$ -factor embeds in a (von Neumann) ultraproduct of the hyperfinite  $II_1$  factor or equivalently iff every non-commutative  $L_1$ -space is finitely representable (see below for the definition) in the Banach space of all trace class operators on  $\ell_2$ .

(See the fascinating discussion at the end of [Ki2].)

Let  $X, Y$  be Banach spaces. We say that  $Y$  is finitely representable in  $X$  if for every  $\epsilon > 0$  and every finite dimensional subspace  $E \subset Y$  there is a finite dimensional subspace  $F \subset X$  such that  $d(E, F) < 1 + \epsilon$ . This notion was used extensively by R. C. James in his theory of “super-reflexivity” (see *e.g.* [DJT]), (but actually Grothendieck already considered it explicitly in the appendix to his famous “Résumé”, see [G] page 108-109; his terminology was “ $Y$  a un type métrique inférieur à celui de  $X$ ”). Of course, this immediately extends to the o.s. setting: when  $X, Y$  are o.s. we say that  $Y$  is o.s.-finitely representable in  $X$  if the preceding property holds with  $d_{cb}(E, F)$  instead of  $d(E, F)$ . Equivalently, we have  $d_{SX}(E) = 1$  for any finite dimensional  $E \subset Y$ .

### 1.11 LOCAL REFLEXIVITY

In Banach space theory, the “principle of local reflexivity” says that every Banach space  $B$  satisfies  $B(F, B)^{**} = B(F, B^{**})$  isometrically for any finite dimensional (normed) space  $F$ . Consequently,  $B^{**}$  is always finitely representable in  $B$ . This useful principle goes back to Lindenstrauss-Rosenthal with roots in Grothendieck’s and Schatten’s early work (see [DJT] p. 178 and references there). Similarly, an o.s.  $E$  is called “locally reflexive” if we have  $cb(F, E)^{**} = cb(F, E^{**})$  isometrically for any finite dimensional o.s.  $F$  (and when this holds for all  $F$ , it actually holds completely isometrically). This property was “exported” first to  $C^*$ -algebra theory by Archbold-Batty, then for operator spaces in [EH]. As the reader can guess, not every o.s. is locally reflexive, so the “principle” now fails to be universal: as shown in [EH],  $C^*(\mathbb{F}_\infty)$  is not locally reflexive. Local reflexivity passes to subspaces (but not to quotients) and is trivially satisfied by all *reflexive* o.s. (a puzzling fact since reflexivity is a property of the underlying Banach space only!). It is known that all nuclear  $C^*$ -algebras are locally reflexive (essentially due to Archbold-Batty, see [EH]). More generally, by Kirchberg’s results, exactness  $\Rightarrow$  local reflexivity for  $C^*$ -algebras (see [Kil] or [Wa]), but the converse remains open. Actually, it might be true that exact  $\Rightarrow$  locally reflexive for all o.s. but the converse is certainly false since there are reflexive but non-exact o.s. (such as  $OH$ ). All this shows that local reflexivity is a rather rare property. Therefore, it came as a big surprise (at least to the author) when, in 97, Effros, Junge and Ruan [EJR] managed to prove that every predual of a von Neumann algebra (a fortiori the dual of any  $C^*$ -algebra) is locally reflexive. This striking result is proved using a non standard application of Kaplansky’s classical density theorem, together with a careful comparison of the various notions of “integral operators” relevant to o.s. theory (see a very recent preprint by M. Junge and C. Le Merdy for an alternate proof). Actually, [EJR] contains a remarkable strengthening: for any von Neumann algebra  $M$ , the dual  $M^* = (M_*)^{**}$  is o.s.-finitely representable in  $M_*$ . This is already nontrivial when  $M = B(H)$ !

## 2 SIMILARITY PROBLEMS

Let  $A, B$  be unital Banach algebras. By a “morphism”  $u: A \rightarrow B$ , we mean a unital homomorphism (*i.e.*  $u$  is a linear map satisfying  $u(1) = 1$  and  $u(xy) = u(x)u(y)$  for all  $x, y$  in  $A$ ). Note that, since  $u(1) = 1$ ,  $u$  contractive means here  $\|u\| = 1$  (and of course  $u$  bounded means  $1 \leq \|u\| < \infty$ ). We will be concerned mainly with the case  $B = B(H)$  with  $H$  Hilbert. We then say that  $u$  is similar to a contractive morphism (in short s.c.) if there is an invertible operator  $\xi: H \rightarrow H$  such that the “conjugate” morphism  $u_\xi$  defined by  $u_\xi(x) = \xi^{-1}u(x)\xi$  is contractive. Moreover, we denote  $\text{Sim}(u) = \inf\{\|\xi\| \|\xi^{-1}\| \mid \|u_\xi\| = 1\}$ . For simplicity, we discuss only the unital case, we denote by  $\mathcal{K}_1$  the unitization of  $\mathcal{K}$  and we set  $\mathcal{K}_1[A] = \mathcal{K}_1 \otimes_{\min} A$ , so that  $\mathcal{K}_1[A]$  is a unital operator algebra whenever  $A$  is one. We will be interested in the following.

GENERAL PROBLEM. Which unital Banach algebras  $A$  have the following similarity property: (SP) Every bounded morphism  $u: A \rightarrow B(H)$  ( $H$  being here an arbitrary Hilbert space) is similar to a contractive one (in short s.c.).

Complete boundedness is the key modern notion behind the advances made recently on several instances of this general problem, some of them formulated about fifty years ago. In most cases of interest, the above problem is equivalent to the following. When is it true that all bounded morphisms  $u: A \rightarrow B(H)$  are “automatically” *completely* bounded? Before stating this precisely in Theorem 2.5, we prefer to discuss some examples.

EXAMPLE 2.1 (UNIFORM ALGEBRAS). Let  $A$  be the disc algebra  $A(D)$ , formed of all bounded analytic functions  $f: D \rightarrow \mathbb{C}$  on the open unit disc  $D \subset \mathbb{C}$  which extend continuously to  $\overline{D}$ , equipped with the norm  $\|f\|_\infty = \sup\{|f(z)| \mid z \in D\}$ . Note that the set of all polynomials is dense in  $A(D)$ . Let  $\varphi_0 \in A(D)$  be the element such that  $\varphi_0(z) = z$ . Since this algebra is singly generated (by  $\varphi_0$ ) a morphism  $u: A(D) \rightarrow B(H)$  is entirely determined by the single operator  $T = u(\varphi_0)$ . Moreover,  $u$  is bounded iff  $T$  is “polynomially bounded” which means that there is a constant  $C$  such that for any polynomial  $P$  we have  $\|P(T)\| \leq C\|P\|_\infty$ , and in addition  $\|u\|$  is the best possible constant  $C$ . On the other hand, by a famous 1951 inequality of von Neumann, any contraction  $T$  satisfies  $\|P(T)\| \leq \|P\|_\infty$  for any  $P$ , *i.e.* we have polynomial boundedness with  $C = 1$ . Therefore,  $u$  is similar to a contractive morphism iff  $T = u(\varphi_0)$  is similar to a contraction, *i.e.* iff there is  $\xi$  invertible such that  $\|\xi^{-1}T\xi\| \leq 1$ . Thus, the problem whether the disc algebra satisfies (SP) coincides with a question raised in 1970 by Halmos: is every polynomially bounded operator  $T: H \rightarrow H$  similar to a contraction? A counterexample was recently given in [Pi8]. The original proof of polynomial boundedness in [Pi8] was rather technical but shortly afterwards simpler proofs have been found by Kislyakov [Kis] and Davidson-Paulsen [DP]. They lead to the same class of examples. Since the disc algebra fails (SP), it is now conceivable that the same is true for any proper uniform algebra, but this remains open in general (even though the case of the polydisc algebra or the ball algebra over  $\mathbb{C}^n$  follows easily from the disc case).

Of course, the similarity problem for continuous semi-groups of operators  $(T_t)_{t \geq 0}$  is also quite natural, see [LM7] and the references there for more on this topic.

EXAMPLE 2.2 ( $C^*$ -ALGEBRAS). Let  $A$  be a unital  $C^*$ -algebra. Then it is easy to check that a morphism  $u: A \rightarrow B(H)$  is contractive (*i.e.* has  $\|u\| = 1$ ) iff  $u$  is a  $*$ -representation (*i.e.*  $u(x^*) = u(x)^*$  for all  $x$ ). We then have automatically  $\|u\|_{cb} = 1$ . It is an outstanding conjecture of Kadison (1955) that all  $C^*$ -algebras have  $(SP)$ . is equivalent to the (open) problem whether, for any  $C^*$ -subalgebra  $A \subset B(H)$ , every bounded derivation  $\delta: A \rightarrow B(H)$  is inner. Many partial results (mainly due to E. Christensen and U. Haagerup) are known (see Remark 2.10 below). In particular, it is known ([C1, H]) that if a bounded morphism has a cyclic vector (or admits a finite cyclic set), then it is similar to a  $*$ -representation. However, the general case remains open (and the author doubts its validity). The reduced  $C^*$ -algebra of the free group with countably infinitely many generators might be a counterexample, but actually even the von Neumann algebra  $A = \bigoplus_n M_n$  ( $\ell_\infty$ -direct sum) is not known to satisfy  $(SP)$ .

EXAMPLE 2.3 (GROUP REPRESENTATIONS). Let  $G$  be a discrete group and let  $A = \ell_1(G)$  be its group algebra under the convolution product. Then  $A$  has  $(SP)$  iff every uniformly bounded representation  $\pi: G \rightarrow B(H)$  is unitarizable. When this holds, we will say that “ $G$  is unitarizable”. Note that we mainly restrict below to the discrete case, but otherwise all representations are implicitly assumed to be continuous on  $G$  with respect to the strong operator topology on  $B(H)$ . Here, we allow non-unitary representations (= homomorphisms from  $G$  to  $GL(H)$ ), and we set  $|\pi| = \sup\{\|\pi(t)\| \mid t \in G\}$ . We say that  $\pi$  is uniformly bounded (u.b. in short) if  $|\pi| < \infty$ , and we call  $\pi$  unitarizable if there is an invertible  $\xi: H \rightarrow H$  such that  $t \rightarrow \xi^{-1}\pi(t)\xi$  is a unitary representation. (Note: There is a one to one correspondence between the bounded morphisms  $u: \ell_1(G) \rightarrow B(H)$  and the u.b. representations  $\pi: G \rightarrow B(H)$ . An operator  $T$  is unitary iff  $T \in B(H)$  is invertible and both  $T, T^{-1}$  are contractions. Hence  $u$  is s.c. iff  $\pi$  is unitarizable.)

Sz.-Nagy proved in 1947 that  $\mathbb{Z}$  is unitarizable. Shortly afterwards (1950), Dixmier and Day independently proved that, for any discrete (actually any locally compact) group  $G$ , amenable implies unitarizable and Dixmier [Di] asked whether the converse also holds. This is still open in full generality. However, in 1955, Ehrenpreis and Mautner showed that  $SL_2(\mathbb{R})$  is not unitarizable. Since “unitarizable” passes to quotients, it follows (implicitly) that non-commutative free groups are not unitarizable, but very explicit constructions by many authors (see [MP]) are now known for this, and, by induction, the same is true for any discrete group containing a copy of  $\mathbb{F}_2$  (the free group on 2 generators). This suggests there might be a counterexample to Dixmier’s question (*i.e.* a unitarizable group which is *not* amenable) among the Burnside groups which are the main examples of non-amenable groups without free subgroups (see Olshanskii’s book [Ol], and see also §5.5 in Gromov’s [Gr] for examples of infinite discrete groups with Kazhdan’s property T and without any free subgroup). Nevertheless, if one takes into account the estimate in Dixmier’s argument for amenable  $\Rightarrow$  unitarizable, then a converse result can be proved (see Theorem 2.11 below).

We now explain the intimate connection of the property  $(SP)$  with dilation theory and complete boundedness. For convenience, we first discuss the completely contractive case. Consider a morphism  $u: A \rightarrow B(H)$  on a unital operator algebra

$A \subset B(\mathcal{H})$ . Then, since  $u$  is assumed unital,  $u$  is completely contractive (this means  $\|u\|_{cb} = 1$ ) iff  $u$  extends completely positively to  $B(\mathcal{H})$  (Arveson) or iff there is a Hilbert space  $K$  containing  $H$  and a  $C^*$ -representation  $\pi: B(\mathcal{H}) \rightarrow B(K)$  such that, for any  $x$  in  $A$ , we have  $u(x) = P_H \pi(x)|_H$ . (One then says that  $\pi$  restricted to  $A$  “dilates”  $u$ , or that  $u$  is a “compression” of it.) Moreover, the subspace  $H \subset K$  is necessarily semi-invariant (in Sarason’s sense) for  $\pi(A)$ , which means that there is a pair of  $\pi(A)$ -invariant (closed) subspaces  $E_2 \subset E_1 \subset K$  such that  $H = E_1 \ominus E_2$ . Thus  $\|u\|_{cb} = 1$  iff  $u$  can be “dilated” to a  $*$ -representation. All this is well known, see Theorem 4.8 in [Pi7] for details. For convenience, we will use the following definition (we prefer to avoid the term “maximal algebras” used in [BP2], which might lead to some confusion with “maximal o.s.”).

**DEFINITION 2.4.** Let  $A \subset B(\mathcal{H})$  be a unital operator algebra. We say that  $A$  satisfies condition *(CC)* if, for any morphism  $u: A \rightarrow B(H)$  ( $H$  arbitrary Hilbert), the implication  $\|u\| = 1 \Rightarrow \|u\|_{cb} = 1$  holds.

The precise class of algebras which satisfy *(CC)* is not clear (see [DoP]). However, it is satisfied by  $A(D), A(D^2)$  (but not by  $A(D^n)$  for  $n > 2$  by an example of S. Parrott, see [P1]), by *all*  $C^*$ -algebras and also by  $\mathcal{K}_1[A]$  for any unital operator algebra  $A$ . Thus the next result, provides a characterization of the morphisms which are s.c. for a broad class of algebras. The  $C^*$ -case is due to Haagerup [H] and the general one to Paulsen (see [P1]).

**THEOREM 2.5.** *Let  $A$  be a unital operator algebra and let  $u: A \rightarrow B(H)$  be a morphism. If  $u$  is c.b. then  $u$  is s.c. and, if  $A$  satisfies *(CC)*, the converse holds. We have then  $\|u\|_{cb} = \text{Sim}(u)$ . Thus, assuming *(CC)*,  $A$  satisfies *(SP)* iff for every morphism  $u: A \rightarrow B(H)$ ,  $\|u\| < \infty$  implies  $\|u\|_{cb} < \infty$ .*

**REMARK 2.6.** Applying this to the disc algebra, we get Paulsen’s useful criterion: an operator  $T: H \rightarrow H$  is similar to a contraction iff it is completely polynomially bounded, which means that there is a constant  $C$  such that, for any  $N$  and any  $N \times N$  matrix  $(P_{ij})$  with polynomial entries we have  $\|(P_{ij}(T))\|_{M_N(B(H))} \leq C \sup_{z \in D} \|(P_{ij}(z))\|_{M_N}$ . Now fix an integer  $N$  and denote by  $C_N(T)$  the smallest  $C$  such that this holds for all  $N \times N$  matrices  $(P_{ij})$ . Then the above question of Halmos is the same as asking whether  $C_1(T) < \infty \Rightarrow \sup_{N \geq 1} C_N(T) < \infty$ , and Theorem 2.5 implies that  $\sup_{N \geq 1} C_N(T) = \inf \{ \|\xi^{-1}\| \|\xi\| \mid \|\xi^{-1} T \xi\| \leq 1 \}$ . It can be shown (see [Pi8, Bo]) that there is a numerical constant  $\beta$  such that  $C_N(T) \leq \beta \sqrt{N} C_1(T)$  for all  $T$  and  $N \geq 1$ . However, the counterexamples in [Pi8] show that this cannot be improved: there is a numerical constant  $\delta > 0$  such that for any  $N \geq 1$  and  $\varepsilon > 0$ , there is a  $T = T_{N,\varepsilon}$  such that  $C_1(T) < 1 + \varepsilon$  but still  $C_N(T) \geq \delta \varepsilon \sqrt{N}$ .

We now turn to a sufficient condition for the property *(SP)*.

**DEFINITION 2.7.** We say that an operator algebra  $A$  has length  $\leq d$  if there is a constant  $K \geq 0$  such that, for any  $x$  in  $\mathcal{K}[A]$ , there are  $\alpha_0, \alpha_1, \dots, \alpha_d$  in  $\mathcal{K}[\mathbb{C}]$  and  $D_1, \dots, D_d$  diagonal in  $\mathcal{K}[A]$  such that  $x = \alpha_0 D_1 \alpha_1 D_2 \dots D_d \alpha_d$  and  $\prod \|\alpha_i\| \prod \|D_i\| \leq K \|x\|$ .

We will denote by  $\ell(A)$  the smallest  $d$  such that this holds. Equivalently,  $\ell(A) \leq d$  iff every  $x$  in  $\mathcal{K}[A]$  can be factorized as above (the constant  $K$  then exists by the open mapping theorem).

*Remark.* This notion from [Pi9] was inspired by the remarkable paper [BP2]. There, Blecher and Paulsen prove that a unital operator algebra  $A$  satisfies (CC) iff any  $x$  in  $\mathcal{K}[A]$  with  $\|x\| \leq 1$  lies in the norm closure of the set of all (arbitrarily long) products of the form  $\alpha_0 D_1 \alpha_1 \dots D_d \alpha_d$  with  $\|\alpha_i\| \|\Pi\| \|D_i\| \leq 1$  and  $d \geq 1$ .

**PROPOSITION 2.8.** *If an operator algebra  $A$  has length  $\leq d$ , then  $A$  satisfies (SP) and more precisely any morphism  $u: A \rightarrow B(H)$  satisfies (with the notation of Definitions 2.7)  $\|u\|_{cb} \leq K \|u\|^d$ .*

*Proof.* Using the notation in §1.1 and Definition 2.7, we have  $u_\infty(x) = \alpha_0 u_\infty(D_1) \alpha_1 \dots u_\infty(D_d) \alpha_d$  hence  $\|u_\infty(x)\| \leq \|\alpha_i\| \|\Pi\| \|u_\infty(D_i)\|$ , but since each  $D_i$  is diagonal, we have  $\|u_\infty(D_i)\| \leq \|u\| \|D_i\|$ , whence  $\|u_\infty(x)\| \leq K \|u\|^d \|x\|$ , and therefore  $\|u\|_{cb} \leq K \|u\|^d$ .  $\square$

Let  $A$  be a unital Banach algebra. For any  $c \geq 1$ , let  $\Phi_A(c) = \sup\{\text{Sim}(u)\}$  where the supremum runs over all morphisms  $u: A \rightarrow B(H)$  ( $H$  arbitrary Hilbert) with  $\|u\| \leq c$ , and let  $d(A) = \inf\{\alpha \geq 0 \mid \exists K \forall c \geq 1 \ \Phi_A(c) \leq K c^\alpha\}$ . Although the preceding criterion seems too restrictive at first glance, it turns out that bounded “length” is essentially the only way that an operator algebra can have (SP), as the next result from [Pi9] shows.

**THEOREM 2.9.** *Let  $A$  be a unital operator algebra satisfying condition (CC). Then  $A$  satisfies (SP) iff there is a  $d$  such that  $A$  has length  $\leq d$ . More precisely,  $\ell(A) = d(A)$  and the infimum defining  $d(A)$  is a minimum attained when  $\alpha = \ell(A)$ .*

*Remark.* One surprising feature of this result is that there is apparently no direct a priori argument showing that  $d(A)$  is an integer. Note that even when  $A$  fails (CC), the preceding result can be applied to a suitably defined “enveloping algebra” of  $A$  satisfying (CC) (see [Pi9]).

**WARNING.** Until progress is made, the really weak point (embarrassing for the author) of the preceding statement is that, up to now, no example is known of  $A$  with  $3 < \ell(A) < \infty$ . However, an analog of the equality  $\ell(A) = d(A)$  is proved in [Pi9] in the more general framework of an operator space generating an operator algebra; in this generalized framework, it is easy to produce the desired examples. We refer the reader to [LM4] for a version of Theorem 2.9 adapted to dual operator algebras and weak- $*$  continuous morphisms.

**REMARK 2.10.** Here is a short list of the  $C^*$ -algebras which are known to have (SP): if  $A$  is a nuclear  $C^*$ -algebra (due to Bunce-Christensen, see [C1]) then  $d(A) \leq 2$  (and actually  $d(A) = 2$  unless  $\dim(A) < \infty$ ), if  $A = B(H)$  and  $\dim(H) = \infty$  we have (SP) and  $d(B(H)) = 3$  (see [H] for  $\leq 3$  and [Pi9] for  $\geq 3$ ). More generally if  $A$  has no tracial state, it has (SP) and  $d(A) \leq 3$ , in particular this holds if  $A = \mathcal{K}_1[B]$  with  $B$  an arbitrary unital  $C^*$ -algebra ([H]). (Note: if  $B$  is a non-self-adjoint unital operator algebra,  $A = \mathcal{K}_1[B]$  satisfies (SP) with  $d(A) \leq 5$ .) Let  $A$  be a  $C^*$ -algebra generating a semi-finite von Neumann algebra  $M$ , then

$d(A) \leq 2$  implies that  $M$  is injective ([Pi9]); in particular, if  $A$  is the reduced  $C^*$ -algebra of a discrete group  $G$ , we conclude that  $G$  is amenable. Finally, if  $A$  is a  $II_1$ -factor with property  $\Gamma$  (in particular if it is hyperfinite), it has  $(SP)$  with  $d(A) \leq 44$  (see [C2], the latter estimate can presumably be improved significantly.)

Let us return to the group case (Example 2.3). Then we define  $d(G) = d(\ell_1(G))$ . The following partial answer to Dixmier's question holds:

**THEOREM 2.11** ([Pi9]). *A discrete group  $G$  is amenable iff  $d(G) \leq 2$ . More precisely,  $G$  is amenable iff there is a constant  $K$  and  $\alpha < 3$  such that, for any u.b. representation  $\pi: G \rightarrow B(H)$ , there is an invertible  $\xi$  with  $\|\xi^{-1}\| \|\xi\| \leq K|\pi|^\alpha$  such that  $\xi^{-1}\pi(\cdot)\xi$  is a unitary representation. (When  $G$  is amenable, Dixmier [Di] and Day proved that the latter holds with  $K = 1$  and  $\alpha = 2$ ).*

**WARNING:** We know of no example of  $G$  such that  $2 < d(G) < \infty$ !

See [Pi9] for an analog of Theorem 2.9 in the group case: the relevant notion of length is like in Definition 2.7 with  $A = C^*(G)$ , but the diagonal matrices  $D_i$  are now restricted to have their entries in the set of scalar multiples of elements of  $G$  viewed, as usual, as embedded into  $A = C^*(G)$ . The notion of length can also be studied in the more general framework of a Banach algebra  $B$  generated by a subset  $\mathcal{B}$  of its unit ball, [Pi9, Pi10].

#### REFERENCES

- [B1] D. Blecher, Tensor products of operator spaces II. *Canad. J. Math.* 44 (1992), 75–90.
- [B2] \_\_\_\_\_, The standard dual of an operator space, *Pacific J. Math.* 153 (1992), 15–30.
- [B3] \_\_\_\_\_, A completely bounded characterization of operator algebras, *Math. Ann.* 303 (1995), 227–240.
- [B4] \_\_\_\_\_, A new approach to Hilbert  $C^*$ -modules, *Math. Ann.* 307 (1997) 253–290.
- [BL] J. Bergh and J. Löfström, *Interpolation spaces. An Introduction*, Springer-Verlag, New York, 1976.
- [BLM] D. Blecher and C. Le Merdy, On quotients of function algebras, and operator algebra structures on  $\ell_p$ , *J. Operator Theory* 34 (1995) 315–346.
- [BMP] D. Blecher, P. Muhly and V. Paulsen, Categories of Operator Modules (Morita Equivalence and projective Modules). *Memoirs Amer. Math. Soc.* To appear.
- [Bo] J. Bourgain, On the similarity problem for polynomially bounded operators on Hilbert space, *Israel J. Math.* 54 (1986), 227–241.
- [BP1] D. Blecher and V. Paulsen, Tensor products of operator spaces, *J. Funct. Anal.* 99 (1991), 262–292.
- [BP2] \_\_\_\_\_, Explicit constructions of universal operator algebras and applications to polynomial factorization, *Proc. Amer. Math. Soc.* 112 (1991), 839–850.

- [BRS] D. Blecher, Z. J. Ruan, and A. Sinclair, A characterization of operator algebras, *J. Funct. Anal.* 89 (1990), 188–201.
- [BS] D. Blecher and R. Smith. The dual of the Haagerup tensor product. *J. London Math. Soc.* 45 (1992) 126–144.
- [C1] E. Christensen, On non-self-adjoint representations of operator algebras , *Amer. J. Math.* 103 (1981), 817–834.
- [C2] \_\_\_\_\_, Similarities of  $II_1$  factors with property  $\Gamma$ , *Journal Operator Theory* 15 (1986), 281–288.
- [CE] M. D. Choi and E. Effros, Injectivity and operator spaces, *J. Funct. Anal.* 24 (1977), 156–209.
- [CES] E. Christensen, E. Effros, and A. Sinclair, Completely bounded multilinear maps and  $C^*$ -algebraic cohomology, *Invent. Math.* 90 (1987), 279–296.
- [CS1] E. Christensen and A. Sinclair, Representations of completely bounded multilinear operators, *J. Funct. Anal.* 72 (1987), 151–181.
- [CS2] \_\_\_\_\_, A survey of completely bounded operators, *Bull. London Math. Soc.* 21 (1989), 417–448.
- [Ca] T. K. Carne, Not all  $H'$ -algebras are operator algebras, *Proc. Camb. Phil. Soc.* 86 (1979), 243–249.
- [DP] K. Davidson and V. Paulsen, On polynomially bounded operators, *J. für die reine und angewandte Math.* 487 (1997), 153–170.
- [Di] J. Dixmier, Les moyennes invariantes dans les semi-groupes et leurs applications, *Acta Sci. Math. Szeged* 12 (1950), 213–227.
- [DJT] J. Diestel, H. Jarchow and A. Tonge, *Absolutely summing operators*, Cambridge University press, 1995.
- [DoP] R. Douglas and V. Paulsen, *Hilbert Modules Over Function Algebras*, Research Notes 217, Pitman-Longman, 1989.
- [E] E. Effros, *Advances in Quantized Functional Analysis*, Proceedings International Congress of Mathematicians, Berkeley, 1986, pp. 906–916.
- [EH] E. Effros and U. Haagerup, Lifting problems and local reflexivity for  $C^*$ -algebras, *Duke Math. J.* 52 (1985), 103–128.
- [EJR] E. Effros, M. Junge, and Z. J. Ruan, Integral mappings and the property of local reflexivity for non-commutative  $L_1$ -spaces, 1998, preprint.
- [ER1] E. Effros and Z. J. Ruan, Representations of operator bimodules and their applications, *J. Operator theory*, 19 (1988) 137–157.
- [ER2] \_\_\_\_\_, On approximation properties for operator spaces, *International J. Math.* 1 (1990), 163–187.
- [ER3] \_\_\_\_\_, A new approach to operator spaces, *Canadian Math. Bull.* 34 (1991), 329–337.
- [ER4] \_\_\_\_\_, Self duality for the Haagerup tensor product and Hilbert space factorization, *J. Funct. Anal.* 100 (1991), 257–284.



- [ER5] \_\_\_\_\_, On the abstract characterization of operator spaces, Proc. Amer. Math. Soc. 119 (1993), 579–584.
- [ER6] \_\_\_\_\_, Mapping spaces and liftings for operator spaces, Proc. London Math. Soc. 69 (1994), 171–197.
- [ER7] \_\_\_\_\_, The Grothendieck-Pietsch and Dvoretzky-Rogers Theorems for operator spaces, J. Funct. Anal. 122 (1994), 428–450.
- [ER8] \_\_\_\_\_, Discrete quantum groups I. The Haar measure, Internat. J. Math. 5 (1994) 681–723.
- [ER9] \_\_\_\_\_, On the  $OL_p$ -spaces. Preprint, 1998.
- [EWi] E. Effros and S. Winkler, Matrix convexity: operator analogues of the bipolar and Hahn-Banach theorems, J. Funct. Anal. 144 (1997) 117–152.
- [G] A. Grothendieck, Résumé de la théorie métrique des produits tensoriels topologiques, Boll. Soc. Mat. São-Paulo 8 (1956), 1–79 and 80–110.
- [Gr] M. Gromov, Hyperbolic groups, p. 75–265 in *Essays in Group Theory* (edited by S. Gersten), Springer-verlag, New-York, 1987.
- [H] U. Haagerup, Solution of the similarity problem for cyclic representations of  $C^*$ -algebras, Annals of Math. 118 (1983), 215–240.
- [HK] U. Haagerup and J. Kraus, Approximation properties for group  $C^*$ -algebras and group von Neumann algebras, Trans. Amer. Math. Soc. 344 (1994) 667–699.
- [JP] M. Junge and G. Pisier, Bilinear forms on exact operator spaces and  $B(H) \otimes B(H)$ , Geometric and Functional Analysis (GAFA Journal) 5 (1995), 329–363.
- [Ju1] M. Junge, *Factorization Theory for Spaces of Operators*, Habilitationsschrift, Kiel University, 1996.
- [Ju2] \_\_\_\_\_, Embeddings of non-commutative  $L_p$ -spaces in non-commutative  $L_1$ -spaces,  $1 < p < 2$ . Preprint Kiel University, June 1998.
- [K] R. Kadison, On the orthogonalization of operator representations, Amer. J. Math. 77 (1955), 600–620.
- [Ka] A. Katavolos (editor), *Operator algebras and applications*, (Proc. Conf. Samos, August 19–28, 1996), NATO ASIC, 495, Kluwer, Dordrecht, 1997.
- [Ki1] E. Kirchberg, Exact  $C^*$ -Algebras, Tensor Products, and Classification of Purely Infinite Algebras, Proceedings ICM 94, Zürich, vol.2, 943–954, Birkhauser, 1995.
- [Ki2] \_\_\_\_\_, On non-semisplit extensions, tensor products and exactness of group  $C^*$ -algebras, Invent. Math. 112 (1993), 449–489.
- [Ki3] \_\_\_\_\_, The derivation and the similarity problem are equivalent, J. Operator Theory, 36 (1996) 59–62.
- [Kis] S. V. Kislyakov. Operators (not) similar to a contraction: Pisier’s counterexample via singular integrals. Zapiski Nauchnykh Seminarov POMI, 247 (1997), p.79–95 (Russian). English translation in J. Math.Sci.

- [LM1] C. Le Merdy, Factorization of  $p$ -completely bounded multilinear maps, *Pacific J. Math.*, 172 (1996) 187-213.
- [LM2] \_\_\_\_\_, Representations of a quotient of a subalgebra of  $B(X)$ , *Math. Proc. Cambridge Phil. Soc.* 119 (1996), 83–90.
- [LM3] \_\_\_\_\_, On the duality of operator spaces, *Canad. Math. Bull.* 38 (1995), 334–346.
- [LM4] \_\_\_\_\_, The weak-\* similarity property on dual operator algebras, Preprint, 1998.
- [LM5] \_\_\_\_\_, The Schatten space  $S_4$  is a  $Q$ -algebra, *Proc. Amer. Math. Soc.* 126 (1998) 715-719.
- [LM6] \_\_\_\_\_, An operator space characterization of dual operator algebras, *Amer. J. Math.* (To appear).
- [LM7] \_\_\_\_\_, The similarity problem for bounded analytic semigroups on Hilbert space, *Semigroup Forum*, 56 (1998) 205–224.
- [Lu] A. Lubotzky, *Discrete groups, Expanding graphs and invariant measures*, Birkhauser 1994.
- [Ma] B. Magajna, Strong operator modules and the Haagerup tensor product, *Proc. London Math. Soc.* 74 (1997), 201–240.
- [MP] A. M. Mantero, J. Pytlik, R. Szwarc, and A. Zappa, Equivalence of two series of spherical representations of a free group. *Ann. Mat. Pura Appl.* 165 (1993) 23–28.
- [Oi] T. Oikhberg, Geometry of operator spaces and products of orthogonal projections, Ph. D. Thesis, Texas A&M University, 1998.
- [OiP] T. Oikhberg and G. Pisier, The “maximal” tensor product of operator spaces, *Proc. Edinburgh Math. Soc.*, to appear.
- [Ol] A. Yu. Olshanskii, *The geometry of defining relations in groups*, Kluwer, Dordrecht, 1991.
- [P1] V. Paulsen, *Completely Bounded Maps and Dilations*, Pitman Research Notes 146, Pitman-Longman, Wiley, 1986.
- [P2] \_\_\_\_\_, Representation of function algebras, abstract operator spaces and Banach space geometry, *J. Funct. Anal.* 109 (1992), 113–129.
- [P3] \_\_\_\_\_, The maximal operator space of a normed space, *Proc. Edinburgh Math. Soc.* 39 (1996), 309–323.
- [Pi1] G. Pisier, The operator Hilbert space  $OH$ , complex interpolation and tensor norms, *Memoirs Amer. Math. Soc.* 122, 585 (1996), 1–103.
- [Pi2] \_\_\_\_\_, Non-commutative vector valued  $L_p$ -spaces and completely  $p$ -summing maps, *Astérisque (Soc. Math. France)*, 247 (1998), 1–111.
- [Pi3] \_\_\_\_\_, A simple proof of a theorem of Kirchberg and related results on  $C^*$ -norms, *J. Operator Theory* 35 (1996), 317–335.

- [Pi4] \_\_\_\_\_, Exact operator spaces. Colloque sur les algèbres d'opérateurs, in *Recent Advances in Operator Algebras*, Astérisque 232 (1995), 159–186.
- [Pi5] \_\_\_\_\_, An introduction to the theory of operator spaces, to appear.
- [Pi6] \_\_\_\_\_, Dvoretzky's theorem for operator spaces and applications, *Houston J. Math.* 22 (1996), 399–416.
- [Pi7] \_\_\_\_\_, *Similarity Problems and Completely Bounded Maps*, Springer Lecture Notes 1618, 1995.
- [Pi8] \_\_\_\_\_, A polynomially bounded operator on Hilbert space which is not similar to a contraction, *J. Amer. Math. Soc.* 10 (1997), 351–369.
- [Pi9] \_\_\_\_\_, The similarity degree of an operator algebra, *St. Petersburg Math. J.* (1998), to appear.
- [Pi10] \_\_\_\_\_, Joint similarity problems and the generation of operator algebras with bounded length, *Integr. Equ. Op. Th.*, to appear.
- [PS] V. Paulsen and R. Smith, Multilinear maps and tensor norms on operator systems, *J. Funct. Anal.* 73 (1987), 258–276.
- [Ro] H. P. Rosenthal, The complete separable extension property, Preprint 1998.
- [Ru1] Z. J. Ruan, Subspaces of  $C^*$ -algebras, *J. Funct. Anal.* 76 (1988), 217–230.
- [Ru2] \_\_\_\_\_, Injectivity and operator spaces, *Trans. Amer. Math. Soc.* 315 (1989) 89-104.
- [Ru3] \_\_\_\_\_, The operator amenability of  $A(G)$ , *Amer. J. Math.* 117 (1995) 1449-1474.
- [Ru4] \_\_\_\_\_, Amenability of Hopf von Neumann algebras and Kac algebras, *J. Funct. Anal.* 139 (1996) 466-499.
- [SSm] A. M. Sinclair and R. R. Smith, *Hochschild cohomology of von Neumann algebras*, Cambridge Univ. Press, LMS lecture notes 203, Cambridge 1995.
- [Sz] A. Szankowski,  $B(H)$  does not have the approximation property, *Acta Math.* 147 (1981), 89–108.
- [Va] A. Valette, An application of Ramanujan graphs to  $C^*$ -algebra tensor products, *Discrete Math.* 167/168 (1997) 597-603.
- [Wa] S. Wassermann, *Exact  $C^*$ -Algebras and Related Topics*, Lecture Notes Series, Seoul Nat. Univ., 1994.
- [Z] C. Zhang, *Representation and Geometry of Operator Spaces*, Ph.D. Thesis, University of Houston, 1995.

Gilles Pisier  
 Texas A&M University,  
 College Station, TX 77843, USA  
 and Université Paris 6,  
 Equipe d'Analyse, Case 186,  
 4 Place Jussieu,  
 75252 Paris Cedex 05, France

## L-FUNCTIONS

PETER SARNAK

### SECTION 1. THE FUNDAMENTAL CONJECTURES

Since Hecke’s work [0], the theories of  $L$ -functions and of automorphic forms have been closely interwoven. In this talk, we review some recent developments concerning the analytic aspects of these topics. In the case of the Riemann Zeta Function  $\zeta(s)$  and Dirichlet’s  $L$ -functions  $L(s, \chi)$  (that is “ $GL_1$  over  $\mathbb{Q}$ ”  $L$ -functions) developments during the 1960’s and 1970’s see [1,2] offer a large body of techniques and results with many striking applications to classical number theory. Today the same can be said about  $L$ -functions of modular forms on the upper half plane  $\mathbb{H}$  (that is “ $GL_2$   $L$ -functions”) these being the main concern below. We begin however with the general  $L$ -function which in any case has important impact on  $GL_2$   $L$ -functions.

Fix  $m \geq 1$  and let  $\pi$  be an automorphic *cuspidal* form (or representation) for  $GL_m(\mathbb{Q})$  (later in connection with Conjecture II below we also allow  $GL_m(K)$ , where  $K$  is a number field). That is  $\pi$  is an irreducible unitary representation of  $GL_m(\mathbb{A})$  (which we assume has a unitary central character) which appears in its regular representation on  $GL_m(\mathbb{Q}) \backslash GL_m(\mathbb{A})$ ,  $\mathbb{A}$  being the adèle ring of  $\mathbb{Q}$ . Then  $\pi \cong \otimes \pi_p$ , where  $\pi_p$  is an irreducible unitary representation of  $GL_m(\mathbb{Q}_p)$  if  $p < \infty$  and of  $GL_m(\mathbb{R})$  if  $p = \infty$ . Moreover, for all but a finite number of places  $p$ ,  $\pi_p$  is unramified. The (standard)  $L$ -function,  $L(s, \pi)$  associated with such a  $\pi$  is an Euler product of degree  $m$ :

$$L(s, \pi) = \prod_{p < \infty} L(s, \pi_p) \tag{1}$$

where

$$L(s, \pi_p) = \prod_{j=1}^m (1 - \alpha_{j,\pi}(p)p^{-s})^{-1} \tag{2}$$

The numbers  $\{\alpha_{j,\pi}(p)\}_{j=1}^m$  are determined from the local representation  $\pi_p$ . At the place  $\infty$  the local factor  $L(s, \pi_\infty)$  is a product of Gamma functions which if  $\pi_\infty$  is unramified takes the form

$$L(s, \pi_\infty) = \prod_{j=1}^m \left( \pi^{-s/2} \Gamma \left( \frac{s - \mu_{j,\pi}(\infty)}{2} \right) \right) \tag{3}$$

As with  $\zeta(s)$  and  $L(s, \chi)$  the key analytic properties of  $L(s, \pi)$  are known [3]. These being the analytic continuation and functional equation:

$$L(s, \pi_\infty) L(s, \pi) = \epsilon_\pi q_\pi^{s-1/2} L(1-s, \tilde{\pi}_\infty) L(1-s, \tilde{\pi}) \tag{4}$$

where  $q_\pi \in N$  is the conductor of  $\pi$ ,  $\epsilon_\pi$  is of modulus 1 and is the “sign” of the functional equation and  $\tilde{\pi}$  is the contragredient of  $\pi$  [4]. We let  $\lambda_\pi$  be the quantity  $(\sum_{j=1}^m |\mu_{j,\pi}(\infty)|^2)^{1/2}$  and call it the archimedean size of  $\pi$ .

General philosophies and conjectures [5] (which among other things encompass the Artin conjectures) assert that any  $L$ -function (from automorphic forms on more general groups over number fields or from varieties defined over number fields) are products of these  $L(s, \pi)$ 's. These are therefore the primitive objects in the theory of  $L$ -functions. Undoubtedly the two central analytic problems in the theory are:

- I. The Grand Riemann Hypothesis (GRH), which asserts that the zeroes of the completed  $L$ -function  $\xi(s, \pi) = L(s, \pi_\infty) L(s, \pi)$  all lie on  $\text{Re}(s) = 1/2$ .
- II. The (generalized) Ramanujan conjectures [100]: if  $\pi_p$  is unramified then

$$|\alpha_{j,\pi}(p)| = 1$$

while if  $\pi_\infty$  is unramified

$$\text{Re}(\mu_{j,\pi}(\infty)) = 0.$$

There are no known direct relations between Conjectures I for these different primitive  $L$ -functions and it is of course possible that the original RH [6] is true for  $\zeta(s)$  but that it fails for some general  $L(s, \pi)$ . This however seems unlikely and the theme of this report is the role played by *families* of  $L$ -functions which may often be employed to analyze a given  $L(s, \pi)$ .

Conjectures I and II have many far reaching implications. The most interesting applications of Conjecture I follow from its use for a *family* of  $L$ -functions rather than for a single function such as  $\zeta(s)$ . While these Conjectures remain out of reach at present, the approximations to them, some of which are described below, lead in many cases to the resolution of the problem at hand. Conjecture II for  $m = 1$  is trivial. For  $m = 2$  there are some important special cases (including Ramanujan's original one) known [7,96,8] (interestingly, the proof in these cases involves reducing Conjecture II to function field generalizations of Conjecture I). The case when  $m = 2$  for the place at  $\infty$  is equivalent to the conjecture that the first eigenvalue of the Laplacian on the hyperbolic quotient  $\Gamma(N)\backslash\mathbb{H}$ ,  $\Gamma(N)$  being the congruence subgroup  $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv I(N); a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$ , is at least  $1/4$  [9]. The local bounds towards II which use only that  $\pi_p$  and  $\pi_\infty$  are generic [10] assert that

$$p^{-1/2} < |\alpha_{j,\pi}(p)| < p^{1/2}$$

and

$$|\text{Re}(\mu_{j,\pi}(\infty))| < \frac{1}{2}$$

To go beyond this basic bound one uses global methods. In particular, the use of *families* of  $L$ -functions as described below lead to the best known results.

Associated with  $\pi$  as above are other  $L$ -functions which have conjectured analytic continuations and functional equations. First and foremost is  $L(s, \pi \otimes \tilde{\pi})$  [11], [12], [13] whose analytic properties are completely understood [14], [15]. The local factor  $L(s, \pi_p \otimes \tilde{\pi}_p)$  at a prime  $p$  at which  $\pi$  is unramified is given by

$$L(s, \pi_p \otimes \tilde{\pi}_p) = \prod_{j,k} \left(1 - \alpha_{j,\pi}(p) \overline{\alpha_{k,\pi}(p)} p^{-s}\right)^{-1} \quad (6)$$

There are other important cases which are partially understood such as  $L(s, \text{sym}^2 \pi)$  where  $\text{sym}^2 \pi$  is the symmetric square representation [16], [17]. In fact, for  $\pi$  on  $GL_2$  the analytic theory of the symmetric square  $L$ -function is complete [18], [19] and recently the same has been achieved for the symmetric cube [20]. For a survey of these techniques, results and their limitations see [21], [22], [23]. We note that establishing the expected analytic properties of  $L(s, \text{sym}^k \pi)$  for all  $k$  would lead to a proof of Conjecture II, as well as the conjecture about the distribution of the  $\{\alpha_{j,\pi}(p)\}_{j=1}^m$  as  $p \rightarrow \infty$ .

The basic result towards I, which in the case of  $\zeta(s)$  is the key ingredient in the proof of the prime number theorem and is based on the non-negativity of the coefficients of associated Dirichlet series, is that  $L(s, \pi) \neq 0$  for  $\text{Re}(s) = 1$ . This general result may be proven by this 100 year old technique together with the analytic properties of  $L(s, \pi \otimes \tilde{\pi})$  (or one may use the Eisenstein series directly [24] which yields the *same* zero-free region). The quality of the lower bound for  $L(1+it, \pi)$  (or equivalently a zero-free region) in terms of the parameters  $t, \lambda_\pi, q_\pi$  is more or less the same in all cases except for one major (and tantalizing) lacuna - the possible “Landau-Siegel Zero.” That is in the case that  $\chi$  is a quadratic ( $\chi^2 = 1$ ) Dirichlet character, then instead of an *effective* lower bound for  $L(1, \chi)$  of the form  $\gg (\log q_\chi)^{-1}$  which is established for the other  $\chi$ 's, only the lower bounds of  $(\log q_\chi)/\sqrt{q_\chi}$  when  $\chi(-1) = 1$  [25] and of  $\frac{\log q_\chi}{\sqrt{q_\chi}} \prod_{\substack{p \mid q_\chi \\ p \neq q_\chi}} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right)$  when

$\chi(-1) = -1$  [26], [27], are known (the latter has striking applications to class numbers of imaginary quadratic fields and is a prime example of an application of  $GL_2$  theory to  $GL_1$ ). Put another way, there may be an  $L(s, \chi)$  with a real zero very close to 1 (in terms of the conductor), which we call a Landau-Siegel Zero [28], [29]. Interestingly, it appears that only such a  $\chi$  ( $\chi^2 = 1$ ) can have such an extreme violation of I. In [30] and [32] it is shown (using the positivity of the coefficients of an appropriate Dirichlet series) that for any  $GL_2$  form  $\pi$  as well as its symmetric square (if it is not of “CM” type) there are no Landau-Siegel zeroes. The last is technically very useful especially when applying the Petersson formula [31] and its generalization [33], see for example [34].

## SECTION 2. SUB-CONVEXITY

A consequence of Conjectures I and II which is used in many of their applications is the “Lindelof Hypothesis” which asserts that for any  $\pi$  on  $GL_m$  ( $m$  fixed) and  $\epsilon > 0$  there is  $C_\epsilon < \infty$  such that

$$\left| L\left(\frac{1}{2} + it, \pi\right) \right| \leq C_\epsilon (|t| + 1)^m (\lambda_\pi + 1) q_\pi^\epsilon \quad (7)$$

The functional equation (4) together with II and a standard convexity argument in complex analysis imply that

$$\left| L\left(\frac{1}{2} + it, \pi\right) \right| \leq C_\epsilon (|t| + 1)^m (\lambda_\pi + 1) q_\pi^{1/4 + \epsilon} \quad (8)$$

Some of the most interesting applications of (7), (for example, to estimation of Fourier coefficients of  $1/2$ -integral weight modular forms [35] or to problems in Quantum Chaos [36]) require only a sub-convexity bound in (8) - that is, in one of the  $t$ ,  $\lambda$  or  $q$  aspects an exponent  $\delta < 1/4$  in (8). In  $GL_1$  the first such bound is essentially due to Weyl [37] in the  $t$ -aspect while [38] is still the best known in the  $q$ -aspect. For  $GL_2$ , the series of papers [39], [40], [41], [42], [43] establish sub-convexity bounds in each of the  $\lambda$ ,  $q$  and  $t$ -aspects. An application of this in the  $t$ -aspect to quantum unique ergodicity is given in [34] while when applied in the  $q$ -aspect to  $L(\frac{1}{2}, \pi \otimes \chi_q)$ ,  $\chi_q^2 = 1$  ( $\pi$  fixed), it yields a solution (albeit ineffective due to the possible Landau-Siegel zero) of the long standing problem of determining which large integers are represented by a positive definite integral ternary quadratic form [44]. The novel technique leading to the sub-convexity estimate is “amplification” which proceeds by embedding  $L(s, \pi)$  in a suitable family  $\mathcal{F}$  of  $L$ -functions. See [45] for a description of the method and [46] and [47] for some other instances of its use. An interesting and basic problem is to develop sub-convexity bounds in the various aspects for  $\pi$ 's on  $GL_m$ ,  $m \geq 3$ .

### SECTION 3. LOCAL DISTRIBUTION OF ZEROES

The asymptotics of the number of zeroes  $\rho_\pi$  of  $\xi(s, \pi)$  is well known. As  $T \rightarrow \infty$

$$\#\{\rho_\pi | 0 \leq \text{Im}(\rho_\pi) \leq T\} \sim \frac{mT \log T}{2\pi} \quad (9)$$

For  $GL_1$   $L$ -functions, it is shown in [48] that a positive proportion of these zeroes are on the line,  $\text{Re}(s) = 1/2$ . The proof is based on a technique called “mollification” and it has been used to establish a similar result for  $GL_2$   $L$ -functions [49]. Another approach to this type of result was introduced in [50]. It has the advantage of producing simple zeroes and in [51] this method was developed further to show that at least 40% of the zeroes of  $\zeta(s)$  are on  $\text{Re}(s) = 1/2$  and are simple.

For the rest of this section we will assume Conjecture I and discuss the fine structure of the distribution of the zeroes. This is of interest both in arithmetic applications as well as giving insight into the nature (eg spectral) of the zeroes. Write the zeroes  $\rho_\pi$  as  $\frac{1}{2} + i\gamma_\pi$  and order them:

$$\dots \leq \gamma_\pi^{(-2)} \leq \gamma_\pi^{(-1)} \leq 0 \leq \gamma_\pi^{(1)} \leq \gamma_\pi^{(2)} \dots \quad (10)$$

In view of (9), in order to examine the distribution of the *local* spacings between the zeroes we re-normalize and consider the numbers  $\hat{\gamma}_\pi^{(j)} = (m\gamma_\pi^{(j)} \log \gamma_\pi^{(j)})/2\pi$ ,  $j \geq 1$ . Their consecutive spacings are the numbers  $\hat{\gamma}_\pi^{(j+1)} - \hat{\gamma}_\pi^{(j)}$ . The pair correlation is the local density of the numbers  $\hat{\gamma}_\pi^{(j)} - \hat{\gamma}_\pi^{(k)}$ ,  $j \neq k \leq N$  (as  $N \rightarrow \infty$ ). The  $k$ -th ( $k \geq 2$ ) consecutive spacings and  $n \geq 3$  correlations are defined similarly

[58]. For the zeroes of  $\zeta(s)$  it was shown in [52] that for a restricted class of test functions the pair-correlation density approaches the density  $\left(1 - \left(\frac{\sin \pi x}{\pi x}\right)^2\right) dx$ , as  $N \rightarrow \infty$ . It was further noted there that this density is the same as the known [53] pair-correlation density for the eigenvalues of a typical (for Haar measure) large unitary matrix [54]. This ensemble of random matrices has been much studied by Physicists [55] (for example in connection with models for the spectral lines of heavy nuclei) and goes by the name the Circular Unitary Ensemble, (CUE). All the local spacing statistics for the eigenvalues of a random matrix in this ensemble are the same as for the related Gaussian Unitary Ensemble (GUE) [54]. In [56] a detailed numerical investigation of the hypothesis that the local spacing distributions of the high zeroes of  $\zeta(s)$  follow CUE laws, has been carried out. In particular, the local spacing distributions for the 70 million zeroes near the  $10^{20}$ -th zero follow the CUE predictions (almost perfectly!). In [57], the  $n = 3$  and in [58] all the  $n$ -level correlations are determined analytically (again in restricted ranges). The results being precisely the CUE  $n$ -level correlation densities. At the phenomenological level, this CUE feature is perhaps the most interesting discovery about  $\zeta(s)$  since Riemann's Conjecture I and it points to the spectral nature of the zeroes. In [58] the  $n \geq 2$  correlations are determined for *any*  $L(s, \pi)$  and are found to be *universally* CUE. Numerical experiments for various  $\pi$ 's in  $GL_1$  [59] and  $GL_2$  [60] strongly confirm this CUE phenomenon. Thus, unlike the distributions of the  $\{\alpha_{j,\pi}(p)\}_{j=1}^m$  as  $p \rightarrow \infty$ , which depend on the symmetry type of  $\pi$ , the local distributions of the high zeroes of any  $L(s, \pi)$  appear to be universally CUE.

The function field analogues of  $\zeta(s)$  offer much insight into the above. Replacing the rational numbers  $\mathbb{Q}$  by a finite extension  $k$  of  $\mathbb{F}_q(t)$ ,  $\mathbb{F}_q$  being a finite field with  $q$ -elements, one obtains an analogue of  $\zeta(s)$  due to Artin [61]. If  $C$  is a curve over  $\mathbb{F}_q$  with function field  $k$  then the associated zeta function  $\zeta(T, C/\mathbb{F}_q)$  is a rational function with  $2g$  zeroes, where  $g$  is the genus of  $C$ . The analogue of Conjecture I in this setting has been known for over 50 years [97]. The Frobenius morphism on  $C$  is intimately related to  $\zeta(T, C/\mathbb{F}_q)$  and is crucial in the proofs of I. In [62] the local spacings between the zeroes of  $\zeta(T, C/\mathbb{F}_q)$  is examined. It is shown that as  $q$  and  $g(C)$  go to infinity the zeroes of the typical (but not every!)  $\zeta(T, C/\mathbb{F}_q)$  obey the CUE spacing laws. The sources of this law are clearly identified as: (A) The monodromy of the representation of  $\pi_1$  of the family of curves of genus  $g$  on  $H^1$  of a given curve is "big," it being  $Sp(2g)$ . (B) The equidistribution of the Frobenius conjugacy classes in the monodromy [8]. (C) The (universal) law for the eigenvalue spacings for the typical matrix in *any* large compact classical group being CUE [62].

In this function field setting, one can also determine the distributions of the zeroes near the point of symmetry (for the functional equation), for a family of zeta or  $L$ -functions. Again, this follows from the calculation of these distributions for the scaling limits of the monodromy groups of the family and unlike the universality above, these are found to be sensitive to the symmetry of the family [62]. The analogous questions in the rational number case, for various families  $\mathcal{F}$  of  $L(s, \pi)$ 's, has been investigated recently [63]. Ordering the  $\pi \in \mathcal{F}$  by their conductors  $q_\pi$  one examines the distribution of the (scaled) *low-lying* zeroes. That is, for  $j \geq 1$  fixed,



the distribution in  $[0, \infty)$  of the numbers  $(\gamma_\pi^{(j)} \log q_\pi)/2\pi$ , as  $\pi$  varies over  $\mathcal{F}^1$ , and the densities of the numbers  $(\gamma_\pi \log q_\pi)/2\pi$  again as  $\pi$  varies over  $\mathcal{F}$ . It is found [63], [64] that these follow the distributions predicted by the symmetry of the family  $\mathcal{F}$ , when the latter can be determined from the function field analogue. For example, for the family  $\mathcal{F}_I$  of  $L(s, \chi)$ 's where  $\chi$  is a quadratic ( $\chi^2 = 1$ ) Dirichlet character, the distribution of the low-lying zeroes follows the *symplectic*  $Sp(\infty)$  scaling distributions [62]. This is convincingly confirmed by numerical experiments [60] for  $q_\chi$ 's of size  $10^{12}$ . Further confirmation is given by the analytic determination (in restricted ranges) of the densities of the low-lying zeroes for this family [65], [63], [60]. Another example is the family  $\mathcal{F}_{II}$  of holomorphic cusp forms  $\pi$  of weight 2 for the congruence subgroups  $\Gamma_0(N)$  of the modular group. The symmetry type of  $\mathcal{F}_{II}$  is *orthogonal* ie  $O(\infty)$ , at least as far as the analytic computations of the densities of the low-lying zeroes [64].

The above densities of the low-lying zeroes in a family determine in particular the percentages of  $\pi \in \mathcal{F}$  for which  $L(1/2, \pi) = 0$  (or it's derivative if  $L(1/2, \pi) = 0$  for the trivial reason of the sign of the functional equation). For certain families such as  $\mathcal{F}_{II}$  above this together with the Birch and Swinnerton-Dyer Conjectures [94] give information about the ranks of the group of rational points on elliptic curves and abelian varieties over  $\mathbb{Q}$ . In particular, for  $\mathcal{F}_{II}$  above one obtains from the analytic results on the densities [66], [67], [64], sharp estimations for the ranks of the Jacobian  $J_0(N)/\mathbb{Q}$  of the curves  $X_0(N)/\mathbb{Q}$  (which analytically is  $\Gamma_0(N)\backslash\mathbb{H}$ ) as well as for the dimension of largest quotient  $M_0(N)/\mathbb{Q}$  ([68], [69]) of  $J_0(N)$  which is of rank zero.

While for the above families  $\mathcal{F}$  as well as for numerous others [63], [64] the proposed symmetry " $G(\mathcal{F})$ " is compelling, it is premature to guess whether it is appropriate for all families. The reason being, that numerical experiments (for moderate size conductors) with certain families of elliptic curves [70], [71] indicate that their ranks are persistently larger than the symmetry (as well as the function field) predicts. Whether this "excess rank" is a consequence of too small a range of computation or whether it is truly there, is a fascinating question whose understanding will no doubt be very instructive.

#### SECTION 4. NON-VANISHING FOR FAMILIES

The question of the number of  $\pi$ 's in  $\mathcal{F}$  (ordered by conductor) for which  $L(s, \pi)$  is non-zero at a special point arises in a number of contexts. In the basic problem of existence of *cusps* forms for general subgroups of  $SL_2(\mathbb{R})$  [72], in the correspondence between forms of  $1/2$ -integral weight and integral weight [73], [74] and in connection with the Birch and Swinnerton-Dyer Conjecture. There are many results asserting that infinitely many  $\pi \in \mathcal{F}$  have their  $L$ -function not zero at a specific point and in some cases even good lower bounds for the number of such  $\pi$ 's. For example, for the family  $\pi_1 \otimes \pi$  with  $\pi_1$  fixed on  $GL_2$  and  $\pi$  varying (with fixed conductor) by increasing  $\lambda_\pi$ , non-vanishing at special points on the critical line are established in [75], [76]. These have applications to the problem of existence of cusp forms mentioned above. For the family of quadratic twists  $\chi$  of

---

<sup>1</sup>We apologize for the bad notation and hope the reader does not get too confused between  $\pi$  the number and  $\pi$  the representation.

a given (modular) elliptic curve  $E/\mathbb{Q}$  it is shown in [77] and [78] that infinitely many of the values  $L(\frac{1}{2}, E \otimes \chi)$  are not zero and also infinitely many of the values  $L'(\frac{1}{2}, E \otimes \chi)$  are not zero for  $\chi$ 's with  $\epsilon_{E \otimes \chi} = -1$ . This, when combined with [79] has applications to the B-S conjecture for elliptic curves. A challenging unsolved problem which as yet is at the limit of the analytic methods [80] is to show that a positive proportion of the values  $L(\frac{1}{2}, E \otimes \chi)$  are not zero. The results on the densities of low-lying zeroes for this family (of Section 3) imply this, however, they appeal to Conjecture I. For special  $E$ 's a positive proportion of non-vanishing has been established by algebraic methods [81], [82]. In the "vertical" case of twisting such  $L$ -functions by  $\chi$ 's of high order, non-vanishing results are proven in [91].

For the family  $\mathcal{F}_{II}$  of Section 3, it is shown in [83] that at least 50% of the  $L(\frac{1}{2}, \pi)$ 's are non-zero, where  $\pi$  varies over cusp forms of (say) weight 2 for  $\Gamma_0(N)$  and with  $\epsilon_\pi = 1$ , as  $N \rightarrow \infty$ . (Based on numerical calculations [66] it is conjectured that 100% of these should be non-zero). This result when combined with [79] implies that the dimension of  $M_0(N)$  is at least 1/4 of the dimension of  $J_0(N)$ , as  $N \rightarrow \infty$ . The number 50% above is of fundamental significance (for this as well as for a number of other families [83]) since any improvement of the percentage (in the quantitative form in which the 50% is established) would lead to a proof that there are no Landau-Siegel zeroes! This type of relation, that the distribution of the low-lying zeroes of a family are controlled by the zeroes of other  $L$ -functions, is not surprising from the function field analysis mentioned in Section 3, see [62]. The proof of this 50% result uses amongst many things an appropriate method of mollification. The proof of the implication to Landau-Siegel zeroes makes use of the following result which is proven either using forms of 1/2-integral weight or the relative trace formula [74], [84]: Let  $\pi$  be a (self-dual) cusp form with trivial central character for  $GL_2/K$ ,  $K$  a number field, then  $L(\frac{1}{2}, \pi) \geq 0$ . Note that since  $L(s, \pi)$  is real for  $s \in \mathbb{R}$  this inequality is an immediate consequence of Conjecture I for  $L(s, \pi)$ . That it can be proven unconditionally is quite striking especially since the  $GL_1$  analogue - that is  $L(\frac{1}{2}, \chi) \geq 0$ ,  $\chi$  quadratic, is not known. Returning  $J_0(N)$ , in [85] and [86] non-vanishing results are established which together with [27] imply that the rank of  $J_0(N)$  is at least 7/16 of  $\dim J_0(N)$ .

The non-vanishing in a family is also a very powerful tool in attacking Conjecture II. The approach via the family of  $L$ -functions,  $L(s, \pi \otimes \bar{\pi} \otimes \chi)$  as  $\chi$  varies over Dirichlet characters was initiated in [87]. It was convincingly applied in [88] to give estimates for  $\alpha_\pi(p)$ ,  $p$  finite, where  $\pi$  is a Maass cusp form on  $GL_2/\mathbb{Q}$ . In [89] a general approach via *non-vanishing* of partial  $L$ -functions at special points in such a family, was introduced. It leads to the best known bounds towards Conjecture II [90]. If  $\pi$  is an automorphic cusp form for  $GL_m(K)$  and  $\pi$  is unramified at a place  $v$  of  $K$ , then

$$\left| \log_{N(v)} |\alpha_{j,\pi}(v)| \right| \leq \frac{1}{2} - \frac{1}{m^2 + 1}, \quad \text{if } v \text{ is finite and } N(v) \text{ its norm} \quad (11)$$

$$\left| \operatorname{Re}(\mu_{j,\pi}(v)) \right| \leq \frac{1}{2} - \frac{1}{m^2 + 1} \quad \text{for } v \text{ archimedean} \quad (12)$$

This result for  $GL_3$  combined with the symmetric square correspondence from

$GL_2 \rightarrow GL_3$  [19] leads to the bounds on  $GL_2$ :

$$\left| \log_{N(v)} |\alpha_{j,\pi}(v)| \right| \leq \frac{1}{5}, \quad \text{if } v \text{ is finite} \quad (13)$$

$$\left| \operatorname{Re}(\mu_{j,\pi}(v)) \right| \leq \frac{1}{5}, \quad v \text{ archimedean} \quad (14)$$

Interestingly (13) was derived earlier in [92] by special use of the exceptional group  $F_4$ . (14) implies a lower bound of 21/100 for the first eigenvalue of the Laplacian on  $\Gamma_0(N)\backslash\mathbb{H}$ . This goes beyond the 3/16 bound [9] which was based on estimating sums of Kloosterman sums using [93]. Thus (14) provides for the first time cancellations in sums of Kloosterman sums on arithmetic progressions [89].

## SECTION 5. FINAL COMMENTS

We note that numerical experimentation played a key role in the discoveries and (or) confirmations of Conjecture I by Riemann, of Conjecture II by Ramanujan, of the Conjecture of Artin [61] and that of Birch and Swinnerton-Dyer [94].

While we may still have to wait for some time for the complete resolutions of Conjectures I and II, these like other fundamental problems have generated marvellous mathematics. Various things are falling into place. The function field analogues are very suggestive and the evidence for there being a natural spectral interpretation of the zeroes <sup>2</sup> as well as a symmetry group for families is rather convincing. The last bodes well since in the function field the proof of the general cases of Conjecture I make essential use of monodromy of families [8]. Similarly at the present time the most powerful techniques (in the number field case) have emerged from considerations of families. Averaging over families in  $GL_2$  theory is usually achieved by the trace formula [95] but often and more profitably, it can be gotten from the older Petersson formula [31]. The approximations to Conjectures I and II that have been established are good enough in many instances to resolve completely some classical problems.

## REFERENCES

0. E. Hecke, "Mathematische Werke", Göttingen, (1959).
1. H. Davenport, "Multiplicative Number Theory", Springer Verlag, G.T.M., (1974).
2. H. Montgomery, "Topics in Multiplicative Number Theory", L.N.M., 227, Springer, (1971).
3. R. Godement and H. Jacquet, "Zeta Functions of Simple Algebras", L.N.M., 260, Springer, (1972).
4. H. Jacquet, "Principal  $L$ -functions of the Linear Group", *Proc. Sym. Pure Math.*, Vol. 33, A.M.S., Part 2, 63–86, (1979).

---

<sup>2</sup>In [98] an interesting possibility for such a spectral interpretation is given while in [99] evidence for a cohomological formalism and interpretation is put forth.

5. R. Langlands, “Problems in the Theory of Automorphic Forms”, Springer, L.N.M., 170, 18–86, (1970).
6. B. Riemann, “Über die Anzahl der Primzahlen über einer gegebenen Größe”, Monatsb. der Berliner Akad., (1858160), 671–680.
7. M. Eichler, “Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion”, *Ark. de Math.*, 5, 355–366, (1954).
8. P. Deligne, “La Conjecture de Weil I and II” *Publ. I.H.E.S.*, 43, 273–307, (1974), 52, 313–428, (1981).
9. A. Selberg “On the Estimation of Fourier Co-efficients of Modular Forms”, *Proc. Sym. Pure Math.*, 8, 1–15, (1965).
10. H. Jacquet and J. Shalika, “On Euler Products and the Classification of Automorphic Representations”, I, II, *Amer. J. Math.*, 103, 499–557, 777–815, (1981).
11. R. Rankin, “Contributions to the Theory of Ramanujan’s Function  $\tau(n)$ ”, *Proc. Camb. Phil. Soc.*, 35, 351–356, (1939).
12. A. Selberg, “Bemerkungen über eine Dirchletsche Reihe, die mit der Theorie der Modulformen nahe verbunden ist”, *Arch. Math. Naturvid*, 43, 47–50, (1940).
13. H. Jacquet, I. Piatetski-Shapiro, J. Shalika, “Rankin-Selberg Convolutions”, *Amer. J. Math.*, 105, 367–464, (1983).
14. F. Shahidi, “On Certain  $L$ -functions”, *Amer. J. Math.*, 103, 297–355, (1981).
15. C. Moeglin, J. Waldspurger, “Le Spectre Residuel de  $GL(n)$ ”, *Ann. Sci. Ecole Norm.*, Sup (4), 22, 605–674, (1989).
16. S. Patterson, I. Piatetski-Shapiro, “The Symmetric-Square  $L$ -function Attached to a Cuspidal Automorphic Representation of  $GL(3)$ ”, *Math. Ann.*, 283, No. 4, 1–72, (1989).
17. D. Bump, D. Ginzburg, “Symmetric Square  $L$ -functions on  $GL(r)$ ”, *Ann. Math.* 136, 137–205, (1992).
18. G. Shimura, “On the Holomorphy of Certain Dirichlet Series”, *Proc. London Math. Soc.*, Soc. (3), 31, 79–98, (1975).
19. S. Gelbart, H. Jacquet, “A relation Between Automorphic Representations of  $GL(2)$  and  $GL(3)$ ”, *Ann. Sci. Ecole Norm. Sup* 4, 11, 471–542, (1978).
20. H. Kim, F. Shahidi, “Symmetric Cube  $L$ -functions for  $GL_2$  are Entire”, (preprint, 1998).
21. D. Bump, “The Rankin-Selberg Method: A Survey”, in Number Theory, Trace Formulas and Discrete Groups, Editors, Aubert, Bombieri, Goldfeld, Academic Press, 49–109, (1988).
22. F. Shahidi, “Automorphic  $L$ -functions: A Survey”, in Automorphic Forms, Shimura Varieties and  $L$ -functions, Editors, Clozel, Milne, Academic Press, 415–437, (1990).

23. D. Ginzburg, S. Rallis, “A Tower of Rankin-Selberg Integrals”, *IMRN*, Vol. 5, 201–208, (1994).
24. H. Jacquet, J. Shalika, “A Non-vanishing Theorem for Zeta Functions on  $GL_n$ ”, *Inv. Math.*, 38, 1–16, (1976).
25. G. Lejeune Dirichlet, “Dirichlet Werke”, Berlin, (1889).
26. D. Goldfeld, “Gauss Class Number Problem for Imaginary Quadratic Fields”, *B.A.M.S.* Vol. 13, 1, 23–37, (1985).
27. B. Gross, D. Zagier, “Heegner Points and Derivatives of  $L$ -series”, *Inv. Math.*, 84, 225–320, (1986).
28. E. Landau, “Bemerkungen zum Heilbronnschen Satz”, *Acta Arith.*, 1, 1–18, (1935).
29. C. Siegel, “Über die Classenzahl quadratischer Zahlkörper”, *Acta Arith.*, 1, 83–86, (1935).
30. J. Hoffstein, P. Lockhart, D. Goldfeld, D. Lieman, “Co-efficients of Maass Forms and the Siegel Zero”, *Annals of Math.*, 140, 177–181, (1994).
31. H. Petersson, “Theorie der automorphen Formen beliebig reeller Dimension und ihre Darstellung durch eine neue Art Poincaré-Reihen”, *Math. Ann.*, 103, 369–436, (1939).
32. J. Hoffstein, D. Ramakrishnan, “Siegel Zeros and Cusp Forms”, *IMRN*, 6, 279–308, (1995).
33. N. Kuznietzov, “Petersson’s Conjecture for Cusp Forms of Weight Zero and Linnik’s Conjecture, Sums of Kloosterman Sums”, *Math. SB.* 111, 334–383, (1980).
34. W. Luo, P. Sarnak, “Quantum Ergodicity of Eigenfunctions on  $PSL_2(\mathbb{Z}) \backslash \mathbb{H}$ ”, *I.H.E.S. Publ. Math.*, 81, 207–237, (1995).
35. P. Sarnak, “Some Applications of Modular Forms”, Cambridge Univ. Press, Vol. 99, (1990).
36. P. Sarnak, “Arithmetic Quantum Chaos”, The Schur Lectures, (1992), Israel Math. Conf. Proceedings, *AMS*, (August, 1995).
37. H. Weyl, “Zur Abschätzung von  $\zeta(1 + it)$ ”, *M.Z.* 10, 88–101, (1921).
38. D. Burgess, “On Character Sums and  $L$ -series II”, *Proc. London Math. Soc.*, 3, 13, 24–36, (1963).
39. H. Iwaniec, “The Spectral Growth of Automorphic  $L$ -functions”, *J. Reine Angew. Math.*, 428, 139–159, (1992).
40. W. Duke, J. Friedlander, H. Iwaniec, “Bounds for Automorphic  $L$ -functions”, *Inv. Math.*, 112, No. 1, 1–8, (1993).
41. W. Duke, J. Friedlander, H. Iwaniec, “Class Group  $L$ -functions”, *Duke Math. J.*, 79, No. 1, 1–56, (1995).
42. A. Good, “The Square Mean of Dirichlet Series Associated with Cusp Forms”, *Mathematika*, 29, 278–295, (1982).

43. T. Meurman, "On the Order of the Maass  $L$ -function on the Critical Line", Number Theory '90, Vol. 1, Budapest Colloq. Math. Soc., Janos Bolyai, 51, (1990).
44. W. Duke, "Some Old Problems and New Results About Quadratic Forms", Notices, AMS, 44, No. 2, 190–196, (1997).
45. J. Friedlander, "Bounds for  $L$ -functions", *Proc. I.C.M.*, Zurich, 363–373, (1994).
46. J. Friedlander, H. Iwaniec, "Estimates for Character Sums", *Proc. Amer. Math. Soc.*, 119, 365–372, (1993).
47. H. Iwaniec, P. Sarnak, " $L^\infty$  Norms of Eigenfunctions of Arithmetic Surfaces", *Annals Math.*, 141, 301–320, (1995).
48. A. Selberg, "On the Zeros of Riemann's Zeta Function", *Skr. Norske Vid.-Akad.*, Oslo I, 10, 1–59, (1942).
49. J. Hafner, "Zeros on the Critical Line for Dirichlet Series Attached to Certain Cusp Forms", *Math. Ann.*, 264, 21–37, (1983).
50. N. Levinson, "More Than One-Third of Zeros of Riemann's Zeta-Function are on  $\sigma = 1/2$ ", *Adv. Math.*, 13, 383–436, (1974).
51. B. Conrey, "More than  $2/5$  of the Zeros of the Riemann Zeta Function are on the Critical Line", *J. Reine Angew. Math.*, 399, 1–26, (1989).
52. H. Montgomery, "The Pair Correlation of Zeroes of the Zeta Function", *Proc. Sym. Pure Math.*, 24, AMS, 181–193, (1973).
53. F. Dyson, "Statistical Theory of Energy Levels III", *J. Math. Phys.*, 3, 166–175, (1962).
54. M. Metha, "Random Matrices", Second Edition, Academic Press, Boston, (1991).
55. E. Wigner, "Random Matrices in Physics", *Siam Review*, 9, 1–23, (1967).
56. A. Odlyzko, "The  $10^{20}$ -th Zero of the Riemann Zeta Function and 70 Million of it's Neighbors", (preprint A.T.T., 1989).
57. D. Hejhal, "On the Triple Correlation of the Zeroes of the Zeta Function", *IMRN*, 293–302, (1994).
58. Z. Rudnick, P. Sarnak, "Principal  $L$ -functions and Random Matrix Theory", *Duke Math. J.*, 81, 2, 269–322, (1996).
59. R. Rumely, "Numerical Computations Concerning ERH", *Math. Comp.*, 61, 415–440, (1993).
60. M. Rubinstein, "Evidence for a Spectral Interpretation of Zeros of  $L$ -functions", Thesis, Princeton University, (1998).
61. E. Artin, "Quadratische Körper im Gebiet der höheren Kongruenzen I und II", *Math. Zeit.*, 19, 153–296, (1924).
62. N. Katz, P. Sarnak, "Random Matrices, Frobenius Eigenvalues and Monodromy", (to appear, 1998).

63. N. Katz, P. Sarnak, “Zeroes of Zeta Functions and Symmetry”, (preprint, 1998).
64. H. Iwaniec, W. Luo, P. Sarnak, “Low Lying Zeroes of Families of  $L$ -functions”, (preprint, 1998).
65. A. Ozluk, C. Snyder, “Small Zeroes of Quadratic  $L$ -functions”, *Bull. Aust. Math. Soc.*, 47, 307–319, (1993).
66. A. Brumer, “The Rank of  $J_0(N)$ ”, *Asterisque*, 228, 41–68, (1995).
67. R. Murty, “The Analytic Rank of  $J_0(N)/Q$ ”, Number Theory, (Halifax, NS), CMS Conf. Proc., *AMS*, 15, 263–277, (1995).
68. B. Mazur, “Modular Curves and the Eisenstein Ideal”, *Publ. Math. I.H.E.S.*, 47, 33–186, (1977).
69. L. Merel, “Bornes pour la Torsion de Courbes Elliptiques sur les Corps de Nombres”, *Inv. Math.*, 124, 437–449, (1996).
70. G. Kramarz, D. Zagier, “Numerical Investigations Related to  $L$ -series of Certain Elliptic Curves”, *J. Indian Math. Soc.*, 97, 313–324, (1987).
71. J. Silverman, “The Average Rank of a Family of Elliptic Curves”, (preprint, 1997).
72. R. Phillips, P. Sarnak, “On Cusp Forms for Cofinite Subgroups of  $PSL(2, \mathbb{R})$ ”, *Inv. Math.*, 80, 339–364, (1985).
73. G. Shimura, “On Modular Forms of Half-Integral Weight”, *Ann. Math.*, 97, 440–481, (1973).
74. J. Waldspurger, “Sur les Coefficients de Fourier des Formes Modulaires de Poids Demi Entier”, *J. Math. Pures. Appl.*, 60, 365–384, (1981).
75. J. Deshouillers, H. Iwaniec, “The Non-vanishing of Rankin-Selberg Zeta Functions at Special Points”, *Contemp. Math.*, 53, *AMS*, 51–95, (1986).
76. W. Luo, “On Non-vanishing of Rankin-Selberg  $L$ -functions”, *Duke Math. J.*, 69, 411–427, (1993).
77. D. Bump, S. Friedberg, J. Hoffstein, “Non-vanishing Theorems for  $L$ -functions of Modular Forms and their Derivatives”, *Inv. Math.*, 102, 543–618, (1990).
78. K. Murty, R. Murty, “Mean Values of Derivatives of Modular  $L$ -series”, *Ann. Math.*, 133, 447–475, (1991).
79. V. Kolyvagin and D. Lugachev, “Finiteness of the Shafarevich-Tate Group and the Group of Rational Points for some Modular Abelian Varieties”, *Leningrad Math. J.*, 1, No. 5, 1229–1253, (1990).
80. A. Perelli, J. Pomykala, “Averages Over Twisted Elliptic  $L$ -functions”, *Acta Math.*, 80, 149–163, (1997).
81. R. Heath-Brown, “The Size of Selmer Groups for the Congruent Number Problem II”, *Inv. Math.*, 118, 331–370, (1994).
82. S. Wong, “Rank Zero Twists of Elliptic Curves”, (preprint, 1996).

83. H. Iwaniec, P. Sarnak, "The Non-vanishing of Central Values of Automorphic  $L$ -functions and Siegel's Zero", (preprint, 1997).
84. J. Guo, "On the Positivity of the Central Critical Values of Automorphic  $L$ -functions", *Duke Math. J.*, 83, 1–18, (1886).
85. J. Vanderkam, "The Rank of Quotients of  $J_0(N)$ ", (preprint, 1997).
86. E. Kowalski, P. Michel, "Sur le Rang de  $J_0(N)$ ", (preprint, 1997).
87. W. Duke, H. Iwaniec, "Estimates for Coefficients of  $L$ -functions I", "Automorphic Forms and Analytic Number Theory", Editor, R. Murty, *CRM*, Montreal, 43–48, (1990).
88. D. Bump, W. Duke, J. Hoffstein, H. Iwaniec, "An Estimate for Hecke Eigenvalues of Maass Forms", *IMRN*, 4, 75–81, (1992).
89. W. Luo, Z. Rudnick, P. Sarnak, "On Selberg's Eigenvalue Conjecture", *GAF*, 5, 387–401, (1995).
90. W. Luo, Z. Rudnick, P. Sarnak, "On the Generalized Ramanujan Conjecture for  $GL(n)$ ", (to appear, 1998).
91. D. Rohrlich, "Non-vanishing of  $L$ -functions for  $GL(2)$ ", *Inv. Math.*, 97, 383–401, (1989).
92. F. Shahidi, "On Ramanujan's Conjecture and the Finiteness of Poles of Certain  $L$ -functions", *Ann. Math.*, 127, 547–584, (1988).
93. A. Weil, "On Some Exponential Sums", *Proc. Nat. Acad. Sci.*, U.S.A., 34, 204–207, (1948).
94. B. Birch, P. Swinnerton-Dyer, "Notes on Elliptic Curves (I) and (II)", *J. Reine Angew. Math.*, 212, 7–25, (1963), 28, 79–108, (1965).
95. A. Selberg, "Harmonic Analysis and Discontinuous Groups in Weakly Symmetric Riemannian Spaces with Applications to Dirichlet Series", *J. Indian Mth. Soc.*, 20, (1956).
96. Y. Ihara, "Hecke Polynomials as Congruence  $\zeta$  Functions in Elliptic Modular Case (to Validate M. Sato's Identity)", *Ann. Math.*, 85, 267–295, (1967).
97. A. Weil, "On the Riemann Hypothesis in Function Fields", *Proc. Nat. Acad. Sci.*, U.S.A., 27, 345–349, (1941).
98. A. Connes, "Formule de Trace en Géométrie Non-commutative et Hypothèse de Riemann", *CR. Acad. Sci.*, Paris, 323, I, 1231–1236, (1996).
99. C. Deninger, "Evidence for a Cohomological Approach to Analytic Number Theory", First European Math Congress, Vol. I, (1992), *Proc. in Math.*, Vol. 119, 491–510, Birkhauser, (1994).
100. I. Satake, "Spherical Functions and the Ramanujan Conjecture", *Proc. A.M.S. Symp.*, Vol. 9, 258–364, (1971).

Peter Sarnak  
Department of Mathematics,  
Princeton University,  
Fine Hall, Washington Road,  
Princeton, New Jersey 08544





## QUANTUM COMPUTING

PETER W. SHOR

ABSTRACT. The Church-Turing thesis says that a digital computer is a universal computational device; that is, it is able to simulate any physically realizable computational device. It has generally been believed that this simulation can be made efficient so that it entails at most a polynomial increase in computation time. This may not be true if quantum mechanics is taken into consideration. A quantum computer is a hypothetical machine based on quantum mechanics. We explain quantum computing, and give an algorithm for prime factorization on a quantum computer that runs asymptotically much faster than the best known algorithm on a digital computer. It is not clear whether it will ever be possible to build large-scale quantum computers. One of the main difficulties is in manipulating coherent quantum states without introducing errors or losing coherence. We discuss quantum error-correcting codes and fault-tolerant quantum computing, which can guarantee highly reliable quantum computation, given only moderately reliable quantum computing hardware.

1991 Mathematics Subject Classification: Primary 68Q05; Secondary 11Y05, 81P99.

Keywords and Phrases: Quantum computer, computational complexity, prime factorization.

## 1 INTRODUCTION.

Quantum computers are hypothetical machines that use principles of quantum mechanics for their basic operations. They will be very difficult to build; currently experimental physicists are working on two- and three-bit quantum computers, and useful quantum computers would require hundreds to thousands of bits. However, there seem to be no fundamental physical laws that would preclude their construction. In 1994, I showed that a quantum computer could factor large numbers in time polynomial in the length of the numbers, a nearly exponential speed-up over classical algorithms. This factoring result was surprising for a number of different reasons. First, the connection of quantum mechanics with number theory was itself surprising. For cryptographers, the result was surprising because the difficulty of factoring is the basis of the RSA cryptosystem [27], and nobody had anticipated the possibility of an attack via quantum physics. For many theoretical computer

scientists, it was surprising because they had more or less convinced themselves that no type of computing machine could offer this large a speed-up over a classical digital computer. In retrospect, several results [7, 30] should have led them to question this; however, not much attention was paid to these results until they led to the development of the factoring algorithm,

A question that has generated much discussion is where the extra power of quantum computers comes from. There are a number of differences between quantum and classical computers, and most appear to be required for the extra power. In particular, quantum interference is needed; one high-level way to describe the quantum factoring algorithm is that the computation is arranged so that computational paths giving the wrong answer interfere to cancel each other out, leaving a high probability of obtaining the right answer. Another property of quantum systems that plays a crucial role is entanglement, or non-classical correlation, between quantum systems. Many non-quantum physical systems such as waves exhibit interference, but none of these systems exhibits entanglement, and they do not appear usable for quantum computation. Finally, a third property required is the high dimensionality of quantum systems; the dimension of the joint quantum state space of  $n$  objects grows exponentially with  $n$ , whereas classically the dimension of the joint state space of  $n$  objects only grows linearly. The factoring algorithm makes critical use of this extra dimensionality.

In the rest of the paper, I describe these results in more detail. In section 2, I start by discussing Church's thesis, which still appears to hold, and an extension of it, to which quantum computers now appear to be a counterexample. In the following section, I describe the quantum circuit model for quantum computation. This is not laid out particularly well anywhere else, so I spend a reasonable amount of space on it. In section 4, I describe the differences between the quantum circuit model and possible physical realizations of quantum computers, and say a little about why the model appears to give the right definition of what is efficiently computable using quantum mechanics. Section 5 describes the factoring algorithm. Section 6 discusses error-correcting codes and fault-tolerant quantum computing. In the final section, I mention some related results.

## 2 THE POLYNOMIAL CHURCH'S THESIS.

Church's thesis says that any computable function can be computed on a Turing machine, which is essentially a mathematical abstraction of a digital computer. This thesis arose in the 1930's, and was motivated by the realization that three apparently quite distinct definitions of computable functions were all equivalent. It is well known that Church's thesis is not a theorem, because it does not specify a rigorous mathematical definition of "computable"; specifying such a definition would lead to a provable theorem (and in many cases has), but would also detract from the generality of the thesis. What is somewhat less commonly realized is that this thesis can be viewed as a statement about the laws of physics, simply by interpreting computable to mean computable in the physical world. For this interpretation, if the laws of physics are computable by a Turing machine, then Church's thesis is true.

The development of digital computers rendered the distinction between computable and uncomputable functions too coarse in practice, as it does not take into account the time required for computation. What was needed for the theory of computation was some characterization of efficiently computable functions. In the early 1970's, theoretical computer scientists reached a good compromise between theory and practice with the definition of polynomial-time computable functions. These are functions whose value can be computed in a number of steps polynomial in the input size. The corresponding set of languages—functions whose range is  $\{0, 1\}$ —is known as P (or PTIME). While nobody claims that a function computable in time  $n^{100}$  is efficiently computable in practice, the set of polynomial time computable functions is structurally nice enough to use in proofs, and for functions arising in practice it appears to include most of the efficiently computable ones and exclude most of those not efficiently computable. This definition naturally gave rise to a “folk thesis,” the polynomial Church's thesis, which says that any function physically computable in time  $t$  on some machine  $X$  can be computed on a Turing machine in time  $p(t)$ , where  $p$  is a polynomial depending only on the machine  $X$ .

Is this folk thesis valid? One good place to start looking for counterexamples is with physical systems which seem to require large amounts of computer time to simulate. Two obvious such candidates are turbulence and quantum mechanics. I will have nothing further to say about turbulence, except that I think the computational complexity of turbulence is a question worthy of serious study. Richard Feynman, in 1982, was the first to consider the case of quantum mechanics [16]. He gave arguments for why quantum mechanical systems should inherently require an exponential overhead to simulate on digital computers. In a lengthy “side remark,” he proposed using quantum computers, operating on quantum mechanical principles, to circumvent this problem. David Deutsch [15] followed up on Feynman's proposal by defining quantum Turing machines, and suggesting that if quantum computers could solve quantum mechanical problems more quickly than digital computers, they might also solve classical problems more quickly. It currently appears that this is indeed the case. One piece of evidence for this is that quantum computers can solve certain “oracle problems” faster than classical computers [7, 30]; here an oracle problem is one where the computer is given a subroutine (oracle) which must be treated as a black box. The behavior of computational complexity with respect to oracles, however, has not proved a reliable guide to its true behavior. Another piece of evidence that quantum computers are a counterexample to the polynomial Church's thesis is that they can factor integers and find discrete logarithms in polynomial time, something which it is not known how to do on classical computers despite many years of study. The factorization algorithm is discussed later in this paper.

### 3 THE QUANTUM CIRCUIT MODEL.

In this section we discuss the *quantum circuit model* [32] for quantum computation. This is a rigorous mathematical model for a quantum computer. It is not the only mathematical model for quantum computation; there are also the *quantum Turing*

*machine model* [7, 32] and the *quantum cellular automata model*. All these models result in the same class of polynomial-time quantum computable functions. Of these, the quantum circuit model is possibly the simplest to describe. It is also easier to connect with possible physical implementations of quantum computers than the quantum Turing machine model. The disadvantage of this model is that it is not naturally a *uniform* model. Uniformity is a technical condition arising in complexity theory, and to make the quantum circuit model uniform, additional constraints must be imposed on it. This issue is discussed later in this section.

In analogy with a classical bit, a two-state quantum system is called a *qubit*, or quantum bit. Mathematically, a qubit takes a value in the vector space  $\mathbb{C}^2$ . We single out two orthogonal basis vectors in this space, and label these  $V_0$  and  $V_1$ . In “ket” notation, which is commonly used in this field, these are represented as  $|0\rangle$  and  $|1\rangle$ . More precisely, quantum states are invariant under multiplication by scalars, so a qubit lives in two-dimensional complex projective space; for simplicity, we work in complex Euclidean space  $\mathbb{C}^2$ . To conform with physics usage, we treat qubits as column vectors and operate on them by left multiplication.

One of the fundamental principles of quantum mechanics is that the joint quantum state space of two systems is the tensor product of their individual quantum state spaces. Thus, the quantum state space of  $n$  qubits is the space  $\mathbb{C}^{2^n}$ . The basis vectors of this space are parameterized by binary strings of length  $n$ . We make extensive use of the tensor decomposition of this space into  $n$  copies of  $\mathbb{C}^2$ , where  $V_{b_1 b_2 \dots b_n} = V_{b_1} \otimes V_{b_2} \otimes \dots \otimes V_{b_n}$ . Generally, we use position to distinguish the  $n$  different qubits. Occasionally we need some other notation for distinguishing them, in which case we denote the  $i$ 'th qubit by  $V^{[i]}$ . Since quantum states are invariant under multiplication by scalars, they can be normalized to be unit length vectors; except where otherwise noted, quantum states in this paper are normalized. Quantum computation takes place in the quantum state space of  $n$  qubits  $\mathbb{C}^{2^n}$ , and obtains extra computational power from its exponential dimensionality.

In a usable computer, we need some means of giving it the problem we want solved (input), some means of extracting the answer from it (output), and some means of manipulating the state of the computer to transform the input into the desired output (computation). We next briefly describe input and output for the quantum circuit model. We then take a brief detour to describe the classical circuit model; this will motivate the rules for performing the computation on a quantum computer.

Since we are comparing quantum computers to classical computers, the input to a quantum computer will be classical information. It can thus be expressed as a binary string  $S$  of some length  $k$ . We need to encode this in the initial quantum state of the computer, which must be a vector in  $\mathbb{C}^{2^n}$ . The way we do this is to concatenate the bit string  $S$  with  $n - k$  0's to obtain the length  $n$  string  $S0\dots 0$ . We then initialize the quantum computer in the state  $V_{S0\dots 0}$ . Note that the number of qubits is in general larger than the input. These extra qubits are often required as workspace in implementing quantum algorithms.

At the end of a computation, the quantum computer is in a state which is a unit vector in  $\mathbb{C}^{2^n}$ . This state can be written explicitly as  $W = \sum_s \alpha_s V_s$  where  $s$  ranges over binary strings of length  $n$ ,  $\alpha_s \in \mathbb{C}$ , and  $\sum_s |\alpha_s|^2 = 1$ . These  $\alpha_s$

Figure 1: Construction of a Toffoli gate using the classical gates AND, OR and NOT. The input is on the left and the output on the right.

are called *probability amplitudes*, and we say that  $W$  is a *superposition* of basis vectors  $V_s$ . In quantum mechanics, the Heisenberg uncertainty principle tells us that we cannot measure the complete quantum state of this system. There are a large number of permissible measurements; for example, any orthogonal basis of  $\mathbb{C}^{2^n}$  defines a measurement whose possible outcomes are the elements of this basis. However, we assume that the output is obtained by projecting each qubit onto the basis  $\{V_0, V_1\}$ . When applied to a state  $\sum_s \alpha_s V_s$ , this projection produces the string  $s$  with probability  $|\alpha_s|^2$ . The quantum measurement process is inherently probabilistic. Thus we do not require that the computation gives the right answer all the time; but that we obtain the right answer at least  $2/3$  of the time. Here, the probability  $2/3$  can be replaced by any number strictly between  $1/2$  and  $1$  without altering what can be computed in polynomial time by quantum computers—if the probability of obtaining the right answer is strictly larger than  $1/2$ , it can be amplified by running the computation several times and taking the majority vote of the results of these separate computations.

In order to motivate the rules for state manipulation in a quantum circuit, we now take a brief detour and describe the classical circuit model. Recall that a classical circuit can always be written solely with the three gates AND ( $\wedge$ ), OR ( $\vee$ ) and NOT ( $\neg$ ). These three gates are thus said to form a *universal* set of gates. Figure 1 gives an example circuit for a computation called a *Toffoli gate* using these three types of gates. Besides these three gates, note that we also need elements which duplicate the values on wires. These duplicating “gates” are not possible in the domain of quantum computing.

A quantum circuit is similarly built out of logical quantum wires carrying qubits, and quantum gates acting on these qubits. Each wire corresponds to one of the  $n$  qubits. We assume each gate acts on either one or two wires. The possible physical transformations of a quantum system are unitary transformations, so each quantum gate can be described by a unitary matrix. A quantum gate on one qubit is then described by a  $2 \times 2$  matrix, and a quantum gate on two qubits by a  $4 \times 4$  matrix. Note that since unitary matrices are invertible, the computation is

reversible; thus starting with the output and working backwards one obtains the input. Further note that for quantum gates, the dimension of the output space is equal to that of the input space, so at all times during the computation we have  $n$  qubits carried on  $n$  quantum wires. Figure 2 contains an example of a quantum circuit for computing a Toffoli gate.

Quantum gates acting on one or two qubits ( $\mathbb{C}^2$  or  $\mathbb{C}^4$ ) naturally induce a transformation on the state space of the entire quantum computer ( $\mathbb{C}^{2^n}$ ). For example, if  $A$  is a  $4 \times 4$  matrix acting on qubits  $i$  and  $j$ , the induced action on a basis vector of  $\mathbb{C}^{2^n}$  is

$$A^{[i,j]} V_{b_1 b_2 \dots b_n} = \sum_{s=0}^1 \sum_{t=0}^1 A_{b_i b_j st} V_{b_1 b_2 \dots b_{i-1} s b_{i+1} \dots b_{j-1} t b_{j+1} \dots b_n}. \quad (1)$$

This is a tensor product of  $A$  (acting on qubits  $i$  and  $j$ ) with the identity matrix (acting on the remaining qubits). When we multiply a general vector by a quantum gate, it can have negative and positive coefficients which cancel out, leading to quantum interference.

As there are for classical circuits, there are also universal sets of gates for quantum circuits; such a universal set of gates is sufficient to build circuits for any quantum computation. One particularly useful universal set of gates is the set of all one-bit gates and a specific two-bit gate called the Controlled NOT (CNOT). These gates can efficiently simulate any quantum circuits whose gates act on only a constant number of qubits [2]. On basis vectors, the CNOT gate negates the second (target) qubit if and only if the first (control) qubit is 1. In other words, it takes  $V_{XY}$  to  $V_{XZ}$  where  $Z = X + Y \pmod{2}$ . This corresponds to the unitary matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (2)$$

Note that the CNOT is a classical reversible gate. To obtain a universal set of classical reversible gates, you need at least one reversible three-bit gate, such as a Toffoli gate; otherwise you can only perform linear Boolean computations. A Toffoli gate is a doubly controlled NOT, which negates the 3rd bit if and only if the first two are both 1. By itself the Toffoli gate is universal for reversible classical computation, as it can simulate both AND and NOT gates [17]. Thus, if you can make a Toffoli gate, you can perform any reversible classical computation. Further, as long as the input is not erased, any classical computation can be efficiently performed reversibly [3], and thus implemented efficiently by Toffoli gates.

Because of the extra possibilities allowed by quantum interference, for quantum circuits the CNOT together with all quantum one-bit gates forms a universal set of gates. Figure 2 gives a construction of a Toffoli gate out of CNOT gates and one-bit gates [2], showing that this set is at least universal for classical computation. This particular construction does not result in a Toffoli gate with all positive

Figure 2: Construction of a Toffoli gate using quantum gates. The gates represented by  $\oplus$  are CNOT's, where the circle identifies the target qubit. The gate  $R$  is  $\begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$ , and  $R^\dagger$  is the Hermitian transpose of  $R$ . In this construction, the phase on  $V_{101}$  is  $-1$ , and all the other phases are  $+1$ ; the phases can all be made  $+1$  by a somewhat more complicated quantum circuit.

phases—multiplying the corresponding matrices in Figure 2 produces the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{3}$$

which is the classical Toffoli gate with a phase of  $-1$  on one of its outcomes. This still acts classically as a Toffoli gate, since phases are irrelevant to classical computation. In quantum computation, however, we must keep careful track of phases. A more complicated circuit can be constructed which eliminates this phase of  $-1$  [2].

We now define the complexity class BQP, which stands for bounded-error quantum polynomial time. This is the class of languages which can be computed on a quantum computer in polynomial time, with the computer giving the correct answer at least  $2/3$  of the time. To give a rigorous definition of this complexity class using quantum circuits, we need to consider uniformity conditions. Any specific quantum circuit can only compute a function whose domain (input) is binary strings of a specific length. To use the quantum circuit model to implement functions taking arbitrary length binary strings as input, we take a family of quantum circuits, containing one circuit for inputs of each length. Without any further conditions on the family of circuits, the designer of this circuit family could hide an uncomputable function in the design of the circuits for each input length.



This definition would thus result in the unfortunate inclusion of uncomputable functions in the complexity class BQP. To exclude this possibility, we require *uniformity* conditions on the circuit family. The easiest way of doing this is to require a classical Turing machine that on input  $n$  outputs a description of the circuit for length  $n$  inputs, and which runs in time polynomial in  $n$ . For quantum computing, we need an additional uniformity condition on the circuits. It would be possible for the circuit designer to hide uncomputable (or hard-to-compute) information in the unitary matrices corresponding to quantum gates. We thus require that the  $k$ 'th digit of the entries of these matrices can be computed by a second Turing machine in time polynomial in  $k$ . Although we do not have space to discuss this fully, the power of the machines designing the circuit family can actually be varied over a wide range; this helps us convince ourselves that we have the right definition of BQP.

The definition of polynomial time computable functions on a quantum computer is thus those functions computable by a *uniform* family of circuits whose size (number of gates) is polynomial in the length of the input, and which for any input gives the right answer at least  $2/3$  of the time. The corresponding set of languages (functions with values in  $\{0, 1\}$ ) is called BQP.

#### 4 RELATION OF THE MODEL TO QUANTUM PHYSICS.

The quantum circuit model of the previous section is much simplified from the realities of quantum physics. There are operations possible in physical quantum systems which do not correspond to any simple operation allowable in the quantum circuit model, and complexities that occur when performing experiments that are not reflected in the quantum circuit model. This section contains a brief discussion of these issues, some of which are discussed more thoroughly in [7].

In everyday life, objects behave very classically, and on large scales we do not see any quantum mechanical behavior. This is due to a phenomenon called decoherence, which makes superpositions of states decay, and makes large-scale superpositions of states decay very quickly. A thorough discussion of decoherence can be found in [35]; one reason it occurs is that we are dealing with open systems rather than closed ones. Although closed systems quantum mechanically undergo unitary evolution, open systems need not. They are subsystems of systems undergoing unitary evolution, and the process of taking subsystems does not preserve unitarity.

However hard we may try to isolate quantum computers from the environment, they will still undergo some decoherence and errors. We need to know that these processes do not fundamentally change their behavior. Using no error correction, if each gate results in an amount of decoherence and error of order  $1/t$ , then  $O(t)$  operations can be performed before the quantum state becomes so noisy as to usually give the wrong answer [7]. Active error correction can improve this situation substantially, and is discussed in section 6.

In some proposed physical architectures for quantum computers, there are restrictions that are more severe than the quantum computing model. Many of these restrictions do not change the class BQP. For example, it could easily be

the case that a gate could only be applied to a pair of *adjacent* qubits. We can still operate on a pair of arbitrary qubits: by repeatedly exchanging one of these qubits with a neighbor we can bring this pair together. If there are  $n$  qubits in the computer, this can only increase the computation time by a factor of  $n$ , preserving the complexity class BQP.

The quantum circuit model described in the previous section postpones all measurements to the end, and assumes that we are not allowed to use probabilistic steps. Both of these possibilities are allowed in general by quantum mechanics, but neither possibility makes the complexity class BQP larger [7]. For fault-tolerant quantum computing, however, it is very useful to permit measurements in the middle of the computation, in order to measure and correct errors.

The quantum circuit model also assumes that we only operate on a constant number of qubits at a time. In general quantum systems, all the qubits evolve simultaneously according to some Hamiltonian describing the system. This simultaneous evolution of many qubits cannot be described by a single gate in our model, which only operates on two qubits at once. In a realistic model of quantum computation, we cannot allow general Hamiltonians, since they are not experimentally realizable. Some Hamiltonians that act on all the qubits at once, however, are experimentally realizable. It would be nice to know that even though these Hamiltonians cannot be directly described by our model, they cannot be used to compute functions not in BQP in polynomial time. This could be accomplished by showing that systems with such Hamiltonians can be efficiently simulated by a quantum computer. Some work has been done on simulating Hamiltonians on quantum computers [1, 24, 33], but I do not believe this question has been completely addressed yet.

An important aspect of quantum mechanics not used in the quantum circuit model is that identical particles are indistinguishable; in general they must obey either Fermi-Dirac or Einstein-Bose statistics when they are interchanged. Particle statistics do not appear to add any power to the quantum computing model, but I do not believe this has been rigorously proved.

From the view of the current state of experimental physics, quantum computers appear to be extremely difficult to build, but do not seem to violate any fundamental physical laws. As qubits, we need to use quantum systems which are relatively stable, which interact strongly with each other (to carry out quantum gates quickly), but which interact weakly with everything else (to avoid errors caused by interaction with the environment). Since the discovery of the factoring algorithm, a variety of proposals for experimental implementation of quantum computers have been made. One of these proposals is to use the electronic states of ions in an electromagnetic ion trap as the qubits, to manipulate them using lasers, and to communicate between different ions using a vibrational mode of the ions, or *phonon* [12]. Another is to use nuclear spins of atoms in a complex molecule as the qubits, and to manipulate them using nuclear magnetic resonance spectroscopy [14, 18]. A quite recent proposal is to use nuclear spins of impurities embedded in a silicon chip as the qubits, and to manipulate them using electronics on the same chip [23]. None of these proposals has been experimentally realized for more than a handful of qubits, but they all have proponents who believe that

they may be scaled up to obtain much larger working quantum computers.

## 5 THE FACTORING ALGORITHM.

For factoring an  $L$ -bit number  $N$ , the best classical algorithm known is the number field sieve, which asymptotically takes time  $O(\exp(cL^{1/3} \log^{2/3} L))$ . On a quantum computer, the quantum factoring algorithm takes asymptotically  $O(L^2 \log L \log \log L)$  steps. The key idea of the quantum factoring algorithm is the use of a Fourier transform to find the period of the sequence  $u_i = x^i \pmod{N}$ , from which period a factorization of  $N$  can be obtained. The period of this sequence is exponential in  $L$ , so this approach is not practical on a digital computer. On a quantum computer, however, we can find the period in polynomial time by exploiting the  $2^{2L}$ -dimensional state space of  $2L$  qubits, and taking a Fourier transform over this space. The exponential dimensionality of this space permits us to take the Fourier transform of an exponential length sequence. How this works should be clearer from the following sketch of the algorithm, the full details of which are in [28], along with a quantum algorithm for finding discrete logarithms.

The idea behind all the fast factoring algorithms (classical or quantum) is fairly simple. To factor  $N$ , find two residues mod  $N$  such that

$$s^2 \equiv t^2 \pmod{N} \quad (4)$$

but  $s \not\equiv \pm t \pmod{N}$ . We now have

$$(s+t)(s-t) \equiv 0 \pmod{N} \quad (5)$$

and neither of these two factors is  $0 \pmod{N}$ . Thus,  $s+t$  must contain one factor of  $N$  (and  $s-t$  another). We can extract this factor by finding the greatest common divisor of  $s+t$  and  $N$ ; this computation can be done in polynomial time using Euclid's algorithm.

In the quantum factoring algorithm, we find the multiplicative period  $r$  of a residue  $x \pmod{N}$ . This period  $r$  satisfies  $x^r \equiv 1 \pmod{N}$ ; if we are lucky then  $r$  is even, so both sides of this congruence are squares, and we can try the above factorization method. If we have just a little bit more luck, then  $x^{r/2} \not\equiv -1 \pmod{N}$ , so we obtain a factor by computing  $\gcd(x^{r/2} + 1, N)$ . It is a fairly simple exercise in number theory to show that for large  $N$  with two or more prime factors, at least half the residues  $x \pmod{N}$  produce prime factors using this technique, and that for most large  $N$ , the fraction of good residues  $x$  is much higher; thus, if we try several different values for  $x$ , we have to be particularly unlucky not to obtain a factorization using this method.

We now need to explain what the quantum Fourier transform is. The quantum Fourier transform on  $k$  qubits maps the state  $V_a$ , where  $a$  is considered as an integer between 0 and  $2^k - 1$ , to a superposition of the states  $V_b$  as follows:

$$V_a \rightarrow \frac{1}{2^{k/2}} \sum_{b=0}^{2^k-1} \exp(2\pi i ab/2^k) V_b \quad (6)$$

It is easy to check that this transformation defines a unitary matrix. It is not as straightforward to implement this Fourier transform as a sequence of one- and two-bit quantum gates. However, an adaption of the Cooley-Tukey algorithm decomposes this transformation into a sequence of  $k(k - 1)/2$  one- and two-bit gates. More generally, the discrete Fourier transform over any product  $Q$  of small primes (of size at most  $\log Q$ ) can be performed in polynomial time on a quantum computer.

We are now ready to give the quantum algorithm for factoring. What we do is design a polynomial-size circuit which starts in the quantum state  $V_{00\dots 0}$  and whose output, with reasonable probability, lets us factor an  $L$ -bit number  $N$  in polynomial time using a digital computer. This circuit has two main registers, the first of which is composed of  $2L$  qubits and the second of  $L$  qubits. It also requires a few extra qubits of work space, which we do not mention in the summary below but which are required for implementing the step (8) below.

We start by putting the computer into the state representing the superposition of all possible values of the first register:

$$\frac{1}{2^L} \sum_{a=0}^{2^{2L}-1} V_a \otimes V_0. \tag{7}$$

This can easily be done using  $2L$  gates by putting each of the qubits in the first register into the state  $\frac{1}{\sqrt{2}}(V_0 + V_1)$ .

We next use the value of  $a$  in the first register to compute the value  $x^a \pmod N$  in the second register. This can be done using a reversible classical circuit for computing  $x^a \pmod N$  from  $a$ . Computing  $x^a \pmod N$  using repeated squaring takes asymptotically  $O(L^3)$  quantum gates using the grade school multiplication algorithm, and  $O(L^2 \log L \log \log L)$  gates using fast integer multiplication (which is actually faster only for relatively large values of  $L$ ). This leaves the computer in the state

$$\frac{1}{2^L} \sum_{a=0}^{2^{2L}-1} V_a \otimes V_{x^a \pmod N}. \tag{8}$$

The next step is to take the discrete Fourier transform of the first register, as in Equation (6). This puts the computer into the state

$$\frac{1}{2^{2L}} \sum_{a=0}^{2^{2L}-1} \sum_{b=0}^{2^{2L}-1} \exp(2\pi iab/2^{2L}) V_b \otimes V_{x^a \pmod N}. \tag{9}$$

Finally, we measure the state. This will give the output  $V_b \otimes V_{x^j \pmod N}$  with probability equal to the square of the coefficient on this vector in the sum (9). Since many values of  $x^a \pmod N$  are equal, many terms in this sum contribute to each coefficient. Explicitly, this probability is:

$$\frac{1}{2^{4L}} \left| \sum_{\substack{a \equiv j \pmod r \\ 0 \leq a < 2^{2L}}} \sum_{b=0}^{2^{2L}-1} \exp(2\pi iab/2^{2L}) \right|^2. \tag{10}$$

This is a geometric sum, and it is straightforward to check that this sum is very small except when

$$rb \approx d2^{2L} \tag{11}$$

for some integer  $d$ . We thus are likely to observe only values of  $b$  satisfying (11). Rewriting this equation, we obtain

$$\frac{b}{2^{2L}} \approx \frac{d}{r}. \tag{12}$$

We know  $b$  and  $2^{2L}$ , and we want to find  $r$ . We chose  $2L$  as the size of the first register in order to make  $d/r$  likely to be the closest fraction to  $b/2^{2L}$  with denominator at most  $N$ . Thus, all we need do to find  $r$  is to round  $b/2^{2L}$  to a fraction with denominator less than  $N$ . This can be done in polynomial time using a continued fraction expansion.

More details of this algorithm can be found in [28]. Recently, Zalka [34] has analyzed the resources required by this algorithm much more thoroughly, improving upon their original values in many respects. For example, he shows that you can use only  $3L + o(L)$  qubits, whereas the original algorithm required  $2L$  extra qubits for workspace, giving a total of  $5L$  qubits. He also shows how to efficiently parallelize the algorithm to run on a parallel quantum computer.

## 6 QUANTUM ERROR CORRECTING CODES.

One of the reactions to the quantum factoring paper was that quantum computers would be impossible to build because it would be impossible to reduce decoherence and errors to levels low enough to ensure reliable quantum computation. Indeed, without error correction, it would probably be an impossible task to build quantum computers large enough to factor 100-digit numbers—factoring such a number requires billions of steps, so each step would need to be accurate to better than one part in a billion, a virtually impossible challenge in experimental physics. Fortunately, it is possible to design fault-tolerant circuits for quantum computers, which allow computations of arbitrary length to be performed with gates having accuracy of only some constant  $c$ . Current estimates using known methods for constructing fault-tolerant quantum circuits put this constant in the range of  $10^{-4}$  [25]; improved techniques could increase this value.

For some time after the factoring algorithm was discovered, however, it was believed that making quantum computers fault-tolerant was impossible. There were a number of plausible arguments for why this should be true. One argument for the impossibility of quantum error correction was based on the theorem, related to the Heisenberg uncertainty principle, that an unknown quantum state cannot be duplicated. The argument was that since you cannot duplicate quantum information, you cannot have more than one copy of a qubit around at any given time, and thus that it was impossible to protect a qubit from errors. Indeed, the simplest classical error correcting code is the 3-repetition code, which triplicates each bit, and other classical error correcting codes also appear to be based on repetition. Despite this pessimistic argument, quantum error correcting codes do exist, and

are generalizations of classical error-correcting codes. The codes protect quantum information from error and decoherence not by duplicating it, but by hiding it in subspaces of  $\mathbb{C}^{2^n}$  which are affected very little by decoherence and errors that act on only one qubit, or only a small number of qubits.

Before we discuss quantum error correcting codes in detail, we need to say more about the measurement process. For every set of orthogonal subspaces of  $\mathbb{C}^{2^n}$  which span the entire space, there is a measurement which outputs one of these subspaces as classical data, and which projects the original quantum state onto this subspace. For example, if our quantum state is  $\sum_{s=0}^{2^n-1} \alpha_s V_s$  and we measure the first qubit, we obtain the (not normalized) quantum state

$$\sum_{s'=0}^{2^{n-1}-1} \alpha_{0s'} V_{0s'} \quad \text{with probability} \quad \sum_{s'=0}^{2^{n-1}-1} |\alpha_{0s'}|^2, \tag{13}$$

and the state

$$\sum_{s'=0}^{2^{n-1}-1} \alpha_{1s'} V_{1s'} \quad \text{with probability} \quad \sum_{s'=0}^{2^{n-1}-1} |\alpha_{1s'}|^2. \tag{14}$$

This measurement corresponds to the partition of  $\mathbb{C}^{2^n}$  into the two subspaces generated by  $\{V_{0s'}\}$  and by  $\{V_{1s'}\}$ .

To illustrate how quantum error correcting codes work, we first explain what goes wrong when we try to extend the straightforward repetition code to the quantum realm. The obvious thing to do is to take

$$\begin{aligned} V_0 &\rightarrow V_{000} \\ V_1 &\rightarrow V_{111} \end{aligned} \tag{15}$$

This indeed does protect against value errors in our qubits. Suppose we apply the error transformation  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  to the first qubit. Then the encodings of  $V_0$  and  $V_1$  get taken to the states  $V_{100}$  and  $V_{011}$ , respectively. The subspace generated by these two quantum states is orthogonal to that generated by the original codewords  $V_{000}$  and  $V_{111}$ . We can thus make a measurement which reveals that there was a bit flip in the first qubit without measuring (and thus disturbing) the encoded quantum state. It is easily seen that bit flips applied to each of the three qubits create subspaces that are orthogonal to each other, so there is a quantum measurement which identifies on which qubit a bit flip error occurred without disturbing the encoded state. It is then straightforward to fix the bit flip error by applying a quantum gate to the qubit in error.

However, a phase error on one of the qubits is disastrous in this code. What happens when the error transformation  $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$  is applied to one of the qubit is that it takes an encoded  $V_0$  to an encoded  $V_0$ , and takes an encoded  $V_1$  to an encoded  $e^{i\phi} V_1$ . Thus, a phase error on any of the three qubits translates to a phase error on the encoded qubit, making the encoding three times as vulnerable to phase errors.

We now explain the above difficulty another way which illuminates the construction of quantum error-correcting codes. We consider phase flip errors, which are phase errors with  $\phi = \pi$ . There is a transformation that takes phase flips to bit flips and vice versa. This is the Hadamard transform, which is

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (16)$$

When this is applied to all the qubits in the code above, as well as the encoded qubits, we get the code

$$\begin{aligned} V_0 &\rightarrow \frac{1}{2}(V_{000} + V_{110} + V_{101} + V_{011}) \\ V_1 &\rightarrow \frac{1}{2}(V_{111} + V_{001} + V_{010} + V_{100}) \end{aligned} \quad (17)$$

Notice that for this code, a single bit flip interchanges  $V_0$  and  $V_1$ , so this code cannot correct bit flips, again showing that code (15) cannot correct phase flips.

What we need to make a good quantum error correcting code is a code having the property that bit flips can be corrected both before and after the application of the Hadamard transformation. Such a code can be found by generalizing the codes (15) and (17), and it was discovered independently by two groups [11, 31]. It is based on the classical 7-bit Hamming code, and is defined as follows:

$$\begin{aligned} V_0 &\rightarrow \frac{1}{\sqrt{8}}(V_{0000000} + V_{1110100} + V_{0111010} + V_{0011101} \\ &\quad + V_{1001110} + V_{0100111} + V_{1010011} + V_{1101001}) \\ V_1 &\rightarrow \frac{1}{\sqrt{8}}(V_{1111111} + V_{0001011} + V_{1000101} + V_{1100010} \\ &\quad + V_{0110001} + V_{1011000} + V_{0101100} + V_{0010110}). \end{aligned} \quad (18)$$

The indices of the basis vectors in the support of the encoded states are exactly the classical 7-bit Hamming code. The fact that the classical Hamming code corrects one error means this code can correct one bit flip. This quantum code is taken to itself under the application of the Hadamard transform (16) both to the encoded qubit and to each encoding qubit, showing that it is also able to correct one phase flip. In fact, it can correct a simultaneous bit flip and phase flip.

We now have a seven bit code that can corrects a phase and/or a bit flip applied to one of its qubits. This is by no means the complete set of possible quantum mechanical errors on one qubit; this set is parameterized by several continuous variables. However, the ability of a quantum code to correct the following set of four one-bit errors confers on it the ability to correct any possible one-bit quantum error:

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \quad (19)$$

These four errors correspond to no error, a bit flip, a phase flip, and a simultaneous bit and phase flip, respectively. We do not have enough space to explain this in

detail, but the fact that these form a basis for the set of  $2 \times 2$  matrices is enough to imply they can correct any one-bit quantum error. The rigorous details of this implication are in [11]; a more intuitive explanation is in [6].

This quantum Hamming code is the smallest nontrivial example of a set of codes based on linear binary codes named CSS codes after their discoverers [11, 31], and which contains codes that are much more efficient than this first one. For fault tolerance, which will be discussed next, we only need to use CSS codes. However, a more general framework that includes these codes was discovered simultaneously by two groups [19, 20, 10]. Substantial work on quantum error correcting codes has occurred since their discovery, much of it referenced in [10].

In classical computers, error correcting codes have been found to be very useful for storing and transmitting information, but not for providing fault-tolerant computing. It is difficult to perform gates on encoded qubits, and once the qubits have been decoded, they are no longer protected from error. Theoretically, the best way to provide high levels of fault tolerance for classical circuits was discovered by von Neumann, who discovered it after reasoning that some means of protection from error had to exist in biological systems. This method involves the use of massive redundancy. If you plan to run your computer for  $t$  steps, you make  $c \log t$  copies of every bit, and during the computation, you continually compare them in order to catch any errors you have made. The drawback of this method is that it requires  $c \log t$  overhead, which is too expensive for use in practice, given the remarkably low levels of error obtainable by current computer hardware. On the other hand, it can be shown that if you must use unreliable gates,  $O(\log t)$  overhead is required to achieve reliable computation, so von Neumann's construction is up to a constant factor best possible.

As in classical computers, quantum error correcting codes should work well for protecting qubits while they are being stored and transmitted. However, because quantum data cannot be cloned, fault tolerance using massive redundancy cannot work in quantum computers. We thus need another method. The methods currently known for providing fault tolerance in quantum computers are based on quantum error correcting codes [25, 29]. To use quantum error correcting codes for reliable computation, we need to show how to do two additional things with them, neither of which is at first glance obviously possible. These are:

1. correct errors using noisy gates so that errors are corrected faster than new errors are introduced;
2. perform quantum gates on encoded bits without decoding them, while making sure that any errors cannot propagate too widely during the computation.

We do not have much space to discuss how to accomplish these tasks, so we say nothing about the first task, and give only a very broad sketch of how the second task can be accomplished.

In order to compute on encoded qubits without decoding, we need fault-tolerant implementations of a universal set of quantum gates on the encoded qubits. What we need are circuits having the property that if errors occur in only a few quantum gates, or are present in a few of the inputs, these errors cannot affect too many of the qubits in the output of the gate (otherwise, there will



Figure 3: Implementation of a CNOT gate on qubits encoded using the quantum Hamming code (18). This circuit can be used in fault-tolerant quantum circuits, since an error in the  $i$ 'th wire of an encoded qubit (or in the  $i$ 'th gate) can only propagate to the  $i$ 'th wire of each of the output qubits. Gates that are implementable on encoded qubits in this fashion are called *transversal* gates.

be more errors than the quantum error-correcting codes we are using can correct). It turns out that certain gates are easy to implement this way. Figure 3 shows how to perform a CNOT on two encoded qubits by performing it on each pair of encoding wires. Similarly, if a Hadamard gate (16) is applied to each quantum wire, a Hadamard gate is performed on the encoded qubit. Implementations of this type are called transversal gates, and these do not form a universal set of quantum gates. We need to supplement the set of transversal gates with an extra gate implemented using another method. It was shown how to perform the Toffoli gate fault-tolerantly on encoded qubits in [29], and the set of transversal gates augmented by this gate is a universal set of gates.

To implement a circuit of size  $t$  fault-tolerantly, the techniques of [29] required gates with error rate at most  $O(1/(\log t)^c)$ . To obtain fault tolerance using gates with constant error rate requires a further idea: the use of concatenated codes. These are nested codes, where each layer catches most of the errors missed by the previous layer. Judicious use of concatenated codes and careful analysis shows that gates with some constant error rate are able to produce fault-tolerant quantum circuits; this constant is currently estimated at around  $10^{-4}$ . For more details, see the excellent survey of fault-tolerance in quantum computing [25].

## 7 OTHER WORK.

This section discusses areas related to quantum computing; it is not intended to be a complete survey, but a somewhat idiosyncratic view of some results I find interesting. I have tried to mention survey articles when they exist, so the interested reader can find pointers to the literature. One excellent resource is the quant-ph

preprint archive, at <http://xxx.lanl.gov/>, containing preprints of many recent research articles in this field. John Preskill, at Caltech, recently taught a course on quantum computing and quantum information, and his excellent set of lecture notes is available on the web [26].

As Feynman suggested, it appears that quantum computing is good at computing simulations of quantum mechanical dynamics. Some work has already appeared showing this [1, 24, 33], but much remains to be done.

A significant algorithm in quantum computing is L. K. Grover's search algorithm, which searches an unordered list of  $N$  items (or the range of an efficiently computable function) for a specific item in time  $O(\sqrt{N})$ , an improvement on the optimal classical algorithm, which must look at  $N/2$  items on average before finding a specific item [21]. The technique used in this algorithm can be applied to a number of other problems to also obtain a square root speed-up [22].

One of the earliest applications of quantum mechanics to areas related to computing is quantum cryptography, more specifically quantum key distribution. Consider two people trying to share some secret information which they can then use as a key for a cryptosystem. If they can only communicate over a phone line possibly open to eavesdroppers, they have no choice but to use public key cryptography [27], which may be open to attack by a quantum computer or (say) discovery of a fast factoring algorithm on a classical computer. However, if they in addition have access to an optical fiber which they can use to transmit quantum states, they can use quantum cryptography [4]. One of them (the sender) transmits states chosen at random from a set of non-orthogonal quantum states (e.g.  $V_0$ ,  $V_1$ ,  $\frac{1}{\sqrt{2}}(V_0 + V_1)$ ,  $\frac{1}{\sqrt{2}}(V_0 - V_1)$ ) The receiver then reads the states in either the basis  $\{V_0, V_1\}$  or  $\{\frac{1}{\sqrt{2}}(V_0 \pm V_1)\}$ , again chosen at random. Communicating over a classical channel using a special protocol, they can figure out the states for which they agree on the measurement basis; they should agree on about half the states, each of which supplies a bit towards a secret key. If an eavesdropper was listening, she cannot have gained too much information—since she does not know in which basis the states were transmitted, any information she gains must cause a disturbance in the states, which the sender and receiver can detect by measuring some of their states instead of using them for the secret key. They can also further sacrifice some of their bits to ensure that the eavesdropper gains virtually no information about the remaining bits of their key, and that they agree on all the bits of this key. Since the original quantum cryptography papers, there have been many articles either proposing other schemes or working towards rigorous proofs that the scheme is secure against all possible quantum attacks (i.e., when the eavesdropper has access to a quantum computer). A good bibliography on quantum cryptography is [8].

Quantum cryptography is but one aspect of a rapidly burgeoning subject, quantum information theory. A startling result in this field, the interest in which helped contribute to its recent rapid growth, was the discovery of quantum teleportation [5]. It is not possible to transmit an unknown quantum state using only classical information (say, over a telephone line). However, if two people share an EPR pair, such as the quantum state  $\frac{1}{\sqrt{2}}(V_{01} - V_{10})$ , with the sender holding

the first qubit and the receiver holding the second, then they can transmit an unknown quantum bit using a classical channel. The sender performs a combined measurement on the unknown state and the EPR pair, and transmits the classical two-bit outcome to the receiver, who then uses this information to reconstruct the unknown state from his half of the EPR pair. The act of teleportation thus uses up the resource of *entanglement* between the sender and the receiver, which is present in the EPR pair. One research direction in quantum information theory is quantifying the amount of entanglement in a quantum state. Another direction is measuring the classical and the quantum capacities of a quantum channel. More information on quantum information theory can be found in Preskill's course notes [26] and in the survey article [6].

Another recent development is the study of quantum communication complexity. If two people share quantum entanglement, as well as a classical communications channel, this permits them to send each other qubits, but does not reduce the number of bits required for transmission of classical information. However, if they both have some classical data, and they wish to compute some classical function of this data, shared quantum entanglement may help reduce the amount of purely classical communication required to compute this function. This was first shown by Cleve and Burhman [13]. More results on communication complexity have since been shown, and some of these were recently used to give lower bounds on the power of quantum computers in the black-box (oracle) model [9].

There has been a substantial amount of recent work on both quantum error correcting codes and quantum fault tolerance. Many results on quantum error correcting codes are reviewed in [10], and Preskill has written an excellent survey of fault tolerant quantum computing [25].

## REFERENCES

- [1] D. S. Abrams and S. Lloyd, Simulation of many-body Fermi systems on a universal quantum computer, *Phys. Rev. Lett.* 79 (1997), 2586–2589.
- [2] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Elementary gates for quantum computation, *Phys. Rev. A* 52 (1995), 3457–3467.
- [3] C. H. Bennett, Logical reversibility of computation, *IBM J. Res. Develop.* 17 (1973), 525–532.
- [4] C. H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (1984) 175–179.
- [5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, *Phys. Rev. Lett.* 70 (1993), 1895–1898.
- [6] C. H. Bennett and P. W. Shor, Quantum information theory, *IEEE Transactions on Information Theory* (1998), to appear.

- [7] E. Bernstein and U. Vazirani, Quantum complexity theory, *SIAM J. Computing* 26 (1997), 1411–1473.
- [8] G. Brassard, Quantum cryptography: a bibliography, *SIGACT News* 24:3 (1993), 16–20. A more recent version is online at:  
<http://www.iro.umontreal.ca/~crepeau/Biblio-QC.html>.
- [9] H. Burhman, R. Cleve and A. Wigderson, Quantum vs. classical communication and computation, in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, ACM Press, New York (1998), 63–69.
- [10] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over  $GF(4)$ , *IEEE Transactions on Information Theory* 44 (1998), 1369–1387.
- [11] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, *Phys. Rev. A* 54 (1995) 1098–1106.
- [12] J. I. Cirac and P. Zoller, Quantum computations with cold trapped ions, *Phys. Rev. Lett.* 74 (1995), 4091–4094.
- [13] R. Cleve and H. Burhman, Substituting quantum entanglement for communication, *Phys. Rev. A* 56 (1997), 1201–1204.
- [14] D. G. Cory, A. F. Fahmy and T. F. Havel, Ensemble quantum computing by nuclear magnetic resonance spectroscopy, *Proc. Nat. Acad. Sci.* 94 (1997), 1634–1639.
- [15] D. Deutsch, Quantum theory, the Church–Turing principle and the universal quantum computer, *Proc. Roy. Soc. London Ser. A* 400 (1985) 96–117.
- [16] R. Feynman, Simulating physics with computers, *Internat. J. Theoret. Phys.* 21 (1982), 467–488.
- [17] E. Fredkin and T. Toffoli, Conservative logic, *Internat. J. Theoret. Phys.* 21 (1982), 219–253.
- [18] N. A. Gershenfeld and I. L. Chuang, Bulk spin resonance quantum computation *Science* 275 (1997), 350–356.
- [19] D. Gottesman, A class of quantum error-correcting codes saturating the quantum Hamming bound, *Phys. Rev. A* 54 (1996), 1862–1868.
- [20] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*, Ph.D. Thesis, California Institute of Technology (1997). Also LANL e-print <http://xxx.lanl.gov/> quant-ph/9705052, available online at <http://xxx.lanl.gov/>.
- [21] L. K. Grover, Quantum mechanics helps in searching for a needle in a haystack, *Phys. Rev. Lett.* 78 (1997), 325–328.

- [22] L. K. Grover, A framework for fast quantum mechanical algorithms, in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, ACM Press, New York (1998), 53–62.
- [23] B. E. Kane, A silicon-based nuclear spin quantum computer, *Nature* 393 (1998), 133–137.
- [24] S. Lloyd, Universal quantum simulators, *Science* 273 (1996), 1073–1078.
- [25] J. Preskill, Fault-tolerant quantum computation, to appear in *Introduction to Quantum Computation*, H.-K. Lo, S Popescu and T. P. Spiller, eds. (1998). Also LANL e-print quant-ph/9712048, available online at <http://xxx.lanl.gov/>.
- [26] J. Preskill, Lecture notes for Physics 229 (1998), available online at <http://www.theory.caltech.edu/people/preskill/ph229/>.
- [27] R. L. Rivest, A. Shamir and L. Adleman, A method of obtaining digital signatures and public-key cryptosystems, *Comm. Assoc. Comput. Mach.* 21 (1978), 120–126.
- [28] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Computing* 26 (1997), 1484–1509.
- [29] P. W. Shor, Fault-tolerant quantum computation, in *Proc. 37th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos, CA (1996), 56–65.
- [30] D. R. Simon, On the power of quantum computation, *SIAM J. Computing* 26 (1997), 1474–1483.
- [31] A. Steane, Multiple particle interference and quantum error correction, *Proc. Roy. Soc. London Ser. A* 452 (1996), 2551–2577.
- [32] A. Yao, Quantum circuit complexity, in *Proceedings of the 34th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos, CA (1993), 352–361.
- [33] C. Zalka, Efficient simulation of quantum systems by quantum computers, *Proc. Roy. Soc. London Ser. A* 454 (1998), 313–322.
- [34] C. Zalka, Fast versions of Shor’s quantum factoring algorithm, LANL e-print quant-ph/9806084 (1998), available online at <http://xxx.lanl.gov/>.
- [35] W. H. Zurek, Decoherence and the transition from quantum to classical, *Physics Today* 44 (1991) 36–44.

Peter W. Shor  
AT&T Labs – Research  
180 Park Ave.  
Florham Park, NJ 07932 USA  
[shor@research.att.com](mailto:shor@research.att.com)

THE POPULATION DYNAMICS  
OF CONFLICT AND COOPERATION

KARL SIGMUND

Keywords and Phrases: Lotka Volterra equations, replicator dynamics, permanence, heteroclinic cycles, iterated games.

1. INTRODUCTION The last decades have seen an explosive growth in biosciences, and astonishing progress in the mathematical modelling of fields as diverse as neurobiology, membrane formation, biomechanics, embryology, etc (see e.g. J. Murray, 1990). The sequencing of biomolecules produces such a vast wealth of data on proteins and polynucleotides that the mere handling of the stored information becomes a computational challenge, let alone the analysis of phylogenetic trees and functional networks which is the main task of bioinformatics.

The recent advances in our understanding of the chemical mechanisms describing the interactions of specific molecules – how virus, for example, use binding proteins to attack and penetrate hosts cells – are spectacular, but do not suffice to tackle basic problems like disease progression or the co-evolution of hosts and parasites. It is *populations* of virus particles, or immune cells, or hosts, that regulate each other's frequencies. The feedback loops of these ecosystems are too complex to be understood by verbal arguments alone. The biological community has come to accept that basic aspects of immunology and evolutionary ecology can only be analysed by mathematical means.

This has not always been the case. The pioneering work in genetics due to Fisher, Haldane, Wright, and Kimura, as well as the epidemiological models of Kermack and McKendrick occupied a marginal position in biology for the most part of this century, while at the same time motivating important mathematical advances in statistics, stochastic processes and dynamical systems (Fisher (1918) on correlation, Kolmogoroff (1937) on travelling waves in a gene pool, May (1976) on chaos). The models of evolutionary biology cannot compete in mathematical depth and sophistication with those of theoretical physics, but they offer a wide range of questions of great intuitive appeal.

This lecture surveys mathematical models in ecology and evolution, emphasising the major feedback mechanisms regulating the population densities of the interacting self-replicating units – be they genes, virus particles, immune cells or host organisms. The great variety of biological examples made it necessary to economise on mathematical diversity, by keeping to the framework of ordinary differential equations. This is certainly not meant to imply that time delays, spatial heterogeneities and stochastic fluctuations are secondary effects. In fact, they have a major impact in many applications (see, e.g., the survey by Levin et al., 1997)

2. POPULATION ECOLOGY If we assume that  $n$  species live in an ecosystem, that  $x_i$  is the density of species  $i$  and that its per capita growth rate  $\dot{x}_i/x_i$  depends on the densities of the interacting populations, then we obtain the ecological equation

$$\dot{x}_i = x_i f_i(x). \quad (1)$$

The state space  $\mathbb{R}_+^n$  is invariant; so are its boundary faces, where one or several of the densities are 0; and the restriction of (1) to a face is again an ecological equation. If the  $f_i$  are affine linear, we obtain – as simplest example – the Lotka-Volterra equation

$$\dot{x}_i = x_i(r_i + \sum a_{ij}x_j) \quad (2)$$

( $i = 1, \dots, n$ ). It should be stated right at the outset that many ecological interactions display more complex interaction terms; but often, (2) offers a first approximation which is flexible enough to embody the main aspects of the community structure (Hofbauer and Sigmund, 1998). For instance, if 1 is a prey species and 2 its predator, we obtain

$$\dot{x}_1 = x_1(a - bx_2) \quad (3)$$

$$\dot{x}_2 = x_2(-c + dx_1). \quad (4)$$

where  $a, b, c, d > 0$ . In  $\text{int}\mathbb{R}_+^2$  there exists a unique fixed point  $(c/d, a/b)$  which is surrounded by periodic orbits. If we add a self-limitation of the prey, i.e. set  $f_1 = a - ex_1 - bx_2$  in (3), we obtain damped oscillations around the fixed point, or (if  $e > 0$  is large) extinction of the predator (see fig. 1).

Fig. 1: Predator-prey equations

On the other hand, if 1 and 2 are species competing for the same resources, we have to assume that the intrinsic growth rates satisfy  $r_i > 0$  and the interaction terms  $a_{ij} < 0$  ( $i, j \in \{1, 2\}$ ). On each positive half-axis, there is one fixed point  $F_i$  corresponding to equilibrium of species  $i$  in the absence of the other species. Generically, there are three possible outcomes (see fig. 2):

(a) *dominance*: all orbits in  $\text{int}\mathbb{R}_+^2$  converge to  $F_i$ ; species  $i$  is said to dominate the other species;

- (b) *coexistence*: there exists a fixed point  $F_{12} \in \text{int}\mathbb{R}_+^2$  which is globally stable (i.e. attracts all orbits in  $\text{int}\mathbb{R}_+^2$ );
- (c) *bistability*:  $F_{12}$  is a saddle; almost all orbits in  $\text{int}\mathbb{R}_+^2$  converge to  $F_1$  or  $F_2$ , depending on the initial condition.

Fig. 2: Competition equations

Because two-dimensional Lotka-Volterra equations admit no limit cycles, their dynamics can be easily classified; for three or more species, this is no longer the case. Systems with two competing species and one prey exhibit chaos and systems with three competing species (which are monotonic and hence admit no chaos, see Hirsch, 1988) have not been classified yet, in spite of impressive progress (van den Driessche and Zeeman, 1998). One of the reasons is the existence of *heteroclinic cycles*, see fig. 3(a) (May and Leonard, 1975). If, in the absence of the third species, species 1 dominates 2, 2 dominates 3 and 3, in turn, dominates 1, then the boundary of  $\mathbb{R}_+^3$  contains a heteroclinic cycle consisting of three saddle points  $F_i$  (with only species  $i$  present) and three connecting orbits (orbit  $o_1$  has  $F_2$  as  $\alpha$ - and  $F_1$  as  $\omega$ -limit etc). Depending on the products of the eigenvalues in the stable and unstable directions, this heteroclinic cycle can attract or repel the neighbouring orbits in  $\text{int}\mathbb{R}_+^3$ . Three competing species with heteroclinic cycles have been found in laboratory populations. In higher dimensional ecological models, heteroclinic cycles become common. Such cycles are non-generic features for general dynamical systems, since saddle-connections can be destroyed by arbitrarily small perturbations. Within the class of ecological equations, however,



which leave the boundary faces of  $\mathbb{R}_+^n$  invariant, heteroclinic cycles and *networks* (where several cycles issue from one saddle) are usually robust. Such attractors offer a new brand of nonlinear dynamics: orbits approach saddle points ever more closely, and remain there for increasingly long times; furthermore, the sequence of saddles visited by an orbit can switch in arbitrary order from one cycle to another (Chawanya, 1995).

Fig. 3: Heteroclinic orbits and networks

3. PERMANENCE If the orbit of an ecosystem reaches the neighborhood of a heteroclinic attractor on the boundary, some species are doomed. The ecosystem, in that case, is unstable: this notion of stability has nothing to do, however, with the usual asymptotic stability of a fixed point, which is a local notion. A more suitable stability notion in this context is that of *permanence*: (1) is said to be permanent if the boundary (including infinity) is a repeller, i.e. if there exists a compact set  $K \subset \text{int}\mathbb{R}_+^n$  such that whenever initially  $x \in \text{int}\mathbb{R}_+^n$ , then  $x(t) \in K$  for  $t$  sufficiently large. (After a transient phase, all densities are uniformly bounded away from 0). This notion has been extensively explored (see the survey by Hutson and Schmitt, 1992). Permanence implies the existence of a fixed point in  $\text{int}\mathbb{R}_+^n$ , but this point need not be locally stable; and indeed ecologists view an ecosystem as stable even if it exhibits violent oscillations, as long as its species remain safe from extinction.

For a dissipative system (all orbits uniformly bounded from above), the most useful sufficient condition for permanence is the existence of an average Lyapunov function. This is a function  $P$  vanishing on the boundary and positive on the interior such that the continuous extension  $\Psi$  of the logarithmic derivative of  $P$  has the property that for every  $\omega$ -limit point  $x$  on  $bd\mathbb{R}_+^n$  there is a  $T > 0$  with

$$\int_0^T \Psi(x(t)) dt > 0. \quad (5)$$

Then  $P$  grows (in the long run) along every interior orbit sufficiently close to the boundary. In particular (2) is permanent if all orbits are uniformly bounded and the set

$$N := \{x \in \mathbb{R}_+^n : r_i + \sum a_{ij}x_j < 0, i = 1, \dots, n\} \quad (6)$$

is disjoint from the convex hull of the fixed points on the boundary. The condition is not necessary for permanence if  $n > 3$ . But if (2) is permanent, then there is a *unique* equilibrium  $\hat{x}$  with all species present, and it is the limit of all time-averages of orbits in the interior of the state-space. If  $D$  is the Jacobian at  $\hat{x}$ , then  $(-1)^n \det D > 0$ , and  $\text{trace } D < 0$ . Furthermore,  $(-1)^n \det A > 0$ , where  $A$  is the matrix of the interaction terms  $a_{ij}$  (Hofbauer and Sigmund, 1998).

4. INVASION Many studies have considered the assembly of ecological communities by sequential invasion (i.e. adding one species at a time). Will species  $n + 1$  grow when introduced in small numbers? If the resident system is in equilibrium  $z = (z_1, \dots, z_n)$ , this simply means to check whether the growth rate  $f_{n+1}(z, 0)$  is positive. If the competition between two species is bistable, for instance, none can invade the other. If there is coexistence, each can invade, etc. Invasion is a question of *transversal stability*, which, if the resident system admits a chaotic attractor, offers subtle ergodic twists involving riddled basins of attraction etc (Ferriere and Gatto, 1995, Ashwin et al, 1996).

If the resident species obey a permanent Lotka-Volterra equation with fixed point  $z \in \text{int}S_n$ , the condition  $f_{n+1}(z, 0) > 0$  implies that the lim sup of the invading species' density is positive, but tells nothing about the lim inf. The new attractor need not be close to the former one; the invading species can drive others to extinction, and even ultimately itself. Hofbauer (1998) has found conditions in terms of spatial or temporal averages of the initial growth rate which guarantee that the invasion of a permanent Lotka-Volterra community succeeds. His bifurcation analysis allows to decide whether, if a parameter changes so that invasion becomes possible, the new attractor is contained in a neighborhood of the resident attractor or not. The invasion of a heteroclinic cycle is a particularly arduous problem.

Evidence from field studies and numerical simulations suggest that ecosystems become increasingly harder to invade as time goes on, and that there is an upper limit to how 'closely packed' species can be; but so far, this has only been demonstrated under restrictive assumptions. Interestingly, predators can stabilise ecosystems: if a 'keystone' predator is removed from a permanent system, the remaining system is no longer permanent. For instance, if species 1 dominates species 2, or if the competition between species 1, 2 and 3 results in a heteroclinic attractor, then a suitable predator can mediate co-existence; Schreiber (1998) has produced systems with  $n$  competing prey, each with its specialised predator, such that removal of any predator species results in only one prey species surviving. Such ecosystems cannot be obtained by simply adding one species at a time; sequential assembly has to proceed in a more roundabout way, using species that are later eliminated like a scaffolding. These results agree well with the current

emphasis of biologists on the role of contingency and history dependence in real ecological succession chronicles, and highlight the fact that a successful invasion can initiate a surprising sequence of changes in the ecosystem (see Mylius et al, 1998).

5. REPLICATOR DYNAMICS Competition between conspecifics drives natural selection. The basic mechanism is simple: an inheritable trait which allows for a higher reproductive success spreads in the population. This can lead to extraordinary feats of adaptation due to relentless *optimisation under constraint*. In fact, some computational approaches to optimisation problems are mimicking the massively parallel algorithm of Darwinian evolution. Within ‘populations’ of possible solutions to a given problem (for instance in aerodynamics), those which perform better are allowed to multiply at the expense of the others. Occasionally, some ‘offspring’ is randomly altered, corresponding to the mutation or recombination of existing solutions. Such *genetic algorithms* allow to explore the space of solutions and often to home in on some optima (Forrest, 1993).

But in biology, it is the population itself that is often the problem. The efficiency of a wing shape may be independent on what the other birds are doing, but the success of a sex ratio or of a given degree of aggressivity is not. In a population with a surplus of males, it pays to produce females; it pays to escalate a conflict if the others are unlikely to escalate, but otherwise it is better to avoid escalating, etc. *Game theory*, rather than optimisation, is appropriate to deal with problems where the success depends on what the others are doing.

Assume that  $x_i$  is the frequency of the individuals using strategy  $i$  ( $i = 1, \dots, n$ ). A strategy, in this context, is simply a trait (behavioural, physiological, morphological) whose payoff, i.e. average reproductive success, depends on the frequencies  $x$  of the competing types. If the traits are inherited, the frequencies will evolve in time, depending on their success. If individuals breed true, the per capita rate of increase  $\dot{x}_i/x_i$  is given by the difference  $f_i - \bar{f}$ , where  $f_i(x)$  is the average payoff for using  $i$  if the population is in state  $x$ , and  $\bar{f} = \sum x_j f_j$  is the average success in the population. This yields the replicator equation

$$\dot{x}_i = x_i(f_i(x) - \bar{f}) \quad i = 1, \dots, n \quad (7)$$

on the simplex  $S_n = \{x \in \mathbb{R}_+^n : \sum x_i = 1\}$ . This simplex is invariant, and so are its faces. The replicator equation is closely related to the ecological equation (1), of course. It introduces an ecological viewpoint into game theory.

Let us consider a conflict between pairs of individuals, for instance some contest over a resource, and assume that the strategies  $i$  correspond to different types of fighting behaviour, and that  $a_{ij}$  is the average payoff for using  $i$  if the co-player uses  $j$ . Then the payoff matrix  $A = (a_{ij})$  determines the average payoff  $(AX)_i = a_{i1}x_1 + \dots + a_{in}x_n$  for strategy  $i$  in the population (assuming that individuals meet randomly) and (7) turns into

$$\dot{x}_i = x_i((AX)_i - x^T Ax). \quad (8)$$

This equation is not only similar, but actually equivalent to a Lotka-Volterra equation for  $n - 1$  species: a diffeomorphism from  $S_n$  (minus one face) to  $\mathbb{R}_+^{n-1}$  maps orbits of one dynamical system onto the other, and vice versa. For  $n = 2$ , we obtain the same generic behaviour as for two competitors: dominance, coexistence or bistability. For  $n = 3$ , heteroclinic cycles show up (not just as a theoretic possibility: the mate guarding strategies of male lizards form a rock-scissors-paper cycle). With  $n > 3$ , limit cycles and chaotic attractors occur. (8) is permanent if there exists a  $\mathbf{p} = (p_1, \dots, p_n)$  with  $p_i > 0$  for all  $i$  such that for every equilibrium  $\mathbf{z}$  on the boundary,

$$\mathbf{p}^T A \mathbf{z} > \mathbf{z}^T A \mathbf{z} \tag{9}$$

(a conditions that can easily be checked by linear programming), etc.

Frequency-dependent selection will not optimise, in general. Only for very special interaction do replicator equations become gradients: if the game is symmetric, for instance ( $A = A^T$ ) or more generally if the partial derivatives  $f_{i,j} = \partial f_i / \partial x_j$  obey

$$f_{i,j} + f_{j,k} + f_{k,l} = f_{l,k} + f_{k,j} + f_{j,i} \tag{10}$$

for all  $i, j, k$  (one has to use a suitable Riemannian metric on  $S_n$ , cf. Hofbauer and Sigmund, 1998).

6. OTHER GAME DYNAMICS Among higher animals, and in particular humans, strategies can also spread by learning and imitation. Depending on the details of transmission, this leads to a large number of game dynamics for the frequencies  $x_i$ , often based on underlying stochastic processes. Again, the replicator dynamics is a kind of benchmark. Another example is the best reply dynamics (a differential inclusion)

$$\dot{x}_i \in \beta(x) - x_i \tag{11}$$

where  $\beta(x)$  is the set of strategies whose payoff (in a population where strategy  $i$  occurs with frequency  $x_i$ ) is maximal. The idea is that in every short time interval, a small fraction of the players updates their strategy: these players know how to optimise, but do not anticipate that others will also update. The orbits of (11) are piecewise linear. Intriguingly, their asymptotic behaviour is often that of the *time averages* of the solutions of the replicator equation (8).

This brings one closer to classical game theory. Let us consider a game with payoff matrix  $A$  and assume that points  $\mathbf{p} \in S_n$  are *mixed strategies* ( $p_i$  being the probability for a player to use strategy  $i$ ). Then  $\mathbf{p}$  is a best reply to  $\mathbf{q} \in S_n$  if  $\mathbf{p}^T A \mathbf{q} \geq \mathbf{x}^T A \mathbf{q}$  for all  $\mathbf{x} \in S_n$ . A point  $\mathbf{p}$  is a (symmetric) Nash equilibrium if it is a best reply against itself. A Nash equilibrium is a fixed point for (8) (and every other decent game dynamics), but the converse need not hold. In fact, the Nash equilibria are precisely the fixed points of (8) which are *saturated* – missing pure strategies have no selective advantage. Every game with finitely many strategies has a Nash equilibrium, but there are games such that almost no solution, under any reasonable adjustment dynamics, converges to a Nash equilibrium.

Evolutionary game theory has originated with the concept of *evolutionarily stable strategies* (ESS). Intuitively, a strategy  $Q$  is said to be an ESS if, whenever all members of the population adopt it, an invading (and sufficiently small) minority using a different strategy has no selective advantage (Maynard Smith, 1982). This means that  $Q$  is Nash, and that whenever  $P$  is an alternative best reply to  $Q$ , then  $Q^T A P > P^T A P$ . Equivalently,  $Q$  is an ESS if

$$Q^T A x > x^T A x \quad (12)$$

for all  $x \neq Q$  in a neighborhood of  $q$ . Not every game has an ESS. The connexion with the replicator equation is given by the following characterisation:  $Q \in S_n$  is an ESS if and only if, whenever  $Q$  is a convex combination of the (possibly mixed) strategies  $P^1, \dots, P^m$ , the *mean population strategy*  $\sum x_i P^i$  converges (under the replicator dynamics) towards  $Q$  if initially it was close to  $Q$  (Cressman, 1992). The idea that evolution always results in an ESS is not justified, however. There exist considerably more complex outcomes, as captured in the notion of an evolutionarily stable *attractor*, for instance (Rand et al, 1994).

7. LONG-TERM EVOLUTION So far we have assumed that offspring are clones of their parent: ‘like begets like’. The machinery of Mendelian inheritance is much more complex, and we have to follow the frequencies of genes in the *gene pool* of the population. As long as the instruction is contained in one genetic locus (an address in the genome, housing two genes – one from the father and the other from the mother), the corresponding dynamics for the gene frequencies in the population is still of replicator type (7). But in general, the trait depends on several genetic loci, which can be recombined during reproduction, and the dynamics becomes challenging.

The state  $x$  of the gene pool determines the frequencies of the different types of individuals, who use different (pure or mixed) strategies. This determines the frequencies  $P(x)$  of the strategies in the population, and hence the reproductive success of each type, and therefore the rate of change in the gene frequencies  $x$ . If the trait is determined by one genetic locus only, and if there are at most two pure strategies, or three types of genes which can occur on that locus, then an ESS  $Q$  which is feasible is *strategically stable* in the sense that if a state  $\hat{x}$  of the gene pool satisfies  $P(\hat{x}) = Q$ , then every near-by state  $x$  remains close to  $\hat{x}$  and  $P(x)$  converges back to  $Q$  (Cressman et al 1996). For more complex genetic mechanisms, the relation between evolutionary stability and long-term stability (i.e. strategic stability against every invasion attempt) remains unclear, and offers a wealth of problems on normal forms and center manifold theory. The replicator dynamics can be used as a first approximation in the absence of more specific information on the genetic background. That kind of information is likely to be provided soon, and will act as a motivational booster for the population genetics of frequency-dependent selection.

At the present state, the best prospects for studying long-term evolution are offered by *adaptive dynamics*. It is based on the assumption that replication is

only almost exact, and that occasional mistakes – mutations – occur so rarely that the fate of one mutation (its extinction or fixation under selection) is settled before the next mutation occurs (Metz et al, 1996). The population is thereby assumed to consist of one type only, which can be substituted by another type etc. This describes a dynamics in trait space which seems utterly remote from the description of population frequencies given by replicator dynamics but which, in important cases, reduces to it. In particular, if the trait space is a simplex (for instance, probabilities for certain types of behaviour) with a suitable Riemannian metric, one obtains (7) again. But this should not obscure the fact that replicator dynamics and adaptive dynamics address fundamentally different processes operating on distinct time-scales. One describes short-term evolution – the population dynamics of the frequencies of a given set of genes, or traits; the other describes long-term evolution, the repeated introduction of new mutations (Eshel, 1996).

If the invader's reproductive success is a linear function of its trait, then an ESS is locally stable for each adaptive dynamics; but for many examples, this assumption does not hold, and the evolution in trait space may well lead *away* from an ESS.

Often, two players engaged in a biological 'game' belong to different populations, with different sets of strategies. Most of the previous results carry over to such two-role games, but the general tendency is that there is still less stability: for instance, no mixed strategy can be an ESS; there exists an incompressible volume form; heteroclinic cycles become more frequent, etc.

The interacting populations can be different species – for instance, predators and their prey – and in this case adaptive dynamics leads to models of *co-evolution*. A typical question in this context is whether co-evolution may lead to interaction parameters such that the population numbers oscillate chaotically – a question on which the jury is still out. The interacting populations can also belong to the same species: males and females have conflicting interests about their amount of parental investment, owners and intruders about territorial issues, etc. In that case, role-specific strategies are likely to evolve, for example 'if owner, be prepared to fight to the end; if intruder, avoid escalation'.

Before turning to some applications, it should be emphasised again that essential aspects can change completely if supplementary effects are included, for instance spatial distribution (Takeuchi, 1996), genetic or physiological heterogeneity, stochastic fluctuations (Durrett, 1991) or time lags (Gopalsamy, 1992).

8. POPULATION DYNAMICS OF INFECTIOUS DISEASES Applications of mathematical modelling to epidemiology, immunology and virology are of increasing biomedical relevance. They help to understand the course of infectious diseases both within organisms and within populations, and suggest guidelines for treatment and vaccination.

Within a population, the interactions of infected, susceptible and immune organisms lead to endemic or epidemic spread of the disease. In a commonly used epidemiological model (Anderson and May, 1991), if frequencies of uninfected and

infected hosts are denoted by  $x$  and  $y$ , this becomes

$$\dot{x} = k - dx + cy - \beta xy \quad (13)$$

$$\dot{y} = y(\beta x - d - v - c) \quad (14)$$

where  $k$  is a constant birth (or immigration) term,  $d$  the mortality of uninfected,  $v$  the extra mortality due to the infection, i.e. the *virulence*, and  $c$  the rate of recovery (which in this simple model does not confer immunity). The model assumes that new infections occur through random contacts between infected and susceptibles. An infection can only spread if the frequency  $x$  of uninfected exceeds  $(d + c + v)/\beta$ . This threshold principle, a cornerstone of epidemiology, holds for most of the variants of the model (including immunity, other transmission mechanisms, periodic oscillations in susceptibility, other birth and death rates, etc). For many diseases, one has to consider several classes of hosts (different risk groups, for instance, in the case of AIDS, see Dietz and Hadeler, 1986). Some of these extensions lead to chaotic dynamics (Grenfell and Dobson, 1995, Olsen and Schaffer, 1990).

Infections are caused by pathogens (virus, bacteria, protozoa), which can all be subsumed as parasites. In (13-14), the pathogen can invade only if the disease-free equilibrium  $x = k/d$  is not saturated, i.e. if the *basic reproductive rate*

$$R_0 = \frac{k\beta}{d(d + v + c)} \quad (15)$$

(the number of secondary infections produced by an infected in a population of susceptibles) exceeds 1.

The population dynamics of disease-carrying parasites, and their impact on the population dynamics of the host, is an area of rapid growth. Even the simplest models display oscillations. The relation between parasites and their host resembles that between predators and prey, of course: parasites can mediate permanent co-existence between competing strains of hosts, etc. Heteroclinic cycles are likely to occur, for instance when two strains of a host engaged in a bistable competition are beset by two suitably specialised strains of parasites: a resident population of host 1 can be invaded by parasite 1, the resulting equilibrium can be invaded by host 2 (eliminating hosts and parasites of type 1), which in turn allows parasite 2 to invade, etc.

The dynamics described so far deal with the course of an infection *within a population*. Its development *within an individual host* is no less dramatic, and constitutes a new chapter in biomathematics, dealing with the population dynamics and evolution of the 'biosphere' beneath the skin of the host organism. These ecological systems are ideally suited for modelling, since they involve huge populations and short generations, and are subject of intensive clinical tests.

HIV offers the most studied example. As is well-known, the full-blown symptoms of AIDS develop only after a latency period of some ten years. But this quietness is misleading. Clinical tests based on simple dynamical models have revealed a fierce battle between the virus and the immune system of the HIV-infected patient. The average rate of HIV production exceeds  $10^{10}$  particles a day. Free

virus particles are cleared within a few hours. Virus infected cells live on average two days.

HIV needs human cells (the ‘target cells’) to reproduce. In doing so, it kills these cells. Hence virus and target cells interact in much the same way as predators and their prey. But HIV is not only a predator, it is also a prey. The immune system contains a vast repertoire of possible responses (different types of antibodies, killer cells, etc), whose production is stimulated by specific pathogens. The immune responses attack and destroy the pathogens. Thus killer cells and virus also interact like predators and prey. Much clinical research has recently gone into finding out which role – prey or predator – has more relevance for HIV dynamics. At present, it appears that target cell limitation and immune control are of the same magnitude. This leads to prey-predator-superpredator systems which, as known from ecology (e.g. Hastings and Powell, 1991), exhibit complex dynamics. In our case, the simplest model reduces to

$$\begin{aligned}\dot{x} &= k - dx - \beta xv \\ \dot{y} &= \beta xv - ay - pyz \\ \dot{v} &= ry - sv \\ \dot{z} &= cyz - bz\end{aligned}\tag{16}$$

Here  $x$  (resp.  $y$ ) are the frequencies of uninfected (resp. infected) cells,  $v$  that of free virus particles and  $z$  the abundance of the killer cells produced by the immune response (Nowak and Bangham 1996, DeBoer and Perelson 1998). There is a minimum threshold of infected cells to activate an immune response ( $y > b/c$ ). The frequencies oscillate around an equilibrium value which can be stable or unstable, i.e. subject to a Hopf bifurcation. The model shows that increasing the responsiveness  $c$  of the immune system decreases the abundance  $y$  of infected cells, but not necessarily the density  $z$  of the killer cells; in other words, there is no simple correlation between virus load and the magnitude of the immune response.

9. THE EVOLUTION OF VIRULENCE Most pathogens evolve very quickly, due to their short generation time, their high mutation rate and the intensive selection pressure acting on them. HIV, for instance, spends on average 1500 generations within the body of a patient. During this time, its genetic diversity increases relentlessly, due to copying errors, so that the immune system is faced with ever new challenges.

Mathematical models of the interaction between virus replication and immune response led to completely new interpretations of disease progression in HIV infection (Nowak et al., 1991). HIV evolution can shift the steady state within an infected individual, and lead to escape from immune responses. Such immune responses are triggered by specific parts (so-called *epitopes*) of the virus. In the simplest model, the virus has two epitopes with two variants each, yielding an eight-dimensional predator-prey equation:

$$\dot{v}_{ij} = v_{ij}(r_{ij} - x_i - y_j)$$



$$\begin{aligned}\dot{x}_i &= x_i(c_i(v_{i1} + v_{i2}) - b) \\ \dot{y}_j &= y_j(k_j(v_{1j} + v_{2j}) - b)\end{aligned}\tag{17}$$

where  $v_{ij}$  is the concentration of the virus with sequence  $i$  at the first and  $j$  at the second epitope ( $1 \leq i, j \leq 2$ ), and  $x_i$  and  $y_j$  are the concentrations of antibodies directed at sequence  $i$  of the first resp.  $j$  of the second epitope. Generically, one or two of the four viral species and the same number of antibody species have to vanish, and the remaining densities oscillate (Nowak et al, 1995). A homogenous virus population induces an ‘immunodominant’ response against a single epitope, but a new variant at this epitope can cause the immune response to shift to the other epitope. Heterogenous virus population stimulate complicated fluctuating responses.

This dynamic picture of HIV infection was confirmed by detailed analysis of virus decay slopes in drug treated patients. Again mathematical models were at the core of this newly developing demography of virus infection.

The extreme mutability of HIV explains also why drug-resistant forms emerge so rapidly. Resistance against combinations of drugs requires several mutations. Mathematical models help in devising optimum treatment schedules based on combination therapy.

This is one chapter of a ‘Darwinian medicine’ grounded in evolutionary biology. In this domain, the evolution of *virulence* (i.e. the parasite-induced mortality of host organisms) is of particular importance (Levin and Pimentel, 1981, Frank, 1996). Pathogens use the bodies of their hosts both as resource and as vehicle. Textbook knowledge presumed that parasites would always evolve towards decreased virulence, since it is better to milk the host rather than butcher it. If parasites become too virulent, they face extinction by depleting their reservoir of susceptibles. It was concluded that successful parasites all become benign. The most impressive example of such an evolution towards harmlessness is the myxoma virus, released in Australia to kill rabbits: within few years, the death rate of infected rabbits dropped from more than 99 percent to less than 25 percent. Similar trends have been observed in many human diseases. Adaptive dynamics shows that evolution can actually turn parasites into mutualists necessary for the survival of their hosts (Law and Dieckmann, 1998).

But not all parasites become harmless. Selection for a higher basic reproductive rate  $R_0$  often leads to conflicting demands on infectivity and long-term exploitation. If in (15), for instance, the virulence  $v$  is an increasing function of the transmission rate  $\beta$ , then  $R_0$  need not necessarily decrease in  $v$ . And in the case of super-infection, i.e. when several strains compete *within a host*, selection on parasites does not optimise  $R_0$ . Roughly speaking, more virulent strains will have a selective advantage in the intra-host competition, and less virulent in the inter-host competition. Parasites face a so-called *tragedy of the commons*: the need to outgrow their rivals forces them to over-exploit the host, thus possibly driving their common resource to extinction. Game theoretical arguments help in analysing such situations. In general, there will be no evolutionarily stable strain (Nowak and May, 1994).

Of particular interest is the adaptive dynamics of viral particles which can

spread either by horizontal transmission, i.e. by infecting of new hosts, or by vertical transmission, in the form of *provirus* integrated into the host's genome. Even if we assume that two strains cannot co-exist within one host (no superinfection), they can coexist within the population if one is favoured by vertical and the other by horizontal transmission (Lipsitch et al, 1996).

10. FROM THE RED QUEEN TO THE MAJOR TRANSITIONS The parasite's ecology is further complicated by countermeasures of the hosts which tend to reduce virulence. Due to their short generation time, parasites can quickly adapt to prevailing host defenses, but sexual reproduction allows host organisms to recombine their genes and thus to present shifting targets to the pathogens trying to enter the cells.

Many evolutionary biologists view this as the main reason for the prevalence of sexual reproduction (Hamilton, 1980). Indeed, the host faces a peculiar problem of frequency dependent selection. Gene combinations for successful immune systems tend to spread, but if they become too widespread, they cannot remain successful, since parasites will adapt. Sexual host species keep reshuffling their gene combinations, thus providing them with the advantage of being rare.

This is the so-called *Red Queen* theory of sex, named after a figure from the sequel of *Alice in Wonderland* in whose realm 'you have to run with all your speed' just to stay in place – a familiar feature in co-evolution. A species can never stop adapting since the other species do not stop either. Mathematical models for the resulting arms races display a profusion of limit cycles, irregular oscillations and heteroclinic attractors.

The Red Queen metaphor makes evolution look like a treadmill rather than a ladder to progress. Nevertheless, evolution has come up with increasingly complex structures, through a sequence of *major transitions* (Maynard Smith and Szathmary, 1996). Cell differentiation, immune systems, or neural networks are examples of breakthrough inventions. Understanding these major transitions necessarily requires thought experiments and mathematical modelling. A major issue for evolutionary biology is sex – a cooperative activity causing an endless series of conflicts. In the wake of the primary question – why should an organism transmit only half of its genes to its offspring? – many other problems surface: Why do sexually reproducing species have two sexes, rather than three, or one? Why are their roles asymmetrical (males producing tiny sperm cells and females large egg cells)? Why is the sex ratio close to one? Why are males fighting for females, and why are females choosier than males? And, since this is biology: why are there exceptions to all these rules? All these questions have been addressed by evolutionary game theory (see e.g. Hutson and Law, 1993, Karlin and Lessard, 1986, or Iwasa and Sasaki, 1987).

Some of the major transitions in evolution led to new levels of organisation, for instance self-replicating molecules, chromosomes, cells, multi-cellular organisms, colonies and societies. In most cases, this emergence of nested hierarchies was due to the fusion of formerly independent units into entities of higher order. These remain threatened by exploitation through mutinies of 'selfish' elements improving

their own propagation at a heavy cost to the larger unit. Cancer cells grow without restraint; within a genome, so-called ‘outlaw genes’ subvert the segregation of chromosomes in a cell division; etc. Each instance of cooperation is riddled with internal conflicts.

Selfishness may have been an issue since the dawn of life, when several types of self-replicating RNA molecules must have ‘ganged up’ in order to code for chemical functions. How could they co-exist? As one possible solution, Eigen and Schuster (1975) suggested the ‘hypercycle’, a closed feedback loop of chemical kinetics, with RNA of type  $M_i$  catalysing the replication of RNA of type  $M_{i+1}$  (counting the indices  $i \bmod n$ ). The equation for the relative densities  $x_i$  of  $M_i$  is given by the replicator equation (7), with  $f_i = x_{i-1}F_i(x)$  and  $F_i > 0$  for all  $i$ . (If the  $F_i$  are constants, there exists a globally stable fixed point in  $\text{int}S_n$  for  $n < 5$ , and a stable periodic orbit for  $n \geq 5$ , see Hofbauer et al, 1991.) This dynamics is always permanent, so that hypercyclic coupling does indeed guarantee the coexistence of all RNA types. But if there occurs an RNA type  $M$  which profits from  $M_i$  more than  $M_{i+1}$  does, then  $M$  will displace  $M_{i+1}$ , even if it confers no catalytic benefits to the other RNA; such a molecular parasite destroys the whole cycle.

11. THE EVOLUTION OF COOPERATION Evolutionary history began with molecular networks and led to tightly-knit societies acting as coherently as single organisms do. Bee hives and termite states furnish striking examples. Their extraordinary degree of cooperation is due to the close kinship between all members of a society: a gene for helping one’s sister is helping copies of itself. The close relatedness within a bee hive is due to the fact that only very few of its members reproduce. This type of cooperation can be explained by *kinship theory*. It is based on the rule that an altruistic act costing  $c$  to the donor (in terms of reproductive success) and benefitting  $b$  to the recipient has a selective advantage if the relatedness between donor and recipient exceeds the cost-to-benefit ratio  $c/b$ .

In human societies, kinship accounts only for a small part of the cooperation: the larger part is due to economic rather than genetic factors. The simplest mechanism is *direct reciprocation*: as long as  $c < b$  it pays to help others if they will return the help. This creates new opportunities for parasitism, by not returning help. Game theory provides a ready-made model succinctly capturing this aspect. The *Prisoner’s Dilemma* (PD) is a symmetric game between two players who can opt between the moves C (to cooperate) and D (to defect). The payoff matrix is

$$\begin{array}{c} \begin{array}{cc} & \begin{array}{cc} \text{C} & \text{D} \end{array} \\ \begin{array}{c} \text{C} \\ \text{D} \end{array} & \left( \begin{array}{cc} R & S \\ T & P \end{array} \right) \end{array} \end{array} \quad (18)$$

with

$$T > R > P > S \quad \text{and} \quad 2R > T + S \quad (19)$$

(the first condition means that the *reward*  $R$  for mutual cooperation is larger than the *punishment*  $P$  for mutual defection, but that the *temptation*  $T$  for unilateral defection is still larger, and the *sucker’s payoff*  $S$  for being exploited ranks lowest.

In our case,  $R = b - c$ ,  $P = 0$ ,  $T = b$  and  $S = -c$ ). Obviously, it is best to play D, no matter what the other is doing.

This changes if we assume that there is always a probability  $w$  for a further round, which is larger than  $(T - R)/(T - P)$ , i.e.  $c/b$ . The *iterated* PD game has a random number of rounds with mean  $(1 - w)^{-1}$  and admits a huge set of strategies. This model led to a vast amount of investigations, often based on computer tournaments simulating populations of players meeting randomly and engaging in an iterated PD game. In Axelrod's first tournaments, (see Axelrod and Hamilton, 1981) the Tit For Tat strategy TFT (play C in the first round and from then on repeat the co-player's previous move) performed extremely well, despite its simplicity. But TFT is not evolutionarily stable: indeed, the strategy of always cooperating can spread by neutral drift in a population of TFT players, and defectors can subsequently invade. Moreover, errors between TFT players lead to costly runs of alternating defections.

To analyse the iterated PD under *noise* (i.e. with a small probability of genetic or strategic errors), let us first consider *memory-one strategies* only. Such strategies are given by the probability to play C in the first round, and a quadruple  $P = (p_R, p_S, p_T, p_P)$ , where  $p_i$  denotes the player's propensity for move C after having experienced outcome  $i \in \{R, S, T, P\}$  in the previous round. Due to occasional mistakes, the initial move plays almost no role in long interactions ( $w$  close to 1). The dynamics becomes extremely complex: for instance, restriction to the following four strategies leads to a heteroclinic network as attractor (see fig. 3b): (1) Tit For Tat  $(1, 0, 1, 0)$ , (2) the more tolerant Firm But Fair  $(1, 0, 1, 1)$  which forgives an opponent's defection if it was matched by an own defection, (3) the parasitic Bully  $(0, 0, 0, 1)$  which cooperates only after punishment and (4) the strategy  $(0, 0, 0, 0)$  which always defects.

But if we introduce occasional mutants, then long-term evolution leads (for  $2R > T + P$ , i.e.  $b > 2c$ ) to the so-called *Pavlov* strategy  $(1, 0, 0, 1)$  which cooperates only if the co-player, in the previous round, acted like oneself (Nowak and Sigmund, 1993). This strategy embodies the simplest learning rule, called 'win-stay, lose-shift' by experimental psychologists. It consists in repeating the previous move if the payoff was high ( $R$  or  $T$ ) and in switching to the other option if it was low ( $P$  or  $S$ ). Pavlov players cooperate with each other; an erroneous defection leads in the next round to both players defecting, and then to a resumption of mutual cooperation. Furthermore, Pavlov populations cannot be invaded by other strategies, and in particular not by indiscriminate cooperators who pave the way for defectors. On the other hand, Pavlov cannot invade a strategy of defectors: this needs a small cluster of strongly retaliatory strategies like TFT, who eliminate unconditional defectors and then yield to Pavlov.

Fig. 4: Dynamics of indirect reciprocity

What about strategies with longer memory, or yet more general *finite-state automata*? Such strategies are defined by a finite set  $\Omega$  of inner states, some (possibly stochastic) rule specifying which move to play when in state  $\omega$ , and a rule specifying the transition to the next state as a function of the previous state and of the outcome of the current round ( $R, S, T$  or  $P$ ). Together with the initial state, this defines a strategy for the iterated PD. An example is given by the following table.

	R	S	T	P
1	1	2	3	1
2	1	2	1	2
3	1	1	3	3

It is easy to check that this example satisfies a variant of evolutionary stability: if all co-players use that strategy, it is best, at every stage of the game, to follow the same strategy. This defines a *social norm*. There are many such norms (including Pavlov, if  $2R > T + P$ ), and it is not easy to decide which will get selected. But this example seems particularly successful, and it has an intuitive appeal, if we interpret state 2 as ‘provoked’ and state 3 as ‘contrite’: indeed, an erroneous defection by one player makes that player feel contrite, and the co-player provoked: the retaliation redresses the balance. Such inner states may correspond to emotions, which are increasingly seen as tools for handling the complexities of social life.

**INDIRECT RECIPROCITY** Obviously, the iterated PD captures only a part of the cooperative interactions in human societies. There is another, *indirect* reciprocity, whereby an altruistic act is returned, not by the recipient (as with direct reciprocity), but by someone else. Indirect reciprocity involves reputation. A simple model assumes that a *score* is attached to each player, which increases (or decreases) whenever the player provides (or withholds) help. Players help whenever the score of the potential recipient exceeds some threshold. This threshold is subject to selection. Punishing a low-scorer is costly, as it decreases one’s own score; but if defectors are not punished, they take over. Assuming that each player is engaged in a few rounds, both as potential donor and recipient (but never meeting the same co-player twice), one finds that mutation-selection chronicles lead toward

cooperation, provided players know their co-players' score sufficiently well (Nowak and Sigmund, 1998).

Occasionally, waves of defection sweep through the population: they are provoked by an excessive frequency of indiscriminate altruists (who are too ready to help low-scorers). Cooperation is more robust if the society is challenged more frequently by invasion attempts of defectors (an intriguing parallel to immune systems). This can be nicely captured by an even simpler model involving only three types of players, with frequencies  $x_1, x_2, x_3$ , namely (a) indiscriminate altruists, (b) defectors, and (c) discriminate altruists who help except if the co-player withheld help. If we assume two rounds per player, for instance, both as a donor and as a recipient, the payoffs are

$$\begin{aligned} f_1 &= 2(b - c - bx_2) \\ f_2 &= 2bx_1 + bx_3 \\ f_3 &= 2(b - c) - cx_2. \end{aligned} \tag{20}$$

If discriminating altruists are too rare, i.e. if  $x_3 < c/(b - c)$ , defectors take over. But all orbits with  $x_3 > c/(b - c)$  lead from the edge  $x_2=0$  (no defectors) back to itself. A mixture of altruists gets established. We may expect that random drift makes the state *fluctuate* along this edge, which consists of fixed points only, and that occasionally, mutation introduces a small quantity  $x_2$  of defectors. What happens? If  $x_3 > 2c/b$ , defectors cannot invade. If

$$\frac{2c}{b} > x_3 > \frac{c}{b - c}, \tag{21}$$

the invading defectors thrive at first, but are subsequently eliminated by discriminating altruists. After such an abortive invasion, the ratio of discriminators is so large that defectors can no longer invade. Only when random fluctuations cross the interval given by (21), will defectors take over. But this takes time. If defectors try too often to invade, they will not succeed (see fig. 4).

Such models show how cooperation emerges through the selection of learning rules, moralistic emotions, social norms and reputation. Thus evolutionary models explain the ceaseless give and take prevailing in human societies, and lead game theory back towards its original economic motivation.

#### REFERENCES

- Anderson, A.M. and R.M. May (1991), *Infectious Diseases of Humans: Dynamics and Control*, Oxford Univ. Press, Oxford.
- Ashwin, P., J. Buescu and I.N. Stewart (1996) From attractor to chaotic saddle: a tale of transverse instability. *Nonlinearity* 9, 703-37.
- Axelrod, R. and Hamilton, W.D. (1981), The evolution of cooperation, *Science* 211, 1390-6.
- Chawanya, T. (1995) A new type of irregular motion in a class of game dynamics systems. *Progress Theor. Phys.* 94, 163-79.

- Cressman, R. (1992) *The stability concept of evolutionary game theory*, Springer, Berlin.
- Cressman, R., J. Hofbauer and W.G.S. Hines (1996), Evolutionary stability in strategic models of single-locus frequency dependent viability selection, *J. Math. Biol.*, 34, 707-733.
- DeBoer, R.J. and A.S. Perelson (1998) Target cell limited and immune control models of HIV infection: a comparison, *Journ. Theor. Biol* 190 201-14.
- Dietz, K. and K.P. Haderl (1986) Epidemiological models for sexually transmitted diseases, *J. Math. Biol.* 26, 1-25.
- Durrett, R. (1991) Stochastic models of growth and competition, *Proc. Int. Cong. Math. Kyoto*, Vol. II, 1049-1056.
- Eigen, M. and P. Schuster (1979), *The hypercycle: a principle of natural self-organisation*. Springer, Berlin-Heidelberg.
- Eshel, I. (1996): On the changing concept of evolutionary population stability as a reflection of a changing point of view in the quantitative theory of evolution, *J. Math. Biol.* 34, 485-510.
- Ferriere, R. and M. Gatto (1995), Lyapunov exponents and the mathematics of invasion in oscillatory or chaotic populations, *Theor. Pop. Biol.* 48, 126-71.
- Fisher, R.A. (1918), The correlation between relatives on the supposition of Mendelian inheritance, *Trans. Roy. Soc. Edinburgh* 52, 399-433.
- Forrest, S. (1993) Genetic algorithms: Principles of natural selection applied to computation, *Science* 261, 872-9.
- Frank, S.A. (1996) Models of parasite virulence, *Quart. Rev. Biol.* 71, 37-78.
- Gopalsamy, K. (1992), *Stability and Oscillations in Delay Differential Equations of Population Dynamics*, Dordrecht, Kluwer.
- Grenfell, B.T. and A.P. Dobson (1995), *Ecology of Infectious Diseases in Natural Populations*, Cambridge Univ. Press, Cambridge.
- Hamilton, W.D. (1980) Sex versus non-sex versus parasites, *Oikos* 35, 282-90.
- Hastings. A. and Powell, T. (1991) Chaos in a three-species food chain, *Ecology* 72, 896-930.
- Hirsch, M.W. (1988) Systems of differential equations which are competitive or cooperative III: Competing species. *Nonlinearity* 1, 51-71
- Hofbauer, J. (1998) Invasion, permanence and heteroclinic cycles. To appear.
- Hofbauer, J., J. Mallet-Paret and H.L. Smith (1991), Stable periodic solutions for the hypercycle system, *J. Dynamics and Diff. Eqs.* 3, 423-36.
- J. Hofbauer and K. Sigmund, (1998) *Evolutionary games and population dynamics*, Cambridge UP
- Hutson, V. and R. Law (1993), Four steps to two sexes, *Proc. Roy. Soc. London B*, 253, 43-51.
- V. Hutson and K. Schmitt, (1992) Permanence and the dynamics of biological systems, *Math Biosci.* 111, 1-71
- Iwasa, Y. and A. Sasaki (1987), Evolution of the number of sexes, *Evolution* 41, 49-65.
- Karlin, S. and S. Lessard (1986) *Sex Ratio Evolution*, Monographs in Population Biology, 22, Princeton UP.

- Kolmogorov, A.N. (1937) (with I.G. Petrovskij and N.S. Piskunov) Studies of the diffusion equation, combined with increase in the amount of matter and its application to a problem in biology, *Bul. Mosk. Gos. Univ. Mat. Mekh.* 1, 1-26.
- Law, R. and U. Dieckmann (1998), Symbiosis through exploitation and the merger of lineages in evolution, *Proc. Roy. Soc. London B*, 265, to appear
- Levin, S.A. and D. Pimentel (1981) Selection of intermediate rates of increase in parasite-host systems, *Amer. Nat.* 117 308-1.
- Levin, S.A., Grenfell, B., Hastings, A. and Perelson, A.S. (1997), Mathematical and computational challenges in population biology and ecosystems science, *Science* 275, 334-343
- Lipsitch, M.S., S. Siller and M.A. Nowak (1996) The evolution of virulence in pathogens with vertical and horizontal transmission, *Evolution* 50, 1729-41.
- May, R.M. (1976) Simple mathematical models with very complicated dynamics, *Nature* 261, 459-467.
- May, R.M. and W.J. Leonard (1975) Nonlinear aspects of competition between three species, *SIAM J. Appl. Math.* 29, 243-253.
- Maynard Smith, J. (1982) *Evolution and the Theory of Games*, Cambridge UP.
- Maynard Smith, J. and Szathmari, E. (1995), *The Major Transitions in Evolution*, Freeman, Oxford.
- Metz, J.A.J., S.A. Geritz, G. Meszner, F.J.A. Jacobs and J.S. van Heerwaarden (1996), Adaptive dynamics: a geometrical study of the consequences of nearly faithful replication. In S.J. Van Strien and S.M. Verduyn Lunel (eds), *Stochastic and spatial structures of dynamical systems*, 183-231. Amsterdam, North Holland.
- Mylius, S.D., Doebeli, M. and Dieckmann, O. (1998) Can initial invasion dynamics correctly predict phenotypic substitution?, to appear.
- Nowak, M.A., R.M. Anderson, A.R. McLean, T. Wolfs, J. Goudsmit and R.M. May (1991), Antigenic diversity thresholds and the development of AIDS, *Science* 254, 963-9.
- Nowak, M.A. and R.M. May (1994), Superinfection and the evolution of parasitic virulence, *Proc. R. Soc. London B* 255, 81-89.
- Nowak, M.A. and Bangham, C.R. (1996), Population dynamics of immune responses to persistent viruses, *Science* 272, 74-9.
- Nowak, M.A. and Sigmund, K. (1993), Win-stay, lose-shift outperforms tit-for-tat, *Nature*, 364, 56-8.
- Nowak, M.A. and Sigmund, K. (1998), Evolution of indirect reciprocity by image scoring, *Nature* 393, 573-577.
- Nowak, M.A., R.M. May and K. Sigmund (1995), Immune response against multiple epitopes, *Jour. Theor. Biol.* 175, 325-53.
- Murray, J. (1990), *Mathematical Biology*, Springer, Heidelberg.
- Olsen, L.F. and Schaffer, W.M. (1990) Chaos in infections? *Science* 249, 499.
- Rand, D., Wilson, H.B. and McGlade, J.M. (1994): Dynamics and evolution: evolutionarily stable attractors, invasion exponents and phenotype dynamics, *Phil. Trans. Roy. Soc. London B* 24, 261-283.
- Schreiber, S. (1998) On the stabilizing effect of predators on founder-controlled communities, to appear in *Canad. Appl. Math. Quarterly*.



- Takeuchi, Y. (1996), *Global dynamical properties of Lotka-Volterra systems*, World Scientific, Singapore.
- van den Driessche, P. and Zeeman, M.L. (1997), Three dimensional competitive Lotka-Volterra systems with no periodic orbits, *SIAM J. Appl. Math* 280, 227-34.

Karl Sigmund  
Institut für Mathematik  
Universität Wien  
Strudlhofgasse 4, A-1090 Wien  
and:  
IIASA, Laxenburg  
Austria  
ksigmund@esi.ac.at

# HUGE RANDOM STRUCTURES AND MEAN FIELD MODELS FOR SPIN GLASSES

MICHEL TALAGRAND

ABSTRACT. To explain (at least qualitatively) the unconventional magnetic behavior of certain materials, the physicists have been led to formulate and to study simple mathematical models. The concepts and methods they developed in this process appear to apply to a number of important random combinatorial optimization problems, for which they have proposed remarkable formulas. Their discoveries point towards a new branch of probability theory. Finding rigorous arguments to support their conjectures is a formidable challenge and a long range program, some steps of which are described in the present paper.

## INTRODUCTION

The research presented in this paper has largely been influenced by the book of M. Mézard, G. Parisi, M. A. Viroso “Spin glass theory and beyond” [M-P-V]. This book is remarkable in many respects, and first of all its topic, which is the study of what are canonical, and even fundamental mathematical objects by physicist’s methods. The book is an attempt by physicists to explain to other physicists the new concepts they have discovered about “spin glasses” and their relevance to a number of fundamental random structures. This could make difficult (and *did* in the case of the author) for an unprepared mathematician to get any idea of what this is all about. The book contains no rigorous results, and it is not obvious at all to even give a precise mathematical content to many of the statements made there. The existence of the topic of spin glasses appears to be known to quite a few mathematicians (see e.g. the recent book [B-P]), but overall it has been considered as an area where rigorous results are notoriously difficult to obtain. One must keep in mind however that it is rather unreasonable to attempt to directly attack the problems that the physicists (who use much less stringent methods) find challenging themselves (see however [N-S 2, 3]). We believe that there is no chance to make advances on the difficult issues until the easier ones have been clarified, and that only a systematic program to investigate the entire circle of ideas can lead to progress. The present paper reports the current status of this program. Beside attempting to provide an introduction to the topic, its main objective is to explain the author’s contributions and point of view, and it should be kept in mind that some of the opinions expressed below are personal and might not be

shared by others. All the results presented are fully rigorous; complete proofs can be found in [T5] to [T13].

There seems to be no better way to introduce the topic than to mimic the introduction of [M-P-V]. Consider a large population of individuals, numbered from 1 to  $N$ . Consider independent identically distributed (i.i.d) random variables (r.v.)  $(g_{ij})_{1 \leq i < j \leq N}$ . (The choice of Gaussian distribution is the simplest one, and is not believed to be essential). The variables  $g_{ij}$  represents the interaction of individuals  $i < j$  (so, the larger  $g_{ij}$ , the more friendly  $i$  and  $j$  are towards each other). The independence requirement implies that for many (actually about  $1/2$ ) of the triples  $i, j, k$ , then  $g_{ij}g_{jk}g_{ik} < 0$ , so that we have unpleasant situations such as  $i$  friend of  $j$  and  $k$  ( $g_{ij}, g_{ik} > 0$ ) but  $j$  and  $k$  enemies ( $g_{jk} < 0$ ). In order to improve upon this tense situation, one tries to split the population in two parts, putting as far as possible friends together and enemies apart. This is done by assigning to each individual a number  $\sigma_i \in \{-1, 1\}$ , and each configuration  $\boldsymbol{\sigma} = (\sigma_i)_{i \leq N}$  defines a splitting of the population in two. How successful this splitting is can be measured by the quantity

$$(1.1) \quad \sum_{1 \leq i < j \leq N} g_{ij} \sigma_i \sigma_j.$$

This adds the interactions between each pair of individuals in the same group, and subtracts the interactions between different groups. We are interested in the maximum of (1.1) over all  $\boldsymbol{\sigma}$ .

The reason why this maximum is very hard to find is that, for a given typical realization of the  $(g_{ij})$ , the function of  $\boldsymbol{\sigma}$  given by (1.1) has apparently very many “near maxima” at locations that are not simply related to each other. Computer simulations seem to show that for large  $N$

$$(1.2) \quad N^{-3/2} \max_{\boldsymbol{\sigma}} \sum_{1 \leq i < j \leq N} g_{ij} \sigma_i \sigma_j \simeq 0.7366$$

with overwhelming probability. It is simple to prove that  $N^{3/2}$  is the correct normalization factor and that the left hand side of (1.2) is essentially independent of the realization of the randomness (more precisely has random fluctuations of order  $N^{-1/2}$ ); but the proof of the existence of the limit as  $N \rightarrow \infty$ , or its rigorous computation are nowhere in sight.

Faced with a very difficult optimization problem such as (1.2), the answer of statistical mechanics is to introduce a parameter  $T \geq 0$  called temperature, and try to recover the case  $T = 0$  as a limit case  $T \rightarrow 0$ . We consider the Hamiltonian (i.e. energy function)

$$(1.3) \quad H_N(\boldsymbol{\sigma}) = -\frac{1}{\sqrt{N}} \sum_{1 \leq i < j \leq N} g_{ij} \sigma_i \sigma_j - h \sum_{i \leq N} \sigma_i.$$

The factor  $\sqrt{N}$  is the correct normalization to ensure that  $H_N/N$  remains bounded; The minus sign follows physics convention (the system is attracted to

low energy configurations) and  $h$  is an “external field” that favors the choice  $\sigma_i = 1$  over  $\sigma_i = -1$ . The previous optimization problem was the search (when  $h = 0$ ) for the ground state (configuration with lowest energy) of  $H_N(\boldsymbol{\sigma})$ , which is the Hamiltonian of the famous Sherrington-Kirkpatrick (SK) model for spin glasses. This Hamiltonian was introduced to model disordered interaction between magnetic impurities (“spins”) in metals. As a first approximation (mean field approximation), the geometric location of atoms is forgotten, and it is assumed that all pairs interact in the same way. The disorder of the system is then modeled by the random interactions  $g_{ij}$ . If the system is in thermal equilibrium at inverse temperature  $\beta = 1/T$ , statistical mechanics asserts that the probability of observing the system in configuration  $\boldsymbol{\sigma}$  is given by Gibbs’ measure

$$(1.4) \quad G_N(\boldsymbol{\sigma}) = \frac{1}{Z_N} \exp -\beta H_N(\boldsymbol{\sigma})$$

where  $Z_N$  is the normalization factor (called the partition function)

$$(1.5) \quad Z_N = Z_N(\beta, h) = \sum \exp -\beta H_N(\boldsymbol{\rho})$$

for a summation over all configurations. The problem is then to understand the structure of Gibbs’ measure for the typical realization of the disorder (that is, of the r.v.  $g_{ij}$ ). The mathematical difficulty is that it is very unclear what is the value of  $Z_N$ , which is a sum of  $2^N$  quantities of wildly different orders of magnitude (the more so at large  $\beta$ , i.e. low temperature). Of particular interest is the “free energy”

$$(1.6) \quad F_N = F_N(\beta, h) = \log Z_N$$

(a physicist would rather use  $-\frac{1}{\beta} \log Z_N$ ) the importance of which can be understood by the fact that its derivation with respect to the various parameters are physically measurable quantities, e.g.

$$(1.7) \quad \frac{1}{\beta} \frac{\partial F_N}{\partial h} = \left\langle \sum_{i \leq N} \sigma_i \right\rangle$$

is the global magnetization. In (1.7), as well as in the rest of the paper  $\langle \cdot \rangle$  denotes thermal average, that is integration with respect to Gibbs’ measure. Of course  $F_N$  is a random quantity (it depends of the disorder). However, it follows from general principles (the “concentration of measure phenomenon” [I-S-T]) that the random fluctuations of  $F_N$  are of order  $N^{1/2}$ , while  $F_N$  is of order  $N$ , so that much of the information about  $F_N$  is captured by  $E F_N$ . There and throughout the paper we denote by  $E$  the average with respect to the disorder. The main difficulty is that the typical value of  $Z_N$  is very different from (and of course smaller than)  $E Z_N$ , and that the bound  $E \log Z_N \leq \log E Z_N$  given by Jensen’s inequality is not an equality in the interesting cases.

It was soon realized that the first attempt to study the SK model [S-K] had serious flaws, and that the solution proposed there was correct only at high temperature. After several trials G. Parisi has proposed a very intricate picture (“the

Parisi solution”) that is believed to be correct. The remarkable objects invented by Parisi start to draw attention from mathematicians [R], [B-S], [A-C1], [A-C2]. Unfortunately, the mathematical study of structures related to Parisi’s solution is distinct from the more important issue as to whether these structures are really relevant to the SK model, and at the present time there is very little rigorous evidence that this is the case. It is of course fascinating that a simple and canonical energy function such as (1.3) can give rise to such extreme subtlety. But, beside the intrinsic interest of the SK model, the great discovery made by the physicists is that the behavior exhibited by this system appears to be rather universal, and to be present in a number of other situations involving random structures, several typical examples of which will be considered here.

Let us now try to draw a very rough picture of the situation. A main feature of the physicist’s prediction is that given  $h$ , above a certain temperature, the system “is in a pure state” while below this temperature it spontaneously decomposes in many “pure states”. The later statement can intuitively be understood by saying that if one studies the system at (extremely) long intervals, it looks like different objects. As we work in a disordered mean field model, it is unfortunately not obvious a priori how to formulate a meaningful definition of a pure state, and even less how to decompose a system in pure states. In standard statistical mechanics, say, on a finite subset  $S_N$  of an infinite lattice  $S$ , this is done by taking “infinite volume limit”,  $N \rightarrow \infty$ . The set of configurations is then  $\{-1, 1\}^S$ . The set of Gibbs’ measures form a convex compact set, the extreme points of which are the pure states. In the present case, if one selects a sequence  $(g_{i,j})_{i,j \in \mathbb{N}}$ , then the structure of the Gibbs’ measure of the  $N$ -spin system defined using  $(g_{ij})_{i,j \leq N}$  varies wildly with  $N$ , the chaotic size dependence of [N-S1]. Despite the many statements of [M-P-V] starting by “in the thermodynamical limit...”, it is not clear how to define a useful limit of the system as  $N \rightarrow \infty$ , that is, a satisfactory set of Gibbs’ measures on  $\{-1, 1\}^N$ . (See [AW],[N-S2] for the most interesting tentatives towards infinite volume limits in the lattice case. These attempts unfortunately still require taking subsequences, an operation that goes somewhat against the very goal of the theory, which is the ability to describe finite samples of matter.) This absence of infinite volume limit makes the topic of spin glasses distinctively different from main stream classical statistical mechanics. In Section 2, we will present a set of equivalent conditions that mean that the system is in a pure state, and for all the systems that we shall study we will define the high temperature region as the set of parameters where these conditions hold. (By definition the low temperature region consists of the other values.) The high temperature region is much simpler than the low temperature region and thereby is the natural starting point of a rigorous investigation. The results of Section 3 to 6 of the present paper assert that for four rather different models, the physicists magic formulas are indeed correct at high enough temperature, and a look at these formulas (such as (3.11)) should convince the reader that non trivial phenomenon occur there.

The author is keenly aware that it is a very risky endeavor to attempt rigorous proofs of results that are “known” by another community, in particular when most of his results bear on situations considered easy (if not trivial) by the physicists. It is thereby necessary to say a few words about the physicists methods, even though

this might spoil some of the excitement the reader might otherwise have felt when discovering them in [M-P-V]. These methods are extremely creative and brilliant, but their purpose is very different from ours. It is not to provide proofs, but rather to discover what happens with reasonable certainty. The favorite method, the replica method, attempts to compute directly the limiting expected free energy density  $\lim_{N \rightarrow \infty} N^{-1} E F_N$ , which, as we mentioned, captures much information about  $F_N$ . The annoying logarithm is disposed of by the formula

$$(1.8) \quad \log x = \lim_{n \rightarrow 0} \frac{x^n - 1}{n}$$

and the issue is then to compute  $E Z_N^n$ , which can be done for  $n$  integer using  $n$  copies (“replicas”) of the system. One then makes an analytic continuation at  $n \rightarrow 0$ . Besides a few lesser problems, the computation of  $E Z_N^n$  in the case of the SK model is done by a saddle point method requiring to minimize a function of  $n(n-1)/2$  variables. To quote [M-P-V], p. 12, “ $n(n-1)/2$  becomes negative for  $0 < n < 1$ , and it is not clear how to give a precise definition of the minimum of a function which depends on a negative number of variables”. As G. Parisi so nicely puts it “the replica method is yet to be put on firm mathematical ground”.

The computations using the replica method involve a tricky issue (the real meaning of which is not clear to me) as to whether the  $n$  ( $0 < n < 1$ ) replicas involved can be assumed to be equivalent (“replica-symmetry”, the easiest case) or not (“replica symmetry breaking”). It seems that the case where the system is in a pure state (as defined in Section 2) corresponds to the case of replica-symmetry. The physicists seem to have absolute faith in the replica method, at least in the replica symmetric case. Typing the words “replica symmetry” on a data base such as INSPEC brings in dozens of papers that rely upon this method. More often than not, these papers “solve” a problem by writing down formulas provided by the replica method (sometimes using Parisi’s scheme of replica-symmetry breaking) and optimizing over the various parameters. These theoretical results are then supplemented by computer studies for large  $N$ , where (due to extreme computational difficulties), “large” means typically of order 100. But despite the fact that it is not clear what the replica method really does (even in the replica symmetric case) it is an amazing tool to discover complicated formulas in a very compact way.

As the mathematical and even the physical contents of the replica method are obscure, physicists have developed an alternative method, the cavity method, which is essentially induction upon  $N$ . (This is the method we will use, even though our computations are very different). A possible reason why the physicists find the high temperature case easy is that they assume from the start “on natural physical grounds” that at high temperature the system is in a pure state (see eg. [M]). At the philosophical level, it requires some faith to believe that a mathematical object such as (1.3), that has very little claim to be a realistic model for matter will obey physical principles. At the mathematical level, once one assumes that the system is in a pure state, the magical formula (2.9) below allows all kinds of computations that readily lead to a rather complete picture of the system. On the other hand

the mathematician, when faced with the system with no a priori information has at first great difficulties to prove anything at all.

Even though the high temperature phase of disordered systems is considered easy in physics, it still has some interest even at this level, in particular because in some important cases (such as that of Section 4) the high temperature region is believed to extend all the way to zero temperature. The real long term challenge is however the low temperature region. The very complicated structure of the predicted low temperature behavior of the SK model does not make it a good place to start from, so we have rather considered the  $p$ -spin interaction model, a model closely related to the SK model and for which the predicted low temperature behavior is much simpler (and, actually the simplest possible). We did succeed in this case to prove (at the “edge” of the low temperature region) the main feature of the Parisi’s prediction, the spontaneous decomposition of the system in pure states “far from each other”. This is the content of Section 7.

ACKNOWLEDGMENT The author will be forever grateful to Erwin Bolthausen for having introduced him to such an immensely enjoyable topic. The author thanks G. Choquet, M. Mézard and many others for useful comments.

## 2. SYSTEMS IN A PURE STATE

We denote throughout the paper the set  $\{-1, 1\}^N$  of all configurations by  $\Sigma_N$ . Since  $(\Sigma_N, G_N)$  is a probability space it is natural to consider powers of it,  $(\Sigma_N^m, G_N^{\otimes m})$  (often  $m \leq 4$ ). These are called replicas. The word “replicas” simply means that we consider several copies of  $(\Sigma_N, G_N)$ . Then copies are taken for the *same* realization of the disorder. A generic point in  $\Sigma_N^m$  is denoted by  $(\sigma^1, \dots, \sigma^m)$ . These replicas are often called in physics “real replicas” to distinguish them for the  $n$  replicas ( $n \rightarrow 0$ ) of the replica formalism (would these be unreal?) and needless to say that we will use only “real” replicas. Replicas are very useful to transform product of integrals for the Gibbs measure into multiple integrals, such as in the formula

$$\langle f_1(\sigma) \rangle \langle f_2(\sigma) \rangle = \langle f_1(\sigma^1) f_2(\sigma^2) \rangle.$$

There, as well as in the rest of the paper,  $\langle \cdot \rangle$  denotes thermal average in  $\Sigma_N^n$  as well as in  $\Sigma_N$ , so that the bracket on the right is a double integral with respect to Gibbs measure.

The overlap between two configurations  $\sigma^1, \sigma^2$  is defined by

$$(2.1) \quad \frac{1}{N} \sigma^1 \cdot \sigma^2 = \frac{1}{N} \sum_{i \leq N} \sigma_i^1 \sigma_i^2,$$

a good measure of their distance. The simplest (although not the most intuitive) way to define a system in a pure state is to say that the function  $\sigma^1, \sigma^2 \rightarrow \frac{1}{N} \sigma^1 \cdot \sigma^2$  is nearly constant on  $\Sigma_N^2$ , as is formalized in (2.2) below. This idea is apparent in [M-V-P]. It is likely that, at least at the intuitive level, many other ideas of this section can also be found there, but of course the point was to identify precise statements that are amenable to proof.

Consider a sequence  $(G_N)_{N \geq 1}$ , where  $G_N$  is an exchangeable random probability measure on  $\Sigma_N$ , that is, such that its distribution is invariant under any permutation of the coordinates (a crucial assumption). Typically  $(G_N)$  will be a sequence of Gibbs' measures such as (1.4), at a given value of the parameters  $\beta, h$ , so it should be self evident what we mean by  $\langle \cdot \rangle$ , replicas, etc. Of course  $E$  will denote expectation with respect to the randomness of  $G_N$ . In the next theorem, all brackets  $\langle \cdot \rangle$  are for  $G_N$ . This seemingly complicated statement is a result of the author's (unreasonable?) attempt not only to give a description of the results, but also some ideas of what are the obstacles to reach them. The reader who is interested only in getting an overview of the results should only read conditions (2.2), (2.7), (2.8). After reading the comments next to Definition 2.2, he should then skip the sketch of proof of Theorem 2.1.

**THEOREM 2.1.** *For a sequence  $G_N$  of exchangeable random probability measures the following properties are equivalent.*

$$(2.2) \quad \lim_{N \rightarrow \infty} E \langle \frac{1}{N} |\sigma^1 \cdot \sigma^2 - \langle \sigma^1 \cdot \sigma^2 \rangle| \rangle = 0$$

$$(2.3) \quad \lim_{N \rightarrow \infty} E \langle (\frac{1}{N} (\sigma^1 - \sigma^2) \cdot (\sigma^3 - \sigma^4))^2 \rangle = 0$$

$$(2.4) \quad \lim_{N \rightarrow \infty} E \langle (\frac{1}{N} (\sigma^1 - \sigma^2) \cdot \sigma^3)^2 \rangle = 0$$

$$(2.5) \quad \lim_{N \rightarrow \infty} E \langle (\sigma_1 \sigma_2) - \langle \sigma_1 \rangle \langle \sigma_2 \rangle \rangle^2 = 0$$

$$(2.6) \quad \lim_{N \rightarrow \infty} E \langle (\sigma_1^1 - \sigma_1^2)(\sigma_2^1 - \sigma_2^2) \langle \sigma_1^3 \sigma_2^3 \rangle \rangle = 0$$

$$(2.7) \quad \forall n, \lim_{N \rightarrow \infty} E \langle (\sigma_1 \cdots \sigma_n) - \langle \sigma_1 \rangle \cdots \langle \sigma_n \rangle \rangle^2 = 0$$

(2.8) *For each  $n$ , the expected total variation distance of the law of  $(\sigma_1, \dots, \sigma_n)$  under  $G_N$  to the set of a product measures on  $\{-1, 1\}^n$  goes to zero.*

(2.9) *For any continuous bounded function  $f$  on  $\mathbb{R}^{n \times m}$ , independent  $N(0, 1)$  variables  $(\xi_i^j)_{i \leq n, j \leq m}, (h^{j\ell})_{j \leq n, \ell \leq m}$  that are independent of the variables  $g_{ij}$ , we have*

$$\lim_{N \rightarrow \infty} E | \langle f(\langle \frac{\xi^j \cdot \sigma^\ell}{\sqrt{N}} \rangle_{\substack{j \leq n \\ \ell \leq m}}) \rangle - E_h f(\langle \frac{\xi^j \cdot \mathbf{b}}{\sqrt{N}} + h^{j\ell} \sqrt{1 - \|\mathbf{b}\|^2/N} \rangle_{\substack{j \leq n \\ \ell \leq m}}) \rangle | = 0$$

where  $\xi^j \cdot \sigma^\ell = \sum_{i \leq N} \xi_i^j \sigma_i^\ell, \mathbf{b} = (\langle \sigma_i \rangle)_{i \leq N} = (\langle \sigma_i^\ell \rangle)_{i \leq N}$ ; and where  $E_h$  denotes expectation in  $(h^{j\ell})_{j \leq n, \ell \leq m}$  only.

**DEFINITION 2.2.** *We say that the sequence  $G_N$  of random measures is in a pure state if the equivalent conditions of Theorem 2.1 hold.*

Conditions (2.2) to (2.4) are global “geometric” conditions. The idea of (2.3) and (2.4) is that the centering in (2.2) is better replaced by symmetrization. The reason for considering these two similar but different expressions will be apparent when we try to prove them. Conditions (2.5) and (2.6) are “local” reformulations of (2.3), (2.4) respectively, that involve only two spins, and are better adapted to



induction over  $N$ . The least expected, and the most useful fact is (2.9), which means that in practice integral  $\langle f(\frac{\xi^j \cdot \sigma^{\ell'}}{\sqrt{N}}) \rangle$  depends upon  $G_N$  only through  $\mathbf{b}$ , a fact that is at the root of the magic formulas of Sections 3 to 5.

Theorem 2.1 provides conceptual clarification, and is very easy to prove, because we do not relate the rates at which the various quantities go to zero and need only “soft” estimates. This is why, when a physicist assumes “on physical grounds” that, say (2.5) holds, he then correctly feels that the problem is easy. On the other hand, *proving* that the conditions of Theorem 2.1 hold require much more precise estimates.

To sketch the proof of Theorem 2.1 let us set  $a_i = (\sigma_i^1 - \sigma_i^2)(\sigma_i^3 - \sigma_i^4)$  so  $|a_i| \leq 4$ , and (2.3) means that  $E(\langle (N^{-1} \sum a_i)^2 \rangle) \rightarrow 0$ , which, by symmetry among the coordinates, is equivalent to  $E\langle a_1 a_2 \rangle \rightarrow 0$ . Now, by independence of the replicas

$$(2.10) \quad \begin{aligned} \langle a_1 a_2 \rangle &= \langle (\sigma_1^1 - \sigma_1^2)(\sigma_2^1 - \sigma_2^2) \rangle^2 \\ &= 4(\langle \sigma_1 \sigma_2 \rangle - \langle \sigma_1 \rangle \langle \sigma_2 \rangle)^2, \end{aligned}$$

which proves the equivalence of (2.3) and (2.5). The equivalence of (2.4) and (2.6) is similar. It is obvious that (2.4) $\Rightarrow$ (2.3) and (2.5) $\Rightarrow$ (2.6), using (2.10) and Cauchy-Schwarz. The equivalence of (2.2) and (2.4) is easy, since  $|(\sigma^1 - \sigma^2) \cdot \sigma^3| \leq 2N$ . It is obvious that (2.6) $\Rightarrow$ (2.8) $\Rightarrow$ (2.5). To prove the more surprising fact that (2.5) $\Rightarrow$ (2.7), we observe that, since  $|\sum_{i \leq N} a_i| \leq 4N$ , then (2.5) implies

$E\langle (N^{-1} \sum_{i \leq N} a_i)^n \rangle \rightarrow 0$ , and proceeding as before  $\lim_{N \rightarrow \infty} E\langle a_1 \cdots a_n \rangle \rightarrow 0$ , which means  $\lim_{N \rightarrow \infty} E\langle \prod_{i \leq n} (\sigma_i^1 - \sigma_i^2) \rangle^2 = 0$ , from which (2.7) follows easily. Thus we have

the equivalence of (2.2) to (2.8). We will not use that (2.9) implies the other conditions, so we just prove that it is a consequence of (2.2). Setting

$$X = \langle f(\frac{\xi^j \cdot \sigma^\ell}{\sqrt{N}}) \rangle; Y = E_h f(\frac{\xi^j \cdot \mathbf{b}}{\sqrt{N}} + h^{j\ell} \sqrt{1 - \|\mathbf{b}\|^2/N}),$$

the proof consists of showing that  $E(X - Y)^2 \rightarrow 0$ , by showing that  $EX^2 - EY^2 \rightarrow 0$  and  $EXY - EY^2 \rightarrow 0$ . We will (to avoid complicated notations) prove only that  $EX - EY \rightarrow 0$ . The argument to prove that (2.2) implies (2.9) is the same. If  $(w^{j\ell})$  is a jointly gaussian family, the quantity  $Ef((w^{j\ell}))$  is determined by the joint law of  $(w^{j\ell})$ , that is by the numbers  $E(w^{j\ell} w^{j'\ell'})$ , and this dependence is of course continuous. Denoting by  $E_\xi$  expectation in the variables  $\xi^j$  only,  $E_\xi f(\frac{\xi^j \cdot \sigma^\ell}{\sqrt{N}})$  depends only upon the numbers  $E(\frac{\xi^j \cdot \sigma^\ell}{\sqrt{N}} \frac{\xi^{j'} \cdot \sigma^{\ell'}}{\sqrt{N}}) = \delta_{jj'} (\sigma^\ell \cdot \sigma^{\ell'} / N)$ . For the generic point  $\sigma^1, \dots, \sigma^m$  of the  $m$ -replica, (2.2) says that all products  $\sigma^\ell \cdot \sigma^{\ell'} / N$  ( $\ell \neq \ell'$ ) are about  $\langle \sigma^\ell \cdot \sigma^{\ell'} \rangle / N = \|\mathbf{b}\|^2 / N$  (and 1 if  $\ell = \ell'$ ). Now if we set  $w^{j\ell} = \frac{\xi^j \cdot \mathbf{b}}{\sqrt{N}} + h^{j\ell} \sqrt{1 - \|\mathbf{b}\|^2/N}$  we see that this jointly gaussian family of r.v. satisfies  $E(w^{j\ell} w^{j'\ell'}) = \delta_{jj'} \|\mathbf{b}\|^2 / N$  for  $\ell \neq \ell'$  and  $\delta_{jj'}$  for  $\ell = \ell'$ . Thus, for the generic point  $\sigma^1, \dots, \sigma^m$  we have  $E_\xi f(\frac{\xi^j \cdot \sigma^\ell}{\sqrt{N}}) \simeq E_\xi Y$ , and the result follows.  $\square$

The reader has observed that Theorem 2.1 does not say that “ $G_N$  resembles  $G_{N+1}$ ” or that quantities such as  $E\langle\sigma^1 \cdot \sigma^2\rangle/N$  converge as  $N \rightarrow \infty$ . Proving this is a different question.

In the situation of Theorem 2.1, since the law of  $(\sigma_1, \dots, \sigma_n)$  under Gibbs’ measure is asymptotically close to a product measure, it is close to the product measure  $\nu$  on  $\{-1, 1\}^n$  such that  $\int \sigma_i d\nu(\sigma_1, \dots, \sigma_n) = \langle\sigma_i\rangle$ . In the cases we will consider, the quantities  $\langle\sigma_i\rangle$  are asymptotically i.i.d. r.v. (and converge in law), thereby providing a precise picture of the finite projections of Gibbs’ measure.

### 3. THE SHERRINGTON-KIRKPATRICK MODEL

The most studied case is when  $h = 0$ . It was proved in [A-L-R] that the system is in a pure state if  $\beta < 1$ . An easy consequence of the result of [C] is that there exists values of  $\beta > 1$ , arbitrarily close to one, for which this is not the case (one expects that this is never the case if  $\beta > 1$ ). There is a very special phenomenon happening in the case  $\beta < 1$ , namely that

$$(3.1) \quad \lim_{N \rightarrow \infty} E \frac{1}{N} \log Z_N = \lim_{N \rightarrow \infty} \frac{1}{N} \log EZ_N (= \frac{\beta^2}{4})$$

(by Jensen’s inequality there is always inequality  $\leq$ ). This apparently makes things much simpler. There are several very interesting methods (such as use of stochastic calculus to prove central limit theorems [C-N]) that seem to work for this case only. Even though some nagging questions remain, there is a rather complete picture of this case ([T5 Section 2]). Unfortunately, a behavior such as (3.1) is exceptional and we will concentrate upon the more challenging case  $h > 0$ . The formula corresponding to (3.1) is then given by (3.13) below, and is remarkable enough to make one wonder how such a formula is possible, and moreover can be proved. It turns out that the proof of (3.13) for small  $\beta$  is rather easy. This proof is also very instructive because the other cases considered in Theorem 3.1 below, as well as the results of Sections 4 to 6, although technically very much more involved do follow the same global strategy, so we will outline the main steps. The central issue is always to prove that the system is in a pure state (after which use of (2.9) allows all kinds of computations). In the present case at high enough temperature, that was actually done in [F-Z] as a special case of a powerful (and complicated) approach that handles much more general cases (such as finite range interactions), but it is very instructive to give here a simple direct argument.

We start with the inequality (implicitly proved in Section 2 by expansion of  $(\tilde{\sigma} \cdot \sigma^*)^2$ )

$$C_N = C_N(\beta, h) := E\langle(\frac{1}{N}\tilde{\sigma} \cdot \sigma^*)^2\rangle \leq \frac{4}{N} + E\langle\tilde{\sigma}_N \sigma_N^* \tilde{\sigma}_{N-1} \sigma_{N-1}^*\rangle$$

where  $\tilde{\sigma} = \sigma^1 - \sigma^2, \sigma^* = \sigma^3 - \sigma^4$ . To compute the last term we use the cavity method; we compute the bracket by regrouping in the Hamiltonian the terms not containing  $\sigma_N$  or  $\sigma_{N-1}$  and we find

$$(3.2) \quad E\langle\tilde{\sigma}_N \sigma_N^* \tilde{\sigma}_{N-1} \sigma_{N-1}^*\rangle \approx E \frac{1}{Z} \langle Av \tilde{\sigma}_N \sigma_N^* \tilde{\sigma}_{N-1} \sigma_{N-1}^* \mathcal{E} \rangle_{N-2}.$$

There  $\langle \cdot \rangle_{N-2}$  denotes Gibbs measure for an  $(N-2)$  spin system at inverse temperature  $\beta' = \beta\sqrt{1-2/N}$ , external field  $h' = h(1-2/N)^{-1/2}$ , and  $Av$  the average over all values of  $\sigma_N^\ell, \sigma_{N-1}^\ell (\ell \leq 4) = \pm 1$ ,

$$\mathcal{E} = \exp \beta \sum_{\ell \leq 4} \sum_{0 \leq j \leq 1} \sigma_{N-j}^\ell \left( \frac{1}{\sqrt{N}} \sum_{i \leq N-2} \sigma_i^\ell g_{i, N-j} + h \right)$$

and  $Z = \langle Av\mathcal{E} \rangle_{N-2}$ . The formidable looking formula (3.2) is actually almost an algebraic identity, except that we have neglected the lower order interaction terms between  $\sigma_N^\ell$  and  $\sigma_{N-1}^\ell$  (hence the small error acknowledged by the  $\approx$ ). The slight change of parameters  $\beta, h$  into  $\beta', h'$  turns out to be a secondary detail, and will be ignored from now on. The difficulty with the cavity method is that we do not know more about  $\langle \cdot \rangle_{N-2}$  than about  $\langle \cdot \rangle$ , so that it is hard to use (3.2). An easy way out is provided by the observation that  $Z \geq 1$  by Jensen's inequality and that  $\langle Av\tilde{\sigma}_N\sigma_N^*\tilde{\sigma}_{N-1}^2\sigma_{N-1}^*\mathcal{E} \rangle_{N-2} \geq 0$ , because it can be written (using thermal independence of the variables with a \* from those with a  $\tilde{\cdot}$ ) as a square. Then the right hand side of (3.2) can be bounded by  $E\langle Av\tilde{\sigma}_N\sigma_N^*\tilde{\sigma}_{N-1}\tilde{\sigma}_{N-1}^*\mathcal{E} \rangle_0$ . (This argument to dispose of the denominator will be referred to later as the positivity argument). This later quantity is much easier to evaluate. Integrating first in the  $g_{i, N-j} (j = 0, 1)$  one obtains after a few lines of straightforward estimates a bound  $\beta^2 L(\beta) C_{N-2}(\beta', h')$ , where  $L(\beta)$  remains bounded with  $\beta$ . This yields the relation  $C_N(\beta, h) \leq \frac{1}{2} C_{N-2}(\beta', h') + o(1)$  if  $\beta$  is small enough, which implies  $\lim_{N \rightarrow \infty} C_N(\beta, h) = 0$ .

The positivity argument used above does not take advantage of the fact that often the denominator is much larger than 1, and as the result of this loss of a constant factor, we cannot expect to reach this way the entire high temperature region. The merit of the positivity argument is that it is the simplest approach we know, and thus it is particularly useful in complicated situations. Unfortunately this argument itself often runs into a serious difficulty (which does not exist in the case of the SK model) namely that the estimation of  $C_N$  usually involves  $D_{N-2}$  (at slightly different parameters), where  $D_N = E\langle (\frac{1}{N}\tilde{\sigma} \cdot \sigma^3)^2 \rangle$ . It seems a posteriori true that  $C_N$  and  $D_N$  are of the same order, but unfortunately we do not see a priori how to prove better than  $C_N \leq \sqrt{D_N}$  (almost proved in Section 2), and this leads to useless relations such as  $C_N \leq \theta\sqrt{C_{N-2}} + o(1)$  where  $\theta < 1$ . Because of this a priori difficulty in relating  $C_N$  and  $D_N$ , one sees that a better strategy is to study  $D_N$ . But then, in the right hand side of (3.2) the numerator has to be replaced by  $\langle Av\tilde{\sigma}_N\tilde{\sigma}_{N-1}\sigma_N^3\sigma_{N-1}^3\mathcal{E} \rangle_{N-2}$  which has no reason to be positive, and the positivity argument does not work. This unfortunate state of affairs is largely responsible for the great technicality of many proofs, even at a very high temperature.

Now that we have proved that for small  $\beta$  the system is in a pure state, we observe that brackets involving  $\mathcal{E}$  resemble the brackets of (2.9). The requirement there that  $f$  was bounded was made only to avoid a technical statement; reasonable growth suffices. This means that we can now use (2.9) to make all sorts of computations, of which we now give a typical example. Proceeding as in 3.2, we

have

$$\langle \sigma_N \rangle = \frac{1}{Z} \langle Av\sigma_N \mathcal{E} \rangle_{N-1}$$

where  $Z = \langle Av\mathcal{E} \rangle_{N-1}$  and  $\mathcal{E} = \exp \beta \sigma_N (N^{-1/2} \sum_{i \leq N-1} \sigma_i g_{i,N} + h)$ . It follows from (2.9) (used for  $m = n = 1, f(x) = \exp \beta \sigma_N x$ ) that

$$(3.3) \quad \langle \sigma_N \rangle \simeq \text{th} \beta (N^{-1/2} \sum_{i \leq N-1} g_{i,N} \langle \sigma_i \rangle_{N-1} + h).$$

If we set  $r_{N-1} = N^{-1} \sum_{i \leq N-1} \langle \sigma_i \rangle_{N-1}^2$ , we then have

$$(3.4) \quad Er_N \simeq E \langle \sigma_N \rangle^2 \simeq E \text{th}^2 \beta (g\sqrt{r_{N-1}} + h)$$

where  $g$  is standard normal independent of  $r_{N-1}$ .

To make full use of this, it would be very nice to know that  $r_N$  is essentially non random, which amounts to show that  $(E \langle \sigma_N \rangle^2)^2 \simeq E \langle \sigma_N \rangle^2 \langle \sigma_{N-1} \rangle^2$ . The right-hand side can be estimated as in (3.4) using cavity and (2.9), and only a few lines of computations are required to get a relation of the type  $\text{Var } r_N \leq \beta^2 L(\beta) \text{Var } r_{N-2} + o(1)$ , so that for small  $\beta$  we have  $\text{Var } r_N \rightarrow 0$ , and (3.4) leads to  $q_N \simeq E \text{th}^2 \beta (g\sqrt{q_{N-1}} + h)$  where  $q_N = E \langle \sigma_N \rangle^2$  and to  $q_N \rightarrow q$  where  $q$  satisfies (3.10) below. To calculate  $F_N$ , we fix  $h\beta = h'$  and we write

$$(3.5) \quad \frac{\partial F_n}{\partial \beta} = \frac{1}{\sqrt{N}} \sum_{i < j} g_{ij} \langle \sigma_i \sigma_j \rangle.$$

We then (following [A-L-R]) apply the (extremely useful) integration by parts formula

$$(3.6) \quad E(gf(g)) = Ef'(g)$$

valid when  $g$  is standard normal and  $f$  smooth enough, to obtain

$$(3.7) \quad E \frac{1}{N} \frac{\partial F_N}{\partial \beta} = \beta \frac{N-1}{2N} (1 - E \langle \sigma_N \sigma_{N-1} \rangle^2) \simeq \frac{\beta}{2} (1 - q_N^2)$$

where we use that  $E \langle \sigma_N \sigma_{N-1} \rangle^2 \simeq E \langle \sigma_N \rangle^2 \langle \sigma_{N-1} \rangle^2 \simeq (E \langle \sigma_N \rangle^2)^2 = q_N^2$ .

To prove (3.13), one simply checks that it is true for  $\beta = 0$ , and the (miraculous) fact that  $\frac{\partial SK}{\partial \beta} = \frac{\beta}{2} (1 - q^2)$ . Concerning the structure of the r.v.  $\langle \sigma_i \rangle$ , we proceed as in (3.3) to obtain that, for any fixed  $n$ , as  $N \rightarrow \infty$ , for  $0 \leq k \leq n - 1$

$$\langle \sigma_{N-k} \rangle \simeq \text{th} \beta (g_k \sqrt{q_{N-n}} + h)$$

where  $(g_k)_{k \leq n-1}$  are i.i.d.  $N(0, 1)$ , so that (3.12) below is obvious.

To go beyond this first round of results, that is to be able to handle cases where the positivity argument does not work, and to perform the previous computations

with a better control of the error terms, we need to develop another technique to estimate  $EU/Z$ , when  $Z$  is a quantity such as in (3.2). The basic procedure is to replace  $Z$  by the quantity  $\hat{Z}$  provided by (2.9) (even when we have not yet proved that the system is in a pure state) and to write

$$(3.8) \quad \frac{U}{Z} = \frac{2U}{\hat{Z}} - \frac{UZ}{\hat{Z}^2} + \frac{U(Z - \hat{Z})^2}{Z\hat{Z}^2}.$$

The idea is that the last term has a tendency to be small because of the factor  $(Z - \hat{Z})^2$ , factor which is not affected when one takes bounds and uses absolute values. On the other hand, the first two terms on the right have a denominator where the dependence in the  $\mathbf{g}^j$  is only through  $\mathbf{g}^j \cdot \mathbf{b}$ , so that they can be evaluated by conditioning upon these. Carrying out that program results in extremely long computations but once the arguments are properly organized these allow to gain a very precise picture of the model. The largest domain in which we know how to control the model is

$$(3.9) D = \{(\beta, h) : \text{either } \beta < \beta_0, \text{ or } h \geq h_1(\beta) \text{ or } 0 < \beta < 1 \text{ and } h \leq h_2(\beta)\}$$

where  $h_1(\beta), h_2(\beta)$  are certain specific positive functions. We consider  $q = q(\beta, h)$ , the root of the equation

$$(3.10) \quad q = E \operatorname{th}^2 \beta(g\sqrt{q} + h)$$

(that is well defined on  $D$ ) and the function

$$(3.11) \quad SK(\beta, h) = \frac{\beta^2}{4}(1 - q)^2 + E \log \operatorname{ch} \beta(g\sqrt{q} + h).$$

In the following statement,  $K$  denotes a number depending upon  $\beta, h$  only.

**THEOREM 3.1.** *If  $(\beta, h)$  belongs to  $D$ , the following occurs*

$$(3.12) \quad E \langle \exp \frac{1}{KN} (\boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2 - q)^2 \rangle \leq K$$

$$(3.13) \quad \lim_{N \rightarrow \infty} N^{-1} EF_N = SK(\beta, h)$$

(3.14) *Given any  $n$ , the r.v.  $\langle \sigma_1 \rangle, \dots, \langle \sigma_n \rangle$  are asymptotically i.i.d., and their limiting law is the law of  $\operatorname{th} \beta(g\sqrt{q} + h)$  where  $g$  is  $N(0, 1)$*

(3.15) *Given replicas  $\boldsymbol{\sigma}^1, \dots, \boldsymbol{\sigma}^p$ , for any expression  $f$  that is the product of  $k$  quantities of the type  $\boldsymbol{\sigma}^\ell \cdot \boldsymbol{\sigma}^{\ell'} - E \langle \boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2 \rangle$  ( $\ell \neq \ell'$ ) then  $\lim_{N \rightarrow \infty} N^{-k/2} E \langle f \rangle$  exists.*

*Comment 1.* The validity of (3.13) was also investigated by M. Shcherbina. In her remarkable recent paper [Sh2] she proves in particular that it holds whenever  $\beta < 1$ .

*Comment 2.* Condition (3.12) is a very precise improvement of (2.1) and moreover it contains the information that  $\langle \sigma^1 \cdot \sigma^2 \rangle$  is nearly  $q$ . In the case  $h = 0, (\beta < 1)$  it is much easier to prove [T5, Section 2]. We feel that the greatest importance of exponential equalities such as (3.12) is that they carry information that can be transferred (with loss) to *different* (but close) values of the parameters. Specifically, one can show that given  $\epsilon > 0$ , if  $\beta', h'$  are close enough (depending upon  $\epsilon$ ) of  $\beta, h$ , then, if (3.12) holds at  $\beta, h$ , then at  $\beta', h'$  the overlap  $N^{-1} \sigma^1 \cdot \sigma^2$  will essentially take values only in an interval of length  $\leq \epsilon$ . This is shown in [T10], and this is how the part  $0 < \beta < 1$  and  $h < h(\beta)$  of  $D$  is controlled, building upon the case  $0 < \beta < 1, h = 0$  that is obtained through special arguments. We believe that such a “transfer principle” has to be a part of a proof that would extend Theorem 3.1 to the entire region (3.12).

*Comment 3.* The limits of (3.15) contain in principle all the information on the (random) joint law under Gibb’s measure of the maps  $(\sigma^1, \dots, \sigma^p) \rightarrow N^{-1/2}(\sigma^\ell \cdot \sigma^{\ell'} - E\langle \sigma^1 \cdot \sigma^2 \rangle)$ , and (3.15) is obtained by an explicit method, allowing in principle computation of the limits. We did check that asymptotically, the law under Gibbs measure of the “symmetrized overlaps”  $N^{-1/2}(\sigma^1 - \sigma^2) \cdot (\sigma^3 - \sigma^4)$  is asymptotically gaussian (independent of the disorder) of variance  $A/(1 - \theta)$ , where

$$(3.16) \quad A = 4E \frac{1}{\text{ch}^2 \beta(g\sqrt{q} + h)}$$

and where  $\theta$  is the quantity (3.17) below. It seems to us that the joint laws under Gibbs measure of the maps  $N^{-1/2}(\sigma^\ell \cdot \sigma^{\ell'} - \langle \sigma^\ell \cdot \sigma^{\ell'} \rangle)$  should be asymptotically gaussian, independent of the disorder, and that the joint laws of the maps  $N^{-1/2} \langle \sigma^\ell \cdot \sigma^{\ell'} \rangle$  should also be gaussian. Checking this is in principle elementary, but the algebraic formalism needed to write nicely such a result remains to be found.

What is the high temperature region? The physicists believe that it is the region defined by

$$(3.17) \quad \theta = \beta^2 E \frac{1}{\text{ch}^4 \beta(g\sqrt{q} + h)} < 1$$

(where  $q$  is as in (3.10)). This conclusion was first obtained in [A-T], literally, by analyzing the eigenvalues of matrices of dimension  $0 \times 0$ . In order to estimate the size of the cultural gap (and, in particular why the notion of “triviality” is very relative) it is instructive to outline the derivation of this using the cavity method from [M-P-V]. After conducting some computations that seem based upon the a priori assumption that most of the conclusions of Theorem 2.1 are valid the authors reach the relation  $C_N = \theta C_N + A/N$  where  $A$  is given by (3.16) and  $\theta$  by (3.17) and conclude “thus we must have  $\theta < 1$  to have  $C_N$  positive”. In other words physicists do not mind purely formal computations, and what is amazing is how well this works.

The predicted structure of the low temperature region involves the mysterious phenomenon of “replica-symmetry breaking” and I am much grateful to

M. Mézard for having explained it to me outside the replica formalism (see [To]). The idea is simply that an arbitrarily small coupling between two replicas has big consequences. Consider, on  $\Sigma_N^2$ , the Hamiltonian  $H_N$  given by  $H_N(\boldsymbol{\sigma}^1) + H_N(\boldsymbol{\sigma}^2) + t\boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2/N$ , and the corresponding Gibbs measure  $\langle \cdot \rangle_t$  on  $\Sigma_N^2$  (which is NOT a product measure). Consider the function  $\varphi_{N,\beta,h}(t) = \varphi_N(t) = \langle N^{-1}\boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2 \rangle_t$ . Replica symmetry breaking means that “ $\lim_N \varphi_N(t)$  is discontinuous at zero”, which, as we cannot prove the existence of the limit, we formulate as follows.

**DEFINITION 3.2.** *We say that there is replica symmetry breaking (RSB) for the parameters  $(\beta, h)$  if the sequence  $\varphi_N$  is not uniformly equicontinuous as  $N \rightarrow \infty$  at the point  $t = 0$ .*

This means that there is an  $\epsilon > 0$  such that there are arbitrarily large values of  $N$  and arbitrarily small values of  $t$  for which  $|\varphi_N(t) - \varphi_N(0)| \geq \epsilon$ .

**THEOREM 3.3.** *There is replica symmetry breaking at the generic point (in the sense of Baire category) of the region  $\theta > 1$ .*

One of course expects that there is RSB at each point of the region  $\theta > 1$ . It is a simple consequence of (3.8) that there is no RSB in the region  $D$  of Theorem 3.1. The status of the other points of the region (3.9) is unknown.

The proof of Theorem 3.3 relies upon the basic observation that if there is no RSB, then (2.2) holds. We then know how to make computations and we can make the physicist’s relation  $C_N \cong \theta C_N + A/N$  rigorous. It is worthwhile to detail a bit what happens here, as this touches what seems to us to be the central obstacle in proving that under (3.17) the system is in a pure state. If there is no RSB, one shows that for any  $\epsilon > 0$ , when  $N$  is large, we essentially always have  $|(\boldsymbol{\sigma}^1 - \boldsymbol{\sigma}^2) \cdot \boldsymbol{\sigma}^3| \leq \epsilon N$ . This implies that if we set  $D_{n,N} = E\langle (N^{-1}(\boldsymbol{\sigma}^1 - \boldsymbol{\sigma}^2) \cdot \boldsymbol{\sigma}^3)^{2n} \rangle$  then for large  $N$ ,  $D_{2,N} \ll D_{1,N}$ . This is extremely valuable because when one tries to compute  $D_N = D_{1,N}$  by the cavity method using an order 2 expansion, we find terms involving  $D_{2,N}$ , and we now know that these are indeed smaller order terms. In contrast, when we try to prove that  $D_{1,N}$  is small under (3.17) we do not know a priori that  $D_{2,N} \ll D_{1,N}$ . This is not a trivial issue. For a related model (to be considered in Section 7) we did prove rigorously that there exist situations where  $D_{2,N}$  and  $D_{1,N}$  are of the same order (and of order at most  $1/\sqrt{N}$ ). Moreover, this issue does not seem to have been considered by the physicists. They seem to ignore it when using either the cavity method or the “stability analysis” of the replica formalism (a personal impression based on the fact that, in particular for the model of Section 7 a wrong solution, that roughly speaking “would be true if  $D_{2,N} \ll D_{1,N}$ ”, is found to be stable in this sense.) To control  $D_{1,N}$  close enough to the low temperature region without a priori assumptions, the most natural way seems to control  $D_{2,N}$ ; but this in turn requires to control  $D_{3,N}$ , etc., leading naturally to the consideration of exponential inequalities such as in Theorem 3.1.

One of the striking and easily formulated predictions of the Parisi solution is that at low temperature certain quantities depend upon the realization of randomness. For different Hamiltonians (that make matters easier) it is shown in [P-S], [Sh1] that the quantity  $q_N = N^{-1} \sum_{i \leq N} \langle \sigma_i \rangle^2$  essentially depends upon the randomness

when  $\beta$  is large enough (its variance does not go to zero as  $N \rightarrow \infty$ ). For the Hamiltonian (1.3) it is shown in [T5] that when  $h = 0$  and  $\beta$  is large enough the quantity  $q' = N^{-2} \sum_{i < j} \langle \sigma_i \sigma_j \rangle^2$  must essentially depend upon the randomness.

(In contrast, in the region  $D$ , this quantity is asymptotically close to  $q^2/2$ .) The basis for the argument is the fact that the random convex function  $F_N/N$  has fluctuations of order  $N^{-1/2}$ , so that for most values of  $\beta$ ,  $F'_N(\beta)/N$  has only small fluctuations. One then computes the variance of this quantity using integration by parts, assuming that  $q'$  has vanishing fluctuations, and this yields the information that  $E\langle |(\frac{\sigma^1 \cdot \sigma^2}{N})^2 - \langle (\frac{\sigma^1 \cdot \sigma^2}{N})^2 \rangle| \rangle \rightarrow 0$ . This is not as good as (2.2), but is sufficient to prove that (3.13) would hold, which is known to be wrong for large  $\beta$  as proved in [C].

The idea for the first part of the above argument is in germ in [A-L-R]. This line of arguments is exquisitely developed by F. Guerra [Gu2]. Using only integration by parts and the fact that  $EF''_N(\beta)/N$  is non negative and of order 1 for most  $\beta$ , he shows that for most values of  $\beta$ ,

$$(3.18) \quad E\langle (\frac{\sigma^1 \cdot \sigma^2}{N})^4 \rangle - 4E\langle (\frac{\sigma^1 \cdot \sigma^2}{N})^2 (\frac{\sigma^1 \cdot \sigma^3}{N})^2 \rangle + 3E\langle (\frac{\sigma^1 \cdot \sigma^2}{N})^2 \rangle^2 \simeq 0.$$

It is explained in [A-C1] why this is less miraculous than it seems at first sight.

#### 4. THE HOPFIELD MODEL

The Hopfield model was introduced by Pastur and Figotin [P-F] in the spin glass context, but became famous only after Hopfield interpreted it as a model for memory. We will refer the reader to [H1], [H2], [H-K-P], [T-D-C] for this aspect of the model, and we will directly turn towards the underlying mathematics. The model involves  $N$  spins, and  $M$  configurations “to be memorized”  $(\eta_k)_{k \leq M}$ , where  $\eta_k = (\eta_{i,k})_{i \leq N}$ . These configurations are called the *prototypes* and are chosen at random in the simplest possible manner, independently, with  $P(\eta_{i,k} = 1) = P(\eta_{i,k} = -1) = \frac{1}{2}$ . The object of interest is the function on  $\Sigma_N$  defined by

$$(4.1) \quad H_{N,M}(\sigma) = -\frac{N}{2} \sum_{k \leq M} m_k(\sigma)^2$$

where

$$(4.2) \quad m_k(\sigma) = \frac{1}{N} \sum_{i \leq N} \sigma_i \eta_{i,k}$$

is the overlap between  $\sigma$  and  $\eta_k$ . The normalizing factor  $N/2$  will be pleasant when we will use a temperature; one way to look at  $H_N$  is that it is among the simplest functions one can write that is a candidate to take a large negative value when  $\sigma = \eta_k$  (since  $m_k(\eta_k) = 1$ ). We will study the Hopfield model only at  $N \rightarrow \infty$ . There are different regimes of growth of  $M = M(N)$  that are of interest; we will consider here only the most challenging one, when  $M = [\alpha N]$  is a proportion of



$N$ . (We consider  $\alpha$  as fixed and no longer write the dependence in  $M$ .) Not surprisingly, the smaller  $\alpha$  is, the easier the model is.

Even though this is not our main line of interest, we will say a few words about the “zero temperature case”, that is the study of the function  $H_N$  itself. The rigorous results concerning that case are not sharp, and often obtained by ad-hoc methods that cannot yield optimal results; but at least they exist.

It is believed that for large  $N$  (and with an overwhelming probability) for  $\alpha \leq .13$  there is an “energy barrier” around each prototype; that is, for some  $\delta > 0$ ,  $\epsilon > 0$

$$\inf_{d(\boldsymbol{\sigma}, \boldsymbol{\eta}_k) = \delta N} H_N(\boldsymbol{\sigma}) > H_N(\boldsymbol{\eta}_k) + \Sigma N$$

where  $d(\boldsymbol{\sigma}, \boldsymbol{\eta}_k)$  is the number of indexes  $i \leq N$  such that  $\sigma_i \neq \eta_{i,k}$ . This was proved for  $\alpha \leq 0.05$  by C. Newman [N],  $\alpha \leq 0.07$  by D. Loukianova [Lou 1] and can be further improved [T6, Section 9]. Let us say that a configuration  $\boldsymbol{\sigma}$  is a local minimum if the value of  $H_{N,M}(\boldsymbol{\sigma})$  cannot be decreased by changing the sign of one single spin. (The importance of these is that they can be thought as the configurations “memorized” by  $H_{N,M}$ .) Possibly the prettiest proof is due to Loukianova [Lou 2], who shows, that, as  $\alpha \rightarrow \infty$ , the function  $H_N$  cannot have a local minimum anywhere close to a prototype. However, nagging questions remain. In particular, it is believed that for  $\alpha = .1$ ,  $H_{N,M}$  has a local minimum near each prototype, but a lower global minimum. (This lower global minimum is believed not to be simply related to any prototype, and does not seem to be accessible by any explicit algorithm.) Our inability to deal rigorously with this question takes its root in the fact that, while we know, at least in principle, how to calculate the order of (the expected value of) the supremum of a gaussian process (see [T1]) we do not know how to do this, say, within 10% (or even a factor 2).

It is natural to study the function  $H_N$  through the introduction of a temperature  $T = 1/\beta$ , and to study the corresponding Gibbs measure (that gives weight  $Z^{-1} \exp -\beta H_N(\boldsymbol{\sigma})$  to  $\boldsymbol{\sigma}$ , where  $Z$  is the normalizing factor). The results of the study through the replica formalism are presented in [A-G-S].

The region  $\beta(1 + \sqrt{\alpha}) < 1$  corresponds to the case  $h = 0, \beta < 1$  of the SK model. In that region we have

$$(4.3) \quad \lim_{N \rightarrow \infty} \frac{1}{N} E \log Z_N = \lim \frac{1}{N} \log E Z_N (= \frac{\alpha}{2} \log \frac{1}{1 - \beta}).$$

As we already mentioned, this seems to make things simpler and this region is rather well understood [T6, Section 2]. The situation can be physically described by saying that the temperature is so high that nothing can be learned about the prototypes by studying Gibbs measure.

At  $\beta = 1$ , there seems to be an instability that has yet to be analyzed, so we will consider directly the case  $\beta > 1$ . Important rigorous work has been done in that case by A. Bovier and V. Gayrard (sometimes jointly with P. Picco) [B], [B-G1, 2, 3, 4], [B-G-P1, 2]. These authors have in particular been interested in the image of  $\overline{G}$  on  $\mathbb{R}^M$  of Gibbs measure under the map  $\boldsymbol{\sigma} \rightarrow (m_k(\boldsymbol{\sigma}))_{k \leq M}$ . It is very natural to consider this measure since  $H_N(\boldsymbol{\sigma})$  is defined in function of the overlaps  $m_k(\boldsymbol{\sigma})$  only. They proved that if  $\alpha \leq L^{-1} \min(1, (\beta - 1)^2)$  (where  $L$  is a universal

constant) then  $\overline{G}$  is essentially supported by the union of  $2M$  disjoint balls of  $\mathbb{R}^M$ . These balls are centered at the points  $m^* \mathbf{e}_k$ , where  $(\mathbf{e}_k)$  is the canonical basis of  $\mathbb{R}^M$  and  $m^* = \text{th } \beta m^*$ . This spontaneous decomposition of  $\overline{G}$  into “states” simply reflects the strong influence of each prototype on the Hamiltonian. Much more precise information on the structure of  $\overline{G}$  is contained in Theorem 4.1 below, so we will not state the results of [B-G1] in detail, but beside the intrinsic interest of these results, it must be pointed out that this a priori information of  $\overline{G}$  is essential for the use of the cavity method.

Since  $\overline{G}$  (and hence  $G$ ) breaks into rather unrelated pieces, it is quite natural to study these separately. One way (introduced in [A-G-S]) to do this is to replace the Hamiltonian (4.1) by

$$(4.4) \quad H_N(\boldsymbol{\sigma}) = -\frac{N}{2} \sum_{k \leq M} m_k(\boldsymbol{\sigma})^2 - hNm_1(\boldsymbol{\sigma})$$

where  $h > 0$  (and small). The effect of the extra term is to favor the part of  $\overline{G}$  close to  $\mathbf{e}_1 m^*$  over the parts close to  $-\mathbf{e}_1 m^*$  or  $\pm \mathbf{e}_k m^*$ ,  $k \geq 2$ .

To state our main result, we consider the domain

$$(4.5) \quad D = \{(\alpha, \beta, h); \beta > 1, \alpha \leq \frac{1}{L} \min((\beta - 1)^2, \frac{1}{\log \beta}); 0 < h < h(\alpha, \beta)\}$$

where  $L$  is a (suitably large) number and  $h(\alpha, \beta)$  is positive (and suitably small). The condition upon  $h$  means that we are interested only in the case of  $h$  very small; the results can be extended to the case of any  $h > 0$  with some extra effort; on the other hand the requirement on  $\alpha$  is essentially the best possible. It should be pointed out that the region  $D$  is a part of what is usually called the low temperature region, but the behavior there is typically high temperature (“replica-symmetry”).

We consider the system of equations

$$(4.6) \quad \mu = E \text{th } \beta(g\sqrt{r} + \mu + h)$$

$$(4.7) \quad q = E \text{th}^2 \beta(g\sqrt{r} + \mu + h)$$

$$(4.8) \quad r = \alpha q(1 - \beta(1 - q))^{-2}$$

It can be shown that if  $(\alpha, \beta, h) \in D$  (and the constant  $L$  of (4.5) is large enough), this system of equations has a unique solution. We consider the function  $\varphi(x) = \min(x, x^2)$ . The somewhat complicated inequalities (4.9) to (4.13) mostly intend to convey the message that great accuracy can be reached, and need not be understood in detail by the casual reader.

**THEOREM 4.1.** *For each value of  $(\alpha, \beta, h)$  in  $D$  there exists a number  $K$  indepen-*

dent of  $N$  with the following properties

$$(4.9) \quad E\langle \exp \frac{1}{KN} (\boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2 - Nq)^2 \rangle \leq K$$

$$(4.10) \quad E\langle \exp \frac{N}{K} \varphi \left( \sum_{2 \leq k \leq M} m_k(\boldsymbol{\sigma}^1) m_k(\boldsymbol{\sigma}^2) - r \right) \rangle \leq K$$

$$(4.11) \quad E\langle \exp \frac{N}{K} (m_1(\boldsymbol{\sigma}) - \mu)^2 \rangle \leq K$$

$$(4.12) \quad \forall k \geq 2, E\langle \exp \frac{N}{K} m_k^2(\boldsymbol{\sigma}) \rangle \leq K$$

$$(4.13) \quad E\langle \exp \frac{N}{K} \varphi \left( \sum_{2 \leq k \leq M} m_k^2(\boldsymbol{\sigma}) - \frac{1 - \beta(1 - q)^2}{(1 - \beta(1 - q))^2} \right) \rangle \leq K$$

$$(4.14) \quad E\langle \exp \frac{N}{K} \varphi \left( \sum_{2 \leq k \leq M} (m_k(\boldsymbol{\sigma}) - \langle m_k(\boldsymbol{\sigma}) \rangle)^2 - \frac{\alpha(1 - q)}{(1 - \beta(1 - q))^2} \right) \rangle \leq K$$

Moreover, for any  $n > 0$ , the r.v.  $\langle \sigma_1 \rangle, \dots, \langle \sigma_n \rangle$  are asymptotically independent; their limit law is the law of  $\text{th } \beta(g\sqrt{q} + \mu + h)$  where  $g$  is standard normal.

The use of the function  $\varphi$  rather than  $x^2$  is motivated by problems with the very large values; the reason why  $m_1(\boldsymbol{\sigma})$  plays a special role should be obvious from (4.4). The meaning of (4.9) is that the measure  $\overline{G}'$  image of Gibbs' measure under the map  $\boldsymbol{\sigma} \rightarrow (m_k)_{2 \leq k \leq M}$  "is in a pure state". The meaning of (4.14) is that this measure is nearly carried by a small shell around the sphere of center  $\mathbf{b} = (\langle m_k(\boldsymbol{\sigma}) \rangle)_{2 \leq k \leq M}$  and of radius  $(\alpha(1 - q))^{1/2} / (1 - \beta(1 - q))$ ; and (4.13) implies that  $\|\mathbf{b}\|^2$  is nearly  $r$ . We thus have very accurate information on  $\overline{G}'$ . We consider now the function

$$(4.15) \quad RS(\alpha, \beta, h) = -\frac{\mu^2 \beta}{2} + \frac{\alpha}{2} \left( \frac{\beta q}{1 - \beta(1 - q)} - \log(1 - \beta(1 - q)) \right) - \beta^2 \frac{r}{2} (1 - q) + E \log \text{ch } \beta(g\sqrt{r} + \mu + h)$$

where of course  $r, q, \mu$  are solutions of (4.6) to (4.8).

**THEOREM 4.2.** *If the parameters  $(\alpha, \beta, h)$  belong to  $D$ , then*

$$(4.16) \quad \lim_{N \rightarrow \infty} N^{-1} E F_N(\alpha, \beta, h) = RS(\alpha, \beta, h).$$

Theorem 4.2 was first proved in [T6] in the smaller domain  $D_1 \subset D$  where, for  $\beta \geq 2$ , the condition  $L\alpha \log \beta \leq 1$  is replaced by the stronger constraint  $L\alpha \beta \leq 1$ . Equality (4.16) extends by continuity to the case  $h = 0$ . The proof of [T6] uses the (somewhat unsatisfactory) technique of adding an appropriate small perturbation term to the Hamiltonian (4.4), a trick that produces magical and mysterious results. This perturbation term is  $\gamma \varphi(N) \sum_{k \leq M} g_k N m_k(\boldsymbol{\sigma})$ , where  $\varphi(N)$  goes to zero but not too fast (say  $\varphi(N) = N^{-1/3}$ ), where  $g_k$  are i.i.d.  $N(0, 1)$ , and

where  $0 \leq \gamma \leq 1$  (say). As  $N \rightarrow \infty$ , for fixed  $\gamma$  the extra term has a vanishing influence on the expected free energy density (because  $\varphi(N) \rightarrow 0$ ). On the other hand, differentiation of  $N^{-1}F_N$  with respect to  $\gamma$  as in [Gu2] leads to precious information. This information comes essentially “for free”, a miraculous fact that it would be nice to really understand. Upon reading [T6], Bovier and Gayraud [B-G3] discovered a very beautiful approach (in the same smaller domain  $D_1$ ) that deals directly with the Hamiltonian (4.4), and where the fact that the system is in a pure state follows from a transparent geometric property. Unfortunately this property is not true in the entire domain  $D$  of (4.5). One can only hope that their approach can be modified to cover the correct domain  $D$  and is not specific to this particular model.

It is possible to explain some of the mystery of the formula (4.15). If we consider the right-hand side of (4.15) as a function of independent variables  $\alpha, \beta, h, q, r, \mu$ , equations (4.6) to (4.8) mean that the partial derivatives of this function with respect to  $\mu, q, r$  respectively are zero, so that even though these depend upon  $\alpha$ , the partial derivative of  $RS(\alpha, \beta, h)$  with respect to  $\alpha$  can be computed as if it were not the case. One simply has to check that this partial derivative coincides with the increase of expected free energy when  $M$  is replaced by  $M + 1$ , that is

$$E \log \langle \exp \beta \left( \sum_{i \leq N} \eta_{i, M+1} \sigma_i \right)^2 \rangle$$

which is calculated with (2.9) showing first that the variables  $\eta_{i, M+1}$  can be replaced by independent gaussian (although non trivial technicalities arise due to lack of boundedness).

**THEOREM 4.3.** *If a function  $W$  on a  $p$  replica is a product of finitely many expressions of one of the following types:*

$$(4.17) \quad N^{-1/2} (\sigma^\ell \cdot \sigma^{\ell'} - E \langle \sigma^\ell \cdot \sigma^{\ell'} \rangle)$$

$$(4.18) \quad N^{1/2} \left( \sum_{2 \leq k \leq M} m_k(\sigma^\ell) m_k(\sigma^{\ell'}) - E \left\langle \sum_{2 \leq k \leq M} m_k(\sigma^\ell) m_k(\sigma^{\ell'}) \right\rangle \right)$$

$$(4.19) \quad N^{1/2} (m_k(\sigma^\ell) - E \langle m_k(\sigma^\ell) \rangle) (k \geq 1)$$

then  $\lim_{N \rightarrow \infty} E \langle W \rangle$  exists.

This theorem is proved by an explicit method allowing in principle explicit computation of the limits. Only remains the uninspiring (and in principle elementary) task to clarify the underlying algebraic structure. Motivated by [B-G4] (that considers the case  $\alpha = \alpha(N) \rightarrow 0$ ) we did check that given any  $n$ , the laws under Gibbs measure of the maps  $\sigma \rightarrow N^{1/2} m_k(\sigma) (2 \leq k \leq n)$  are asymptotically i.i.d. gaussian centered, of variance  $(1 - \beta(1 - q)^2)(1 - \beta(1 - q))^{-2}$ .

Let us now outline the main aspect in which the proofs differ from the case of the SK model. When one tries to compute a quantity such as  $D_N = E \langle (\tilde{\sigma} \cdot \sigma^3)^2 \rangle$  in function of  $D_{N-2}$ , by regrouping in the Hamiltonian the terms containing  $\sigma_N^\ell, \sigma_{N-1}^\ell (\ell \leq 3)$  one rather finds terms such as  $A_{N-2}$ , where

$$(4.20) \quad A_N = E \left\langle \left( \sum_{2 \leq k \leq M} \tilde{m}_k \cdot m_k^3 \right)^2 \right\rangle$$

(again with a small change of temperature) where  $\tilde{m}_k = m_k(\sigma^1) - m_k(\sigma^2)$ ,  $m_k^3 = m_k(\sigma^3)$ , and to obtain a useful relation one would have to relate such terms to terms such as  $D_{N-2}$ . Since it is not obvious how to do this, we chose the alternate strategy to show first that  $A_N$  is small. To relate  $A_N$  with  $A_{N-1}$ , the first step is to isolate in  $\tilde{m}_k, m_k^3$  the contribution of  $\tilde{\sigma}_N, \sigma_N^3$ . After expansion, one faces dangerous sums of the type  $E \sum_k \eta_{k,N} \langle f_k \rangle$ . In these terms  $f_k$  is not small, but does not depend upon  $\eta_{k,N}$ . Cancellation occurs because the bracket  $\langle \cdot \rangle$  depends only weakly upon  $\eta_{k,N}$ ; this is expressed by an extension of the integration by parts formula (3.6) to Bernoulli r.v. (with now an error term). After integration by parts the various terms can then be related to a  $N - 1$  spin situation via the scheme (3.8). The only drawback of this approach is that integration by parts creates numerous terms, and from each of these (3.8) creates numerous new terms, so that the computations soon reach gargantuan proportions; but once one has learned how to identify the leading terms, all it really takes to go through them is a few weeks of patience.

## 5. INTERSECTING RANDOM HALF SPACES: THE CAPACITY OF THE PERCEPTRON

The problem to be discussed in this section originates in the theory of neural networks. Its basic nature makes it however of interest well beyond this theory, and the reader interested in neural networks is referred to [G2], [H-K-P]. We will consider random half spaces in  $\mathbb{R}^N$  that are at a given distance from the origin. The random direction will be modeled by a sequence  $\xi = (\xi_i)_{i \leq N}$  of r.v. with  $P(\xi_i = 1) = P(\xi_i = -1) = 1/2$ . This choice (rather than the most canonical choice of gaussian r.v.) is motivated by the origin of the problem. The same result (often quite easier) can be obtained in the Gaussian case. Given a number  $\kappa$ , we consider the half space  $H(\xi) = \{\mathbf{x} \in \mathbb{R}^N; \xi \cdot \mathbf{x} \geq \kappa\sqrt{N}\}$ : Given independent choices  $\xi^1, \dots, \xi^M$  of random directions, we would like to know whether typically  $\bigcap_{k \leq M} H(\xi^k)$  meets  $\Sigma_N$ . If  $\lambda_N$  denotes the homogeneous probability on  $\Sigma_N$ , when  $\kappa = 0$  (the most important case) and (to avoid minor complications)  $N$  is odd, it is trivial that  $E\lambda_N(\bigcap_{k \leq M} H(\xi^k)) = 2^{-M}$ , and this shows that if  $M > (1 + \epsilon)N$  the answer is no. It is proved in [K-R] that there is  $\epsilon > 0$  such that for large  $N$  the set  $\bigcap_{k \leq M} H(\xi^k)$  typically meets  $\Sigma_N$  if  $M \leq \epsilon N$ , but not if  $M \geq (1 - \epsilon)N$ , a result that is somewhat streamlined and improved in [T13]. It is conjectured in [K-M] that the critical value of  $M$  is about  $M = .83N$ . One would like to compute exactly (in the limit) the "typical value" of  $N^{-1} \log \lambda_N(\bigcap_{k \leq M} H(\xi^k))$  (the mean is not defined since  $\bigcap_{k \leq M} H(\xi^k)$  can be empty). There is an obstacle to the study of a quantity such as  $\bigcap_{k \leq M} H(\xi^k)$ , namely that the size of this set is extremely dependent upon each direction  $\xi^k$  (e.g. the set is empty if  $\xi^M = -\xi^1, \kappa > 0$ ). Of course one expects that "in general configurations" this is not the case, but showing this requires works. It does not seem even trivial to show that the random quantity

$N^{-1} \log \lambda_N(\bigcap_{k \leq M} H(\xi^k))$  has small fluctuations around its median value, and this despite a well developed machinery that has been constructed to handle such problems [T2], [T4]. It is currently not known how to show that these fluctuations are of order  $N^{-1/2}$ , as one should expect (see [T9] for a weaker result). It is thus natural to study first a version of the problem “with temperature”, by considering the Hamiltonian

$$(5.1) \quad H_{N,M}(\sigma) = - \sum_{k \leq M} \theta\left(\frac{\xi^k \cdot \sigma}{\sqrt{N}}\right)$$

where  $\theta(x) = 1_{\{x \geq \kappa\}}$ . One will then consider the corresponding Gibbs measure  $G_N$  at inverse temperature  $\beta$ . When  $\theta(x) = x^2/2$  (5.1) is the Hamiltonian of the Hopfield model; but the fact that  $\theta$  is now bounded suppresses the strong attraction of the system towards the configurations  $\xi^k$ .

Given a function  $\theta$ , and  $\beta > 0$ , we consider the function (defined for  $y < 1$ )

$$(5.2) \quad \Phi(x, y) = \frac{1}{\sqrt{1-y}} \frac{Eg \exp \beta\theta(x + g\sqrt{1-y})}{E \exp \beta\theta(x + g\sqrt{1-y})}$$

where  $g$  is  $N(0, 1)$ . In the next statement,  $z$  also denotes a  $N(0, 1)$  variable independent of  $g$ , and  $E_g$  denotes integration in  $g$  only.

**THEOREM 5.1.** *Given  $\beta > 0$ , there exists a number  $\alpha_0(\beta) > 0$  with the following property. Consider a nondecreasing function  $\theta : \mathbb{R} \rightarrow [-1, 1]$ , and the function  $\Phi$  given by (5.2). Then, if  $\alpha \leq \alpha_0(\beta)$  the system of equations*

$$(5.3) \quad q = E \operatorname{th}^2(z\sqrt{\hat{q}}); \hat{q} = \alpha E \Phi^2(z\sqrt{q}, q)$$

has a unique solution  $q = q(\alpha, \theta, \beta), \hat{q} = \hat{q}(\alpha, \theta, \beta)$ . Moreover, if  $Z_{N,M}$  denotes the partition function of the system governed by the Hamiltonian (5.1) at inverse temperature  $\beta$ , we have

$$(5.4) \quad \lim_{N \rightarrow \infty} \frac{1}{N} E \log Z_{N,M} = RS(\alpha, \beta)$$

when  $M = [\alpha N]$  and

$$(5.5) \quad RS(\alpha, \beta) = -\frac{1}{2} \hat{q}(1 - q) + E \log 2 \operatorname{ch} z\sqrt{\hat{q}} + \alpha E \log E_g \exp \beta\theta(z\sqrt{q} + g\sqrt{1-q}).$$

It is of interest to compare this formula with the corresponding formula for the Hopfield model. When  $\theta(x) = x^2, \Phi$  is well defined for  $\beta(1 - y) < 1$ , and the second equation of (5.3) becomes  $\hat{q} = \alpha\beta^2 q(1 - \beta(1 - q))^{-2}$ . Then (5.5) gives the formula (4.15) in the case  $\mu = h = 0$ .

The reader has noted that Theorem 5.1 does *not* require that  $\theta$  be smooth. On the other hand, we do not know how to relate an  $N$  spin system with an

$(N - 1)$  spin system unless  $\theta$  is smooth and we can make power expansions. To prove Theorem 5.1, we first assume that  $\theta$  is smooth, and we use the monotonicity of  $Z_{N,M}$  in  $\theta$ . With this approach, it is not clear how to prove (2.2), or even whether this is true when  $\theta$  is an indicator function. The difficulty is a problem of interversion of limits. The useful estimates when  $\theta$  is smooth require  $N$  large, where “large” seems to depend on how large the derivative of  $\theta$  can be.

When relating an  $N$  spin system with an  $(N - 1)$  spin system, the role that was played by the quantities  $m_k$  in the case of the Hopfield model is now played by  $\theta'(s_k)/\sqrt{N}$ , where  $s_k = N^{-1/2} \sum_{i \leq N} \xi_i^k \sigma_i$ . A first observation is that

$\sum_{k \leq M} (\theta'(s_k)/\sqrt{N})^2$  (among other quantities) will not be bounded by a quantity

depending upon  $\|\theta\|_\infty = \sup |\theta|$  only. In order to be able to prove Theorem 5.1, we must make estimates that (for large  $N$ ) do not depend on  $\|\theta'\|_\infty$  but only on  $\|\theta\|_\infty$ ; not surprisingly, the main tool for that purpose is integration by parts. A second observation is that we no longer benefit as in the Hopfield case from the fact that  $\theta'(x) = \beta x$  is a very simple function. This made possible (through integration by parts) to relate quantities such (4.20) (quantifying that the image of Gibbs measure under the map  $\sigma \rightarrow (\theta'(s_k)/\sqrt{N})_{k \leq M}$  is nearly in a pure state) with quantities such as  $E\langle (\frac{1}{N} \tilde{\sigma} \cdot \sigma^3)^2 \rangle$  that involve only configurations. As a substitute to these explicit evaluations, we use another version of the cavity method (that we learned in [M]), which relies on the simple observation that for any function  $f$ ,

$$(5.6) \quad \langle f(s_k) \rangle = \frac{\langle f(s_k) \exp \beta \theta(s_k) \rangle_1}{\langle \exp \beta \theta(s_k) \rangle_1}$$

where  $\langle \cdot \rangle_1$  denotes Gibbs relative to the Hamiltonian  $H_{N,M-1}$  of (5.1) (thus the summation is over  $k \leq M - 1$ ). In order to compute expectation of the right hand side of (5.6) (and of the similar quantities required to work with several replicas) one first integrates in  $\xi^k = (\xi_i^k)_{i \leq N}$ . To do this one shows first that we can replace the  $\xi_i^k$  by i.i.d.  $N(0, 1)$  variables. One then uses a decomposition of the type (3.8), where now  $Z = \langle \exp \beta \theta(s_k) \rangle_1$  and where  $\hat{Z}$  (motivated by (2.9)) is

$$\hat{Z} = E_g \exp \beta \theta(\xi^k \cdot \mathbf{b} + g \sqrt{1 - \|\mathbf{b}\|^2})$$

for  $\mathbf{b} = (\langle \sigma_i \rangle_1 / \sqrt{N})_{i \leq N}$ . In these computations, we are not dealing with explicit functions (and thus cannot make explicit computations); instead we obtain estimates through comparison theorems for Gaussian processes.

### 6. THE RANDOM $p$ -SAT PROBLEM

Consider independent Boolean variables  $x_1, \dots, x_N$ . A  $p$ -clause is a Boolean function  $y_{i_1} \vee y_{i_2} \vee \dots \vee y_{i_p}$  where  $i_1 < \dots < i_p$ , and where, for each  $\ell \leq p$ , either  $y_{i_\ell} = x_{i_\ell}$  or  $y_{i_\ell} = \bar{x}_{i_\ell}$ . Thus there is exactly one truth assignment of the variables  $(x_{i_\ell})_{\ell \leq p}$  that does not satisfy the clause. Given  $M$  clauses, the satisfiability problem is the question of whether or not there is a truth assignment of the variables that satisfies them all. It is a fundamental problem of computer science. In the

random model of the  $p$ -sat problem the set of  $M$  clauses is chosen independently uniformly among all sets of  $Mp$ -clauses. The question is then to decide whether in the typical case these  $M$  random clauses can be simultaneously satisfied, and, more generally, what is the typical proportion of truth assignments that will satisfy them all. To see the relation with previous sections, we replace “true” by 1 and “false” by  $-1$ . We denote by  $[N]^p$  the collection of subsets of  $\{1, \dots, N\}$  of cardinal  $p$ . Given  $I \in [N]^p$  and  $\rho \in \Sigma_N$ , we consider the set

$$(6.1) \quad A_{I,\rho} = \{\sigma \in \Sigma_N; \exists i \in I, \sigma_i \neq \rho_i\}$$

and the problem is now to find the typical proportion of configurations that belong to  $M$  random sets  $A_{I,\rho}$ . This problem is formally very close to the perceptron capacity problem of Section 6. The big difference is that the random sets depend only upon finitely many coordinates; but as previously the important case is when  $M = \lfloor \alpha N \rfloor$ .

In order to introduce a temperature, we consider (following [M-Z]) the Hamiltonian

$$(6.2) \quad H_N(\sigma) = - \sum_{k \leq M} 1_{\{\sigma \in A_k\}}$$

where  $A_k, k = 1, \dots, M$  are  $M$  sets of the type (6.1) chosen uniformly among all possibilities.

In order not to be hypnotized by the specific form of (6.2), we consider a more general setting, as follows. Consider a function  $f : [0, 1] \times \{-1, 1\}^p \rightarrow [-1, 1]$ . For each set  $I \in [N]^p$  consider the random function  $f_I(\sigma) = f(X_I, \sigma_{i_1}, \dots, \sigma_{i_p})$  where  $I = \{i_1 < \dots < i_p\}$  and where the collection  $(X_I)_{I \in [N]^p}$  is independently uniform over  $[0, 1]$ . We then consider the more general form of (6.2)

$$(6.3) \quad H_N(\sigma) = - \sum_{k \leq M} f_{I_k}(\sigma)$$

and the corresponding random Gibbs measure  $G_N$  on  $\Sigma_N$ . The expected number of intervals  $I_k$  that contain  $N$  is  $pM/N$ , so that the conditional distribution of  $\sigma_N$  (for Gibbs’ measure) given  $\sigma_1, \dots, \sigma_{N-1}$  depends of  $(\sigma_1, \dots, \sigma_{N-1})$  through only finitely many components, a fact that is expressed in physics by saying that the  $N^{\text{th}}$  site interacts with finitely many other sites. We cannot expect the central limit theorem to come into effect, and the gaussian r.v. that were ubiquitous in the previous sections will not appear here. This makes the situation more complicated. The formal computations of the physicists that lead then to (e.g.) (4.15) make it natural for them to think of the Hopfield model as depending upon these parameters  $(\mu, q, r)$ , that are determined by the relations (4.6) to (4.8). They say that the system “depends on the order parameters  $\mu, q, r$ ”. The situation is more complex here, and the central object is the limiting distribution of  $\langle \sigma_1 \rangle$ , a fact expressed in physics by saying that “the order parameter of the system is a function”. (In that case the replica formalism involves yet another arbitrary step. Namely, one has to look for the extremum of a certain functional over a very large function space, and one restricts a priori the search to a more manageable very small subspace.)



**THEOREM 6.1.** *Given the integer  $p$ , and  $\alpha > 0$ , there exists a number  $\beta(p, \alpha) > 0$  with the following property. Whenever  $\beta < \beta(p, \alpha)$ , the system governed by (6.3) at inverse temperature  $\beta$  is in a pure state. Given any  $n$ , the r.v.  $\langle \sigma_1 \rangle, \dots, \langle \sigma_n \rangle$  are asymptotically identically distributed and the expected free energy density converges as  $N \rightarrow \infty$ .*

The limit law  $\nu = \nu(f, \beta, \alpha)$  of  $\langle \sigma_1 \rangle$  appears as the fixed point of a certain operator (in the spirit of the previous sections). The limiting expected free energy density can be in principle computed in function of  $\nu$  (see [M-Z] for a rather formal expression, obtained through the replica formalism, in the case of (6.2)).

To prove Theorem 6.1, the main difficulty is to prove the conditions of Theorem 2.1. The positivity argument is very precious here because, if one tries an approach along the lines of (3.8), the natural candidate for  $\hat{Z}$  is complicated enough so that it is not clear how to estimate simply  $EU/\hat{Z}$ . The statement about the limiting behavior of  $\langle \sigma_1 \rangle, \dots, \langle \sigma_n \rangle$ , which, as we explained, is an essentially obvious consequence of the conditions of Theorem 1.2 in the previous examples lies somewhat deeper here. The basic idea is however simple. The last spin  $\sigma_N$  interacts with only finitely many other spins. Each of these in turn interacts only with finitely many other spins, etc. The key point is that the (global) influence upon  $\sigma_N$  of the finitely many spins obtained at the  $k$ -stage decreases with  $k$ , so that the behavior of  $\sigma_N$  is essentially controlled by a finite set of other spins. When applying the same principle to  $\sigma_{N-1}$ , another finite set of spins is involved, that is generically disjoint of the previous one, and this creates independence. The reader has noticed that the role of  $\alpha$  and  $\beta$  are reversed in Theorem 6.1 compared to Theorem 5.1. It is true that given  $f, \beta$ , the conclusion of Theorem 6.1 does hold for small  $\alpha$ , but for uninteresting reasons. In fact if  $\alpha(p-1) < 1$ , with high probability the interactions “die out” and the set  $\{1, \dots, N\}$  decomposes in small pieces that do not interact with each other.

We have given Theorem 6.1 as an illustration of the fact that even the case of “functional order parameter” is amenable to rigorous results because it relates to a known famous problem. There are, however, simpler situations of the same nature. One of them is the diluted SK model, where the Hamiltonian (1.3) is replaced by

$$(6.4) \quad H_N(\boldsymbol{\sigma}) = - \sum_{i < j} \eta_{ij} g_{ij} \sigma_i \sigma_j - h \sum_{i < j} \sigma_i.$$

There, the r.v.  $\eta_{ij}$  are independent among themselves and of the  $g_{ij}$ , and satisfy  $P(\eta_{ij} = 1) = \gamma/N$ ,  $P(\eta_{ij} = 0) = 1 - \gamma/N$  so that each spin interacts with an average number of  $\gamma$  other spins. A result similar to Theorem 6.1 can be proved at high temperature. The proof is much easier because (2.2) can be obtained through an immediate adaptation of the argument we outlined in Section 3.

## 7. THE $p$ -SPIN INTERACTION MODEL: LOW TEMPERATURE

The  $p$ -spin model is a generalization of the SK model. If  $p$  is an integer  $\geq 2$ , the

Hamiltonian is

$$(7.1) \quad H(\boldsymbol{\sigma}) = -\left(\frac{p!}{2N^{p-1}}\right)^{1/2} \sum_{1 \leq i_1 < \dots < i_p \leq N} g_{i_1 \dots i_p} \sigma_{i_1} \dots \sigma_{i_p}.$$

The summation is over all possible choices of  $i_1, \dots, i_p$  and the  $g_{i_1 \dots i_p}$  are i.i.d. standard normal. A basic observation is that (neglecting terms of order one)

$$(7.2) \quad 2EH(\boldsymbol{\sigma})H(\boldsymbol{\sigma}') = \frac{p!}{N^{p-1}} \sum_{i_1 < \dots < i_p} \sigma_{i_1} \dots \sigma_{i_p} \sigma'_{i_1} \dots \sigma'_{i_p} \simeq N\left(\frac{\boldsymbol{\sigma} \cdot \boldsymbol{\sigma}'}{N}\right)^p.$$

Thus the complicated covariance structure of the gaussian variables  $(H(\boldsymbol{\sigma}))_{\boldsymbol{\sigma}}$  (that is responsible for the difficulty of the problem) simplifies as  $p \rightarrow \infty$  and the r.v.  $(H(\boldsymbol{\sigma}))_{\boldsymbol{\sigma}}$  become independent, a situation that can be analyzed in great detail [D]. We are however not interested in having  $N$  fixed,  $p \rightarrow \infty$ , but rather  $p$  fixed,  $N \rightarrow \infty$ . Still, (7.2) indicates that the larger  $p$ , the easier the model should be. Physics predicts that for low (but not too low) temperature, the behavior of the model is non trivial, yet much simpler than the conjectured behavior of the SK model [G-M], [G1]. The different behavior starts at  $p = 3$  for reasons that will soon be obvious.

The basic idea to obtain information about the low temperature region is to use the “transfer principle” outlined in Section 3. This principle allows only a small change of inverse temperature, so that in order to reach the low temperature region we must first be able to control most of the high temperature region, which we know best how to do when there is no external field (our results can be extended to small external field, say  $h$  of order  $2^{-p}$ , but we do not see how to handle the case where  $h$  is not small, say,  $h = 1$ ). But what is the high temperature region? Let us define the critical number  $\beta_p$  as the supremum of the numbers  $\beta$  for which

$$(7.3) \quad \lim_{N \rightarrow \infty} \frac{1}{N} E \log Z_N = \lim_{N \rightarrow \infty} \frac{1}{N} \log EZ_N (= \frac{\beta^2}{4}).$$

We do not know the exact value of  $\beta_p$  if  $p > 2$ , but we proved that  $2\sqrt{\log 2} - 2^{-p} < \beta_p < 2\sqrt{\log 2}$  for large  $p$ . To obtain information about the range of the overlaps at high temperature, the idea is as follows. We write, for an interval  $I$ ,

$$G_N^2(\{(\boldsymbol{\sigma}^1, \boldsymbol{\sigma}^2); \boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2 / N \in I\}) = Z_N^{-2} \sum_{\boldsymbol{\sigma}^1, \boldsymbol{\sigma}^2} \exp -\beta(H_N(\boldsymbol{\sigma}^1) + H_N(\boldsymbol{\sigma}^2))$$

where the summation is over  $\boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2 / N \in I$ . We control  $EZ_N$  from (6.3), and we use that from general principles (concentration of measure [I-S-T])  $Z_N$  is very close from its expectation so that it can be controlled from below. To control the summation from above, we then estimate

$$E \sum \exp -\beta(H(\boldsymbol{\sigma}^1) + H(\boldsymbol{\sigma}^2)) = \sum \exp \frac{\beta^2}{2} E(H(\boldsymbol{\sigma}^1) + H(\boldsymbol{\sigma}^2))^2$$

using (7.2), where now appears the importance of the exponent  $p$ , contrasted with the fact that the proportion of configurations  $\boldsymbol{\sigma}^1, \boldsymbol{\sigma}^2$  for which  $\boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2 = Nt$  is about  $\exp -Nt^2/2$ . (In practice some technicalities like truncation are required). To avoid complications, let us give a typical result (which is not the best we can prove).

**THEOREM 7.1.** *There exists a number  $L$  with the following property. If  $p \geq L$ ,  $x \leq 1/L$  and if  $\beta \leq \beta_p + x/L$ , then the overlap of two replicas essentially never belongs to the set  $J \cup -J$  where  $J = [x, 1 - (x + 2^{-p/L})]$ .*

There (and below) “essentially never belongs” means

$$EG_N^2(\{\boldsymbol{\sigma}^1, \boldsymbol{\sigma}^2; \boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2/N \in J \cup -J\}) \leq \exp -N/K$$

where  $K$  does not depend upon  $N$ .

Let us now consider a probability  $\nu$  on the sphere  $S_N$  of  $\mathbb{R}^N$  of radius  $\sqrt{N}$  (so that  $\Sigma_N \subset S_N$ ) such that the overlap  $\boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2/N$  of two independent configurations belong to  $J \cup -J$  only with very small probability where  $J$  is, say, the interval  $[.01, .99]$ . (Thus, for  $p$  large enough and  $\beta \leq \beta_p + 1/L$ ,  $G_N$  has this property with overwhelming probability). Then it is intuitively clear, and easy to prove, that almost all the mass  $\nu$  must be carried by a union  $\bigcup_{\alpha \geq 1} C_\alpha$  of sets  $C_\alpha$  such that each

$C_\alpha$  is the union of two opposite small caps. The decomposition is finite ( $C_\alpha = \emptyset$  for  $\alpha$  large enough). It is such that when  $\boldsymbol{\sigma}$  and  $\boldsymbol{\sigma}'$  belong to two different sets  $C_\alpha$ , then  $|\boldsymbol{\sigma} \cdot \boldsymbol{\sigma}'/N|$  is small (say,  $\leq 1/10$ ). The fact that  $C_\alpha$  has to be the union of two pieces is clear when  $\nu$  is invariant by symmetry about zero, as is the case for Gibbs measure when  $p$  is even. Moreover, the decomposition is essentially unique “within sets of small measure”.

Thus, Theorem 7.1 proves that if  $\beta \leq \beta_p + \beta_0$  (where  $\beta_0$  is a fixed number) and  $p$  is large enough, the Gibbs measure is supported by a union of small sets  $(C_\alpha)_{\alpha \geq 1}$  that are far apart. The remarkable feature here is that this decomposition is **not** (in contrast with the case of the Hopfield model) apparent from the form of the Hamiltonian. We will call the sets  $C_\alpha$  the *lumps*, to avoid the overused word “state”. (We will consider later the question of whether they are “pure states”.)

**THEOREM 7.2.** *There exists a number  $L$  such that if  $p \geq L$  and  $\beta \leq \beta_p + 1/L$ , then*

$$\lim_{N \rightarrow \infty} E \left\langle \left( \frac{\boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2}{N} \right)^2 1_{\{|\boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2| \leq N/2\}} \right\rangle \rightarrow 0.$$

This means that two configurations in different lumps have generically a zero overlap, so that the lumps are as far from each other as they can possibly be. They are also small, since  $\boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2/N$  is close to 1 for  $\boldsymbol{\sigma}^1, \boldsymbol{\sigma}^2$  in the same lump, so they are well separated from each other, which of course greatly helped us to construct them. Theorem 7.2 is proved by the cavity method; due to the restriction to integration over the region where overlaps are  $\leq 1/2$ , it does not seem possible to use a positivity argument, but here again gaussian processes are very useful.

Let us now denote by  $w_\alpha$  the weight  $G_N(C_\alpha)$  of lump  $\alpha$ , and assume that the numbering is such that  $w_1 \geq w_2 \geq \dots$ . The random sequence  $(w_\alpha)_{\alpha \geq 1}$  is obviously crucial for the understanding of the model; it is unfortunately not easy to obtain information about it. From Theorem 7.2, we have

$$E \left\langle \left( \frac{\boldsymbol{\sigma}^1 \cdot \boldsymbol{\sigma}^2}{N} \right)^p \right\rangle \leq \sum w_\alpha^2 + o(1)$$

where  $o(1) \rightarrow 0$  as  $N \rightarrow \infty$ .

Combining with the relation

$$E \frac{1}{N} \frac{\partial}{\partial \beta} \log Z_N = \frac{\beta}{2} (1 - \langle (\frac{\sigma^1 \cdot \sigma^2}{N})^p \rangle)$$

(that is obtained as the first equality of (3.7)) one can prove that for  $\beta > 2\sqrt{\log 2}$  and large  $N$  we have  $E \sum w_\alpha^2 > \epsilon(p) > 0$  where  $\epsilon(p)$  does not depend upon  $N$ . (This ought to be true for all  $\beta > \beta_p$  but we do not know how to show this. Note however that the restriction  $\beta \leq \beta_p + 1/L$  does allow values of  $\beta > 2\sqrt{\log 2}$ ). The condition  $E \sum w_\alpha^2 > \epsilon(p)$ , together with  $\sum w_\alpha = 1$ , shows that at least some of the weights  $w_\alpha$  are “macroscopic”, i.e. of order 1.

The distribution predicted (and reinvented) by the physicists for the weights ( $w_\alpha$ ) is of interest (see [P-Y] for a modern view and earlier references). Consider a number  $m \in (0, 1)$  and a Poisson point process on  $\mathbb{R}^+$  such that its intensity measure has density  $mx^{-m-1}$  with respect to Lebesgue measure. Consider a realization  $(x_\alpha)_{\alpha \geq 1}$  of this process. Then  $S = \sum x_\beta < \infty$  a.s, and it is believed that as  $N \rightarrow \infty$ , the distribution of the weights  $w_\alpha$  converges to the distribution of  $v_\alpha = x_\alpha/S$ , where the parameter  $m = m(p, \beta)$  is such that  $(1 - m)$  is about  $(\beta - \beta_p)/\beta_p$  for  $\beta - \beta_p$  small and  $p$  large. There would be some hope to prove this conjecture [A-C2] if we knew that the distribution of the weights  $w_\alpha$  has a limit as  $N \rightarrow \infty$ ; but, unfortunately, the best argument to date towards the existence of such a limit seems to be that there is no reason why it should not exist!

In this situation, it makes sense to try to go forward and examine the fundamental question of whether the lumps are “pure states” by assuming as weak as possible unproven properties of the weight distribution. One particularly useful such condition is as follows.

(H) There exists  $\delta > 0, p_0 > 0$  such that, if  $p \geq p_0$ , we have for each  $\epsilon > 0$

$$\limsup_{N \rightarrow \infty} P\left(\sum_{\alpha \leq 200} w_\alpha \geq 1 - \epsilon\right) \leq \epsilon^\delta.$$

The number 200 is of course somewhat arbitrary. This condition simply means that it is rare that a few weights carry almost all the mass, and is (of course) satisfied by the conjectured distribution. To simplify the statement of the following result, we consider only the case  $p$  even.

**THEOREM 7.3.** (informal version). *There exists a constant  $L$  with the following property. If (H) is true, then for  $p$  large enough, and  $\beta \leq \beta_p + 1/pL$ , the lumps ( $C_\alpha$ ) are in the limit the union of two pure states related by a global symmetry around zero.*

Thus, we will have  $C_\alpha = \Sigma_\alpha \cup (-\Sigma_\alpha)$ , where  $\Sigma_\alpha$  is a “pure state”. A physicist would define a pure state by saying that the overlap of two independent configurations belonging to  $\Sigma_\alpha$  are generically constant (which is a way to express that (2.2) holds for the restriction of  $G_N$  to  $\Sigma_\alpha$ ). How to express this mathematically is a bit more tricky. One way to do this is to introduce the quantity

$$(7.4) \quad E_N = E\langle (N^{-1}(\sigma^1 - \sigma^2) \cdot (\sigma^3 - \sigma^4))^2 1_A \rangle$$

where  $A = \{\sigma^1, \sigma^2, \sigma^3, \sigma^4, \forall i, j \leq 4, \sigma^i \cdot \sigma^j \geq N/2\}$ . Restricting the thermal integral to  $A$  essentially means that we force  $\sigma^1, \sigma^2, \sigma^3, \sigma^4$  to belong simultaneously to a set of the type  $\Sigma_\alpha$  or to a set of the type  $-\Sigma_\alpha$ . The final statement of Theorem 7.3 is that  $\lim_{N \rightarrow \infty} E_N = 0$ , which essentially means that “(2.3) holds in each  $\Sigma_\alpha$ ”. The proof again relies upon relating  $E_N$  and  $E_{N-1}$  via the cavity method.

Thus Theorem 7.3 asserts that if  $\sigma^1, \sigma^2 \in \Sigma_\alpha$  then (generically)  $\sigma^1 \cdot \sigma^2 = \pm Nq_\alpha$ , where  $q_\alpha$  is a certain (possibly random) quantity depending possibly upon  $\alpha$ . Physicists believe that for each  $\alpha, q_\alpha = q$ , where  $q$  is non random; but it unfortunately seems to be difficult to gather evidence in this direction unless one has a much better control of the weights distribution.

## REFERENCES

- [A-C1] M. Aizenman, P. Contucci, *On the stability of the quenched state in Mean Field Spin Glass Models*, Manuscript, 1997.
- [AC2] ———, *The Indy 500 model*, Manuscript, 1998.
- [A-L-R] M. Aizenman, J. L. Lebowitz, D. Ruelle, *Some rigorous results on the Sherrington-Kirkpatrick model*, Commun Math. Phys., 112 (1987), 3-20.
- [A-W] M. Aizenman, J. Wehr, *Rounding effects of quenched randomness of first-order phase transitions*, Commun. Math. Phys. 130, 1990, 485-528.
- [A-G-S] D.J. Amit, H. Gutfreund, H.Sompolinsky, *Statistical Mechanics of Neural Networks near Saturation*, Annals of Physics 173, 1987, 30-67.
- [A-T] J. R. L. Almeida, D. T. Thouless, *Stability of the Sherrington-Kirkpatrick solution of a spin glass model*, J. Phys. A: Math, Gen., II (1978), 983-990.
- [B] A. Bovier, *Comment on “Capacity of Hopfield model”*, J. Phys. A 30, 1997, 7993-7996.
- [B-G1] A. Bovier, V. Gayrard, *The retrieval phase of the Hopfield Model*, Prob. Theor. Relat. Fields 107, 1997, 61-98.
- [B-G2] ———, *An almost sure large deviation principle for the Hopfield model*, Ann. Probab. 24, 1996, 1444-1475.
- [B-G3] ———, *Hopfield models as generalized random mean field models*, Mathematical aspects of spin glasses and neural networks, A. Bovier and P. Picco editors, Progress in Probability, Vol 41, Birkäuser, Boston, 1997..
- [B-G4] ———, *An almost sure central limit theorem for the Hopfield model*, Markov Proc. Rel. Fields 3, 1997, 151-173.
- [B-G-P1] A. Bovier, V. Gayrard, P. Picco, *Gibbs states for the Hopfield model in the regime of perfect memory*, Prob. Theory. Relat. Fields 100, 1994, 329-363.
- [B-G-P2] ———, *Gibbs states of the Hopfield model with extensively many patterns*, J. Stat. Phys. 79, 1995, 395-414.
- [B-P] A. Bovier, P. Picco (editors), *Mathematical aspects of Spin Glasses and Neural Networks*, Progress in Probability, Vol. 41, Birkhäuser, Boston, 1997.
- [B-S] E. Bolthausen, A. S. Sznitman, *On Ruelle’s probability cascades and an abstract cavity method*, Manuscript, 1997.
- [C] F. Comets, *A spherical bound for the Sherrington-Kirkpatrick model*, in “Hommage à P.-A. Meyer et J. Neveu”, Astérisque 236, 103-108, 1996.
- [C-N] F. Comets, J. Neveu, *Sherrington-Kirkpatrick model of spin glasses and stochastic calculus: the high temperature case*, Commun Math. Phys. 166 (1995), 549-564.
- [C-S] A. Crisanti, H. J. Sommers, *The spherical p-spin interaction spin glass model: the statics*, Z. Phys. B. Condensed Matter 87, 341-354 (1992).
- [D] B. Derrida, *Random energy model: An exactly solvable model of disordered systems*, Phys. Rev. B, 24 # 5, 2613-2626, 1981.

- [D-G] B. Derrida, E. Gardner, *Optimal storage properties of Neural Network models*, J. Phys. A. 21, 271-284, 1988.
- [F] F. Friedgut, *Necessary and sufficient conditions for sharp threshold for graph properties and the  $k$ -sat problem*, Manuscript, 1996.
- [F-Z] J. Fröhlich, B. Zegarlini, *Some comments on the Sherrington-Kirkpatrick model of spin glasses*, Commun. Math. Phys. 112 (1987), 553-566.
- [G1] E. Gardner, *Spin glasses with  $p$ -spin interactions*, Nuclear Phys. B 257, #6, 747-765, 1985.
- [G2] ———, *The space of interactions in neural network models*, J. Phys. A. 21, 257-270, 1988.
- [Gu1] F. Guerra, *Fluctuations and thermo dynamic variables in mean field spin glass models in: Stochastic Processes, Physics and Geometry*, S. Albeverio et. al. editors, World Scientific, Singapore, 1995.
- [Gu2] ———, *About the overlap distribution in mean field spin glass models*, Int. J. Modern Physics B, 1996, 1675-1684.
- [G-M] D. Gross, M. Mézard, *The simplest spin glass*, Nuclear Phys. B 240, [F 512], 1984, 431-452.
- [H1] J. J. Hopfield, *Neural networks and physical systems with emergent collective computational abilities*, Proc. Natl. Acad. Sci. USA 79, 1982, 1554-2558.
- [H2] ———, Proc. Natl. Acad. Sci. USA 81, 1982, 3088.
- [H-K-P] J. Hertz, A. Krogh, R. C. Palmer, *Introduction to the theory of Neural computation*, Addison Wesley, 1991.
- [I-S-T] A. Ibragimov, V. N. Sudakov, B.S. Tsirelson, *Norms of Gaussian sample functions*, Proceedings of the Third Japan USSR Symposium on Probability theory, Lecture Notes in Math 550, Springer Verlag, 20-41, 1976.
- [K-M] Krauth W. and Mézard M., *Storage capacity of memory network with binary couplings*, J. Phys. 50, 1989, 3057-3066.
- [K-R] Kim J.H., Roche J.R., *On the Optimal Capacity of Binary Neural Networks: Rigorous Combinatorial approaches*, Preprint, 1996.
- [L-T] M. Ledoux, M. Talagrand, *Probability in a Banach Space*, Springer-Verlag, 1991.
- [Lou1] D. Loukianova, *Capacité de mémoire dans le modèle de Hopfield*, C. R. Acad. Sci. Paris 318, Serie I, 1994, 157-160.
- [Lou2] D. Loukianova, *Lower bounds on the restitution error of the Hopfield model*, Probab. Th. Relat. Fields 107, 1997, 161-176.
- [M] M. Mézard, *The space of interactions in neural networks: Gardner's computation with the cavity method*, J. Phys. A. 22, 2181-2190, 1988.
- [M-P-V] M. Mézard, G. Parisi, M. Virasiro, *Spin glass theory and beyond*, World Scientific, Singapore, 1987.
- [M-Z] R. Monasson, R. Zecchina, *Statistical Mechanics of the Random  $K$ -Sat Model*, Phys. Rev. E, 1997, 1357-1370.
- [N] C. Newman, *Memory capacity in neural network models: Rigorous lower bounds*, Neural Networks I, 1988, 223-238.
- [N-S1] C. Newman, D. Stein, *Chaotic size dependence in spin glasses. Cellular automata and cooperative systems*, (Les Houches, 1992), 525-529, NATO. Adv. Sci. Inst. Ser. C Math. Phys. Sci., 396, Kluwer Acad. Publ. Dordrecht, 1993.
- [N-S2] ———, *Non-mean-field behavior of realistic spin glasses*, Phys. Rev. Letters 76, 1997, 515-518.
- [N-S3] ———, *Spatial inhomogeneity and thermodynamic chaos*, Phys. Rev. Letters 76, 1997, 4821-4824.
- [N-S4] ———, *Thermodynamic chaos and the structure of short-range spin glasses*, *Mathematical aspects of Spin Glasses and Neural networks*, A. Bovier and P. Picco editors, Progress in Probability Vol. 41, Birkhäuser, Boston, 1998, 243-287.
- [P-F1] L. Pastur, A. Figotin, *Exactly soluble model of a spin glass*, Sov. J. Low Temp. Phys. 3, 1977, 378-383.

- [P-F2] ———, *On the theory of disordered spin systems*, Theor. Math. Phys. 35, 1978, 403-414.
- [P-S] L. Pastur, M. Shcherbina, *Absence of Self-Averaging of the order parameter in the Sherrington-Kirkpatrick model*, J. Stat. Phys. 62 (1991), 1-19.
- [Pe1] D. Petritris, *Thermodynamic formalism of Neural computing*, Dynamics of Complex interacting systems (Santiago, 1994), 81-146, Nonlinear Phenom. Complex Systems, 2, Kluwer Acad. Publ.
- [Pe2] ———, *Equilibrium statistical mechanics of frustrated spin glasses: a survey of mathematical results*, Am. Inst. H. Poincaré Phys. Théor. 64, 1996, 255-288.
- [Pi] J. Pitman, *Coalescents with multiple collisions*, Manuscript, 1997.
- [P-Y] J. Pitman, M. Yor, *The two-parameter Poisson-Dirichlet distribution derived from a stable subordinator*, Ann. Probab. 25, 1997, 855-900.
- [R] D. Ruelle, *A mathematical reformulation of Derrida's REM and GREM*, Comm. Math. Phys. 108, 1987, 225-239.
- [Sh1] M. Shcherbina, *More about Absence of Self averages of the order parameter in the Sherrington-Kirkpatrick Model*, CARR Reports in Mathematical Physics, no 3/91, Department of Mathematics, University of Rome "la Sapienza", 1991.
- [Sh2] ———, *On the Replica-Symmetric Solution for the Sherrington-Kirkpatrick Model*, Helv. Phys. Acta. 70, 1997, 838-853.
- [S-K] D. Sherrington, S. Kirkpatrick, *Solvable model of a spin glass*, Phys. Rev. Lett. 35, 1972, 1792-1796.
- [T1] M. Talagrand, *Regularity of Gaussian processes*, Acta. Math. 159, 1987, 99-149.
- [T2] ———, *Concentration of measure and isoperimetric inequalities in product spaces*, Publ. Math. I.H.E.S. 81, 1995, 73-205.
- [T3] ———, *Rigorous results for the Hopfield model*, C. R. A. S. 321, 1995, 109-112.
- [T4] ———, *A New look at independence*, Ann. Probab. 24, 1996, 1-34.
- [T5] ———, *The Sherrington-Kirkpatrick model: a challenge to mathematicians*, Prob. Th. Relat. Fields 110, 1998, 109-176.
- [T6] ———, *Rigorous results for the Hopfield model with many patterns*, Prob. Th. Relat. Fields 110, 1998, 177-276.
- [T7] ———, *Rigorous low temperature results for the p-spin interaction model*, Manuscript, 1997.
- [T8] ———, *The high temperature case of the K-sat problem*, Manuscript, 1998.
- [T9] ———, *Self averaging and the space of interactions in neural networks*, Manuscript, 1998.
- [T10] ———, *Exponential inequalities and replica-symmetry breaking for the Sherrington-Kirkpatrick model*, Manuscript, 1998.
- [T11] ———, *Exponential inequalities and convergence of moments in the replica-symmetric regime of the Hopfield model*, Manuscript, 1998.
- [T12] ———, *Intersecting random half spaces and the Perception capacity formula*, Manuscript, 1998.
- [T13] ———, *Intersecting random half cubes*, Manuscript, 1998.
- [To] G. Toulouse, *Frustration and disorder, new problems in statistical mechanics, spin glasses in a historical perspective*, Heidelberg Colloquium on Spin Glasses, J. L. van Hemmen and I. Morgenstern eds., Lecture Notes in Physics 192, Springer Verlag, 1983.
- [T-D-C] G. Toulouse, S. Dehaene and J. P. Changeux, *Spin glass model of learning by selection*, Proc. Natl. Acad. Sci. USA 83, 1986, 1695-1698.

Michel Talagrand  
 Equipe d'Analyse-Tour 46,  
 E.S.A. au C.N.R.S. no. 7064,  
 Université Paris VI  
 Homepage [www.proba.jussieu.fr](http://www.proba.jussieu.fr)

## GEOMETRIC PHYSICS

CUMRUN VAFA

ABSTRACT. Over the past two decades there has been growing interaction between theoretical physics and pure mathematics. Many of these connections have led to profound improvement in our understanding of physics as well as of mathematics. The aim of my talk is to give a non-technical review of some of these developments connected with string theory. The central phenomenon in many of these links involves the notion of *duality*, which in some sense is a non-linear infinite dimensional generalization of the Fourier transform. It suggests that two physical systems with completely different looking properties are nevertheless isomorphic if one takes into account “quantum geometry” on both sides. For many questions one side is simple (quantum geometry is isomorphic to classical one) and the other is hard (quantum geometry deforms the classical one). The equivalence of the systems gives rise to a rich set of mathematical identities. One of the best known examples of duality is known as “mirror symmetry” which relates topologically distinct pairs of Calabi-Yau manifolds and has applications in enumerative geometry. Other examples involve highly non-trivial “S-dualities” which among other things have found application to the study of smooth four manifold invariants. There have also been applications to questions of quantum gravity. In particular certain properties (the area of the horizon) of black hole solutions to Einstein equations have been related to growth of the cohomology of the moduli space of certain minimal submanifolds in a Calabi-Yau threefold. A central theme in applications of dualities is a physical interpretation of singularities of manifolds. The most well known example is the  $A - D - E$  singularities of the  $K3$  manifold which lead to  $A - D - E$  gauge symmetry in the physical setup. The geometry of contracting cycles is a key ingredient in the physical interpretation of singularities. More generally, singularities of manifolds encode universality classes of quantum field theories. This leads not only to a deeper understanding of the singularities of manifolds but can also be used to “geometrically engineer” new quantum field theories for physics.



## 1. INTRODUCTION

The history of physics and mathematics is greatly interconnected. Sometimes new mathematics gets developed in connection with understanding physical questions (for example the development of Calculus was not independent of the questions raised by classical mechanics). Sometimes new physics gets developed from known mathematics (for example general theory of relativity found its natural setting in the context of Riemannian geometry). I believe we are now witnessing perhaps an unprecedented depth in this interaction between the two disciplines. It is thus a great pleasure to explain some of the recent progress which has been made in our understanding of quantum field theories, string theory and quantum gravity to a mathematical audience. The works I will be explaining here is a result of the work of many physicists and mathematicians.<sup>1</sup>

Many of the key elements in these recent advances have a deep mathematical content. These involve new predictions for answers to some very difficult mathematical questions as well as new interpretations of some old mathematical results. It also sometimes hints at the existence of whole new branches of mathematics which does not exist yet.

In preparing this talk, I have had to make some choices. First of all I have had to decide which topics to cover and which ones to leave out. This has been very difficult because there are many interesting interaction points between theoretical physics and pure mathematics today, and unfortunately I only have a very limited time here. My choice was motivated by the degree of my familiarity with the subject as well as by attempts at trying to give a unified exposition of the seemingly unrelated topics. Secondly I have had to assume a certain level of familiarity of this mathematical audience with physics. This is also unavoidable, if we are to make any connection to interesting new developments. However, I have tried to make this assumption in the weakest possible sense. Thirdly I have chosen a list of questions which I find interesting for physics which I hope the mathematicians will help us solve.

The organization of my talk is as follows: In section 2 I will describe the basic notion of *duality* which is the key notion in recent advances. In sections 3-5 I give examples of dualities. Section 3 is devoted to a review of what mirror symmetry is. Section 4 explains the physical interpretation of singularities of certain manifolds. Section 5 is devoted to the notion of black hole entropy and what duality predicts about that. Section 6 is devoted to a list of questions which I raise in connection with the topics discussed.

## 2. WHAT IS MEANT BY DUALITY?

I will try to define a very general notion of duality first, a priori nothing to do with physics, and then try to be a little more particular in what it means in the physical context.

---

<sup>1</sup> I will not make any attempts to present a complete list of references to all the relevant literature, though some illustrative references, in the spirit of the presentation here will be given.

Suppose we have two classes of objects. Moreover suppose these two objects satisfy identical properties. Then in a mathematical context they usually will be called *isomorphic*. Very often this is a trivial isomorphism. For example if a property of geometry on a 2 dimensional plane is true, it will also be true for the mirror reflection of the same geometry (Fig. 1).

FIG.1: Reflection on the plane is an example of a “trivial” duality.

However there are times where the fact that the objects and operations are isomorphic is less trivial, because the maps between these two classes of objects is not so trivial. As an example, suppose we wish to solve a linear differential equation of the form

$$F = \sum_k a_k \frac{d^k}{dx^k} \psi(x) = 0$$

with constant coefficients  $a_k$ . Consider instead the *polynomial* equation in one variable  $p$ :

$$G = \sum a_k (ip)^k = 0$$

Apriori the two problems seem unrelated. In fact the second problem on the face of it sounds much simpler. However, as is well known the two problems are related by Fourier transform, and the general solution to the first problem is given by

$$\psi(x) = \int dp \phi(p) \exp(ipx) \delta(G(p))$$

This isomorphism of functions in  $x$  and functions in  $p$  with the map between them being Fourier transform allows us to solve a ‘hard’ problem in the  $x$  space setup in terms of an easy problem in the  $p$  space setup. Isomorphisms of this type which are *non-trivial* we will call *dualities*. As it is clear from this example dualities will be very useful in solving problems. Dualities very often transform a difficult problem in one setup to an easy problem in the other. In some sense very often the very act of ‘solving’ a non-trivial problem is finding the right ‘dual’ viewpoint.

Now I come to specializing this idea in the context of a physical system. Consider a physical system  $Q$  (which I will not attempt to define). And suppose

this system depends on a number of parameters  $[\lambda_i]$ . Collectively we denote the space of the parameters  $\lambda_i$  by  $\mathcal{M}$  which is usually called the moduli space of the coupling constants of the theory. The parameters  $\lambda_i$  could for example define the geometry of the space the particles propagate in, the charges and masses of particles, etc. Among these parameters there is a parameter  $\lambda_0$  which controls how close the system is to being a classical system (the analog of what we call  $\hbar$  in quantum mechanics). For  $\lambda_0$  near zero we have a classical system and for  $\lambda_0 \geq 1$  quantum effects typically dominate the description of the physical system. Typically physical systems have many observables which we could measure. Let us denote the observables by  $\mathcal{O}_\alpha$ . Then we would be interested in their correlation functions which we denote by<sup>2</sup>

$$\langle \mathcal{O}_{\alpha_1} \dots \mathcal{O}_{\alpha_n} \rangle = f_{\alpha_1 \dots \alpha_n}(\lambda_i)$$

Note that the correlation functions will depend on the parameters defining  $Q$ . The totality of such observables and their correlation functions determine a physical system. Two physical systems  $Q[\mathcal{M}, \mathcal{O}_\alpha], \tilde{Q}[\tilde{\mathcal{M}}, \tilde{\mathcal{O}}_\alpha]$  are dual to one another if there is an isomorphism between  $\mathcal{M}$  and  $\tilde{\mathcal{M}}$  and  $\mathcal{O} \leftrightarrow \tilde{\mathcal{O}}$  respecting all the correlation functions. Sometimes this isomorphism is trivial and in some cases it is not. We are interested in the cases where this isomorphism is non-trivial. In such cases typically what happens is that a parameter which controls quantum corrections  $\lambda_0$  on one side gets transformed to a parameter  $\tilde{\lambda}_k$  with  $k \neq 0$  describing some classical aspects of the dual side. This in particular implies that quantum corrections on one side has the interpretation on the dual side as to how correlations vary with some classical concept such as geometry. This allows one to solve difficult questions involved in quantum corrections in one theory in terms of simple geometrical concepts on the dual theory. This is the power of duality in the physical setup. Mathematics parallels the physics in that it turns out that the mathematical questions involved in computing quantum corrections in certain cases is also very difficult and the questions involved on the dual side are mathematically simple. Thus non-trivial duality statements often lead to methods of solving certain difficult mathematical problems.

One should note, however, that very rarely can one actually *prove* (even in the physics sense of this word) that two given physical systems are dual to one another. Often the existence of dualities between two systems is guessed at based on some physical consistency arguments. Testing many non-trivial consequences of duality conjectures leads us to believe in their validity. In fact we have observed that duality occurs very generically, for reasons we do not fully understand. This lack of deep understanding of duality is not unrelated to the fact that it leads to solutions of otherwise very difficult problems. At the mathematical level, evidence for duality conjectures amounts to checking validity of proposed solutions to certain difficult mathematical problems.

---

<sup>2</sup> One could attempt to define a physical system by an infinite dimensional bundle over  $\mathcal{M}$  where the fiber space is identified with the space of observables  $\mathcal{O}_\alpha$ , together with a rank  $n$  multi-linear map from the fiber to  $C$ , for each  $n$ , satisfying some compatibility conditions.

In the next three sections I will consider examples of duality and some of its mathematical consequences. In section 3 we will start with the best understood duality known as mirror symmetry, which relates string theory on one target manifold with another. In section 4 we discuss how singularities of the geometry get related to gauge bundles for the dual theory. In section 5 we discuss a dual description of black hole geometry which is intimately related to properties of minimal submanifolds in Calabi-Yau manifolds.

### 3. MIRROR SYMMETRY

String theory, which is the only known consistent framework for a quantum theory of gravity, involves the study of quantum properties of one dimensional extended objects. The spacetime picture corresponds to a two dimensional Riemann surface  $\Sigma$  mapped to a target spacetime Riemannian manifold  $M$ . The sliced Riemann surfaces give the picture of strings propagating in time (Fig. 2).

FIG.2: Strings propagating in spacetime span a Riemann surface known as the worldsheet.

In string theory we are instructed to “sum” over all such maps

$$\phi : \quad \Sigma \rightarrow M$$

weighted with  $\exp(-S(\phi))$  where  $S(\phi)$  denotes the integral

$$S(\phi) = \int_{\Sigma} |d\phi|^2$$

where we use the metric on  $M$  to define  $|d\phi|^2$ . (For superstrings which is the case of most interest, there are also some fermionic fields, which I suppress in this discussion.)

One of the most amazing properties of string theory is that strings moving on one manifold may behave identically with strings moving on a different manifold. Any pair of manifolds  $M_1$  and  $M_2$  which behave in this way are called mirror pairs. Of course this would be a trivial duality if  $M_1$  and  $M_2$  are isomorphic Riemannian manifolds. The interesting dualities arise when  $M_1$  and  $M_2$  are distinct

Riemannian manifolds. In some cases  $M_1$  and  $M_2$  are topologically the same, but in some cases they are distinct even topologically. In such cases the equivalence of the two manifolds for string theory will be only a statement about correlation functions after summing over *all* maps  $\phi$ . The act of summing over all maps  $\phi$  is what we mean by the quantum theory. So only in the quantum theory, i.e. after summing over all  $\phi$  the two computations would be related (i.e. we should not try to compare individual maps). The parameter controlling the significance of quantum corrections, for a fixed genus surface  $\Sigma$ , is the volume of  $M$ ,  $V(M)$ . In particular, the parameter we called  $\lambda_0$  in the previous discussion in this case is  $\lambda_0 = 1/V(M)$  (and thus in the large volume limit the quantum corrections are suppressed).

The simplest example of mirror symmetry corresponds to choosing  $M_1$  to be a circle of circumference  $L$  and  $M_2$  to be a circle of circumference  $1/L$ . This is a case of mirror symmetry which can be rigorously proven (see [1] for a review). However here we will just illustrate why such a statement is not unreasonable.

This statement would definitely be unreasonable for point particle theories: If we consider a particle in a circle of size  $L$ , the momentum states are quantized as the allowed wave functions

$$\psi_n(x) = \exp(2\pi i n x / L)$$

compatible with the invariance under  $x \rightarrow x + L$  gives the spectrum of allowed momenta (which for massless particles is the same as energy) to be  $n/L$ , where  $n \in \mathbb{Z}$ . If we consider the circle of circumference  $1/L$  the allowed energies are now  $nL$ . Thus the energy spectrum of the two theories do not match. The story changes dramatically for strings: We will still have the same excitations as in the point particle case, after all the string mapped to a point looks like a point particle. However we have in addition other states corresponding to winding states of the string around the circle. Consider the first circle of circumference  $L$  and assume a string wraps around it  $m$  times, then its energy is  $mL$  (I am working in units where the string tension is one). Now the full spectrum of momentum and winding states does have  $L \rightarrow 1/L$  symmetry where in the process momentum states get exchanged with winding states (Fig. 3).

FIG.3: Momentum modes, with energy  $n/L$  get exchanged with winding modes with energy  $mL$  under mirror symmetry  $L \rightarrow 1/L$ .

There is one context in which a similar duality is already well known mathematically: Consider a  $U(1)$  bundle on a circle. Then the choice of the bundle (i.e. the choice of the holonomy of  $U(1)$  around the circle) is equivalent to the choice of a point on the dual circle. This also turns out to have a very important physical analog [2]. If we consider open strings, in addition to closed strings, we would be considering Riemann surfaces with boundaries. In such a case in addition to specifying the target geometry  $M$  where the closed strings are mapped to, we have to specify where the boundaries are mapped to. In general they could map to some subspaces of  $M$  of various dimensions  $p$ . Such a  $p$ -dimensional subspace of  $M$  is called a  $p$ -brane or  $Dp$ -brane ( $D$  signifying the fact that the maps from the Riemann surface have *Dirichlet* conditions in codimension  $p$ , and “brane” generalizing the terminology of membranes which are 2-branes, to the higher dimensional objects). Moreover it turns out that a  $Dp$ -brane will carry a  $U(1)$  gauge field and so can be viewed as a sheaf in  $M$ . Physically a  $Dp$ -brane corresponds to some charged matter localized in a  $p$ -dimensional subspace of  $M$ . From the string viewpoint D-branes are regions where an open string can end on (Fig. 4).

FIG.4: A  $Dp$  brane is a subspace of the target manifold  $M$  where a string can end on.

Returning to the case of a circle, if we consider a  $D1$  brane which includes the entire circle of circumference  $L$ , we can ask what happens under mirror symmetry to the D-brane. The answer is that it gets transformed to a  $D0$  brane on the mirror. This is in accord with the mathematical fact mentioned before (where the holonomy of a  $U(1)$  bundle gets transformed to the choice of a point on the dual circle). This has also a natural generalization to the case where we consider  $N$   $D1$  branes wrapping the  $S^1$  which in physics leads to a  $U(N)$  bundle on  $S^1$  and choosing a flat  $U(N)$  connection on  $S^1$  amounts to choosing  $N$  points on the dual circle, i.e. it is transformed to  $N$   $D0$  branes on the mirror.

It is natural to ask how mirror symmetry extends in cases where the target manifold is more complicated than  $S^1$ . One simple example consists of taking a  $d$ -dimensional torus  $T^d = (S^1)^d$  and doing inversion on each of the  $S^1$ 's. The action of this on the  $Dp$  branes, viewed as subspaces  $T^p \subset T^d$  is also clear where they get transformed to a dual  $T^{*d-p} \subset T^{*d}$ . However for more interesting examples we need the following idea <sup>3</sup>.

### 1. The Adiabatic Principle

Consider a family of flat  $d$ -dimensional tori  $T^d$  varying slowly, i.e. *adiabatically* over some base space  $B$ . Consider the total space  $M_1$  over  $B$  with  $T^d$  as the fiber. Consider another space consisting of the same base space  $B$ , where over each point we replace the fiber  $T^d$  with the mirror torus where all lengths are inverted. Call the total space  $M_2$ . Then it is natural to believe that the spaces  $M_1$  and  $M_2$  are mirror to one another. However the interesting examples arise when the assumption of adiabaticity is violated over some subspaces of  $B$ . For example the  $T^d$  may degenerate over some loci. If the category of objects we are dealing with is sufficiently nice one may hope that the mirror property will continue to hold. One nice category<sup>4</sup> seems to be when the base  $B$  is also  $d$ -dimensional and the total space is a Calabi-Yau  $d$ -fold (a Kähler manifold of complex dimension  $d$  whose bundle of holomorphic  $d$ -forms is trivial) where the fibers  $T^d$  are viewed as Lagrangian submanifolds relative to the Kähler form. In fact the non-trivial data specifying the geometry of the Calabi-Yau is precisely how the degeneration of  $T^d$  over  $B$  takes place. This construction corresponds to describing a hypersurface in a toric variety, in a degenerate limit. In a singular limit the Calabi-Yau may be viewed as a  $T^d$  fiber space over the base being a boundary of some simplex (in the sense of toric geometry), where  $T^d$  degenerates to  $T^k$  over  $d - k$  dimensional subspaces of  $B$ . The data defining the mirror, after suitably rescaling the metric on  $B$  looks like the dual geometry where the regions where the  $T^d$  shrinks to  $T^k$  is replaced by the dual  $k$ -dimensional subspaces where the  $T^{d-k} \subset T^d$  shrinks and the dual survives, this being consistent with the small/large radius exchange (Fig. 5). This gives what is known as Batyrev's construction of mirror pairs using the toric description.

---

<sup>3</sup> The presentation here of the mirror symmetry for more complicated target spaces does not follow the historical order of its discovery. Mirror symmetry was first conjectured to exist for Calabi-Yau manifolds in [3][4], with the concrete examples being found in [5] followed by a concrete application to counting holomorphic curves in [6]. The construction of mirror pairs was systematized by [7]. The presentation here follows the approach in [8] developed further in [9] which explains the construction of [7] from this viewpoint.

<sup>4</sup> There may well be other categories, such as the category of manifolds of  $Sp(n)$ ,  $Spin(7)$  or  $G_2$  holonomy.

FIG.5: An application of inversion duality of tori when tori are varying leads to an explanation of mirror symmetry in more complicated examples.

2. *Kähler-Complex Deformation Exchange*

It would be nice to examine some of the consequences of the existence of mirror geometries. To get a feeling for this it is useful to start at the level of  $S^1$  fibered trivially over  $B = S^1$ . This is a simple case, as a constant fibration admits the flat metric. Let  $R_f, R_b$  denote the radii of the fiber and a section respectively. Note that the complex structure (shape) of the torus is determined by

$$C = R_b/R_f$$

and its Kähler class (size) is determined by

$$K = R_b R_f$$

Now if we do mirror transform on the fiber  $S^1$  it again leads to a torus. However since  $R_f \rightarrow 1/R_f$  but  $R_b \rightarrow R_b$  the parameters controlling the complex and Kähler deformations get exchanged:

$$C \leftrightarrow K \quad \text{under mirror transform}$$

This turns out to be the general feature of mirror symmetry for Calabi-Yau manifolds, and the Kähler and complex structures always get exchanged. In the case of Calabi-Yau manifold of complex dimension  $d$  the number of complex moduli is determined by  $h^{1,d-1}$  (where  $h^{p,q}$  denotes the dimension of the cohomology of  $p$ -holomorphic and  $q$  anti-holomorphic forms). Thus if  $M$  and  $W$  are mirror Calabi-Yau manifolds we learn in particular that

$$h^{1,1}(M) = h^{1,d-1}(W) \quad h^{1,d-1}(M) = h^{1,1}(W).$$

This in particular implies that the topology of the manifold and the mirror will in general be very different. In fact it turns out that  $h^{p,q}(M) = h^{p,d-q}(W)$  for all  $p, q$ .



Moreover, as mentioned before, the parameter controlling quantum corrections is the Kähler class of the Calabi-Yau, which gets transformed under mirror transform to complex deformation parameter of the mirror. Thus the question of quantum corrections for one manifold get transformed to the question involving the variation of complex structure on the other, which is classical. This leads to some very non-trivial implications of mirror symmetry.

The most concrete prediction this leads to is to the question of counting the “number” of holomorphic curves mapped from a Riemann surface of genus  $g$  to the threefold. For example the intersection numbers of cycles in the Calabi-Yau receives a quantum correction coming from holomorphic curves (recall this is natural from the string theory viewpoint, where the worldsheet is a Riemann surface) (Fig. 6). This “quantum intersection theory” for triple intersections allows, in addition to the classical intersection, the possibility that the three cycles meet a holomorphic curve weighted by the quantum deformation parameter  $q = e^{-A}$  where  $A$  is the area of the holomorphic curve<sup>5</sup>.

FIG.6: Quantum intersection of three cycles  $A, B, C$  in addition to the classical piece has corrections where  $A, B, C$  meet on a holomorphic rational curve.

This very difficult mathematical problem, i.e. counting holomorphic curves in Calabi-Yau manifolds, gets transformed on the mirror to a question involving the variation of Hodge structures (in this case it is the study of how the middle dimensional  $H^{p,d-p}$  cohomology elements vary as we vary the complex structure on the mirror). This is a well studied mathematical subject<sup>6</sup>. The genus 0 version of the prediction has been confirmed recently [11][12]. The higher genus version

---

<sup>5</sup> The fact that classical cohomology ring is deformed by instantons and gives rise to a quantum cohomology ring was pointed out in [3]. The precise definition of this deformation was given in [10].

<sup>6</sup> To be precise, the counting of genus 0 curves gets transformed to this question. The higher genus version gets transformed to a quantum version of variation of Hodge structure known as *Kodaira-Spencer theory of gravity* which is only slightly more complicated.

[13] has not been proven yet (except in some special cases), but there is little doubt that it is generally valid.

### 3. Extension to Bundles

It is clear from the discussion of D-branes in the context of circles that we can extend mirror symmetry to Calabi-Yau manifolds with bundles. In particular let  $c \in \oplus_p H^{p,p}(M)$  denote the chern class of a holomorphic vector bundle on Calabi-Yau manifold  $M$ . Represent this by a collection of Poincaré dual holomorphic cycles. Consider D-branes wrapped over them. This is a D-brane made up of various even dimensional branes. Each  $(p, p)$  cycle projects to a  $p$  real dimensional subspace of  $B$  with typical fiber a  $p$  dimensional subtorus. On the mirror, the  $p$  dimensional subspace of  $T^d$  gets transformed to the dual torus  $T^{d-p}$ . Thus on the mirror Calabi-Yau, the whole bundle represented by the collection of D-branes is mirror to a submanifold  $C$  of real dimension  $d$ .<sup>7</sup> The condition that the original bundle be holomorphic translates to the condition that  $C$  is Lagrangian relative to the Kähler form on the mirror. If we further impose that the original bundle be stable, this translates to the cycle  $C$  being of minimal area. This extension of mirror symmetry to include bundles conjectured in [18] (see also related works [19][20][21][22]) has only recently been made and checks on its prediction are underway. It makes certain predictions for the enumerative geometry of holomorphic maps from Riemann surfaces with boundaries being mapped holomorphically to Calabi-Yau, with boundaries being mapped to Lagrangian cycles on it.<sup>8</sup> For example the Ray-Singer Torsion associated to the bundle  $V$  is transformed to counting holomorphic maps from the annulus to the Calabi-Yau whose boundary is on the mirror minimal cycle.

### 4. PHYSICAL INTERPRETATION OF GEOMETRIC SINGULARITIES

One of the remarkable aspects of string theory is the existence of a few different types of consistent theories (5 in 10 dimensions and one in 11 dimensions) which are dual to one another. This is known as S-duality. For example, Type IIA strings in a 10 dimensional space having a  $K3$  fibration ( $K3$  being a Calabi-Yau manifold of complex dimension 2) is dual to heterotic strings in a space admitting a  $T^4$  fibration. This is very surprising because in particular the two string theories and the two target spaces look very different. Moreover on the heterotic side one has to choose flat bundles of rank 16. Moreover as we change the size of the  $T^4$  and the choice of the flat bundle (and some choice of a constant field belonging to

---

<sup>7</sup> This leads to a new application of mirror symmetry: For example consider a rational elliptic surface inside a 3-fold. Then the study of rank  $N$  stable bundles on it gets transformed to the study of spectral curves on the dual rational elliptic surface (by viewing the bundle as D4 brane wrapped the rational elliptic surface and doing mirror symmetry along  $T^2$  fiber)[14][15]. The Euler class of the moduli space can be computed using mirror symmetry techniques [16] (this prediction has been recently confirmed for the rank 2 case [17]).

<sup>8</sup> For this to make sense beyond Disc one should restrict to the category of stable bundles on one side and minimal Lagrangian submanifolds on the mirror.

$H^2(T^4)$ ) one can get various different gauge groups. For example one can obtain  $SU(N)$ ,  $SO(2N)$  (for small enough  $N$ ) and  $E_{6,7,8}$ . The question is how all this is reflected on the  $K3$  geometry? It is well known that  $K3$  can have singularities corresponding to contracting 2 spheres. Moreover the intersection matrix of the contracting 2 spheres is given by the Cartan matrix of the A-D-E groups. The appearance of the Dynkin structure for the  $K3$  singularities appears mathematically as purely “accidental”. However this accident gets explained in this duality context: One identifies the singular  $K3$  geometries with A-D-E singularities with the points on the heterotic side with enhanced A-D-E gauge symmetry. The physical explanation of enhanced symmetries on the  $K3$  side has to do with the existence of D2 branes, which can wrap around the contracting 2-cycles, and give rise to massless particles. The wrapped D2 branes encode in a beautiful way the connection of the bundle anticipated from the heterotic dual (Fig. 7). Thus the non-abelian enhancement of gauge symmetry on heterotic side is transformed to appearance of geometric singularities on the type IIA side.

FIG. 7: A wrapped D2-brane over a sphere of blown up A-D-E- singularity is the origin of gauge symmetry enhancement when the spheres shrink.

Similar considerations suggest interesting physical interpretations whenever one has geometric singularities. For example if one considers a Calabi-Yau 3-fold, one has sometimes contracting  $S^3$ 's. In this context there are two ways to get rid of the singularity. One either deforms the polynomial equations defining the manifold (which effectively gives a finite size to the contracting  $S^3$ 's) or replaces the singular point by a higher dimensional geometry (in this case  $S^2$ 's) which is known as blowing up the singularities, changing the geometry of the 3-fold in the process. The singular manifold can thus be viewed as belonging to two distinct families of Calabi-Yau manifolds. The physical interpretation of this is that there are two ways to get rid of the extra massless fields, one is by preserving a  $U(1)^k$  gauge symmetry which is called the “Coulomb branch” (corresponding in type IIA string to blowing up  $S^2$ 's) the other is going to the “Higgs branch” (which corresponds to making  $S^3$ 's have finite volume)[23][24].

One can use these ideas to construct the geometric versions of quantum field theories with desired properties. This is called *geometric engineering of quantum*

*field theories.* For example, if we have a shrinking  $CP^1$  in  $K3$  we already mentioned that this gives rise to  $SU(2)$  gauge symmetry. If we fiber this over a complex curve, depending on what curve we choose we get different theories in the 4 left-over dimensions. For example if we consider the simple product with  $T^2$ , then we obtain a theory in four dimensions with  $N = 4$  supersymmetric  $SU(2)$  Yang-Mills theory. Moreover the coupling constant of the gauge theory  $1/g^2$  (which appears in the action in 4 dimensions in the form  $\frac{1}{g^2} Tr F \wedge *F$ ) gets identified with the volume of  $T^2$ . As discussed before string theory has volume inversion symmetry for  $T^2$ . This implies, therefore, that  $N = 4$  Yang-Mills should have  $g \rightarrow 1/g$  inversion symmetry as well. This in fact was anticipated long ago [25]. This duality has interesting consequences for four-manifolds: Consider taking as the four left-over dimensions a smooth four manifold  $K$ . Then the (topological) partition function of  $N = 4$  Yang-Mills is given by

$$F_{G,K}(q) = \sum_{\text{instantons}} q^n \chi(\mathcal{M}_n)$$

where  $q = \exp(-1/g^2)$  and  $\chi(\mathcal{M}_n)$  denotes the Euler characteristic of the moduli space of instantons of gauge group  $G$  (in the case at hand  $G = SU(2)$ ) with instanton number  $n$  on  $K$ . The duality just discussed implies that this is a modular form (after shifting by an overall coefficient  $q^a$  for some constant  $a$ ). This has been tested in some cases (see [26] and references therein). This modular form is a smooth invariant of  $K$ , for each group  $G$ .<sup>9</sup>

If we fiber the  $A_1$  singularity instead of  $T^2$  over a  $CP^1$  we obtain an  $N = 2$  supersymmetric gauge theory in 4 dimensions with  $SU(2)$  gauge symmetry. If different singularities exist over different curves which intersect (what is sometimes called *colliding singularities*) we typically get “matter” in the physical language transforming according to a representation of the product of the two groups (Fig. 8) [27].

FIG.8: Matter arises where two loci of singularities intersect. The matter is localized at the intersection.

---

<sup>9</sup> The subgroup of  $SL(2, Z)$  for which this is a modular form depends on  $G$ .

This geometric construction of quantum field theories allows us to have a new viewpoint in solving aspects of them. For example consider the  $N = 2$  supersymmetric  $SU(2)$  gauge theory in 4 dimensions. As just mentioned this can be viewed as fibering a contracting  $CP^1$  over a base  $CP^1$ . The instantons of this theory in four dimensions, which are relevant to questions involving Donaldson invariants of four manifolds, correspond to holomorphic curves mapped to a Calabi-Yau 3-fold whose local geometry is a line bundle over a  $CP^1$  fibered over  $CP^1$ . In particular the instanton class in four dimension gets identified with the number of times the curve gets wrapped around the base  $CP^1$ . These can be counted thanks to mirror symmetry discussed before. Thus Donaldson invariants [28] through this geometric construction and by an applications of mirror symmetry can be reduced to Seiberg-Witten invariants [29][30].

Sometimes the physics of the singularities are unconventional. For example when a 4-cycle (say a  $CP^2$ ) shrinks in a Calabi-Yau threefold, it gives rise to very interesting unconventional new physical theories which were not anticipated! This is thus a great source of insight into new physics. In particular what types of singularities occur as well as what are the ways to resolve them will be of extreme importance for unravelling aspects of this new physics. It is tempting to speculate that these singularities may also lead to new invariants for four manifolds.

## 5. BLACK HOLES AND MINIMAL CYCLES

Black holes are solutions to the Einstein equations which represent matter with sufficient concentration in some region.<sup>10</sup> Consider a  $d$  dimensional spacetime. The idealized version of a black hole would correspond to a spherically symmetric distribution of possibly charged matter. This would correspond to solving Euler-Lagrange equations for the action of the form (suppressing all constants)

$$S = \int (R + \sum_i F_i \wedge *F_i)$$

where  $R$  denotes the scalar curvature of the metric and  $F_i$  denote the curvature of some  $U(1)^k$  gauge fields. One solves these equation with the assumption of spherical symmetry with some asymptotic condition imposed on the metric which corresponds to a total mass  $M$  black hole and on the gauge fields with charge  $Q_i = \int_{S^{d-2}} *F_i$ .<sup>11</sup>

Black holes have a causal structure which separates it into two parts by a "horizon"  $H = S^{d-2}$ , for which the future light cone of points inside the sphere does not include exterior points (Fig. 9).

---

<sup>10</sup> The following discussion is somewhat oversimplified to make the essential point more clear.

<sup>11</sup> If  $d=4$  we can also consider having magnetic charges  $M_i = \int_{S^2} F_i$ .

FIG.9: From the regions interior to the horizon no light can come out.

By some semiclassical arguments one expects that black hole carry entropy  $S$ , which is the logarithm of the number of its states, is given by

$$S = \frac{A(H)}{4}$$

where  $A(H)$  denotes the  $d - 2$  dimensional “area” of the horizon  $H$ . For the black hole solution to make physical sense one finds a lower bound on mass for a fixed set of charges  $Q_i$ , namely  $M^2 \geq \sum_i Q_i^2$ . Physically what will happen is that if the mass is above this bound the black hole radiates and loses mass until it reaches this bound, at which point it becomes a stable stationary state. These are known as *extremal black holes*. The entropy, which is defined as a quarter of the horizon area now becomes

$$S = c_d M^{\frac{d-2}{d-3}}$$

where  $c_d$  is some universal constant, depending on  $d$ . It has been a challenge of quantum gravity to explain the microscopic origin of this entropy, i.e. what counting do we do to get this entropy.

In string theory, for large enough charges  $Q_i$ , the charged black holes are realized as branes wrapped around cycles of the Calabi-Yau, and the condition for extremality of the black hole is that the corresponding cycle be minimal in the given class. Thus the charge lattice corresponds to  $H_*(M)$  where the target space is  $R^d \times M$ .<sup>12</sup> Thus the question of black hole entropy gets transformed to counting of the “number” of minimal submanifolds for a fixed class  $Q \in H_*(M)$ . In case there are moduli for such cycles, what is meant by the “number” is the number of cohomology elements of the moduli space. The non-minimal surfaces correspond to non-extremal black holes which “decay” to the extremal ones.

I will now discuss one concrete example to illustrate how the counting works. Consider the 11 dimensional supergravity theory (“M-theory”) on target space  $R^5 \times T^6$  (which is closely related to type IIA on  $R^4 \times T^6$ ), which I will use to

---

<sup>12</sup> The homology dimensions which are allowed charges correspond to the allowed dimensions of the branes in the corresponding theory.

count the number of black holes in 5 dimensions, with charges given by an element in  $H_2(T^6, \mathbb{Z})$  (this is related to black hole count in [31]). Let us think of  $T^6 = (T^2)^3$  and consider the 2-class of each  $T^2$  being represented by  $e_i$  where  $i = 1, 2, 3$ . Let us consider an extremal black hole made of 2-branes whose class is  $Ne_1 + Me_2 + Pe_3$ . We will consider the regime of parameters where  $N \gg M, P \gg 1$ . Let  $\Sigma$  denote a holomorphic curve in the class  $[\Sigma] = Me_2 + Pe_3$  (being holomorphic guarantees being minimal in that class). To construct a 2-surface in the class  $Ne_1 + Me_2 + Pe_3$  we choose  $N$  points on  $\Sigma$  and attach a copy of the first  $T^2$  on each of those points (Fig. 10).

FIG.10: A 2-brane constructed out of  $\Sigma$  and the attachment of  $N$  copies of  $T^2$  at  $N$  points.

This gives rise to a degenerate minimal 2-cycle. The moduli of this  $D2$  brane will in addition correspond to choosing a flat connection on it, which for each  $T^2$  corresponds to choosing a point on the dual  $T^2$ . Thus this surface together with the choice of a flat connection is specified by  $N$  points in  $\hat{T}^2 \times \Sigma$  where  $\hat{T}^2$  denotes the dual torus. Of course the choice of  $N$  points has no ordering so that the moduli space of this minimal cycle, for a *fixed*  $\Sigma$  is given by

$$\mathcal{M}_N = \text{Sym}^N(T^2 \times \Sigma)$$

Since we are interested in the regime where  $N$  is much larger than the other two parameters, we can treat  $\Sigma$  as fixed (i.e. the moduli degrees of freedom coming from it are negligible in comparison). We are thus interested in the growth for the cohomology of  $\mathcal{M}_N$  for large  $N$ . This space is singular and this cohomology should be understood in the sense of the Hilbert Scheme. The answer is well known [32][33] and is given by the coefficient  $d_N$  of  $q^N$  in

$$F = \frac{\prod_n (1 + q^n)^{b_{\text{odd}}}}{\prod_n (1 - q^n)^{b_{\text{even}}}}$$

where  $b_{\text{odd}} = b_{\text{even}} = 4(MP + 2)$  denote the odd and even betti numbers of  $T^2 \times \Sigma$ .  $F$  has modular properties which allows one to estimate the growth of the coefficient of  $q^N$ , following Hardy-Ramanujan, to be

$$d_N \sim \exp(2\pi\sqrt{N(MP + 2)})$$

Thus we obtain a prediction for the entropy to be

$$S = 2\pi\sqrt{N(MP + 2)}$$

The computation of the area of this 5 dimensional black hole by solving the Einstein's equations in this case gives

$$S_{BH} = \frac{A(H)}{4} = 2\pi\sqrt{NMP}$$

which agrees with what we have found in the range of validity of the parameters  $N \gg M, P \gg 1$ .

## 6. A LIST OF QUESTIONS

I will list a number of questions which I believe would be interesting to understand further.

1- I have discussed some aspects of mirror symmetry. The physical and mathematical properties of mirror symmetry without including the D-branes is more or less understood. The case involving the D-branes, which is mirror symmetry for (stable) sheaves on Calabi-Yau and is transformed to (minimal) Lagrangian mid-dimensional cycles on the mirror is stated in this note. However the prediction this entails has not been checked yet. In particular both sides of the mirror transform in this case, regardless of the relationship between the two, deserve further study. Even though some aspects of stable bundles on Calabi-Yau are known, it is rather far from a complete understanding. The properties of minimal Lagrangian cycles and enumerative questions in that context are even less understood. Thus the existence of mirror symmetry in this case may lead to many valuable mathematical insights into both questions.

2- We have mentioned that  $A-D-E$  singularities of  $K3$  lead to the appearance of the corresponding gauge group in physics. We have also noted that some other singularities, such as a contraction of  $CP^2$  in a Calabi-Yau threefold leads to novel physics, not described by a conventional gauge theory. It is thus a pretty exciting link to develop further. To what extent can one classify singularity types of Calabi-Yau (and other Kähler) manifolds, for three and fourfolds? How about transitions among manifolds mediated through singularity types? What is a general way to think about all manifolds at once, having in mind their connectivity by passing through singular ones? Among all singularities is the appearance of  $A-D-E$  singularity a rare phenomenon? If so, what explains the fact that we seem to live in a world with gauge symmetries?

3- Another issue we discussed was the counting of minimal submanifolds. This has some applications in the context of counting black hole states. There are many puzzles still to resolve in this context. In the context of minimal 2 dimensional submanifolds mirror symmetry gives us a way to count them in many cases of interest. However even here there are some puzzles: We consider a fixed class  $Q \in H_2(M, Z)$  in a Calabi-Yau threefold  $M$  and ask how many black holes exist in that class. The predicted answer from solving the Einstein equations is given



as follows. Consider an arbitrary Kähler metric  $k$  with volume 1 on Calabi-Yau  $M$ . Find the Kähler metric which minimizes the area of  $Q$

$$V = k[Q]$$

Call the minimum value  $V_{min}$ , and assume this is achieved for a non-degenerate Kähler metric. Then the prediction for the entropy of the black hole [34], and thus the growth of moduli of holomorphic curves in the class  $Q$  is that it goes as

$$S = \exp(cV_{min}^{3/2})$$

where  $c$  is a universal constant independent of Calabi-Yau. Note that the exponent picks up a factor of  $\lambda^{3/2}$  once we rescale  $Q \rightarrow \lambda Q$ . Mirror symmetry allows us to compute the Euler class (of an appropriate bundle) on the moduli space of curves and that has typical growth which upon the same rescaling of  $Q$  picks up only a  $\lambda$  in the exponent. The discrepancy of this growth with that obtained in mirror computation is presumably because the number that mirror symmetry computes is an Euler class, whereas the number the black hole degeneracy predicts is the growth of cohomologies of the moduli space. It also suggests there must be an enormous cancellation among even and odd cohomology states for such a dramatic change in the growth of states. It would be interesting to verify this.

For other types of black holes other counting problems arise. For example, for type IIB strings with target space being a Calabi-Yau threefold times  $R^4$  we need to count the growth in the cohomology of the moduli space of minimal Lagrangian 3-submanifolds in a given class  $Q \in H_3(M)$ . The prediction from the black hole side is that if we denote by  $\Omega$  the holomorphic 3-form on the Calabi-Yau and minimize

$$V = \frac{|\Omega(Q)|}{\sqrt{\int_M \Omega \wedge \bar{\Omega}}} \tag{1}$$

over the moduli space of complex structure of the Calabi-Yau, assuming that the minimum exists and does not correspond to a degenerate Calabi-Yau, then the growth in the cohomology of moduli space of the minimal submanifold in that class (together with a flat connection) is given by

$$S = \exp(c'V_{min}^2)$$

where  $c'$  is a universal constant. In order to verify such predictions we need to be able to count minimal Lagrangian submanifolds. The basic question is how to enumerate them and check this prediction? What is the analog of "mirror symmetry" which allows counting  $p$  branes with  $p > 2$ ? In fact I would conjecture, based on a few examples (not predicted from physics) that for a Calabi-Yau of complex dimension  $d$ , if we consider real minimal Lagrangian submanifolds of dimension  $d$  and minimize  $V$  again as given by (1) then the growth of the cohomology of their moduli space (together with a flat connection) is given by

$$S = \exp(c(d)V_{min}^{d-1})$$

where  $c(d)$  is a universal constant depending only on  $d$ . This formula is true for  $d = 2, 1$  (in the  $d = 1$  case it is vacuous and in the  $d = 2$  case it can be verified) and is predicted to be true as discussed above for  $d = 3$ , and I am conjecturing it to be true for all  $d$ . Is this true? (Note that by mirror symmetry, this conjecture gets transformed to counting the growth of the cohomology of moduli of stable bundles on the mirror Calabi-Yau.)

4-We have seen many instances of dualities in physical systems and we have explained here some of its mathematical implications. We do not have a deep understanding of *why* these dualities even exist. Does studying the mathematical consequences of it shed any light on this question? In other words, why should seemingly difficult mathematical questions find answers in terms of very simple dual mathematical problems? What is the mathematical meaning of duality?

Given all this relation between physics and mathematics one recalls Wigner's thoughts on this relationship and in particular the "unreasonable effectiveness of mathematics" in solving physical problems. With recent developments in physics and its mathematical implications one may also reverse the arrow and wonder about the unreasonable effectiveness of physics in solving mathematical problems.

I would like to thank the many collaborators I have worked with over the years, who have greatly influenced my understanding of the subject presented here. I would also like to thank Sheldon Katz for a careful reading of this manuscript and for his suggestions for improvement.

## REFERENCES

- [1] C. Vafa, in *Geometry, Topology, and Physics for Raoul Bott*, ed. S.-T. Yau, International Press 1995.
- [2] J. Polchinski, Phys. Rev. Lett. 75 (1995) 4724.
- [3] W. Lerche, C. Vafa and N. P. Warner, Nucl.Phys. B324 (1989) 427.
- [4] L. Dixon in Proc. of the 1987 ICTP Summer Workshop in High Energy Physics and Cosmology, Trieste.
- [5] B. R. Greene and M. R. Plesser, Nucl. Phys. B338 (1990) 15.
- [6] P. Candelas, Xenia C. de la Ossa, Paul S. Green and L. Parkes, Nucl. Phys. B359 (1991) 21
- [7] V. Batyrev, J. Alg. Geom. 3 (1994) 493.
- [8] A. Strominger, S.-T. Yau and E. Zaslow, Nucl. Phys. B479 (1996) 243.
- [9] N.C. Leung and C. Vafa, Adv. Theor. Math. Phys. 2 (1998) 91.
- [10] E. Witten, Nucl. Phys. B340 (1990) 281.
- [11] A. Givental, Internat. Math. Res. Notices (1996), 613 .
- [12] B.H. Lian, K. Liu and S.-T. Yau, Asian J. Math. 1 (1997), 729.
- [13] M. Bershadsky, S. Cecotti, H. Ooguri and C. Vafa, Comm. Math. Phys. 165 (1994) 311.
- [14] R. Friedman, J.W. Morgan and E. Witten, *Vector Bundles over Elliptic Fibrations* alg-geom/9709029.
- [15] M. Bershadsky, A. Johansen, T. Pantev and V. Sadov, Nucl. Phys. B505 (1997) 165.

- [16] J. Minahan, D. Nemeschansky, C. Vafa and N.P. Warner, *E-strings and  $N=4$  Topological Yang-Mills Theories*, hep-th/9802168.
- [17] K. Yoshioka, *Euler characteristics of  $SU(2)$  instanton moduli spaces on rational elliptic surfaces*, math.AG/9805003.
- [18] C. Vafa, *Extending Mirror Conjecture to Calabi-Yau with Bundles*, hep-th/9804131.
- [19] M. Kontsevich, Proceedings of the 1994 ICM I, Birkäuser, Zürich, 1995, p.120; alg-geom/9411018.
- [20] K. Fukaya, The Proceedings of the 1993 GARC Workshop on Geometry and Topology, H.J. Kim, ed., Seoul National University.
- [21] A. Polishchuk and E. Zaslow, *Categorical Mirror Symmetry: The Elliptic Case*, math.AG/9801119.
- [22] A.N. Tyurin, *Non-Abelian analogues of Abel's Theorem*, I.C.T.P. preprint (1997).
- [23] A. Strominger, Nucl. Phys. B451 (1995) 96.
- [24] B. Greene, D.R. Morrison and A. Strominger, Nucl. Phys. B451 (1995) 109.
- [25] C. Montonen and D. Olive, Phys. Lett. B72 (1977) 117.
- [26] C. Vafa and E. Witten, Nucl. Phys. B431 (1994) 3.
- [27] S. Katz and C. Vafa, Nucl. Phys. B497 (1997) 146 ;  
S. Katz, A. Klemm and C. Vafa, Nucl. Phys. B497 (1997) 173;  
S. Katz, P. Mayr and C. Vafa, Adv. Theor. Math. Phys. 1 (1998) 53.
- [28] S.K. Donaldson, Proc. London. Math. Soc. 50 (1985) 1.
- [29] N. Seiberg and E. Witten, Nucl. Phys. B431 (1994) 484.
- [30] G. Moore and E. Witten, *Integration over the  $u$ -plane in Donaldson theory*, hep-th/9709193.
- [31] A. Strominger and C. Vafa, Phys. Lett. B379 (1996) 99.
- [32] L. Göttsche, Math. Ann. 286 (1990) 193.
- [33] F. Hirzebruch and T. Höfer, Math. Ann. 286 (1990) 255.
- [34] S. Ferrara and R. Kallosh, Phys. Rev. D54 (1996) 1514; Phys. Rev. D54 (1996) 1525.

Cumrun Vafa  
Lyman Laboratory of Physics  
Harvard University  
Cambridge, MA 02138, USA

DYNAMICS:  
A PROBABILISTIC AND GEOMETRIC PERSPECTIVE

MARCELO VIANA<sup>1</sup>

ABSTRACT. An overview of recent developments and open questions aiming at a global theory of general (non-conservative) dynamical systems.

1991 Mathematics Subject Classification: 58, 34, 60

Keywords and Phrases: uniformly hyperbolic system, attractor, sensitive dynamics, non-uniform hyperbolicity, physical measure, structural stability, stochastic stability, homoclinic orbit, heteroclinic cycle, partial hyperbolicity, dominated splitting, robust transitivity, singular hyperbolicity, singular attractor.

## 1 INTRODUCTION

In general terms, Dynamics is concerned with describing for the majority of systems how the majority of orbits behave, specially as time goes to infinity. And with understanding when and in which sense this behaviour is robust under small modifications of the system. For instance, most gradient flows on a compact manifold have finitely many singularities, with almost every orbit converging to some of the attracting ones (stable equilibria). And the same is true about any nearby flow, with the same number of attractors. General systems can behave in much more complicated ways, though. Here I consider both discrete time systems – smooth transformations  $f : M \rightarrow M$ , possibly invertible – and continuous time systems – smooth flows or semi-flows  $X^t : M \rightarrow M$ ,  $t \in \mathbb{R}$  – on manifolds  $M$ .

In the early sixties, Smale was proposing the notion of uniformly hyperbolic system, a broad class that includes the diffeomorphisms and flows named after Anosov [4], most gradient-like systems, and the “horseshoe” map. See [101]. A *hyperbolic set*, or generalized horseshoe, is an invariant subset  $\Lambda \subset M$  such that the tangent space over it splits into two invariant subbundles  $T_\Lambda M = E^s \oplus E^u$  so that  $E^s$  is uniformly contracted by future iterates, and similarly for  $E^u$  in past iterates. The *system* is *uniformly hyperbolic*, or *Axiom A*, if its *limit set* – the closure of all future and past accumulation sets of orbits – is hyperbolic. A prototype is the diffeomorphism induced on the 2-torus by  $(x, y) \mapsto (2x + y, x + y)$ , with  $E^s$  and  $E^u$  corresponding to the eigenspaces of this linear map. This, just as many other uniformly hyperbolic systems, is also an example of “chaotic” (or *sensitive*) behaviour: orbits of typical nearby points move away from each other exponentially fast, under forward and backward iterations.

---

<sup>1</sup>Partially supported by PRONEX - Dynamical Systems, Brazil

Nevertheless, uniformly hyperbolic systems admit a very precise description of their behaviour: there are compact invariant subsets  $\Lambda_1, \dots, \Lambda_N$  that are transitive (dense orbits) and such that almost every forward orbit of the system accumulates on one of them [101]. And, though the dynamics near these *attractors*  $\Lambda_j$  may be quite “chaotic”, it is strikingly well behaved from a statistical point of view: there exists a *physical probability measure*  $\mu_j$  supported on  $\Lambda_j$ , such that the time average ( $\delta_p$  stands for Dirac measure at  $p$ )

$$\lim_{n \rightarrow +\infty} \frac{1}{n} \sum_{j=0}^{n-1} \delta_{f^j(z)}, \quad \text{or} \quad \lim_{T \rightarrow +\infty} \frac{1}{T} \int_0^T \delta_{X^t(z)} dt,$$

exists and coincides with  $\mu_j$  for Lebesgue almost every point  $z$  whose orbit accumulates on  $\Lambda_j$ . Cf. Sinai, Ruelle, Bowen [100], [95], [20], [19].

Another major breakthrough was the proof that uniformly hyperbolic systems are, essentially, the structurally stable ones. This was completed by Mañé [63], and Hayashi [43] for flows, in the  $C^1$  setting, after crucial contributions from several mathematicians, specially Anosov, Palis, Smale, Robbin, de Melo, Robinson. See [84] for an extended list of references. The notion of *structural stability*, introduced by Andronov-Pontryagin in the thirties, means that all nearby systems are equivalent up to continuous global change of coordinates.

On the other hand, striking examples like Newhouse’s maps with infinitely many periodic attractors [74], or the “strange” attractors of Lorenz [56] and Hénon [44], showed that uniform hyperbolicity is too strong a condition for a general description of dynamics: systems can be persistently non-hyperbolic (persistently unstable). As the hope to describe generic dynamical systems in a uniformly hyperbolic scope was gradually abandoned, still other important developments were taking place concerning enlarged settings of dynamics.

Starting from Oseledets [78], Pesin [87] developed a theory of *non-uniform hyperbolicity*, dealing with general systems endowed with an invariant probability measure with respect to which almost every point exhibits asymptotic contraction and expansion along complementary directions (non-zero Lyapunov exponents). Then almost every point has a stable and an unstable manifold, whose points are exponentially asymptotic to it, respectively, in the future and in the past. See Katok-Hasselblatt [48] for an account of the theory and references.

There was also considerable progress in studying the modifications (bifurcations) through which a system may cease to be stable. Global bifurcations like *homoclinic tangencies* and *heteroclinic cycles*, that affect the system’s behaviour on large regions of the ambient  $M$ , are accompanied by such a wealth of dynamical changes that one must aim at describing the main phenomena occurring for most nearby systems, specially in terms of probability in parameter space. See Palis-Takens [84] and Section 5 below.

And one could attain substantial understanding of some “chaotic” systems, such as Lorenz-like flows, quadratic maps of the interval, period-doubling cascades, and Hénon-like attractors. Since orbits are sensitive to initial conditions, and so essentially unpredictable over long periods of time, one focus on statistical properties of large sets of trajectories, a point of view pioneered by

Sinai and by Ruelle back in the seventies. See [106] and Sections 3, 4, 6 below.

Building on this, we are again trying to develop a global picture of Dynamics recovering, in a new and more probabilistic formulation, much of the paradigm of finitude and stability for most systems that inspired Smale's proposal about four decades ago. Palis conjectured that every dynamical system can be approximated by another having only finitely many attractors, supporting physical measures that describe the time averages of Lebesgue almost all points. This is at the core of a program [81] that also predicts that statistical properties of such systems are stable, namely under small random perturbations.

In this note I survey some of the recent, rather exciting progress in the general direction of such a program, as well as related open problems and conjectures, mostly in the context of general dissipative systems.

## 2 SETTING THE SCENARIO

In what follows I refer mostly to transformations, since the definitions and results for flows are often similar. Except where otherwise stated, manifolds are smooth, compact, without boundary, and measures are probabilities on the Borel  $\sigma$ -algebra. Lebesgue measure means any measure generated by a smooth volume form.

*Time averages* of continuous functions  $\varphi : M \rightarrow \mathbb{R}$

$$\lim_{n \rightarrow +\infty} \frac{1}{n} \sum_{j=0}^{n-1} \varphi(f^j(z))$$

are the most basic statistical data on the system's asymptotic behaviour. An invariant measure  $\mu$  is a *physical measure* if the time average of every  $\varphi$  coincides with the spatial  $\mu$ -average  $\int \varphi d\mu$ , for a positive Lebesgue measure subset of points  $z \in M$ . And the *basin* of  $\mu$  is the set  $B(\mu)$  of points  $z$  for which this happens.

Physical measures are often called *SRB measures*, after Sinai, Ruelle, Bowen, who first constructed them for Anosov systems [100] and then for general uniformly hyperbolic diffeomorphisms [95] and flows [20]. For these systems there are finitely many SRB measures  $\mu_1, \dots, \mu_N$ , and their basins cover Lebesgue almost all of the phase space  $M$ . Each support  $\Lambda_i = \text{supp } \mu_i$  is an *attractor*, meaning that it is an invariant transitive set whose basin of attraction has positive Lebesgue measure. An invariant set  $\Lambda$  is *transitive* if there exists  $z \in \Lambda$  whose forward orbit  $\{f^n(z) : n \geq 0\}$  is dense in  $\Lambda$ . The *basin of attraction* (or stable set)  $B(\Lambda)$  is the set of points whose forward orbits accumulate in  $\Lambda$ . In this hyperbolic setting, as well as in all known cases that are relevant here, the basin contains a full neighbourhood of the attractor.

For systems preserving a smooth measure, Birkhoff's ergodic theorem ensures that time averages are defined Lebesgue almost everywhere. It is widely believed that the same should be true for *most* non-conservative systems, but this is not known, and there are examples showing that it is not the case for *all* systems. For instance, Bowen exhibited a simple flow on the plane where time averages fail to exist on a whole open region bounded by two saddle connections; see e.g. [106].

On the other hand, existence results for SRB measures are now available for some large classes of systems, as we shall see.

SRB measures are sometimes defined differently, by a property of absolute continuity of their conditional measures on unstable manifolds; see e.g. Eckmann-Ruelle [37]. The definition adopted above is a bit more general, but all the SRB measures we meet in the present paper also have this absolute continuity property.

Palis proposed a few years ago that, for a dense subset of all systems statistical properties should be essentially as nice as in the Axiom A case. In more precise terms, he conjectured that *every system can be approximated by another having only finitely many attractors* (approximation in the  $C^k$  topology, any  $k \geq 1$ ) *supporting SRB measures whose basins cover a full Lebesgue measure subset of the manifold*; see [81]. He also conjectured that those properties should be very stable under small perturbations of the system. Here one thinks of modifications of the system along generic parametrized families, i.e. finite-dimensional submanifolds in the space of systems. For Lebesgue almost all parameters there should be finitely many attractors, supporting SRB measures whose basins cover nearly all of  $M$ , also in terms of Lebesgue measure. Moreover, time averages should not be much affected if small random errors in parameter space are introduced at each iteration: stochastic stability.

This last notion is most relevant when dealing with concrete situations modeled by mathematical systems (which are always only approximately correct): in many cases, features of the actual system that are unaccounted for by the model are well represented by random fluctuations around it. For a definition, let us consider first the situation where the initial map  $f$  has some attractor  $\Lambda$  supporting a unique SRB measure  $\mu$ , and whose basin contains a trapping open region  $U$ : the closure of  $f(U)$  is contained in  $U$ . One considers sequences  $x_j$ ,  $j \geq 0$ , with  $x_0 \in U$  and  $x_{j+1} = g_j(x_j)$  for  $j \geq 0$ , where the maps  $g_j$  are chosen at random (independently) in the  $\epsilon$ -neighbourhood of  $f$ , according to some probability  $\mathcal{P}_\epsilon$ . Here  $\epsilon$  should not be too large, to ensure that these sequences  $x_j$  do not escape  $U$ . Then  $f$  is *stochastically stable* on the basin of  $\Lambda$  if for each continuous function  $\varphi$

$$\lim_{n \rightarrow +\infty} \frac{1}{n} \sum_{j=0}^{n-1} \varphi(x_j) \quad \text{is close to} \quad \int \varphi d\mu,$$

for almost every random orbit  $(x_j)_j$  (Lebesgue almost every  $x_0 \in U$  and  $\mathcal{P}_\epsilon$  almost every  $g_j$ ,  $j \geq 0$ ) if  $\epsilon$  is small. More concretely, I propose to take these small random perturbations along generic parametrized families through  $f$ :  $\mathcal{P}_\epsilon$  is given by Lebesgue measure in the corresponding parameter space.

There are other perturbation schemes, for instance, random orbits may be formed by choosing each  $x_{j+1}$  at random close to  $f(x_j)$ , following some probability measure  $P_\epsilon(x_j, \cdot)$ . The random noise  $P_\epsilon(x, \cdot)$  is usually taken absolutely continuous with respect to Lebesgue measure, and supported on the  $\epsilon$ -neighbourhood of  $f(x)$  or, more generally, converging to Dirac measure at  $f(x)$  as  $\epsilon \rightarrow 0$ . See Kifer [52], [53]. Stochastic stability with respect to this perturbation scheme is defined as before. Although it is not logically related to the notion in the previous paragraph,

which corresponds to

$$P_\epsilon(x, A) = \mathcal{P}_\epsilon(\{g : g(x) \in A\}),$$

the two definitions agree for the systems known to be stable, such as uniformly hyperbolic attractors Kifer [53], Young [108], and other cases mentioned below.

So far, I restricted to attractors with a unique SRB measure and whose basin contains some trapping region: this is true for essentially all known cases, although it is not yet clear in which generality it holds. If the basin of attraction is just a positive Lebesgue measure set (or if one considers random noise which is not supported on small neighbourhoods), then random orbits may escape from it. In such cases, as well as for transitive attractors supporting several SRB measures, a more global notion of stochastic stability can be applied: denoting  $\mu_i$  the SRB measures of  $f$ , time averages of each continuous  $\varphi$  along almost all random orbits should be close to the convex hull of the  $\int \varphi d\mu_i$  when  $\epsilon$  is small.

The main random perturbation scheme for flows  $X^t$  is by diffusion. That is, letting  $X$  be the corresponding vector field, one considers the flow  $\xi_t$  associated to the stochastic equation (for simplicity, pretend  $M = \mathbb{R}^d$ )

$$d\xi_t = X(\xi_t) dt + \epsilon A(\xi_t) dw_t \quad (1)$$

where  $A(\cdot)$  is matrix-valued and  $dw_t$  is the standard Brownian motion. See e. g. Friedman [38]. Then stochastic stability is defined essentially as before, if  $X^t$  has a unique SRB measure  $\mu$ : the time averages of each continuous  $\varphi$  over almost all stochastic orbits  $\xi_t$  should be close to  $\int \varphi d\mu$  if  $\epsilon$  is small. More generally, since solutions of (1) usually spread over the whole ambient manifold  $M$ , one should use a global notion of stability as in the previous paragraph.

Before proceeding, let me recall another probabilistic notion, expressing sensitivity of the dynamics, that plays an important role in the characterization of complex systems: decay of correlations. The definition applies to general maps  $f$  (or flows) endowed with some invariant measure  $\mu$ , though the most interesting case is when  $\mu$  is a physical measure. Informally, this notion can be motivated as follows. Sensitiveness means that orbits, in some sense, forget their initial state as time increases to infinity. So, given real functions  $\varphi$  and  $\psi$  on  $M$ , knowledge of  $\varphi(z)$  should provide little information about  $\psi(f^n(z))$  for large  $n \geq 1$ . This may be expressed in terms of their *correlations*

$$C_n(\varphi, \psi) = \int \varphi(\psi \circ f^n) d\mu - \int \varphi d\mu \int \psi d\mu,$$

that should converge rapidly to zero as time increases to infinity. In general, one must restrict to some subspace  $\mathcal{F}$  of functions  $\varphi, \psi$  with a minimum amount of regularity. This is because the systems we deal with are actually deterministic (and, in many cases, reversible): loss of memory resulting from sensitiveness appears only at a coarse level of observation of the system, through quantities  $\varphi, \psi$  that do not distinguish nearby points well. One speaks of (*exponential*) *decay of correlations* in the space  $\mathcal{F}$  if  $C_n(\varphi, \psi)$  goes to zero (exponentially fast) as  $n$  goes to infinity, for all  $\varphi, \psi \in \mathcal{F}$ .



## 3 ONE-DIMENSIONAL MAPS

Let  $f_a$  be the real quadratic map given by  $f_a(x) = x^2 + a$ . If  $a \notin [-1/4, 2]$  then the orbit  $f^n(0)$  of the critical point goes to infinity as  $n \rightarrow +\infty$ , and so does the orbit of Lebesgue almost every point  $x$ . Let us look at the more interesting case  $a \in [-1/4, 2]$ . Then there exists a maximal compact interval  $I_a$  containing  $x = 0$  and invariant under  $f_a$ , in the sense that  $f_a(I_a) \subset I_a$ . Two main types of behaviour are known, depending on the value of the parameter  $a$ .

A first type (periodic, uniformly hyperbolic, regular) corresponds to  $f_a$  having a periodic attractor, i.e. a point  $p$  such that  $f_a^k(p) = p$  and  $|(f_a^k)'(p)| < 1$  for some  $k \geq 1$ . Then, the orbit of Lebesgue almost every  $x \in I_a$  converges to the orbit of  $p$ . It is easy to see that this behaviour corresponds to an open set of parameters, and it was conjectured for a long time that this set is also dense in  $[-1/4, 2]$ . This statement, known as the hyperbolicity conjecture, was eventually settled affirmatively by Świątek with the aid of Graczyk [40], and by Lyubich [60].

A second kind of behaviour (chaotic, non-uniformly hyperbolic, stochastic) is displayed by maps  $f_a$  that admit an invariant measure  $\mu_a$  absolutely continuous with respect to Lebesgue measure. It is a theorem of Jakobson [46] that this occurs for a set of parameters with positive Lebesgue measure. When it exists, such a measure  $\mu_a$  is unique and ergodic, and it gives the time average of Lebesgue almost every  $x \in I_a$ , Blokh-Lyubich [13].

Do these cases exhaust all the possibilities for a full Lebesgue measure set of parameters? Remarkably, the answer is affirmative, as shown by Lyubich:

**THEOREM 1** ([59]). *For Lebesgue almost every  $a \in [-1/4, 2]$ , the quadratic map  $f_a$  has either a periodic attractor or an absolutely continuous invariant measure.*

In particular, Palis' finitude conjecture in Section 2 holds in this context: Lebesgue almost every quadratic map admits a unique SRB measure (either a Dirac measure on a periodic orbit or an absolutely continuous measure), whose basin contains Lebesgue almost every bounded orbit. It is interesting to point out that quadratic maps without SRB measures do exist, cf. Hofbauer-Keller [45].

Most of this holds for general unimodal or multimodal maps of the interval or the circle, though the extension may be far from trivial. A proof of the hyperbolicity conjecture in a general setting of unimodal maps was announced by Kozlovski [54]. An analog of Theorem 1 is also conjectured for general families of one-dimensional maps, but this has not yet been proved.

Jakobson's theorem does extend beyond quadratic maps, and many general criteria for the existence of absolutely continuous invariant measures were obtained since then. This is the most interesting case from an ergodic point of view, and there are several works concerning statistical properties of non-uniformly hyperbolic maps in dimension one, such as the results of Keller-Nowicki [51] and Young [109] on exponential decay of correlations, and those of Collet [28], Katok-Kifer [49], Benedicks-Young [10], and Baladi-Viana [6] on stochastic stability.

*Infinite-modal maps* – one-dimensional maps with infinitely many maxima and minima – come up in many natural contexts of Dynamics, but they are mostly unexplored. Recently, Pacifico-Rovella-Viana [80] proved that non-uniform hyper-

bolicity is persistent – positive Lebesgue measure set of parameters – in a large class of parametrized families of infinite-modal maps, thus setting a way to a more complete study of such maps and their statistical properties. It is an interesting problem to carry out such a study.

#### 4 HÉNON-LIKE ATTRACTORS

This class of systems is modeled by the Hénon map [44]

$$(x, y) \mapsto f(x, y) = (1 - ax^2 + y, bx),$$

where  $a, b$  are real parameters. A main feature is the coexistence of hyperbolic and *folding* behaviour: at points away from the line  $x = 0$  one may find complementary directions that are geometrically contracted and expanded by the derivative of the map; but these directions do not extend across the *critical region*  $\{x \approx 0\}$ , where the phase space is “folded” by the map.

For a large domain in parameter space, e.g.  $1 < a < 2$  and  $b$  not too large, one may find some rectangle  $R$  which is positively invariant –  $f$  maps  $R$  to its interior – and this is the most interesting case. Computer pictures of the “strange attractor”, where orbits of points inside  $R$  seem to accumulate, were produced by Hénon [44] for parameters  $a \approx 1.4, b \approx 0.3$ . But it was only some ten years ago that Benedicks-Carleson could prove that there is indeed a non-trivial (non-periodic) attractor, with positive probability in parameter space:

**THEOREM 2** ([7]). *For every sufficiently small  $b > 0$  there exists a positive Lebesgue measure subset  $E \subset \mathbb{R}$  so that for all  $a \in E$  there exists a compact invariant subset  $\Lambda \subset R$  such that  $B(\Lambda)$  has non-empty interior, and  $\|Df^n(z)\| \rightarrow +\infty$  exponentially fast when  $n \rightarrow +\infty$ , for some  $z$  with forward orbit dense in  $\Lambda$ .*

This was a major achievement, opening the way to a theory of *Hénon-like maps*, which are the first class of genuinely non-uniformly hyperbolic systems in dimension larger than 1 to be understood specially from an ergodic point of view (Lorenz-like flows can be reduced to hyperbolic maps, cf. Section 6).

On the one hand, it was shown that attractors combining hyperbolic and critical behaviour are a very general phenomenon occurring, with positive probability in parameter space, in many bifurcations of diffeomorphisms or flows: homoclinic tangencies Mora-Viana [64], saddle-node cycles Díaz-Rocha-Viana [35], Costa [31], saddle-focus connections Pumariño-Rodríguez [92]. Colli [30] proved that infinitely many of these attractors may coexist, for many parameter values, in the unfolding of homoclinic tangencies. Henceforth, I refer to all these attractors as *Hénon-like*.

On the other hand, Benedicks-Young proved that these non-hyperbolic attractors have, nevertheless, well defined statistical properties:

**THEOREM 3** ([11], [12]). *Let  $\Lambda$  be a Hénon-like attractor of a surface diffeomorphism  $f$ , as above. Then there exists a unique SRB measure  $\mu$  supported on  $\Lambda$ , and  $(f, \mu)$  is equivalent to a Bernoulli shift. Moreover,  $(f, \mu)$  has exponential decay of correlations in the space of Hölder continuous functions.*

Their strategy in [11] was to find an ergodic invariant measure  $\mu$  supported on  $\Lambda$ , with absolutely continuous conditional measures along Pesin's unstable manifolds. Then, the basin of  $\mu$  must contain a positive Lebesgue measure set, cf. Pugh-Shub [90]. This construction of the SRB measure could not decide whether Lebesgue almost every point that is attracted to  $\Lambda$  is in  $B(\mu)$  or, on the contrary, there are sizable sets ("holes") of points in  $B(\Lambda)$  whose time average is not given by  $\mu$ . This *basin problem* was raised by Sinai and by Ruelle back in the seventies, and is also related to the following question: is Lebesgue almost every orbit in the basin of attraction asymptotic to some orbit inside the attractor? For uniformly hyperbolic attractors the answers are well-known and affirmative, see Bowen [19].

Then, Benedicks and I solved both questions for Hénon-like attractors: there are no "holes" in their basins. More recently, we also proved that these attractors are stochastically stable, thus bringing the ergodic theory of these systems close to completion.

**THEOREM 4** ([9], [8]). *Let  $\Lambda$  be a Hénon-like attractor of a surface diffeomorphism  $f$ , as before, and  $\mu$  be the SRB measure. Then*

$$B(\Lambda) = \bigcup_{\xi \in \Lambda} W^s(\xi) = B(\mu), \quad \text{up to zero Lebesgue measure sets.}$$

*Moreover,  $(f, \mu)$  is stochastically stable under small random perturbations.*

The proofs of these results depend on an assumption of strong area dissipativeness, e.g. in Theorem 2 the Jacobian of  $f$  must be very small (much smaller than Hénon's  $b \approx 0.3$ ). In particular, we are still far from understanding non-uniformly hyperbolic behaviour in area-preserving systems such as the conservative Hénon family  $(x, y) \mapsto (1 - ax^2 + y, \pm x)$ , or the *standard family* of maps on the 2-torus

$$f_k(x, y) = (-y + 2x + k \sin(2\pi x), x)$$

For the latter, Duarte [36] proved abundance of KAM islands for generic (Baire second category) large parameters  $k$ . But the standing conjecture is that, from a measure-theoretical point of view, non-uniform hyperbolicity – non-zero Lyapunov exponents on a positive Lebesgue measure subset, possibly even non-existence of elliptic islands – should prevail in parameter space. To settle this is a major challenge in Dynamics nowadays.

## 5 HOMOCLINIC TANGENCIES - FRACTAL DIMENSIONS

A *homoclinic tangency* is a non-transverse intersection between the stable manifold and the unstable manifold of some periodic point  $p$ . In this section I want to explain why this phenomenon is a main ingredient for non-hyperbolic dynamics: homoclinic tangencies are always an obstruction to hyperbolicity and, for low dimensional systems such as surface diffeomorphisms, this is likely to be *the* essential obstruction.

Palis conjectured that every surface diffeomorphism can be  $C^k$  approximated by another which either is uniformly hyperbolic or has a homoclinic tangency. This was recently established by Pujals-Sambarino, for  $k = 1$ :

THEOREM 5 ([91]). *The set of diffeomorphisms on a surface  $M$  which are either uniformly hyperbolic or have a homoclinic tangency is dense in  $\text{Diff}^1(M)$ .*

Their arguments, inspired by Mañé's proof of the  $C^1$  stability conjecture [61], [62], [63], have other important consequences, including the following corollary of Theorem 5 that gives a partial converse to Newhouse's theorem [75]:  $C^1$  open sets where coexistence of infinitely many periodic attractors occurs densely must contain diffeomorphisms with homoclinic tangencies.

There are other results showing that specific phenomena of complicated dynamics, such as saddle-node cycles, cascades of bifurcations, or Hénon-like attractors, can be approximated by maps with homoclinic tangencies; see Newhouse-Palis-Takens [77], Catsigeras [25], Ures [103]. Conversely, surface diffeomorphisms with homoclinic tangencies are approximated by others exhibiting any of these phenomena; see Newhouse [75], Yorke-Alligood [107], Mora-Viana [64], Colli [30]. In these situations one gets approximation in the  $C^k$  sense, any  $k \geq 1$ , and so these results indicate that the space of non-hyperbolic  $C^k$  surface diffeomorphisms should be rather homogeneous, even if there is little hope to settle the general case  $k \geq 2$  of the conjecture above in a near future.

Let  $f_\mu$ ,  $\mu \in \mathbb{R}$ , be a generic parametrized families of diffeomorphisms on a surface  $M$ , such that  $f = f_0$  has a homoclinic tangency. What can one say about the dynamics of  $f_\mu$ , for the majority of parameters  $\mu$  close to zero? In some cases  $f_\mu$  turns out to be uniformly hyperbolic for a set of parameters  $H$  with full Lebesgue density at  $\mu = 0$ :

$$\lim_{\varepsilon \rightarrow 0} \frac{\text{Leb}(H \cap [-\varepsilon, \varepsilon])}{2\varepsilon} = 1.$$

This is due to Palis-Takens [82], [83], extending Newhouse-Palis [76], where a main assumption is that the periodic point  $p$  is in a hyperbolic set  $\Lambda$  whose Hausdorff dimension  $HD(\Lambda)$  is less than 1. On the other hand, Palis-Yoccoz [86] showed that this is generically not true if the Hausdorff dimension is larger than 1.

These works, as well as Newhouse [74], displayed a crucial role played by fractal dimensions and related geometric invariants in the theory of bifurcations, and inspired some general problems about Cantor subsets of the real line with important consequences in the dynamical setting. Another conjecture of Palis claimed that for generic regular Cantor sets  $K_1, K_2 \subset \mathbb{R}$ , the arithmetic difference  $K_2 - K_1 = \{a_2 - a_1 : a_1 \in K_1, a_2 \in K_2\}$  either has zero Lebesgue measure or contains an interval. A *regular Cantor set* is one which is generated by a smooth expanding map defined on a finite union of intervals. The space of regular Cantor sets inherits a topology from the space of such expanding maps, and the word generic refers to a residual (Baire second category) subset in this topology. The arithmetic difference always has measure zero if  $HD(K_1) + HD(K_2) < 1$ , so the interesting case of the conjecture corresponds to the sum being larger than 1. This was achieved a couple of years ago by Moreira-Yoccoz who, in fact, proved a stronger statement:

THEOREM 6 ([73]). *There exists an open and dense subset of the space of pairs of regular Cantor sets  $(K_1, K_2)$  with  $HD(K_1) + HD(K_2) > 1$ , such that  $K_1$  intersects stably some translate  $K_2 + t$ .*

Partial results had been obtained by Moreira [71], who introduced the notion of *stable intersection*: given any  $\tilde{K}_1$  close to  $K_1$  and  $\tilde{K}_2$  close to  $K_2+t$ , then  $\tilde{K}_1 \cap \tilde{K}_2$  is non-empty. In particular,  $K_2 - K_1$  contains an interval around  $t$ . Theorem 6 has the following important translation in the dynamical setting [72]: for a generic family of diffeomorphisms  $f_\mu$  unfolding a homoclinic tangency the set of parameters for which  $f_\mu$  is either uniformly hyperbolic or has *persistent homoclinic tangencies* has full density at  $\mu = 0$ . This second possibility corresponds to intervals in parameter space where densely one observes homoclinic tangencies, cf. [75].

Of course, one also wants to describe the structure of the limit set  $L(f_\mu)$ , for most small values of  $\mu$ , specially when it is not uniformly hyperbolic. Palis-Yoccoz announced recently that  $L(f_\mu)$  does have a property of *weak hyperbolicity* for a set of parameters with full density at zero, if the Hausdorff dimension of the horseshoe  $\Lambda$  involved in the tangency is not too large, e.g.  $HD(\Lambda) < 3/2$ . Roughly, the part of the limit set that is related to the unfolding of the tangency looks like a saddle-type version of the Hénon attractor: in particular, its stable and unstable sets have zero Lebesgue measure.

Several of these results hold in any dimension, or have been subsequently extended to that generality, see Viana [104], Palis-Viana [85], Romero [93], Gonchenko-Shil'nikov-Turaev [39], and references therein. As a rule, results involving fractal dimensions are much harder in higher dimensions, and this is a subject of current research. On the other hand, for high dimensional diffeomorphisms and flows, new key phenomena enter the scene, besides homoclinic tangencies, and problems and conjectures must be restated accordingly. This I discuss in the next sections.

## 6 SINGULAR FLOWS

In the early sixties, Lorenz [56] observed that the solutions of a simple differential equation in dimension 3,

$$\dot{x} = -10x + 10y, \quad \dot{y} = 28x - y - xz, \quad \dot{z} = -\frac{8}{3}z + xy \quad (2)$$

related to a model of atmospheric convection, seemed to depend sensitively on the initial point. Thus, in practice, their behaviour over long periods of time can not be effectively predicted (and so neither can the weather, according to Lorenz): one would need to know the initial point with infinite precision.

Geometric models were proposed by Afraimovich-Bykov-Shil'nikov [1] and Guckenheimer-Williams [42], to interpret the behaviour observed by Lorenz in the equation (2). These are smooth flows  $X^t$  in three dimensions, admitting a trapping region  $U$  – the closure of  $X^t(U)$  is contained in  $U$  for every  $t > 0$  – such that the maximal invariant set  $\Lambda = \bigcap_{t>0} X^t(U)$  contains both a singularity (equilibrium point) and regular orbits dense in  $\Lambda$ . The flow leaves invariant a foliation of  $U$ , a key property that permits to reduce the dynamics to that of an expanding map of the interval. Moreover, these attractors are robust: the maximal invariant set in  $U$  of any nearby flow  $Y^t$  also has all these properties.

These Lorenz models attracted a lot of attention, and their geometric, dynamical, and ergodic properties are now well understood: in particular, they support a unique SRB measure and they are stochastically stable. See e.g. Bunimovich [22], Collet-Tresser [29], Kifer [52], Pesin [88], Sataev [97], and references therein. On the other hand, Lorenz' original conjecture that a sensitive attractor  $\Lambda$  exists in the specific system (2) remained an open problem for more than three decades. Remarkably, a positive solution has just been announced by Tucker [102].

With these examples in mind, let us call a compact invariant set  $\Lambda$  of a flow  $X^t$  a *singular transitive set* if it is the maximal invariant set  $\Lambda = \bigcap_{t \in \mathbb{R}} X^t(U)$  in some open neighbourhood  $U$ , and contains both singularities and dense regular orbits. We also call  $\Lambda$  a *singular (or Lorenz-like) attractor* if  $U$  can be taken positively invariant (trapping), and a *singular repeller* if it is a singular attractor for the flow  $X^{-t}$  obtained from  $X^t$  by reversing the direction of time. In general, we say that the singular transitive set  $\Lambda$  is  $C^1$  *robust* if  $\Lambda_Y = \bigcap_{t \in \mathbb{R}} Y^t(U)$  is also a singular transitive set for any flow  $Y^t$  in a  $C^1$  neighbourhood of  $X^t$ .

Robust singular transitive sets are a main novelty in the dynamics of flows, relative to discrete time systems. In the last few years, Morales-Pacifico-Pujals have been developing a general theory of such sets, specially in the 3-dimensional case. A related goal is to characterize the flows whose singularities and periodic orbits are robustly hyperbolic, meaning that they remain so for every  $C^1$  nearby flow, see [66]. Morales-Pacifico-Pujals construct new types of flows with singular attractors, some of which can be obtained from hyperbolic flows through a single bifurcation [65], [70], [67]. Most specially, they prove that a  $C^1$  robust singular transitive set  $\Lambda$  must have the following hyperbolicity property [68]. A compact invariant set  $\Lambda$  is *singular hyperbolic* for the flow  $X^t$  if there exists a decomposition of the tangent space

$$T_\Lambda M = E^1 \oplus E^2$$

invariant under every  $DX^t$ , where  $E^1$  is 1-dimensional and (norm) contracting, and  $E^2$  is 2-dimensional and volume expanding. The latter may contain directions that are contracted, but the decomposition must be *dominated*: possible contraction along  $E^2$  is weaker than the contraction along  $E^1$ . We also say that  $\Lambda$  is singular hyperbolic for  $X^t$  if it is singular hyperbolic for the dual flow  $X^{-t}$ .

**THEOREM 7 ([68]).** *Let  $\Lambda$  be a  $C^1$  robust singular transitive set of a flow on a 3-dimensional manifold  $M$ . Then all the singularities in  $\Lambda$  have the same stable dimension, either 1 or 2. In the first case  $\Lambda$  is a singular repeller, in the second one it is a singular attractor. In either case,  $\Lambda$  is a singular hyperbolic set.*

A key tool in Theorem 7, and in other important results in this area, is Hayashi's connecting lemma [43]: a system exhibiting some unstable manifold accumulating on a stable manifold may be  $C^1$  perturbed to have the two invariant manifolds intersect.

A next step is to understand the structure of singular hyperbolic sets. In this direction, Morales-Pacifico-Pujals can give a pseudo Markov description reminiscent of [20], and they also have made progress towards a converse to Theorem 7, characterizing when a singular hyperbolic set is  $C^1$  robustly transitive. In the

proof of the theorem they also get that in the attractor case the eigenvalues at the singularities  $\lambda_1 < \lambda_2 < 0 < \lambda_3$  must satisfy  $\lambda_2 + \lambda_3 > 0$ , just as in the classical Lorenz models. A dual fact holds in the repeller case.

Rovella [94] had given the first examples of singular transitive attractors that, although not robust, are *persistent* in a probabilistic sense: positive probability in parameter space, in generic parametrized families of flows through the initial one. For this he considered a modification of the geometric Lorenz flows where the eigenvalues at the singularity satisfy  $\lambda_2 + \lambda_3 < 0$  instead. New examples are provided by the extended model for the behaviour of the Lorenz equations over a large parameter range proposed by Luzzatto-Viana [58], [57]: a main novelty with respect to the usual geometric models and Rovella's flows is that these systems admit no invariant foliation. Moreover, Pacifico-Rovella-Viana [80], [79] proved that global spiral attractors exist, as conjectured by Sinai, in fact they occur persistently in many families of flows. These are attractors containing a saddle-focus singularity (two contracting complex and one real expanding eigenvalue), which forces an extremely complicated spiraling geometry.

The theory of singular flows in dimension larger than 3 is mostly open. Until very recently it was not even known whether robust transitive attractors can contain singularities with unstable dimension larger than 1, an old problem posed by the introduction of the geometric Lorenz models in the seventies. This was solved by Bonatti-Pumariño-Viana [17] who proved that such *multidimensional Lorenz-like attractors* do exist, with arbitrary unstable dimension  $k \geq 1$ . Moreover, they support a unique SRB measure. Examples persisting in codimension 2 subsets of flows were found by Morales-Pujals [69].

Let me also briefly comment on piecewise smooth maps, an important class of systems including e.g. Poincaré maps of flows with singularities, some Markov or non-Markov extensions of smooth maps, and billiards. See [50]. Liverani [55] proved exponential decay of correlations for area-preserving uniformly hyperbolic piecewise smooth maps. Young [110] extended this to the dissipative case, and also proved exponential decay of correlations for planar Sinai billiards [99]. Chernov [26], [27] extended these results to arbitrary dimension. Alves [2] constructed absolutely continuous invariant measures for piecewise expanding maps with countably many domains of smoothness, in any dimension.

## 7 CYCLES - PARTIAL HYPERBOLICITY

For high dimensional maps and flows, more generally than homoclinic tangencies one must take into account *heteroclinic cycles*: periodic points with variable stable dimensions cyclic related through intersections between their invariant manifolds. A general version of the conjecture at the beginning of Section 5 was also proposed by Palis: every diffeomorphism can be  $C^k$  approximated by another which either is uniformly hyperbolic or has a homoclinic tangency or a heteroclinic cycle.

A key fact about uniformly hyperbolic diffeomorphisms (or flows), is that the limit set  $L(f)$  can be partitioned into finitely many *basic pieces*  $\Lambda_1, \dots, \Lambda_K$  (among which are the attractors of  $f$ ) that are invariant, transitive, and *isolated*: each  $\Lambda_i$  is the maximal invariant set in a neighbourhood  $U_i$ . In fact,  $\Lambda_i$  is  $C^1$  *robustly*

*transitive*: the continuation  $\Lambda_i(g) = \bigcap_{n \in \mathbb{Z}} g^n(U_i)$  of  $\Lambda_i$  is also transitive, for any diffeomorphism  $g$   $C^1$  close to  $f$ . See [101]. Can one find something on the way of such a decomposition for general diffeomorphisms? Recently, there has been some remarkable progress towards understanding how the building blocks could look like. Let  $\Lambda$  be an isolated  $C^1$  robustly transitive set of a diffeomorphism  $f$ . What can be said about  $\Lambda$ ?

For surface diffeomorphisms, Mañé [61] proved that  $\Lambda$  must be a hyperbolic set. He also observed that this can not be true in higher dimensions: there exist open sets of  $C^1$  diffeomorphisms of the 3-torus which are transitive in the whole ambient, and yet have periodic saddles with different stable dimensions (so they can not be Anosov diffeomorphisms). Notice that  $C^1$  robustly transitive diffeomorphisms that are not uniformly hyperbolic had been exhibited before by Shub [98], in dimension 4 or higher. In both constructions, the diffeomorphisms admit a continuous invariant splitting  $TM = E^s \oplus E^c \oplus E^u$  such that  $E^s$  is contracting,  $E^u$  is expanding, and they dominate  $E^c$ . Bonatti-Díaz [14], building on Díaz[32], gave the first examples of robustly transitive diffeomorphism with central bundle  $E^c$  having dimension larger than 1.

Next, Díaz-Pujals-Ures [33] proved that  $C^1$  robustly transitive sets of diffeomorphisms in dimension 3 must be partially hyperbolic. A compact set  $\Lambda$  invariant under a diffeomorphism  $f$  is *partially hyperbolic* if there are  $C > 0, \lambda < 1$ , and an invariant splitting of the tangent space  $T_\Lambda M = E^1 \oplus E^2$  which is *dominated*

$$\|Df^n|E_z^1\| \|(Df^n|E_z^2)^{-1}\| \leq C\lambda^n \text{ for all } z \in M \text{ and } n \geq 1$$

and such that either  $E^1$  is contracting or  $E^2$  is expanding: either

$$\|Df^n|E^1\| \leq C\lambda^n \text{ for all } n \geq 1, \quad \text{or} \quad \|(Df^n|E^2)^{-1}\| \leq C\lambda^n \text{ for all } n \geq 1.$$

It is common to write the splitting  $E^1 \oplus E^2$  as  $E^s \oplus E^c$  in the first case, and as  $E^c \oplus E^u$  in the second one, and I shall keep this convention in what follows. Still in dimension 3, Bonatti observed that  $C^1$  robustly transitive sets need not be strongly partially hyperbolic (three invariant subbundles), see [18] for other examples. Also related to this, Díaz-Rocha [34] prove that near a diffeomorphism with a heteroclinic cycle there are others with either homoclinic tangencies or robustly transitive sets that are strongly partially hyperbolic.

In [18], Bonatti and I also constructed the first examples of robustly transitive diffeomorphisms having neither contracting nor expanding subbundles. Our examples, e.g. in the 4-torus, do admit a dominated splitting, though, with  $E^1$  volume contracting and  $E^2$  volume expanding. Then, Bonatti-Díaz-Pujals [16] rounded off this series of results, by proving that a dominated splitting is indeed a necessary condition for robust transitivity, in any dimension. Summarizing:

**THEOREM 8.** *Let  $\Lambda$  be a  $C^1$  robustly transitive set of  $f : M \rightarrow M$ .*

1. ([61]) *If  $\dim M = 2$  then  $\Lambda$  is a hyperbolic set.*
2. ([33]) *If  $\dim M = 3$  then  $\Lambda$  is a partially hyperbolic set.*
3. ([16]) *If  $\dim M \geq 4$  then  $\Lambda$  admits a dominated splitting.*



Actually, Mañé [61] had proved a stronger fact than 1 above, implying that a transitive isolated set of a surface diffeomorphism either is hyperbolic or its continuation for some  $C^1$  near map contains infinitely many periodic attractors or repellers. This is also extended to any dimension in [16], with hyperbolicity replaced by existence of a dominated splitting.

Diffeomorphisms with infinitely many periodic attractors or repellers are still a mystery: little is known apart from the fact that they are generic in some open sets of  $\text{Diff}^2(M)$ , cf. [74], [75], [85], and of  $\text{Diff}^1(M)$  if  $\dim M \geq 3$ , cf. [15]. Pujals-Sambarino report some progress in the direction of proving that such diffeomorphisms can be approximated by others having (codimension 1) homoclinic tangencies, in the  $C^1$  topology. This would be an important step towards incorporating this phenomenon into the theory. Another point of view is to try to show that it is negligible from a probabilistic point of view. It is not yet known if coexistence of infinitely many attractors or repellers corresponds to zero Lebesgue probability sets in parameter space, for generic families of maps. But Araújo [5] proves that some general maps with random noise have only finitely many attractors, including one-parameter families of diffeomorphisms through homoclinic tangencies (as originally considered in [74]) with small random errors in parameter space.

## 8 ERGODIC PROPERTIES OF PARTIALLY HYPERBOLIC SYSTEMS

Then, a central problem is to understand the structure and properties of partially hyperbolic transitive sets or, more generally, invariant transitive sets supporting a dominated splitting. Here is a couple of my favourite questions: Do these sets have some shadowing property (approximation of pseudo-orbits by actual orbits)? Can one give some description of the dynamics in symbolic terms (semi-conjugacy to a shift map)?

In general, these questions are wide open, but for  $C^2$  diffeomorphisms on a surface Pujals-Sambarino [91] provide a rather precise description of sets  $\Lambda$  with a dominated splitting: if all the periodic points in  $\Lambda$  are hyperbolic saddles, then it is the union of a hyperbolic set and finitely many invariant closed curves which are normally hyperbolic and support an irrational rotation.

On the other hand, there is substantial progress in the ergodic theory of partially hyperbolic systems. Much of the foundations concerning invariant foliations were set by Brin-Pesin [21], and they investigated the relations between topological properties of these foliations and ergodic properties of the system, specially when it preserves volume. This was pursued more recently by Grayson-Pugh-Shub [41], leading to several other results providing conditions for a diffeomorphism to be *stably ergodic*: every volume preserving diffeomorphism in a  $C^1$  neighbourhood is ergodic with respect to Lebesgue measure.

For general partially hyperbolic attractors  $\Lambda$ , Pesin-Sinai [89] constructed *Gibbs  $u$ -states*: invariant measures with absolutely continuous conditional measures along strong-unstable leaves (leaves of the unique integral foliation of  $E^u$ ). Then Carvalho [23] proved that in some cases, e.g. diffeomorphisms derived from Anosov ones, these Gibbs  $u$ -states are SRB measures. Kan [47] gave examples of

transitive partially hyperbolic diffeomorphisms having more than one SRB measure, with the basin of each of these measures dense in the ambient.

In [105], I introduced a class of maps exhibiting non-hyperbolic attractors with a multidimensional character: there are several expanding directions (positive Lyapunov exponents) at Lebesgue almost every point in the basin of attraction. The simplest case corresponds to cylinder maps like

$$\varphi : S^1 \times \mathbb{R} \rightarrow S^1 \times \mathbb{R}, \quad \varphi(\theta, x) = (g(\theta), a(\theta) - x^2)$$

where  $g$  is strongly expanding, and  $a(\cdot)$  is a convenient Morse function (diffeomorphisms in compact manifolds and/or higher dimensions may be constructed along similar lines). They present some notable differences with respect to low dimensional non-hyperbolic systems such as unimodal or Hénon maps, in particular they are robust (not just metrically persistent): chaotic behaviour – several positive Lyapunov exponents – occurs for a full open set of perturbations. In this context, Alves obtained the first examples of SRB measures with non-uniform multidimensional expansion:

**THEOREM 9** ([2]). *Every map in a neighbourhood of  $\varphi$  in the space of  $C^3$  self maps of  $S^1 \times \mathbb{R}$  admits an absolutely continuous invariant measure  $\mu$ . Moreover, this measure is unique and ergodic.*

These last results inspired two general statements of existence and finitude of SRB measures for partially hyperbolic attractors that I condense in the following theorem. They concern partially hyperbolic diffeomorphisms whose central direction is either mostly contracting – negative Lyapunov exponents along  $E^c$  – or mostly expanding – positive Lyapunov exponents along  $E^c$ . Without going into technicalities (nor maximum generality) let me say that, given a diffeomorphism  $f$  partially hyperbolic over the whole  $M$  with invariant splitting  $TM = E^c \oplus E^u$ , then  $E^c$  is *mostly contracting* if  $\|Df^n(z)v\| \rightarrow 0$  exponentially fast as  $n \rightarrow +\infty$ , for every  $v \in E_z^c$  and Lebesgue almost every  $z \in M$ . And, given  $f$  with invariant splitting  $TM = E^s \oplus E^c$ , we say that  $E^c$  is *mostly expanding* if  $\|Df^n(z)v\| \rightarrow \infty$  exponentially fast as  $n \rightarrow +\infty$ , for every  $v \in E_z^c$  and Lebesgue almost every  $z \in M$ , like in (3) below.

**THEOREM 10.** *Let  $f$  be a partially hyperbolic  $C^2$  diffeomorphism on a manifold  $M$ . We have*

1. ([18]) *If the central direction is mostly contracting, then the Gibbs  $u$ -states of  $f$  are SRB measures, there are finitely many of them, and their basins cover a full Lebesgue measure subset of  $M$ .*
2. ([3]) *If the central direction is mostly expanding, then Lebesgue almost every point is in the basin of some SRB measure. If the central Lyapunov exponents are bounded away from zero then there are finitely many SRB measures.*

Pushing part 1 of the theorem further on, Castro [24] has just proved exponential decay of correlations for a large class of partially hyperbolic attractors. Related to the examples of Kan [47] I mentioned before, which also fit in this

setting, it is interesting to mention that if all the leaves of the strong-unstable foliation are dense in  $M$  then there is a unique SRB measure [18]. Is this generic among the transitive diffeomorphisms satisfying the assumptions of part 1?

The proof of part 2 includes a generalization of Ruelle's theorem [96] on the existence of absolutely continuous invariant measures for uniformly expanding maps. Let  $f : M \rightarrow M$  be any  $C^2$  covering map which is *non-uniformly expanding* in the sense that  $m(L) = 1/\|L^{-1}\|$  is the minimum expansion of a linear map  $L$ )

$$\liminf_{n \rightarrow +\infty} \frac{1}{n} \log \prod_{j=0}^{n-1} m(Df(f^j(z))) > 0 \quad (3)$$

Lebesgue almost everywhere. Then  $f$  has some ergodic invariant measure absolutely continuous with respect to Lebesgue measure and, indeed, the basins of such measures cover almost all of  $M$ . There is a version of this last result for piecewise smooth maps, assuming that most points do not visit the singular set (where the map fails to be smooth, or the derivative fails to be surjective) too close too often; see [3].

Such results suggest that non-uniform hyperbolicity may suffice for a system to have good statistical properties. In this spirit, I state the following

CONJECTURE: *If a smooth map has only non-zero Lyapunov exponents at Lebesgue almost every point, then it admits some SRB measure.*

#### REFERENCES

- [1] V. S. Afraimovich, V. V. Bykov, and L. P. Shil'nikov. On the appearance and structure of the Lorenz attractor. *Dokl. Acad. Sci. USSR*, 234:336–339, 1977.
- [2] J. Alves. *SRB measures for nonhyperbolic systems with multidimensional expansion*. PhD thesis, IMPA, 1997.
- [3] J. Alves, C. Bonatti, and M. Viana. SRB measures for partially hyperbolic systems whose central direction is mostly expanding. In preparation.
- [4] D. V. Anosov. Geodesic flows on closed Riemannian manifolds of negative curvature. *Proc. Steklov Math. Inst.*, 90:1–235, 1967.
- [5] V. Araújo. *Random perturbations of maps with infinitely many attractors*. PhD thesis, IMPA, 1998.
- [6] V. Baladi and M. Viana. Strong stochastic stability and rate of mixing for unimodal maps. *Ann. Sci. École Norm. Sup.*, 29:483–517, 1996.
- [7] M. Benedicks and L. Carleson. The dynamics of the Hénon map. *Ann. of Math.*, 133:73–169, 1991.
- [8] M. Benedicks and M. Viana. Random perturbations and statistical properties of some Hénon-like maps. In preparation.
- [9] M. Benedicks and M. Viana. Solution of the basin problem for certain non-uniformly hyperbolic attractors. In preparation.

- [10] M. Benedicks and L.-S. Young. Absolutely continuous invariant measures and random perturbations for certain one-dimensional maps. *Ergod. Th. & Dynam. Sys.*, 12:13–37, 1992.
- [11] M. Benedicks and L.-S. Young. SBR-measures for certain Hénon maps. *Invent. Math.*, 112:541–576, 1993.
- [12] M. Benedicks and L.-S. Young. Markov extensions and decay of correlations for certain Hénon maps. Preprint, 1996.
- [13] A. M. Blokh and M. Yu. Lyubich. Ergodicity of transitive maps of the interval. *Ukrainian Math. J.*, 41:985–988, 1989.
- [14] C. Bonatti and L. J. Díaz. Nonhyperbolic transitive diffeomorphisms. *Ann. of Math.*, 143:357–396, 1996.
- [15] C. Bonatti and L. J. Díaz. Connexions heterocliniques et genericité d’une infinité de puits ou de sources. Preprint PUC-Rio, 1998.
- [16] C. Bonatti, L. J. Díaz, and E. Pujals. Genericity of Newhouse’s phenomenon vs. dominated splitting. In preparation.
- [17] C. Bonatti, A. Pumariño, and M. Viana. Lorenz attractors with arbitrary expanding dimension. *C. R. Acad. Sci. Paris*, 325, Série I:883–888, 1997.
- [18] C. Bonatti and M. Viana. SRB measures for partially hyperbolic systems whose central direction is mostly contracting. Preprint IMPA, 1997.
- [19] R. Bowen. *Equilibrium states and the ergodic theory of Anosov diffeomorphisms*, volume 470 of *Lect. Notes in Math.* Springer Verlag, Berlin, 1975.
- [20] R. Bowen and D. Ruelle. The ergodic theory of Axiom A flows. *Invent. Math.*, 29:181–202, 1975.
- [21] M. Brin and Ya. Pesin. Partially hyperbolic dynamical systems. *Izv. Acad. Nauk. SSSR*, 1:170–212, 1974.
- [22] L. A. Bunimovich. Statistical properties of Lorenz attractors. In *Nonlinear dynamics and turbulence*, pages 71–92. Pitman, Boston, 1983.
- [23] M. Carvalho. Sinai-Ruelle-Bowen measures for  $n$ -dimensional derived from Anosov diffeomorphisms. *Ergod. Th. & Dynam. Sys.*, 13:21–44, 1993.
- [24] A. A. Castro. *Backwards inducing and statistical properties for some partially hyperbolic attractors*. PhD thesis, IMPA, 1998.
- [25] E. Catsigeras. Cascades of period doubling bifurcations in  $n$  dimensions. *Nonlinearity*, 9:1061–1070, 1996.
- [26] N. I. Chernov. Statistical properties of piecewise smooth hyperbolic systems in high dimensions. Preprint, 1997.
- [27] N. I. Chernov. Decay of correlations and dispersing billiards. Preprint, 1998.
- [28] P. Collet. Ergodic properties of some unimodal mappings of the interval. Technical report, Institute Mittag-Leffler, 1984.
- [29] P. Collet and C. Tresser. Ergodic theory and continuity of the Bowen-Ruelle measure for geometrical Lorenz flows. *Fyzika*, 20:33–48, 1988.

- [30] E. Colli. Infinitely many coexisting strange attractors. *Ann. Inst. H. Poincaré Anal. Non Linéaire*. To appear.
- [31] M. J. Costa. *Global strange attractors after collision of horseshoes with periodic sinks*. PhD thesis, IMPA, 1998.
- [32] L. J. Díaz. Robust nonhyperbolic dynamics and heterodimensional cycles. *Ergod. Th. & Dynam. Sys.*, 15:291–315, 1995.
- [33] L. J. Díaz, E. Pujals, and R. Ures. Normal hyperbolicity and robust transitivity. Preprint PUC-Rio, 1997.
- [34] L. J. Díaz and J. Rocha. Partial hyperbolicity and transitive dynamics generated by heteroclinic cycles. In preparation.
- [35] L. J. Díaz, J. Rocha, and M. Viana. Strange attractors in saddle-node cycles: prevalence and globality. *Invent. Math.*, 125:37–74, 1996.
- [36] P. Duarte. Plenty of elliptic islands for the standard family of area preserving maps. *Ann. Inst. H. Poincaré Anal. Non. Linéaire*, 11:359–409, 1994.
- [37] J.-P. Eckmann and D. Ruelle. Ergodic theory of chaos and strange attractors. *Rev. Mod. Phys.*, 57:617–656, 1985.
- [38] A. Friedman. *Stochastic differential equations and applications*. Academic Press, New York, 1975.
- [39] S. V. Gonchenko, L. P. Shil’nikov, and D. V. Turaev. Dynamical phenomena in systems with structurally unstable Poincaré homoclinic orbits. *Chaos*, 6:15–31, 1996.
- [40] J. Graczyk and G. Świątek. Generic hyperbolicity in the logistic family. *Annals of Math.*, 146:1–52, 1997.
- [41] M. Grayson, C. Pugh, and M. Shub. Stably ergodic diffeomorphisms. *Annals of Math.*, 140:295–329, 1994.
- [42] J. Guckenheimer and R. F. Williams. Structural stability of Lorenz attractors. *Publ. Math. IHES*, 50:59–72, 1979.
- [43] S. Hayashi. Connecting invariant manifolds and the solution of the  $C^1$  stability and  $\Omega$ -stability conjectures for flows. *Annals of Math.*, 145:81–137, 1997.
- [44] M. Hénon. A two dimensional mapping with a strange attractor. *Comm. Math. Phys.*, 50:69–77, 1976.
- [45] F. Hofbauer and G. Keller. Quadratic maps without asymptotic measure. *Comm. Math. Phys.*, 127:319–337, 1990.
- [46] M. Jakobson. Absolutely continuous invariant measures for one-parameter families of one-dimensional maps. *Comm. Math. Phys.*, 81:39–88, 1981.
- [47] I. Kan. Open sets of diffeomorphisms having two attractors, each with an everywhere dense basin. *Bull. Amer. Math. Soc.*, 31:68–74, 1994.
- [48] A. Katok and B. Hasselblatt. *Introduction to the modern theory of dynamical systems*. Cambridge University Press, Cambridge, 1995.

- [49] A. Katok and Yu. Kifer. Random perturbations of transformations of an interval. *J. Analyse Math.*, 47:193–237, 1986.
- [50] A. Katok and J. M. Strelcyn. *Invariant manifolds, entropy and billiards. Smooth maps with singularities*, volume 1222 of *Lect. Notes in Math.* Springer Verlag, 1986.
- [51] G. Keller and T. Nowicki. Spectral theory, zeta functions and the distribution of periodic points for Collet-Eckmann maps. *Comm. Math. Phys.*, 149:31–69, 1992.
- [52] Yu. Kifer. *Ergodic theory of random perturbations*. Birkhäuser, Basel, 1986.
- [53] Yu. Kifer. *Random perturbations of dynamical systems*. Birkhäuser, Basel, 1988.
- [54] O. Kozlovski. *Structural stability in one-dimensional dynamics*. PhD thesis, Univ. Amsterdam, 1998.
- [55] C. Liverani. Decay of correlations. *Ann. of Math.*, 142:239–301, 1995.
- [56] E. N. Lorenz. Deterministic nonperiodic flow. *J. Atmosph. Sci.*, 20:130–141, 1963.
- [57] S. Luzzatto and M. Viana. Lorenz-like attractors without invariant foliations. In preparation.
- [58] S. Luzzatto and M. Viana. Positive Lyapunov exponents for Lorenz-like maps with criticalities. *Astérisque*, 1998.
- [59] M. Lyubich. Almost every real quadratic map is either regular or stochastic. Preprint Stony Brook, 1997.
- [60] M. Lyubich. Dynamics of quadratic maps I-II. *Acta Math.*, 178:185–297, 1997.
- [61] R. Mañé. Contributions to the stability conjecture. *Topology*, 17:383–396, 1978.
- [62] R. Mañé. Hyperbolicity, sinks and measure in one-dimensional dynamics. *Comm. Math. Phys.*, 100:495–524, 1985.
- [63] R. Mañé. A proof of the  $C^1$  stability conjecture. *Publ. Math. I.H.E.S.*, 66:161–210, 1988.
- [64] L. Mora and M. Viana. Abundance of strange attractors. *Acta Math.*, 171:1–71, 1993.
- [65] C. Morales and M. J. Pacifico. New singular strange attractors arising from hyperbolic flows. Submitted for publication.
- [66] C. Morales, M. J. Pacifico, and E. Pujals. Singular hyperbolic systems. *Proc. Amer. Math. Soc.* To appear.
- [67] C. Morales, M. J. Pacifico, and E. Pujals. Global attractors from the explosion of singular cycles. *C. R. Acad. Sci. Paris*, 325, Série I:1217–1322, 1997.

- [68] C. Morales, M. J. Pacifico, and E. Pujals. On  $C^1$  robust singular transitive sets for three-dimensional flows. *C. R. Acad. Sci. Paris*, 1997.
- [69] C. Morales and E. Pujals. Strange attractors containing a singularity with two positive multipliers. *Comm. Math. Phys.* To appear.
- [70] C. Morales and E. Pujals. Singular strange attractors on the boundary of Morse-Smale systems. *Ann. Sci. École Norm. Sup.*, 30:693–717, 1997.
- [71] C. G. Moreira. Stable intersections of Cantor sets and homoclinic bifurcations. *Ann. Inst. H. Poincaré Anal. Non. Linéaire*, 13:741–781, 1996.
- [72] C. G. Moreira and J.-C. Yoccoz. Tangences homocliniques stables pour les ensembles hyperboliques de grande dimension fractale. In preparation.
- [73] C. G. Moreira and J.-C. Yoccoz. Stable intersections of regular Cantor sets with large Hausdorff dimension. Preprint IMPA, 1998.
- [74] S. Newhouse. Diffeomorphisms with infinitely many sinks. *Topology*, 13:9–18, 1974.
- [75] S. Newhouse. The abundance of wild hyperbolic sets and nonsmooth stable sets for diffeomorphisms. *Publ. Math. I.H.E.S.*, 50:101–151, 1979.
- [76] S. Newhouse and J. Palis. Cycles and bifurcation theory. *Astérisque*, 31:44–140, 1976.
- [77] S. Newhouse, J. Palis, and F. Takens. Bifurcations and stability of families of diffeomorphisms. *Publ. Math. I.H.E.S.*, 57:5–71, 1983.
- [78] V. I. Oseledets. A multiplicative ergodic theorem: Lyapunov characteristic numbers for dynamical systems. *Trans. Moscow Math. Soc.*, 19:197–231, 1968.
- [79] M. J. Pacifico, A. Rovella, and M. Viana. Persistence of global spiraling attractors. In preparation.
- [80] M. J. Pacifico, A. Rovella, and M. Viana. Infinite-modal maps with global chaotic behaviour. *Annals of Math*, 1998.
- [81] J. Palis. A global view of Dynamics and a conjecture on the denseness of finitude of attractors. *Astérisque*, 1998.
- [82] J. Palis and F. Takens. Cycles and measure of bifurcation sets for two-dimensional diffeomorphisms. *Invent. Math.*, 82:397–422, 1985.
- [83] J. Palis and F. Takens. Hyperbolicity and the creation of homoclinic orbits. *Annals of Math.*, 125:337–374, 1987.
- [84] J. Palis and F. Takens. *Hyperbolicity and sensitive-chaotic dynamics at homoclinic bifurcations*. Cambridge University Press, 1993.
- [85] J. Palis and M. Viana. High dimension diffeomorphisms displaying infinitely many periodic attractors. *Annals of Math.*, 140:207–250, 1994.
- [86] J. Palis and J.-C. Yoccoz. Homoclinic tangencies for hyperbolic sets of large Hausdorff dimension. *Acta Math.*, 172:91–136, 1994.

- [87] Ya. Pesin. Families of invariant manifolds corresponding to non-zero characteristic exponents. *Math. USSR. Izv.*, 10:1261–1302, 1976.
- [88] Ya. Pesin. Dynamical systems with generalized hyperbolic attractors: hyperbolic, ergodic and topological properties. *Ergod. Th. & Dynam. Sys.*, 12:123–151, 1992.
- [89] Ya. Pesin and Ya. Sinai. Gibbs measures for partially hyperbolic attractors. *Ergod. Th. & Dynam. Sys.*, 2:417–438, 1982.
- [90] C. Pugh and M. Shub. Ergodic attractors. *Trans. Amer. Math. Soc.*, 312:1–54, 1989.
- [91] E. Pujals and M. Sambarino. Homoclinic tangencies and hyperbolicity for surface diffeomorphisms: a conjecture of Palis. Preprint IMPA, 1998.
- [92] A. Pumariño and A. Rodríguez. *Persistence and coexistence of strange attractors in homoclinic saddle-focus connections*, volume 1658 of *Lect. Notes in Math.* Springer Verlag, Berlin, 1997.
- [93] N. Romero. Persistence of homoclinic tangencies in higher dimensions. *Ergod. Th. & Dynam. Sys.*, 15, 1995.
- [94] A. Rovella. The dynamics of perturbations of the contracting Lorenz attractor. *Bull. Braz. Math. Soc.*, 24:233–259, 1993.
- [95] D. Ruelle. A measure associated with axiom A attractors. *Amer. J. Math.*, 98:619–654, 1976.
- [96] D. Ruelle. The thermodynamical formalism for expanding maps. *Comm. Math. Phys.*, 125:239–262, 1989.
- [97] E. A. Sataev. Invariant measures for hyperbolic maps with singularities. *Russ. Math. Surveys*, 47:191–251, 1992.
- [98] M. Shub. *Topologically transitive diffeomorphisms on  $T^4$* , volume 206 of *Lect. Notes in Math.*, page 39. Springer Verlag, Berlin, 1971.
- [99] Ya. Sinai. Dynamical systems with elastic reflections: ergodic properties of scattering billiards. *Russian Math. Surveys*, 25:137–189, 1970.
- [100] Ya. Sinai. Gibbs measure in ergodic theory. *Russian Math. Surveys*, 27:21–69, 1972.
- [101] S. Smale. Differentiable dynamical systems. *Bull. Am. Math. Soc.*, 73:747–817, 1967.
- [102] W. Tucker. PhD thesis, Univ. Uppsala.
- [103] R. Ures. On the approximation of Hénon-like attractors by homoclinic tangencies. *Ergod. Th. & Dynam. Sys.*, 15, 1995.
- [104] M. Viana. Strange attractors in higher dimensions. *Bull. Braz. Math. Soc.*, 24:13–62, 1993.
- [105] M. Viana. Multidimensional nonhyperbolic attractors. *Publ. Math. IHES*, 85:69–96, 1997.



- [106] M. Viana. *Stochastic dynamics of deterministic systems*. Lecture Notes XXI Braz. Math. Colloq. IMPA, Rio de Janeiro, 1997.
- [107] J. A. Yorke and K. T. Alligood. Cascades of period doubling bifurcations a prerequisite for horseshoes. *Bull. A.M.S.*, 9:319–322, 1983.
- [108] L.-S. Young. Stochastic stability of hyperbolic attractors. *Ergod. Th. & Dynam. Sys.*, 6:311–319, 1986.
- [109] L.-S. Young. Decay of correlations for certain quadratic maps. *Comm. Math. Phys.*, 146:123–138, 1992.
- [110] L.-S. Young. Statistical properties of dynamical systems with some hyperbolicity. Preprint, 1996.

Marcelo Viana  
IMPA, Est. D. Castorina 110  
22460-320 Rio de Janeiro, Brazil  
e-mail: viana@impa.br

# A<sup>1</sup>-HOMOTOPY THEORY

VLADIMIR VOEVODSKY

ABSTRACT.  $\mathbf{A}^1$ -homotopy theory is the homotopy theory for algebraic varieties and schemes which uses the affine line as a replacement for the unit interval. In the paper I present in detail the basic constructions of the theory following the sequence familiar from standard textbooks on algebraic topology. At the end I define motivic cohomology and algebraic cobordisms and describe algebraic K-theory in terms of this theory.

## CONTENTS

1	Introduction . . . . .	579
2	Spaces . . . . .	581
3	Unstable homotopy category . . . . .	584
4	Spanier-Whitehead category . . . . .	587
5	Spectra and the stable homotopy category . . . . .	591
6	Three cohomology theories . . . . .	595
	6.1 Motivic cohomology . . . . .	595
	6.2 Algebraic K-theory . . . . .	598
	6.3 Algebraic cobordism . . . . .	601
7	Concluding remarks . . . . .	601

## 1 INTRODUCTION

In my talk I will outline the foundations of the  $\mathbf{A}^1$ -homotopy theory. This theory is based on the idea that one can define homotopies in the algebro-geometrical context using the affine line  $\mathbf{A}^1$  instead of the unit interval. My exposition will follow the sequence familiar from the standard textbooks on topological homotopy theory which roughly looks as follows.

Let  $\mathcal{C}$  be a category which we want to study by means of homotopy theory. Usually  $\mathcal{C}$  itself is not “good enough” and first one has to choose a convenient category of “spaces”  $Spc$  which contains  $\mathcal{C}$  and has good categorical properties (in particular has internal Hom-objects and all small limits and colimits). In topology  $\mathcal{C}$  may be the category of CW-complexes and  $Spc$  the category of compactly generated spaces ([8, §6.1]). Then one defines the class of weak equivalences on  $Spc$ . The localization of the category of spaces with respect to this class is then the (unstable) homotopy category  $H$ . To make the localization procedure effective one usually chooses in addition classes of cofibrations and fibrations such as to get

a closed model structure in the sense of Quillen (see [8, Def. 3.2.3] for the modern formulation of Quillen's axioms).

Next one considers suspension functors. Stabilizing with respect to these functors in the naive way one obtains a new category  $SW$  called the Spanier-Whitehead category. If the suspensions satisfy some natural conditions this new category is additive and triangulated. As a result it is more accessible to study than the original unstable category. One of the necessary conditions for this to work is that the category  $H$  should be pointed i.e. its initial and final object should coincide. Thus one always applies the stabilization construction to the homotopy category of pointed spaces.

The Spanier-Whitehead categories lack an important property - they do not have infinite coproducts (= infinite direct sums). This is a result of the naive procedure used to invert the suspension functors. To obtain a category where suspensions are inverted and which still has infinite direct sums one uses the idea of spectra. This approach produces another triangulated category which is called the stable homotopy category  $SH$ . The reason infinite direct sums are so important lies in the fact that once we have them we can apply to  $SH$  the representability theory of in [16], [17] and [18].

Thus the standard sequence of constructions in homotopy theory leads to a sequence of categories and functors of the form

$$\mathcal{C} \rightarrow Spc \rightarrow H \rightarrow SW \rightarrow SH$$

In what follows I will construct such a sequence starting with the category  $Sm/S$  of smooth schemes over a Noetherian base scheme  $S$ . A reader who is more comfortable with the language of algebraic varieties may always assume that  $S = Spec(k)$  for a field  $k$  in which case  $\mathcal{C}$  is the category of smooth algebraic varieties over  $k$ . At the end I will define three cohomology theories on  $Spc(S)$  for any  $S$  - algebraic K-theory, motivic cohomology and algebraic cobordism. In each case one defines the theory by giving an explicit description on the spectrum which represents it. Algebraic K-theory defined this way coincides on  $Sm/S$  with homotopy algebraic K-theory of Chuck Weibel [27], motivic cohomology coincide for smooth varieties over a field of characteristic zero with higher Chow groups of S. Bloch [2] and algebraic cobordism is a new theory originally introduced in [26].

Modulo the general nonsense of the abstract homotopy theory *all* the statements of this paper except for Theorem 6.2 have simple proofs. The hard part of the work which was needed to develop the theory presented here consisted in choosing among many different plausible variants of the main definitions. I believe that in its present form the  $\mathbf{A}^1$ -homotopy theory gives a solid foundation for the study of cohomology theories on the category of Noetherian schemes.

Individual constructions which remind of  $\mathbf{A}^1$ -homotopy theory go back to the work of Karoubi-Villamayor on K-theory and more recently to the work of Rick Jardine [9],[10] and Chuck Weibel [27]. For me the starting point is [21] where the first nontrivial theorem showing that this theory works was proven. The first definition of the unstable  $\mathbf{A}^1$ -homotopy category equivalent to the one presented here was given by Fabien Morel.  $\mathbf{A}^1$ -homotopy theory for varieties over a field of characteristic zero was the main tool in the proof of the Milnor conjecture given

in [26]. The current work on the Bloch-Kato conjecture which is a generalization of Milnor conjecture to odd primes uses even more of it.

This text was written during my stay at FIM which is a part of ETH in Zurich. I am very glad to be able to use this opportunity to say that this was a very nice place to work. My special thanks go to Ruth Ebel for her help with all kinds of everyday problems.

## 2 SPACES

The main problem which prevents one from applying the constructions of abstract homotopy theory directly to the category  $Sm/S$  of smooth schemes over a base  $S$  is nonexistence of colimits. In classical algebraic geometry this is known as nonexistence of “contractions”. One can solve this problem for particular types of contractions by extending the category to include nonsmooth varieties, algebraic spaces etc. For our purposes it is important to have *all* colimits which is not possible in any of these extended categories.

There is a standard way to formally add colimits of all small diagrams to a category  $\mathcal{C}$ . Consider the category of contravariant functors from  $\mathcal{C}$  to the category of sets. Following Grothendieck one calls such functors *presheaves* on  $\mathcal{C}$ . We denote the category of all presheaves by  $PreShv(\mathcal{C})$ . Any object  $X$  of  $\mathcal{C}$  defines a presheaf  $R_X : Y \mapsto Hom_{\mathcal{C}}(Y, X)$  which is called the presheaf representable by  $X$ . By Yoneda Lemma the correspondence  $X \mapsto R_X$  identifies  $\mathcal{C}$  with the subcategory of representable presheaves on  $\mathcal{C}$ . The category  $PreShv(\mathcal{C})$  has all small colimits (and limits). Moreover any presheaf is the colimit of a canonical diagram of representable presheaves. Thus  $PreShv(\mathcal{C})$  is in a sense the category obtained from  $\mathcal{C}$  by formal addition of all small colimits.

It is quite possible to develop homotopy theory for algebraic varieties taking the category  $PreShv(Sm/S)$  as the category  $Spc$  of spaces. However this approach has a disadvantage which can be illustrated by the following example. For two subspaces  $A, B$  of a space  $X$  denote by  $A \cup B$  the colimit of the diagram

$$\begin{array}{ccc} A \cap B & \rightarrow & A \\ \downarrow & & \\ B & & \end{array} \quad (1)$$

where  $A \cap B = A \times_X B$  is the fiber product of  $A$  and  $B$  over  $X$ . This is the categorical definition of union which makes sense in any category with limits and colimits. Consider now a covering  $X = U \cup V$  of a scheme  $X$  by two Zariski open subsets  $U$  and  $V$ . The square

$$\begin{array}{ccc} U \cap V & \rightarrow & U \\ \downarrow & & \downarrow \\ V & \rightarrow & X \end{array} \quad (2)$$

is a pushforward square in  $Sm/S$  and thus  $X$  is the categorical union of  $U$  and  $V$

in  $Sm/S$ . However the corresponding square of representable presheaves

$$\begin{array}{ccc} R_{U \cap V} & \rightarrow & R_U \\ \downarrow & & \downarrow \\ R_V & \rightarrow & R_X \end{array} \quad (3)$$

is *not* a pushforward square in  $PreShv(Sm/S)$  unless  $U = X$  or  $V = X$ . Thus if we define spaces as presheaves the union  $U \cup_{PreShv} V$  of  $U$  and  $V$  as spaces is not the same as  $X$ . There is a morphism  $j_{U,V} : U \cup_{PreShv} V \rightarrow X$  but it is not an isomorphism.

DEFINITION 2.1 *An elementary distinguished square in  $Sm/S$  is a square of the form*

$$\begin{array}{ccc} p^{-1}(U) & \rightarrow & V \\ \downarrow & & \downarrow p \\ U & \xrightarrow{j} & X \end{array} \quad (4)$$

*such that  $p$  is an étale morphism,  $j$  is an open embedding and  $p^{-1}(X-U) \rightarrow X-U$  is an isomorphism (here  $X-U$  is the maximal reduced subscheme with support in the closed subset  $X-U$ ).*

An important class of elementary distinguished squares is provided by coverings  $X = U \cup V$  by two Zariski open subsets. In this case  $p = j_V$  is an open embedding and the condition that  $p^{-1}(X-U) \rightarrow X-U$  is an isomorphism is equivalent to the condition that  $U \cup V = X$ . One can easily see that an elementary distinguished square is a pushforward square in  $Sm/S$  i.e.  $X$  is the colimit of the diagram

$$\begin{array}{ccc} p^{-1}(U) & \rightarrow & V \\ \downarrow & & \\ U & & \end{array} \quad (5)$$

We want to define our category of spaces in such a way that elementary distinguished squares remain pushforward squares when considered in this category of spaces. The technique which allows one to add new colimits taking into account already existing ones is the theory of sheaves on Grothendieck topologies.

DEFINITION 2.2 *A contravariant functor  $F : Sm/S \rightarrow Sets$  (= a presheaf on  $Sm/S$ ) is called a sheaf in Nisnevich topology if the following two conditions hold*

1.  $F(\emptyset) = pt$
2. *for any elementary distinguished square as in Definition 2.1 the square of sets*

$$\begin{array}{ccc} F(X) & \rightarrow & F(V) \\ \downarrow & & \downarrow \\ F(U) & \rightarrow & F(p^{-1}(U)) \end{array} \quad (6)$$

*is Cartesian i.e.  $F(X) = F(U) \times_{F(p^{-1}(U))} F(V)$ .*

Denote the full subcategory of  $PreShv(Sm/S)$  which consists of sheaves in Nisnevich topology by  $Shv_{Nis}(Sm/S)$ . This is our category of spaces. Because elementary distinguished squares are pushforward squares in  $Sm/S$  any representable presheaf belongs to  $Shv_{Nis}(Sm/S)$ . Thus the functor  $X \mapsto R_X$  factors through an embedding  $Sm/S \rightarrow Shv_{Nis}(Sm/S)$ . We will use this embedding to identify smooth schemes with the corresponding spaces (= representable sheaves). By Yoneda Lemma and our definition the square of representable sheaves corresponding to an elementary distinguished square is a pushforward square in  $Shv_{Nis}(Sm/S)$ . The following result is a corollary of the general theory of sheaves on Grothendieck topologies.

**THEOREM 2.3** *The category  $Shv_{Nis}(Sm/S)$  has all small limits and colimits. The inclusion functor  $Shv_{Nis}(Sm/S) \rightarrow PreShv(Sm/S)$  has a left adjoint  $a_{Nis} : PreShv(Sm/S) \rightarrow Shv_{Nis}(Sm/S)$  which commutes with both limits and colimits.*

The functor  $a_{Nis}$  is called the functor of associated sheaf. To compute a colimit in  $Shv_{Nis}(Sm/S)$  one first computes it in  $PreShv(Sm/S)$  and then applies functor  $a_{Nis}$ . Starting from this point we denote the category  $Shv_{Nis}(Sm/S)$  by  $Spc$  or  $Spc(S)$  and its final object i.e. the space corresponding to the base scheme  $S$  by  $pt$ .

We will need a definition of a subcategory  $Spc^{ft}$  of spaces of finite type in  $Spc$  whose objects play the role of compact spaces in topology. We define  $Spc^{ft}$  as the smallest subcategory in  $Spc$  which satisfies the following two conditions

1. spaces corresponding to smooth schemes over  $S$  belong to  $Spc^{ft}$

2. if in a pushforward square
 
$$\begin{array}{ccc} A & \xrightarrow{i} & X \\ \downarrow & & \downarrow \\ B & \rightarrow & Y \end{array}$$
 spaces  $A, X$  and  $B$  belong to  $Spc^{ft}$

and  $i$  is a monomorphism then  $Y$  belongs to  $Spc^{ft}$ .

The following proposition shows that spaces of finite type are compact objects of  $Spc$  in the sense of the categorical definition of compactness.

**PROPOSITION 2.4** *For any space of finite type  $X$  and any filtered system of spaces  $X_\alpha$  the canonical map  $colim_\alpha Hom(X, X_\alpha) \rightarrow Hom(X, colim_\alpha X_\alpha)$  is a bijection.*

A pointed space  $(X, x)$  is a space together with a morphism  $x : pt \rightarrow X$ . We will also denote by  $x$  the subspace  $x(pt) = Im x$  of  $X$ . For a space  $X$  and a subspace  $A \subset X$  denote by  $X/A$  the “quotient space” i.e. the colimit of the diagram

$$\begin{array}{ccc} A & \rightarrow & X \\ \downarrow & & \\ pt & & \end{array} \tag{7}$$

We always consider  $X/A$  as a pointed space with the distinguished point given by the canonical morphism  $pt \rightarrow X/A$ . For two pointed spaces  $(X, x), (Y, y)$  define their smash product as  $(X, x) \wedge (Y, y) = X \times Y / (X \times y) \cup (x \times Y)$ .

As an example of how all these definitions work consider Thom spaces of vector bundles. For a vector bundle  $E \rightarrow U$  over a smooth scheme  $U$  over  $S$  set  $Th(E) = E/(E - s(U))$  where  $s : U \rightarrow E$  is the zero section. For two vector bundles  $E \rightarrow X$  and  $F \rightarrow Y$  we have

$$Th(E \times F) = E \times F / (E \times F - s(X \times Y)) = Th(E) \wedge Th(F)$$

Note that in order to have this equality we need to know that

$$E \times F - s(X \times Y) = ((E - s(X)) \times F) \cup (E \times (F - s(Y)))$$

i.e. that the square

$$\begin{array}{ccc} (E - s(X)) \times (F - s(Y)) & \rightarrow & (E - s(X)) \times F \\ \downarrow & & \downarrow \\ E \times (F - s(Y)) & \rightarrow & E \times F - s(X \times Y) \end{array} \tag{8}$$

is a pushforward square. It is true in our case because this is the elementary distinguished square associated to a Zariski open covering.

### 3 UNSTABLE HOMOTOPY CATEGORY

To do homotopy theory in  $Spc$  we have to define classes of weak equivalences, fibrations and cofibrations. We start with the class of weak equivalences. We shall proceed in the same way as one does in homotopy theory of simplicial sets. We first define an analog of Kan simplicial sets and Kan completion functor. Then the analog of homotopy groups and then define weak equivalences as morphisms inducing isomorphisms on homotopy groups. Theorem 3.6 below shows that this definition is equivalent to another, more technical one, given in [14].

Denote by  $\Delta_S^n$  the closed subscheme in  $\mathbf{A}_S^{n+1}$  given by the equation  $\sum_{i=0}^n x_i = 1$ . Clearly  $\Delta_S^n$  is a smooth scheme over  $S$  which is noncanonically isomorphic to  $\mathbf{A}_S^n$ . For any map of sets  $\phi : \{0, \dots, n\} \rightarrow \{0, \dots, m\}$  define a morphism  $\phi_S : \Delta_S^n \rightarrow \Delta_S^m$  setting  $\phi_S^*(x_i) = \sum_{j \in \phi^{-1}(i)} x_j$ . This gives us a functor from the standard simplicial category  $\Delta$  to  $Sm/S$  and thus to  $Spc$ . Since  $Spc$  has all colimits this functor has the right Kan extension  $|-|_S : \Delta^{op} Sets \rightarrow Spc$  which is characterized by the properties that it commutes with colimits and  $|\Delta^n|_S = \Delta_S^n$ .

EXAMPLE 3.1 Let  $\partial\Delta^2$  be the boundary of the standard 2-simplex i.e. the simplicial set whose geometrical realization looks like the boundary of an equilateral triangle. Then  $|\partial\Delta^2|_S$  is the space which is a union of three affine lines in the form of a triangle with sides extended to infinity. Similarly  $|\partial\Delta^3|_S$  is the union of four affine planes in the form of a tetrahedra.

For a space  $X$  and a smooth scheme  $U$  consider the sets  $Sing_n(X)(U) = Hom(U \times \Delta_S^n, X)$ . Since  $\Delta_S^\bullet$  is a cosimplicial space these sets form a simplicial set  $Sing_*(X)(U)$  which is a direct analog of the singular simplicial set of a topological space in the  $\mathbf{A}^1$ -theory.

DEFINITION 3.2 *A space  $X$  is called almost fibrant if for any open embedding  $j : V \rightarrow U$  of smooth schemes over  $S$  the associated morphism of simplicial sets  $Sing_*(X)(U) \rightarrow Sing_*(X)(V)$  is a Kan fibration.*

Note in particular that for any almost fibrant space  $X$  and any smooth scheme  $U$  the simplicial set  $Sing_*(X)(U)$  is a Kan simplicial set.

Let  $i_k^n : \Lambda_k^n \rightarrow \Delta^n$  be the inclusion of the “hat” simplicial set to the standard simplex and let  $j : V \rightarrow U$  be an open embedding of smooth schemes over  $S$ . Consider the following embedding of spaces

$$i_{n,k,j} : U \times |\Lambda_k^n|_S \cup_{V \times |\Lambda_k^n|_S} V \times |\Delta^n|_S \rightarrow U \times |\Delta^n|_S$$

These embeddings for all  $n, k$  and  $j : V \rightarrow U$  form the set of elementary “anodyne” morphisms which we can use to define our analog of Kan completion functor. For a space  $X$  let  $A_X$  be the set of all triples of the form  $(\Lambda_k^n \rightarrow \Delta^n, j : V \rightarrow U, f : U \times |\Lambda_k^n|_S \cup_{V \times |\Lambda_k^n|_S} V \times |\Delta^n|_S \rightarrow X)$ . We have a canonical diagram

$$\begin{array}{ccc} \coprod_{A_X} U \times |\Lambda_k^n|_S \cup_{V \times |\Lambda_k^n|_S} V \times |\Delta^n|_S & \rightarrow & X \\ \downarrow & & \\ \coprod_{A_X} U \times \Delta_S^n & & \end{array} \tag{9}$$

and we define  $Ex^1(X)$  as the colimit of this diagram. Clearly  $Ex^1(X)$  is functorial in  $X$  and there is a canonical morphism  $X \rightarrow Ex^1(X)$ . Set  $Ex^n(X) = Ex^1(Ex^{n-1}(X))$  and  $Ex^\infty(X) = \text{colim}_n Ex^n(X)$ . Proposition 2.4 immediately implies the following fact.

LEMMA 3.3 *The space  $Ex^\infty(X)$  is almost fibrant for any space  $X$ .*

Let  $X$  be a space,  $U$  a smooth scheme and  $x$  an element in  $Sing_0(X)(U) = Hom(U, X)$ . Define homotopy “groups”  $\pi_{i,U}^{\mathbf{A}^1}(X, x)$  as homotopy groups of the Kan simplicial set  $C_*(Ex^\infty(X))(U)$  with respect to the base point  $x$ .

DEFINITION 3.4 *A morphism of spaces  $f : X \rightarrow Y$  is called an  $\mathbf{A}^1$ -weak equivalence (or just weak equivalence) if for any smooth scheme  $U$ , any  $x \in Hom(U, X)$  and any  $i \geq 0$  the corresponding map of homotopy groups*

$$\pi_{i,U}^{\mathbf{A}^1}(X, x) \rightarrow \pi_{i,U}^{\mathbf{A}^1}(Y, f(x))$$

*is a bijection.*

DEFINITION 3.5 *The  $\mathbf{A}^1$ -homotopy category  $H^{\mathbf{A}^1}(S)$  of smooth schemes over  $S$  is the localization of the category of spaces over  $S$  with respect to the class of weak equivalences.*

The following is the list of basic properties of weak equivalences. They can either be deduced from [14] using Theorem 3.6 or proven directly.

1. the canonical morphism  $\Delta_S^1 \rightarrow pt$  is a weak equivalence



2. if  $f : X \rightarrow Y$  and  $f' : X' \rightarrow Y'$  are weak equivalences then  $f \times f' : X \times X' \rightarrow Y \times Y'$  is a weak equivalence

3. if in a pushforward square
- $$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ g \downarrow & & \downarrow g' \\ X' & \xrightarrow{f'} & Y' \end{array}$$
- $f$  is a weak equivalence and either  $f$  or  $g$  is a monomorphism then  $f'$  is a weak equivalence

4. let  $(X_\alpha, f_{\alpha\beta} : X_\alpha \rightarrow X_\beta)$  be a filtered system of spaces such that the morphisms  $f_{\alpha\beta}$  are weak equivalences. Then the morphisms  $X_\gamma \rightarrow \text{colim } X_\alpha$  are weak equivalences.

Another approach to homotopy theory of spaces over  $S$  based on the use of homotopy theory of simplicial sheaves is developed in [14]. The following result shows that these two approaches are equivalent and therefore we can use the technical results of [14] in the context of definitions given above.

**THEOREM 3.6** *A morphism of spaces is a weak equivalence in the sense of definition 3.4 if and only if it is an  $\mathbf{A}^1$ -weak equivalence in the sense of [14]. The category  $H^{\mathbf{A}^1}(S)$  defined above is equivalent to the category  $\mathcal{H}^{\mathbf{A}^1}(S)$  defined in [14].*

Let  $\mathbf{W}$  be the class of weak equivalences. Define the class of cofibrations  $\mathbf{C}$  in  $Spc$  as the class of all monomorphisms and the class of fibrations  $\mathbf{F}$  as the class of morphisms having the right lifting property with respect to morphisms from  $\mathbf{C} \cap \mathbf{W}$  (see [8, p.26]). As a corollary of Theorem 3.6 we have.

**THEOREM 3.7** *The classes  $(\mathbf{W}, \mathbf{F}, \mathbf{C})$  form a proper closed model structure on  $Spc$ .*

Once we know the notions of weak equivalences, fibrations and cofibrations for spaces we can define them for pointed spaces. A morphism of pointed spaces is called a weak equivalence, fibration or cofibration if it is a weak equivalence, fibration or cofibration as a morphism of spaces with forgotten distinguished points. Standard reasoning shows that so defined classes form a proper closed model structure on the category  $Spc_\bullet$  of pointed spaces. We denote the pointed homotopy category by  $H_\bullet^{\mathbf{A}^1}(S)$ . Properties 2 and 3 of weak equivalences from the list given above imply that the smash product gives a symmetric monoidal structure ([11, p.180]) on  $H_\bullet^{\mathbf{A}^1}(S)$ . The unit object of this monoidal structure is the space  $(S \amalg S, i_S)$  which one denotes  $S^0$  and calls 0-sphere.

The functor  $|-|_S$  from simplicial sets to spaces takes weak equivalences of simplicial sets to weak equivalences of spaces and thus defines a functor from the ordinary homotopy category  $H^{top}$  to  $H^{\mathbf{A}^1}$  (and from  $H_\bullet^{top}$  to  $H_\bullet^{\mathbf{A}^1}$ ). For any two simplicial sets  $X, Y$  one has a canonical morphism  $|X \times Y|_S \rightarrow |X|_S \times |Y|_S$  which is not an isomorphism but always a weak equivalence. Therefore the functor from  $H^{top}$  to  $H^{\mathbf{A}^1}$  commutes with products and the functor from  $H_\bullet^{top}$  to  $H_\bullet^{\mathbf{A}^1}$  commutes with smash products.

Define the *simplicial circle*  $S_s^1$  as  $|\Delta^1/\partial\Delta^1|_S$ . Geometrically  $S_s^1$  is the space obtained from the affine line  $\mathbf{A}^1$  by identification of points 0 and 1. The smash product with  $S_s^1$  is the *simplicial suspension functor*. We denote  $(S_s^1)^{\wedge n}$  by  $S_s^n$ . This is the space obtained from  $\mathbf{A}_S^n$  by contraction of the union of hyperplanes  $x_i = 1, x_i = 0, i = 1, \dots, n$  to the point. One can use the simplicial suspension to describe homotopy groups  $\pi_{i,U}^{\mathbf{A}^1}(X, x)$  in terms of morphisms in the pointed homotopy category as follows.

LEMMA 3.8 *For any pointed space  $(X, x)$ , smooth scheme  $U$  and  $i \geq 0$  one has*

$$\pi_{i,U}^{\mathbf{A}^1}(X, x) = \text{Hom}_{H_{\bullet}^{\mathbf{A}^1}}(S_s^i \wedge U_+, (X, x))$$

where  $U_+$  is the pointed space  $(U \amalg S, i_S)$ .

The notion of almost fibrant space turns out to be too restrictive in concrete applications. For example the Eilenberg-MacLane spaces used in Section 6.1 to build the Eilenberg-MacLane spectrum representing motivic cohomology are not almost fibrant. A wider class of quasi-fibrant spaces defined below turns out to be more useful.

DEFINITION 3.9 *A space  $X$  is called quasi-fibrant if for any smooth scheme  $U$  over  $S$  which is quasi-projective over an affine open subset in  $S$  the map of simplicial sets  $\text{Sing}_*(X)(U) \rightarrow \text{Sing}_*(Ex^\infty(X))(U)$  is a weak equivalence.*

The role of quasi-fibrant spaces in the theory is partly explained by the following corollary of Lemma 3.8.

PROPOSITION 3.10 *Let  $(X, x)$  be a pointed quasi-fibrant space and  $U$  be a smooth scheme over  $S$  which is quasi-projective over an affine open subset in  $S$ . Then for any  $i \geq 0$  one has  $\text{Hom}_{H_{\bullet}^{\mathbf{A}^1}}(S_s^i \wedge U_+, (X, x)) = \pi_i(\text{Sing}_*(X)(U), x)$ .*

#### 4 SPANIER-WHITEHEAD CATEGORY

One of the fundamental differences between  $H = H^{\mathbf{A}^1}$  and the ordinary homotopy category  $H^{top}$  lies in the fact that besides the simplicial circle  $S_s^1$  there is another circle  $S_t^1$  which we call Tate circle and which is defined as the space  $\mathbf{A}^1 - \{0\}$  pointed by 1. The following lemma shows how different types of “spheres” can be expressed in  $H_{\bullet}$  in terms of  $S_t^n$  and  $S_s^n$ .

LEMMA 4.1 *There are canonical isomorphisms in  $H_{\bullet}$  of the form*

$$(\mathbf{A}^n - \{0\}, \mathbf{1}) \cong S_t^n \wedge S_s^{n-1}; \quad \mathbf{P}^n/\mathbf{P}^{n-1} \cong \mathbf{A}^n/\mathbf{A}^n - \{0\} \cong S_t^n \wedge S_s^n;$$

The Spanier-Whitehead category  $SW = SW^{\mathbf{A}^1}(S)$  is the category obtained from  $H_{\bullet}$  by stabilization with respect to the suspensions associated to the circles  $S_s^1$  and  $S_t^1$ . For technical reasons it is more convenient to talk about stabilization with respect to one suspension associated with  $S_s^1 \wedge S_t^1$  which leads to an equivalent category. Note that by Lemma 4.1  $S_t^1 \wedge S_s^1$  is canonically weakly equivalent to  $\mathbf{A}^1/\mathbf{A}^1 - \{0\}$  and to  $(\mathbf{P}^1, \infty)$ .

The construction of  $SW$  from  $H_\bullet$  is an example of a very simple general construction which allows one to “invert” an object in a symmetric monoidal category. Let  $(\mathcal{C}, \wedge, \mathbf{1})$  be a symmetric monoidal category (here  $\wedge$  denotes the monoidal structure and  $\mathbf{1}$  is the unit object) and  $T$  an object in  $\mathcal{C}$  ([11, p.157,180]). Denote by  $\mathcal{C}[T^{-1}]$  the category whose objects are pairs of the form  $(X, n)$ ,  $X \in \text{ob}(\mathcal{C})$ ,  $n \in \mathbf{Z}$  and morphisms are given by

$$\text{Hom}((X, n), (X', n')) = \text{colim}_{m \geq -n, -n'} \text{Hom}_{\mathcal{C}}(T^{\wedge(m+n)} \wedge X, T^{\wedge(m+n')} \wedge X')$$

One can easily define composition of morphisms and check that  $\mathcal{C}[T^{-1}]$  is indeed a category. The assignment  $X \mapsto (X, 0)$  gives us a functor from  $\mathcal{C}$  to  $\mathcal{C}[T^{-1}]$ .

DEFINITION 4.2  $SW = H_\bullet[(S_s^1 \wedge S_t^1)^{-1}]$ .

The next step is to define a symmetric monoidal structure on  $\mathcal{C}[T^{-1}]$  such that the canonical functor from  $\mathcal{C}$  is a symmetric monoidal functor and the object  $(T, 0)$  is invertible in  $\mathcal{C}[T^{-1}]$ . It turns out that there is an obvious obstruction to the existence of such a structure. Indeed, the group of automorphisms of an invertible object in a symmetric monoidal category is necessarily abelian. Thus the cyclic permutation on  $T \wedge T \wedge T$  being in the commutator of  $\Sigma_3$  must become identity in  $\text{Aut}_{\mathcal{C}[T^{-1}]}((T, 0))$ . If one tries to extend directly the monoidal structure from  $\mathcal{C}$  to  $\mathcal{C}[T^{-1}]$  one discovers that this condition is indeed necessary and sufficient for the obvious constructions to be well defined. Thus one gets the following general result.

THEOREM 4.3 *Let  $(\mathcal{C}, \wedge, \mathbf{1})$  be a symmetric monoidal category and  $T$  an object such that the cyclic permutation on  $T \wedge T \wedge T$  equals identity in  $\mathcal{C}[T^{-1}]$ . Then there exists a symmetric monoidal structure  $\wedge$  on  $\mathcal{C}[T^{-1}]$  such that  $(X, n) \wedge (Y, m) = (X \wedge Y, n + m)$ .*

*The canonical functor  $\mathcal{C} \rightarrow \mathcal{C}[T^{-1}]$  is then a symmetric monoidal functor and the object  $T = (T, 0)$  is invertible with the canonical inverse given by  $T^{-1} = (\mathbf{1}, -1)$ .*

LEMMA 4.4 *The cyclic permutation on  $(S_s^1 \wedge S_t^1)^{\wedge 3}$  equals identity in  $H_\bullet$ .*

Combining Theorem 4.3 and Lemma 4.4 we get:

PROPOSITION 4.5 *The category  $SW$  has a structure of a symmetric monoidal category  $(\wedge, S^0)$  such that the canonical functor  $(H_\bullet, \wedge, S^0) \rightarrow (SW, \wedge, S^0)$  is symmetric monoidal and  $((X, x), n) \wedge ((Y, y), m) = ((X, x) \wedge (Y, y), n + m)$ .*

Denote the object  $(S^0, n)$  of  $SW$  by  $T^n$  and objects of the form  $((X, x), 0)$  simply by  $(X, x)$ . Then for any  $n \in \mathbf{Z}$  one has a canonical isomorphism  $((X, x), n) = T^n \wedge (X, x)$  which we will use to avoid notations of the form  $((X, x), n)$  below.

PROPOSITION 4.6 *The category  $SW$  is an additive category.*

To get the abelian group structures on the Hom-sets in  $SW$  one observes that the image of  $S_s^2$  in  $SW$  is an abelian cogroup object which is invertible with respect to the monoidal structure.

The last structure on  $SW$  which we want to describe is a structure of a *triangulated* category ([6, ch.IV]). To specify a triangulated structure on an additive category  $\mathcal{D}$  one has to describe two things. One is an additive autoequivalence  $S : \mathcal{D} \rightarrow \mathcal{D}$  which is called the shift functor and denoted by  $X \mapsto X[1]$ . Another one is a class of diagrams of the form  $X \rightarrow Y \rightarrow Z \rightarrow X[1]$  called *distinguished triangles* (all such diagrams are called triangles). These data should satisfy some conditions listed for example in [6, p.239]. These conditions have the following fundamental corollary which makes triangulated structure into a surprisingly effective tool to produce long exact sequences and, more generally, spectral sequences.

LEMMA 4.7 *Let  $X \rightarrow Y \rightarrow Z \rightarrow X[1]$  be a distinguished triangle in a triangulated category and  $U$  be any object of this category. Then the sequences of abelian groups*

$$\begin{aligned} &\rightarrow \text{Hom}(U, X[n]) \rightarrow \text{Hom}(U, Y[n]) \rightarrow \text{Hom}(U, Z[n]) \rightarrow \text{Hom}(U, X[n+1]) \rightarrow \\ &\rightarrow \text{Hom}(Z[n], U) \rightarrow \text{Hom}(Y[n], U) \rightarrow \text{Hom}(X[n], U) \rightarrow \text{Hom}(Z[n-1], U) \rightarrow \\ &\text{are exact.} \end{aligned}$$

All known long exact sequences can be traced back to this lemma applied to distinguished triangles in different triangulated categories. In our case we will construct the Mayer-Vietoris, Gysin and blow-up long exact sequences in homology and cohomology as the long exact sequences associated with distinguished triangles in the Spanier-Whitehead category  $SW$  (see Propositions 4.11-4.13).

Let us describe now the triangulated structure on  $SW$ . We define the shift functor by  $X[1] = X \wedge S^1_s$ . To define distinguished triangles we have to recall the notion of cofibration sequences in our context. Let  $f : (X, x) \rightarrow (Y, y)$  be a morphism of pointed spaces. Define  $\text{cone}(f)$  as the colimit of the diagram

$$\begin{array}{ccc} (X, x) & \xrightarrow{Id \wedge 1} & (X, x) \wedge \Delta^1_S \\ \downarrow & & \\ (Y, y) & & \end{array} \tag{10}$$

where the vertical arrow is  $f$  and  $\Delta^1_S \cong \mathbf{A}^1_S$  is considered as a pointed space with the distinguished point 0. We have a canonical morphism  $(Y, y) \rightarrow \text{cone}(f)$  which we denote  $\eta_f$ . For any commutative square

$$\begin{array}{ccc} (X, x) & \xrightarrow{f} & (Y, y) \\ \downarrow & & \downarrow \\ (X', x') & \xrightarrow{f'} & (Y', y') \end{array} \tag{11}$$

we have a canonical morphism  $\text{cone}(f) \rightarrow \text{cone}(f')$  which makes the diagram

$$\begin{array}{ccc} (Y, y) & \xrightarrow{\eta_f} & \text{cone}(f) \\ \downarrow & & \downarrow \\ (Y', y') & \xrightarrow{\eta_{f'}} & \text{cone}(f') \end{array} \tag{12}$$

commutative. In particular for any  $f$  we have a canonical morphism  $\text{cone}(f) \rightarrow \text{cone}((X, x) \rightarrow pt)$ . The space on the right hand side is canonically isomorphic to  $(X, x) \wedge S_s^1$  and therefore to any  $f$  we assigned in a canonical way a sequence

$$(X, x) \xrightarrow{f} (Y, y) \xrightarrow{\eta_f} \text{cone}(f) \xrightarrow{\epsilon_f} (X, x) \wedge S_s^1$$

which is called the *cofibration sequence* of  $f$ . The idea of the following definition is that the distinguished triangles in  $SW$  are exactly the triangles isomorphic to suspensions of images of cofibration sequences from  $\text{Spc}_\bullet$ .

DEFINITION 4.8 *A sequence of morphisms of the form  $A \rightarrow B \rightarrow C \rightarrow A[1]$  in  $SW$  is called a distinguished triangle if there exist a morphism  $f : X \rightarrow Y$  in  $\text{Spc}_\bullet$ , an integer  $n$  and isomorphisms*

$$\phi_1 : T^n \wedge X \rightarrow A; \quad \phi_2 : T^n \wedge Y \rightarrow B; \quad \phi_3 : T^n \wedge \text{cone}(f) \rightarrow C$$

in  $SW$  such that the following diagram commutes

$$\begin{array}{ccccccc} T^n \wedge X & \xrightarrow{Id \wedge f} & T^n \wedge Y & \xrightarrow{Id \wedge \eta_f} & T^n \wedge \text{cone}(f) & \xrightarrow{\alpha \circ (T^n \wedge \epsilon_f)} & (T^n \wedge X)[1] \\ \phi_1 \downarrow & & \phi_2 \downarrow & & \phi_3 \downarrow & & \phi_1[1] \downarrow \\ A & \rightarrow & B & \rightarrow & C & \rightarrow & A[1] \end{array} \tag{13}$$

(here  $\alpha = \alpha_{T^n, X}$  is the canonical isomorphism  $T^n \wedge X[1] \rightarrow (T^n \wedge X)[1]$ ).

THEOREM 4.9 *The category  $SW$  with the shift functor and the class of distinguished triangles defined above is a triangulated category.*

The main application of Theorem 4.9 is that in combination with Lemma 4.7 it implies that any distinguished triangle in  $SW$  generates two long exact sequences of Hom-groups. To take advantage of this fact one has to have a way to produce interesting distinguished triangles. At the moment we know of three main types of such triangles which generate correspondingly Mayer-Vietoris, Gysin and blow-up long exact sequences. They are described in Propositions 4.11-4.13 below. In all three cases the proof is based on an unstable result from [14] combined with the following general lemma.

LEMMA 4.10 *Consider a commutative square in  $\text{Spc}_\bullet$ .*

$$\begin{array}{ccccc} (A, a) & \xrightarrow{i} & (X, x) & & \\ p \downarrow & & \downarrow & p' & \\ (Y, y) & \xrightarrow{i'} & (Z, z) & & \end{array} \tag{14}$$

such that  $i$  is a monomorphism (= cofibration) and the canonical morphism  $(X, x) \cup_{(A, a)} (Y, y) \rightarrow (Z, z)$  is a weak equivalence. Then there is a canonical morphism  $(Z, z) \rightarrow (A, a) \wedge S_s^1$  in  $H_\bullet$  such that the sequence

$$(A, a) \xrightarrow{p \oplus i} (Y, y) \oplus (X, x) \xrightarrow{i' \oplus p'} (Z, z) \rightarrow (A, a)[1]$$

is a distinguished triangle in  $SW$ .

In the propositions below we denote by  $X_+$  the pointed space  $(X \coprod pt, i_{pt})$  associated with a space  $X$ .

PROPOSITION 4.11 *For any elementary distinguished square as in Definition 2.1 there is a canonical distinguished triangle in  $SW$  of the form*

$$p^{-1}(U)_+ \rightarrow U_+ \oplus V_+ \rightarrow X_+ \rightarrow p^{-1}(U)_+[1]$$

*In particular for the distinguished square associated to a Zariski open covering  $X = U \cup V$  we get the Mayer-Vietoris distinguished triangle*

$$(U \cap V)_+ \rightarrow U_+ \oplus V_+ \rightarrow X_+ \rightarrow (U \cap V)_+[1]$$

PROPOSITION 4.12 *Let  $i : Z \rightarrow X$  be a closed embedding of smooth schemes over  $S$  and  $N$  the normal bundle to  $Z$  in  $X$ . Then there is a canonical Gysin distinguished triangle of the form  $(X - Z)_+ \rightarrow X_+ \rightarrow Th(N) \rightarrow (X - Z)_+[1]$ .*

PROPOSITION 4.13 *Let  $i : Z \rightarrow X$  be a closed embedding of smooth schemes over  $S$  and  $p : X_Z \rightarrow X$  the blow-up of  $Z$  in  $X$ . Then there is a canonical blow-up distinguished triangle of the form*

$$p^{-1}(Z)_+ \rightarrow Z_+ \oplus (X_Z)_+ \rightarrow X_+ \rightarrow p^{-1}(Z)_+[1]$$

The following Connectivity Theorem is the basis for the proof of convergence results for spectral sequences in the homotopy theory of algebraic varieties.

THEOREM 4.14 *Let  $(X, x)$  be a pointed smooth scheme over  $S$ ,  $(Y, y)$  a pointed space and  $m \in \mathbf{Z}$  an integer. Then one has*

$$Hom_{SW}((X, x), S_s^n \wedge S_t^m \wedge (Y, y)) = 0$$

*for any  $n > dim(X)$  where  $dim(X)$  is the absolute dimension of  $X$*

Denote by  $SW^{ft}$  the full subcategory in  $SW$  which consists of objects isomorphic to objects of the form  $T^n \wedge (X, x)$  for  $(X, x) \in Spc^{ft}$ . By definition of cofibration sequences and spaces of finite type this is a triangulated subcategory of  $SW$ . Lemma 4.10 implies that it coincides with the triangulated subcategory generated by objects of the form  $T^n \wedge (X, x)$  for smooth schemes  $X$  over  $S$ . This category actually plays more important role in the theory than the category  $SW$  itself which is a wrong category to work with if we are interested in spaces not of finite type. The correct replacement for  $SW$  is the stable homotopy category  $SH = SH^{\mathbf{A}^1}(S)$  discussed in the following section.

## 5 SPECTRA AND THE STABLE HOMOTOPY CATEGORY

The stabilization construction used to define the Spanier-Whitehead category in the previous section has a serious drawback. One of the good properties of the homotopy category  $H = H_{\bullet}^{\mathbf{A}^1}(S)$  is the existence of infinite coproducts. For

any collection of pointed spaces  $(X_\alpha, x_\alpha)$  the space  $\vee_\alpha(X_\alpha, x_\alpha)$  represents the coproduct of  $(X_\alpha, x_\alpha)$ 's in  $H$  i.e. for any  $(Y, y)$  one has

$$\text{Hom}_H(\vee_\alpha(X_\alpha, x_\alpha), (Y, y)) = \prod_\alpha \text{Hom}_H((X_\alpha, x_\alpha), (Y, y))$$

When we invert  $S_s^1 \wedge S_t^1$  to get the Spanier-Whitehead category we lose this property. For a family of objects like  $\{T^{-i}\}_{i \geq 0}$  there is clearly no coproduct (= direct sum) in  $SW$ . Moreover for an infinite family of pointed spaces  $(X_\alpha, x_\alpha)$  the space  $\vee_\alpha(X_\alpha, x_\alpha)$  considered as an object of  $SW$  is not the coproduct of  $(X_\alpha, x_\alpha)$ 's in this category because infinite colimits do not commute with infinite products.

There is another way to stabilize  $H$  with respect to the suspension functor  $(X, x) \mapsto T \wedge (X, x)$  associated to any pointed space  $T$ . The resulting category which we denote by  $H[[T^{-1}]]$  is called the stable homotopy category of  $T$ -spectra or just the  $T$ -stable homotopy category. It has all coproducts and the canonical functor  $\Sigma_T^\infty : H \rightarrow H[[T^{-1}]]$  takes  $\vee_\alpha(X_\alpha, x_\alpha)$  to the direct sum of  $(X_\alpha, x_\alpha)$ 's in  $H[[T^{-1}]]$ . Unfortunately no one knows how to construct a category  $H[[T^{-1}]]$  with properties described above from  $H$ . Instead we will have to build it directly from spaces.

Let  $T$  be a pointed space of finite type. A  $T$ -spectrum  $\mathbf{E}$  is a sequence of pointed spaces  $E_i, i \geq 0$  which are called terms of  $\mathbf{E}$  and morphisms  $e_i : T \wedge E_i \rightarrow E_{i+1}$  which are called the assembly morphisms of  $\mathbf{E}$ . A morphism of  $T$ -spectra  $\mathbf{E} \rightarrow \mathbf{F}$  is a collection of morphisms of pointed spaces  $E_i \rightarrow F_i$  which commute with the assembly morphisms. Denote the category of  $T$ -spectra by  $Sp(Spc_\bullet, T)$ . For a  $T$ -spectrum  $\mathbf{E}$  define a family of functor  $E^n : Spc_\bullet^{ft} \rightarrow Sets, n \in \mathbf{Z}$  setting

$$E^n(X, x) = \text{colim}_{i \geq \max\{0, -n\}} \text{Hom}_H(T^{\wedge i} \wedge (X, x), T^{\wedge(i+n)} \wedge E_i)$$

where the maps in the inductive system are defined by the assembly morphisms of  $\mathbf{E}$ . A morphism of  $T$ -spectra  $\mathbf{E} \rightarrow \mathbf{F}$  is called a stable weak equivalence if the corresponding natural transformations of functors  $E^n(-) \rightarrow F^n(-)$  are isomorphisms for all  $n \in \mathbf{Z}$ .

DEFINITION 5.1 *The category  $H[[T^{-1}]]$  is the localization of  $Sp(Spc_\bullet, T)$  with respect to the class of weak equivalences.*

The category of  $T$ -spectra has all small limits and colimits which are defined termwise. In particular for a collection of spectra  $\mathbf{E}_\alpha = (E_{i,\alpha}, e_{i,\alpha})$  their coproduct in  $Sp(Spc_\bullet, T)$  is given by  $\oplus_\alpha \mathbf{E}_\alpha = (\vee_\alpha E_{i,\alpha}, (\delta_i \circ (\vee e_{i,\alpha})))$  where  $\delta_i$  is the canonical isomorphism  $T \wedge (\vee_\alpha E_{i,\alpha}) \rightarrow \vee_\alpha (T \wedge E_{i,\alpha})$ . One can verify easily that it is also the direct sum in  $H[[T^{-1}]]$  i.e. that for any spectrum  $\mathbf{F}$  one has

$$\text{Hom}_{H[[T^{-1}]]}(\oplus_\alpha \mathbf{E}_\alpha, \mathbf{F}) = \prod_\alpha \text{Hom}_{H[[T^{-1}]]}(\mathbf{E}_\alpha, \mathbf{F})$$

For a pointed space  $(X, x)$  denote by  $\Sigma_T^\infty(X, x)$  the  $T$ -spectrum  $(T^{\wedge n} \wedge (X, x), Id)$ . The functor  $\Sigma_T^\infty$  takes weak equivalences to stable weak equivalences and for any collection of spaces we have a canonical isomorphism

$\Sigma_T^\infty(\bigvee_\alpha(X_\alpha, x_\alpha)) \rightarrow \bigoplus_\alpha \Sigma_T^\infty(X_\alpha, x_\alpha)$ . One can also verify easily that the functor  $H \rightarrow H[[T^{-1}]]$  admits a canonical decomposition of the form  $H \rightarrow H[[T^{-1}]] \rightarrow H[[T^{-1}]]$  where the second functor takes  $((X, x), n)$  to the spectrum

$$\Sigma^\infty((X, x), n)_i = \begin{cases} pt & \text{for } i < -n \\ T^{\wedge(i+n)} & \text{for } i \geq -n \end{cases} \tag{15}$$

The following result is the main technical thing one needs to know to be able to use the construction described above.

**THEOREM 5.2** *For any space of finite type  $(X, x)$  and any  $T$ -spectrum  $\mathbf{E}$  one has*

$$Hom_{H[[T^{-1}]]}(\Sigma_T^\infty(X, x), \mathbf{E}) = \text{colim}_n Hom_H(T^{\wedge n} \wedge (X, x), E_n)$$

where the maps in the inductive system are defined by the assembly morphisms of  $\mathbf{E}$ .

**COROLLARY 5.3** *Let  $(X, x), (Y, y)$  be spaces of finite type. Then one has*

$$Hom_{H[[T^{-1}]]}(\Sigma_T^\infty(X, x), \Sigma_T^\infty(Y, y)) = \text{colim}_n Hom_H(T^{\wedge n} \wedge (X, x), T^{\wedge n} \wedge (Y, y))$$

For a  $T$ -spectrum  $\mathbf{E}$  define  $\mathbf{E}[1]$  to be the spectrum  $(E_i \wedge S_s^1, e_i \wedge Id_{S_s^1})$ . For a morphism of  $T$ -spectra  $f : \mathbf{E} \rightarrow \mathbf{F}$  define the associated cofibration sequence

$$\mathbf{E} \rightarrow \mathbf{F} \rightarrow \text{cone}(f) \rightarrow \mathbf{E}[1]$$

in exactly the same way as we did for morphisms of pointed spaces in the previous section setting  $\mathbf{E} \wedge \Delta_S^1$  to be the spectrum of the form  $(E_i \wedge \Delta_S^1, e_i \wedge Id_{\Delta_S^1})$ . A sequence of morphisms in  $H[[T^{-1}]]$  is called a *distinguished triangle* if it is isomorphic to the image of the cofibration sequence for a morphism in  $Sp(\text{Sp}_\bullet, T)$ .

**PROPOSITION 5.4** *For any pointed space  $T$  of finite type the category  $H[[S_s^1 \wedge T']^{-1}]$  is additive and the shift functor and the class of distinguished triangles defined above satisfy the axioms of a triangulated structure.*

The following technical result allows one to apply the general representability theorems proven in [16], [17], [18] to the stable homotopy category of algebraic varieties.

**PROPOSITION 5.5** *For any space of finite type  $T$  and any Noetherian base scheme  $S$  the category  $H[[T^{-1}]]$  is compactly generated and suspension spectra of spaces of finite type are compact. If in addition  $S$  can be covered by affine open subsets  $U_i = \text{Spec}(R_i)$  such that  $R_i$  are countable rings then the subcategory of compact objects in  $H[[T^{-1}]]$  is equivalent to a countable category.*

**THEOREM 5.6** *Let  $T$  be a space of finite type such that the cyclic permutation on  $T^{\wedge 3}$  equals identity in  $H[[T^{-1}]]$ . Then the category  $H[[T^{-1}]]$  has a symmetric monoidal structure  $(\wedge, \mathbf{1})$  such that:*



1. for a spectrum  $\mathbf{E}$  and a pointed space  $(X, x)$  the spectrum  $\mathbf{E} \wedge \Sigma_T^\infty(X, x)$  is canonically isomorphic to  $(E_i \wedge (X, x), e_i \wedge Id_{(X, x)})$
2. for a collection of spectra  $\mathbf{E}_\alpha$  and a spectrum  $\mathbf{F}$  there is a canonical isomorphism

$$(\bigoplus_\alpha \mathbf{E}_\alpha) \wedge \mathbf{F} \rightarrow \bigoplus_\alpha (\mathbf{E}_\alpha \wedge \mathbf{F})$$

3. for a cofibration sequence  $\mathbf{E} \rightarrow \mathbf{F} \rightarrow \text{cone}(f) \xrightarrow{\epsilon} \mathbf{E}[1]$  and a spectrum  $\mathbf{G}$  the sequence  $\mathbf{E} \wedge \mathbf{G} \rightarrow \mathbf{F} \wedge \mathbf{G} \rightarrow \text{cone}(f) \wedge \mathbf{G} \rightarrow \mathbf{E} \wedge \mathbf{G}[1]$  where the last morphism is the composition of  $\epsilon \wedge Id_G$  with the canonical isomorphism  $\mathbf{E}[1] \wedge \mathbf{G} \rightarrow (\mathbf{E} \wedge \mathbf{G})[1]$  is isomorphic to a cofibration sequence.

All the results of this section except for Theorem 5.6 have simple proofs. I know of two ways to prove Theorem 5.6. One is to explicitly construct the symmetric monoidal structure on  $H[[T^{-1}]]$  starting with the obvious badly defined smash product in  $Sp(Spc_\bullet, T)$  and checking that all the ambiguities disappear when one passes to the homotopy category. In the case of the ordinary topological stable category a detailed exposition of this approach is given for example in [1, pp. 158-190]. It takes Adams thirty pages to verify that nothing goes wrong and it is terrible. Also it is hard to see that the cyclic permutation condition is indeed the key. Another way to prove Theorem 5.6 is to use the idea of symmetric spectra introduced recently by Jeff Smith (see [8] for an exposition in the context of simplicial sets and topological spaces). In this approach one defines first the category  $Sp^\Sigma(Spc_\bullet, T)$  of so called symmetric T-spectra and the associated stable homotopy category which I denote  $H[[T^{-1}, \Sigma]]$ . These categories have symmetric monoidal structures for any  $T$  and one can construct a functor  $H[[T^{-1}]] \rightarrow H[[T^{-1}, \Sigma]]$  which commutes in the obvious sense with the suspension spectrum functors. The cyclic permutation condition is then necessary and sufficient for this functor to be an equivalence [19].

This ends our discussion of the general stabilization construction  $H \mapsto H[[T^{-1}]]$ . Now we specialize to the only case which we are really interested in namely  $T = S_s^1 \wedge S_t^1$ . For the reasons which will become clear in the next section when we consider concrete examples of spectra we choose  $(\mathbf{P}^1, \infty)$  as the model for  $S_s^1 \wedge S_t^1$  used in the definition of  $SH$ .

DEFINITION 5.7 *The stable  $\mathbf{A}^1$ -homotopy category over  $S$  is the category*

$$SH(S) = H_\bullet^{\mathbf{A}^1}(S)[[(\mathbf{P}^1, \infty)^{-1}]]$$

We denote  $SH(S)$  simply by  $SH$  and the suspension spectrum functor  $\Sigma_{(\mathbf{P}^1, \infty)}^\infty$  by  $\Sigma^\infty$ . The canonical functor  $SW \rightarrow SH$  described on objects by (15) respects both the symmetric monoidal and the triangulated structures. In particular Propositions 4.11-4.13 have straightforward analogs in  $SH$  and in view of Theorem 5.2 the same is true for the Connectivity Theorem 4.14.

According to Theorem 5.6(1) and Lemma 4.1 for any  $n \geq 0$  we have canonical isomorphisms

$$\Sigma^\infty(S_s^n) \wedge \Sigma^\infty(S_t^n, -n) \cong \mathbf{1}; \quad \Sigma^\infty(S_t^n) \wedge \Sigma^\infty(S_s^n, -n) \cong \mathbf{1}$$

and therefore we can define objects  $S_s^n$  and  $S_t^n$  of  $SH$  for all  $n \in \mathbf{Z}$  as follows

$$S_s^n = \begin{cases} \Sigma^\infty(S_s^n) & \text{for } n \geq 0 \\ \Sigma^\infty(S_t^n, -n) & \text{for } n \leq 0 \end{cases} \quad S_t^n = \begin{cases} \Sigma^\infty(S_t^n) & \text{for } n \geq 0 \\ \Sigma^\infty(S_s^n, -n) & \text{for } n \leq 0 \end{cases} \quad (16)$$

6 THREE COHOMOLOGY THEORIES

To any object  $\mathbf{E}$  of  $SH$  we assign a *cohomology theory*  $E^{p,q}(-)$  and a homology theory  $E_{p,q}(-)$  on  $Spc_\bullet$  given by

$$E^{p,q}(X, x) = Hom_{SH}(\Sigma^\infty(X, x), S_s^{p-q} \wedge S_t^q \wedge \mathbf{E})$$

$$E_{p,q}(X, x) = Hom_{SH}(S_s^{p-q} \wedge S_t^q, \mathbf{E} \wedge \Sigma^\infty(X, x))$$

The reason for this somewhat strange indexing is hidden in connections with the theory of motives. Propositions 4.11-4.13 together with Lemma 4.7 imply that any cohomology or homology theory constructed in this way has three types of long exact sequences called respectively Mayer-Vietoris, Gysin and blow-up exact sequences.

One can give a formal definition of a cohomology theory as a collection of functors  $Spc_\bullet \rightarrow Ab$  satisfying some simple axioms and use Theorem 5.5 together with [16, Th. 3.1] to prove that any such theory is of the form  $E^{p,q}$  for an object  $\mathbf{E}$  of  $SH$ . Usefulness of this construction is restricted by the fact that in any formulation I know one has to start with a family of functors defined on the category of all spaces or, at least, on the subcategory of spaces of finite type and not just on the category of smooth schemes over  $S$ . On the other hand as the example of algebraic cobordism considered below shows the direct correspondence  $\mathbf{E} \mapsto (E^{p,q}(-))_{p,q \in \mathbf{Z}}$  allows one to give simple definition for theories which would otherwise be hard to construct. The possibility to use the stable homotopy category to produce theories with desired properties is one of the key ingredients in the proof of the Milnor conjecture given in [26].

6.1 MOTIVIC COHOMOLOGY

Let us first define the *Eilenberg-MacLane spectrum*  $\mathbf{H}_\mathbf{Z}$  which represents a theory  $H_\mathbf{Z}^{p,q}(-) = H^{p,q}(-, \mathbf{Z})$  called *motivic cohomology* (with integral coefficients). It is an analog of ordinary cohomology in the  $\mathbf{A}^1$ -homotopy theory. The theory of motivic cohomology described here was developed in [5] and [25] before the  $\mathbf{A}^1$ -homotopy theory was introduced. The first definition in terms of the stable homotopy category was given in [26]. The only technical result about motivic cohomology which we can not obtain as a specialization of general results in  $\mathbf{A}^1$ -homotopy theory is Theorem 6.2. If we knew how to prove this theorem without going through all the moves of [24] and [5] a major part of these papers would become obsolete at least as far as the theory of motivic cohomology is concerned. But we do not.

The tricky part in getting the  $\mathbf{A}^1$ -analog of the topological Eilenberg-MacLane spectrum is to guess what the Eilenberg-MacLane spaces in  $Spc_\bullet$  are. The obvious

idea to take a space  $K(\mathbf{Z}, n)$  which has the property that for any connected  $U$

$$\pi_{i,U}(K(\mathbf{Z}, n)) = \begin{cases} 0 & \text{for } i \neq n \\ \mathbf{Z} & \text{for } i = n \end{cases} \quad (17)$$

does not work. To build a spectrum out of  $K(\mathbf{Z}, n)$ 's we would have to specify assembly morphisms  $(\mathbf{P}^1, \infty) \wedge K(\mathbf{Z}, n) \rightarrow K(\mathbf{Z}, n+1)$  but a simple computation shows that any morphism of the form  $(\mathbf{P}^1, \infty) \wedge (X, x) \rightarrow K(\mathbf{Z}, n+1)$  is trivial in the  $\mathbf{A}^1$ -homotopy category. The correct approach was discovered by A. Suslin around 1987. The idea is to define the  $\mathbf{A}^1$ -analogs of the Eilenberg-MacLane spaces through the Dold-Thom Theorem. For a pointed topological space  $(T, *)$  let  $Symm^\infty(T, *)$  be its infinite symmetric product  $Symm^\infty(T, *) = \text{colim}_n Symm^n(T, *)$  where  $Symm^n(T, *) = (T, *)^{\times n} / \Sigma_n$  and the maps  $Symm^n \rightarrow Symm^{n+1}$  send  $(x_1, \dots, x_n)$  to  $(x_1, \dots, x_n, *)$ . The Dold-Thom Theorem [4] says that for a connected pointed CW-complex  $(T, *)$  the space  $Symm^\infty(T, *)$  is weakly equivalent to the product  $\prod_{i \geq 0} K(H_i(T), i)$  where  $H_i(T)$  are the integral homology of  $T$ . To formulate Dold-Thom Theorem for spaces which are not necessarily connected one considers  $Symm^\infty(T, *)$  as a topological monoid with respect to the obvious addition and takes its group completion  $(Symm^\infty(T, *))^+$ . The general Dold-Thom theorem then says that

$$(Symm^\infty(T, *))^+ \cong \prod_{i \geq 0} K(H_i(T), i)$$

for any  $T$  and that in the case of a connected  $T$  the group completion does not change the homotopy type of  $Symm^\infty(T, *)$ . In particular one way to define  $K(\mathbf{Z}, n)$  for all  $n \geq 0$  is to set

$$K(\mathbf{Z}, n) = (Symm^\infty(S^n))^+$$

Once we understand the correct analog of the symmetric product construction in the  $\mathbf{A}^1$ -context this definition works perfectly well and gives us Eilenberg-MacLane spaces which fit together into the Eilenberg-MacLane spectrum representing motivic cohomology.

Assume for a moment that the base scheme  $S$  is regular. For a smooth scheme  $X$  over  $S$  and a smooth connected scheme  $U$  define  $c(U, X)$  as the free abelian group generated by closed irreducible subsets  $Z$  of  $U \times X$  which are finite and surjective over  $U$ . For any morphism  $U_1 \rightarrow U_2$  over  $S$  one can define the base change homomorphism  $c(U_2, X) \rightarrow c(U_1, X)$  which makes  $c(-, X)$  into a contravariant functor from  $Sm/S$  to abelian groups. One can verify easily that this functor takes elementary distinguished squares to Cartesian squares i.e. that it is a *space* in the sense of our definition. We consider it as a pointed space with the distinguished point given by zero and denote by  $L(X)$ . If  $S$  is not regular the correct definition of  $c(U, X)$  and  $L(X)$  becomes more technical and requires the theory of realtive equidimensional cycles developed in [22]. In the notations of that paper  $c(U, X) = c(U \times_S X/U, 0)$  ([22, p.30]). The graph of any morphism  $U \rightarrow X$  is an element of  $c(U, X)$  which gives us canonical maps  $Hom(U, X) \rightarrow c(U, X)$  i.e. a morphism of spaces  $X \rightarrow L(X)$ .

It turns out that the space  $L(X)$  plays the role of  $(Symm^\infty(X_+))^+$  in our context. Intuitively one can see this as follows. Assume  $S = Spec(k)$  and  $X$  is a smooth variety over  $k$ . Consider first the subspace  $L^{eff}(X)$  in  $L(X)$  which consists of formal linear combinations of closed subsets with nonnegative coefficients. A point in  $L^{eff}(X)$  i.e. an element in  $Hom_{Spec}(pt, L^{eff}(X)) = c^{eff}(Spec(k), X)$  is, by definition, a formal linear combination of closed points of  $X$  with nonnegative coefficients which is exactly what one would expect from points of the infinite symmetric product. The whole space  $L(X)$  is clearly obtained from  $L^{eff}(X)$  by the naive group completion with respect to the obvious abelian monoid structure on  $L^{eff}(X)$ . A detailed discussion of how  $L(X)$  relates to usual symmetric products for quasi-projective varieties over a field  $k$  can be found in [21, §6] and especially in [21, Th. 6.8] where

$$z_0^{eff}(Z) = \begin{cases} L(Z) & \text{if } char(k) = 0 \\ L(Z)[1/char(k)] & \text{if } char(k) > 0 \end{cases} \tag{18}$$

To define Eilenberg-MacLane spaces we should apply this construction to our spheres  $S_s^n \wedge S_t^m$ . To do it we have to say what  $L(X)$  is for a space which is not a smooth scheme. Instead of giving a general definition we only consider spaces of the form  $X/(\cup_{i=1}^n Z_i)$  where  $X$  is a smooth scheme and  $Z_i$ 's are smooth subschemes in  $X$  such that all the intersections of  $Z_i$ 's are also smooth over  $S$ . We call such spaces scheme-like. This class includes in particular the spaces  $S_s^n \wedge S_t^m$  for all  $n, m \geq 0$  and it is closed under smash products. We set

$$L(X/(\cup_{i=1}^n Z_i)) = (L(X)/(\sum_{i=1}^n L(Z_i)))_{ab}$$

where the subscript  $ab$  indicates that we take the quotient in the category of abelian group spaces and then forget the abelian group structure. It can be shown that any morphism of scheme-like spaces  $f : X \rightarrow Y$  induces homomorphism  $L(f) : L(X) \rightarrow L(Y)$  and that for an **A<sup>1</sup>**-weak equivalence  $f$  the morphism  $L(f)$  is also an **A<sup>1</sup>**-weak equivalence.

**DEFINITION 6.1**  $K(\mathbf{Z}(n), 2n) = L((\mathbf{P}^1, \infty)^{\wedge n})$

The notation  $K(\mathbf{Z}(n), 2n)$  has the same origin as the indexing in the definition of  $E^{p,q}$ 's and as Theorem 6.3 below shows is consistent with this indexing. In view of Lemma 4.1 and previous discussion this definition reads

$$K(\mathbf{Z}(n), 2n) \cong (Symm^\infty((S_s^1 \wedge S_t^1)^{\wedge n}))^+$$

One can show that the “wrong” Eilenberg-MacLane space  $K(\mathbf{Z}, n)$  specified by (17) is weakly equivalent to  $L(S_s^n)$ .

For any smooth schemes  $X, Y$  over  $S$  there is a bilinear morphism  $L(X) \times L(Y) \rightarrow L(X \times Y)$  defined by external product of relative cycles (see [22, p. 54]) which is natural in  $X$  and  $Y$ . This implies that for scheme-like spaces  $X, Y$  we have a canonical morphism  $L(X) \wedge L(Y) \rightarrow L(X \wedge Y)$ . In particular we have canonical morphisms

$$m_{m,n} : K(\mathbf{Z}(m), 2m) \wedge K(\mathbf{Z}(n), 2n) \rightarrow K(\mathbf{Z}(n + m), 2n + 2m)$$

Composing  $m_{1,n}$  with the morphism  $i \wedge Id$  where  $i$  is the canonical morphism  $(\mathbf{P}^1, \infty) \rightarrow L(\mathbf{P}^1, \infty)$  we get the *assembly morphisms* of the Eilenberg-MacLane spectrum  $\mathbf{H}_{\mathbf{Z}}$

$$e_n : (\mathbf{P}^1, \infty) \wedge K(\mathbf{Z}(n), 2n) \rightarrow K(\mathbf{Z}(n+1), 2n+2)$$

The main technical result about the motivic cohomology spectrum is the following theorem. This is the only theorem in the paper for which we do not know a good proof.

**THEOREM 6.2** *Let  $S$  be a smooth variety over a field  $k$  of characteristic zero. Then the spaces  $K(\mathbf{Z}(n), 2n)$  are quasi-fibrant (Definition 3.9) and the morphisms*

$$\tilde{e}_n : K(\mathbf{Z}(n), 2n) \rightarrow \Omega_{(\mathbf{P}^1, \infty)}^1 K(\mathbf{Z}(n+1), 2n+2)$$

*adjoint to the assembly morphisms are  $\mathbf{A}^1$ -weak equivalences.*

Conjecturally the statement of Theorem 6.2 should be true for any regular base scheme  $S$ . There is an example of a normal surface over  $\mathbf{C}$  with an isolated nonrational singularity for which the second half of the theorem does not hold. The only reason the condition on the characteristic of the base field appears in the theorem is because the proof is based on techniques developed in [5] and in particular requires [5, Lemma 5.4] which in turn uses Hironaka's resolution of singularities. Theorem 6.3 has the following corollary.

**THEOREM 6.3** *Let  $U$  be a smooth quasi-projective variety over a field of characteristic zero. Then for any  $n, i \geq 0$  there is a canonical isomorphism*

$$H_{\mathbf{Z}}^{2n-i,n}(U_+) = \pi_i(\text{Sing}_*(K(\mathbf{Z}(n), 2n)(U), *))$$

The groups on the right hand side can be easily identified with the motivic cohomology groups defined in [5, Definition 9.2] where the notation  $H^p(-, \mathbf{Z}(q))$  is used instead of  $H_{\mathbf{Z}}^{p,q}(-)$ . Together with [5, Th. 8.2, Th. 8.3(1)] and [25, Prop. 4.2.9] this gives the following comparison between our motivic cohomology and higher Chow groups introduced by S. Bloch in [2].

**THEOREM 6.4** *Let  $U$  be a smooth quasi-projective variety over a field of characteristic zero. Then there are canonical isomorphisms*

$$H_{\mathbf{Z}}^{p,q}(U_+) = CH^q(U, 2q-p)$$

## 6.2 ALGEBRAIC K-THEORY

The next cohomology theory which we are going to discuss is *algebraic K-theory*. This theory is the best known one of the three theories considered here and it is also the least convenient one to define in terms of the stable homotopy category. The first definition of higher K-groups which works properly for all Noetherian schemes was given by B. Thomason in [23]. An  $\mathbf{A}^1$ -homotopy invariant version of algebraic K-theory which agrees with Thomason K-theory for regular schemes

was defined by C. Weibel in [27]. What follows gives a description of a spectrum **BGL** which represents a theory which after reindexing coincides on  $Sm/S$  with Weibel's homotopy K-theory. The construction given here is very ugly and I am sure that there exists a better way to do it.

Denote by  $BGL(d)$  the infinite Grassmannian  $BGL(d) = colim_{N \geq d} G(d, N)$  where  $G(d, N)$  is the Grassmannian of linear subspaces of dimension  $d$  in the standard linear space of dimension  $N$  which we denote by  $\mathcal{O}^N$ . The maps  $G(d, N) \rightarrow G(d, N + 1)$  take  $L \subset \mathcal{O}^N$  to  $L \oplus \{0\} \subset \mathcal{O}^N \oplus \mathcal{O}$ . We have canonical monomorphisms  $BGL(d) \rightarrow BGL(1 + d)$  which take  $L \subset \mathcal{O}^N$  to  $\mathcal{O} \oplus L \subset \mathcal{O} \oplus \mathcal{O}^N$  and we denote by  $BGL$  the colimit  $colim_{d \geq 0} BGL(d)$ . The spectrum representing algebraic K-theory is defined as follows

$$\mathbf{BGL} = (Ex^{\mathbf{A}^1}(BGL \times \mathbf{Z}), e : (\mathbf{P}^1, \infty) \wedge Ex^{\mathbf{A}^1}(BGL \times \mathbf{Z}) \rightarrow Ex^{\mathbf{A}^1}(BGL \times \mathbf{Z}))$$

where  $BGL \times \mathbf{Z} = \coprod_{i \in \mathbf{Z}} BGL$  and  $Ex^{\mathbf{A}^1}(BGL \times \mathbf{Z})$  is a fibrant replacement of  $BGL \times \mathbf{Z}$  in the sense of the closed model structure of Theorem 3.7. The reason we have to take  $Ex^{\mathbf{A}^1}(BGL \times \mathbf{Z})$  instead of  $BGL \times \mathbf{Z}$  itself is that the only way I know to define the assembly morphism is to define first a morphism  $\bar{e} : (\mathbf{P}^1, \infty) \wedge (BGL \times \mathbf{Z}) \rightarrow BGL \times \mathbf{Z}$  in the homotopy category and then say that any morphism in the homotopy category with values in a fibrant object can be lifted to the category of spaces. It is a little ugly but it works. To specify  $e$  we will use the following result proven in [14].

**THEOREM 6.5** *For any smooth scheme  $X$  over  $S$  and any  $i \geq 0$  there is a canonical map*

$$K_i(X) \rightarrow Hom_{H_\bullet}(S_s^i \wedge X_+, BGL \times \mathbf{Z})$$

*which is a bijection if  $S$  is regular (the  $K$ -groups on the left are Thomason  $K$ -groups [23]).*

For a pointed scheme  $(X, x)$  denote by  $K_n(X, x)$  the subgroup of  $K_n(X)$  which consists of elements vanishing on  $x$ . For a pair of pointed smooth schemes  $(X, x), (Y, y)$  denote by  $K_i((X, x) \wedge (Y, y))$  the subgroup in  $K_i(X \times Y)$  which consists of elements vanishing on  $X \times \{y\} \subset X \times Y$  and on  $\{x\} \times Y \subset X \times Y$ . Note that this is always a direct summand in  $K_i(X \times Y)$ . Theorem 6.5 has the following corollary.

**COROLLARY 6.6** *Let  $(X, x), (Y, y)$  be pointed smooth schemes over  $S$ . Then for any  $i \geq 0$  there is a canonical map*

$$K_i((X, x) \wedge (Y, y)) \rightarrow Hom_{H_\bullet}(S_s^i \wedge (X, x) \wedge (Y, y), BGL \times \mathbf{Z})$$

*which is a bijection if  $S$  is regular.*

To define the assembly morphism of the spectrum **BGL** we want to use Corollary 6.6 to compute the set of morphisms  $(\mathbf{P}^1, \infty) \wedge (BGL \times \mathbf{Z}) \rightarrow BGL \times \mathbf{Z}$  in the  $\mathbf{A}^1$ -homotopy category. Unfortunately  $BGL$  is not a smooth scheme but a colimit of filtered system of such schemes which makes us to use the following lemma.

LEMMA 6.7 *Let  $(X_n, i_n : (X_n, x_n) \rightarrow (X_{n+1}, x_{n+1}))$  be an inductive system of pointed spaces such that all the morphisms  $i_n$  are monomorphisms and  $(Y, y)$  be a pointed space such that all the maps*

$$\text{Hom}_H(S_s^1 \wedge (X_{n+1}, x_{n+1}), (Y, y)) \rightarrow \text{Hom}_H(S_s^1 \wedge (X_n, x_n), (Y, y))$$

*induced by  $\text{Id} \wedge i_n$  are surjective. Then the canonical map*

$$\text{Hom}_H(\text{colim}_n (X_n, x_n), (Y, y)) \rightarrow \text{lim}_n \text{Hom}_H((X_n, x_n), (Y, y))$$

*is bijective.*

Projective bundle theorem for algebraic K-theory together with standard geometrical constructions imply that the embeddings of Grassmannians  $G(d, N) \rightarrow G(1+d, 1+N+1)$  induce surjections of K-groups  $K_n(G(1+d, 1+N+1)) \rightarrow K_n(G(d, N))$  for all  $n \in \mathbf{Z}$ . The same projective bundle theorem applied to the trivial bundle of dimension one implies that  $K_n((\mathbf{P}^1, \infty) \wedge (X, x)) = K_n(X, x)$  for any pointed smooth scheme  $(X, x)$  over  $S$ . Thus Lemma 6.7 implies that for a regular scheme  $S$  one has

$$\begin{aligned} & \text{Hom}_H((\mathbf{P}^1, \infty) \wedge (BGL \times \mathbf{Z}), BGL \times \mathbf{Z}) = \\ & = \text{lim}_d \text{Hom}_H((\mathbf{P}^1, \infty) \wedge (\prod_{i=-d}^d G(d, 2d)), BGL \times \mathbf{Z}) = \\ & \text{lim}_d K_0((\mathbf{P}^1, \infty) \wedge (\prod_{i=-d}^d G(d, 2d))) = \text{lim}_d K_0(\prod_{i=-d}^d G(d, 2d)) = \\ & \text{lim}_d \text{Hom}_H(\prod_{i=-d}^d G(d, 2d), BGL \times \mathbf{Z}) = \text{Hom}_H(BGL \times \mathbf{Z}, BGL \times \mathbf{Z}) \end{aligned}$$

Denote by  $e$  the morphism  $(\mathbf{P}^1, \infty) \wedge (BGL \times \mathbf{Z}) \rightarrow BGL \times \mathbf{Z}$  corresponding under these identifications to the identity morphism of  $BGL \times \mathbf{Z}$  and define the assembly morphism of the spectrum  $\mathbf{BGL}$  as a morphism of spaces which projects to  $e$  in the homotopy category. This defines  $\mathbf{BGL}$  for regular base schemes  $S$ . To get  $\mathbf{BGL}$  for any  $S$  one uses the inverse image functor on the homotopy categories associated with the canonical morphism  $S \rightarrow \text{Spec}(\mathbf{Z})$ . As an easy corollary of this construction of  $\mathbf{BGL}$  we get the following *periodicity theorem*.

THEOREM 6.8 *There is a canonical isomorphism  $\mathbf{BGL} = S_s^1 \wedge S_t^1 \wedge \mathbf{BGL}$ .*

Thus from the point of view of the  $\mathbf{A}^1$ -theory algebraic K-theory is periodic with period  $(2, 1)$  which is why it is usually written with only one index instead of two. While the construction of  $\mathbf{BGL}$  presented here is not very nice it is actually easy to prove comparison theorems with it.

THEOREM 6.9 *For any Noetherian base scheme  $S$  and any smooth scheme  $X$  over  $S$  one has canonical isomorphisms*

$$BGL^{p,q}(X_+) = KH_{2q-p}(X)$$

where  $KH$  is the homotopy  $K$ -theory of [27]. In particular for a regular base  $S$  one has

$$BGL^{p,q}(X_+) = K_{2q-p}(X)$$

where  $K$  is the  $K$ -theory of [23].

### 6.3 ALGEBRAIC COBORDISM

Algebraic cobordism was introduced in [26] as one of the tools necessary for the proof of the Milnor conjecture. According to our current understanding it is the universal cohomology theory which has direct image homomorphisms for all smooth proper morphisms. It is represented by a spectrum  $\mathbf{MGL} = (MGL(n), e_n)$  completely analogous to the Thom spectrum representing complex cobordism in the topological homotopy theory.

Recall that for a vector bundle  $E$  over  $X$  we defined its Thom space as  $Th(E) = E/(E - s(X))$  where  $s : X \rightarrow E$  is the zero section. For any morphism  $f : X \rightarrow Y$  and a vector bundle  $E$  over  $Y$  we have a canonical morphism of spaces  $Th(f^*E) \rightarrow Th(E)$ . Let  $E_{n,N}$  be the universal bundle over the Grassmannian  $G(n, N)$ . The embeddings  $G(n, N) \rightarrow G(n, N + 1)$  induce morphisms  $Th(E_{n,N}) \rightarrow Th(E_{n,N+1})$  and we define  $MGL(n)$  as  $\text{colim}_N Th(E_{n,N})$ . To define assembly morphisms note that if  $\mathcal{O}$  is the trivial bundle of dimension one then  $Th(\mathcal{O} \oplus E) = (\mathbf{A}^1/\mathbf{A}^1 - \{0\}) \wedge Th(E)$ . For the embeddings  $f : G(n, N) \rightarrow G(1 + n, 1 + N)$  we have canonical isomorphisms  $f^*(E_{1+n,1+N}) = \mathcal{O} \oplus E_{n,N}$  which implies that we have canonical morphisms  $e'_n : (\mathbf{A}^1/\mathbf{A}^1 - \{0\}) \wedge MGL(n) \rightarrow MGL(n + 1)$ . Since the elementary distinguished square corresponding to the standard covering  $\mathbf{P}^1 = \mathbf{A}^1 \cup \mathbf{A}^1$  is a pushforward square the morphism of quotient spaces  $\mathbf{A}^1/(\mathbf{A}^1 - \{0\}) \rightarrow \mathbf{P}^1/(\mathbf{P}^1 - \{0\})$  is an isomorphism. The inverse gives us a morphism  $\phi : (\mathbf{P}^1, \infty) \rightarrow \mathbf{A}^1/(\mathbf{A}^1 - \{0\})$ . We define the *assembly morphisms* of the Thom spectrum  $\mathbf{MGL}$  as compositions  $e_n = e'_n \circ (\phi \wedge Id)$ .

Since algebraic cobordism is a new theory we can not formulate here a comparison theorem as we have done with motivic cohomology and algebraic  $K$ -theory. Instead I will end this section with a conjecture which describes a part of algebraic cobordisms in terms of the usual complex cobordism ring  $MU^*$ .

**CONJECTURE 1** *For any  $S$  there is a natural homomorphism  $\bigoplus_{i=-\infty}^{\infty} MU^{2i} \rightarrow \bigoplus_{i=-\infty}^{\infty} MGL^{2i,i}(S)$  which is an isomorphism if  $S$  is local and regular.*

## 7 CONCLUDING REMARKS

This paper outlines the very basics of the  $\mathbf{A}^1$ -homotopy theory. One reason I did not say more about concrete computations such as the description of the motivic Steenrod algebra is that at the moment these computations can only be done in the case when  $S$  is a variety over a field of characteristic zero. This is partly due to the conditions of Theorem 6.2 and partly to technical difficulties in the proof of Spanier-Whitehead duality.

One of the two major directions of current work on the theory is to eliminate this restriction. There are two sources of new techniques which I believe will allow us to do it. One is related to the study of functoriality of the stable homotopy



categories with respect to  $S$ . There is a theory here which is largely parallel to the functoriality for the constructible sheaves in the étale topology [13, Ch.VI]. It allows in particular to prove the Spanier-Whitehead duality for smooth proper schemes over any base. However, just as in the étale theory there are certain statements which apparently require some kind of resolution of singularities (in the étale case this is for example the theorem saying that  $\mathbf{R}p_*(\mathbf{Z}/n)$  is constructible for any morphism  $p$  of finite type [13, VI.5.7]). Surprisingly the same kind of problems comes up when one tries to generalize Theorem 6.2. I am rather optimistic about these problems at the moment. My optimism is mostly based on the amazing proof which Spencer Bloch gave for his localization theorem for higher Chow groups in [3]. It seems that he found a way to use Spivakovsky's solution of Hironaka's polyhedra game ([20]) instead of resolution of singularities to deal with problems essentially similar to the ones mentioned above.

The second main direction of current work can be described as an attempt to find an algebro-combinatorial description of  $\mathbf{A}^1$ -homotopy types. We do have a very hypothetical theory of *rational* homotopy type. The rational homotopy type of a scheme  $S$  is a differential graded Hopf algebra (commutative, not cocommutative)  $\mathcal{H}_{\mathbf{Q}}(S)$  over  $\mathbf{Q}$  such that the derived category of modules over  $\mathcal{H}_{\mathbf{Q}}(S)$  is equivalent to the triangulated subcategory  $DM^{lc}(S, \mathbf{Q})$  of local systems in the derived category  $DM(S, \mathbf{Q})$  of modules over the Eilenberg-MacLane spectrum  $\mathbf{H}_{\mathbf{Q}}$  over  $S$ .

In topological context  $\mathcal{H}_{\mathbf{Q}}(T)$  is the differential graded Hopf algebra associated with the cosimplicial Hopf algebra  $C^*(\Omega^1 T)$  of singular cochains on the first loop space of  $T$  and  $DM^{lc}(T, \mathbf{Q})$  is the full subcategory of complexes with locally constant cohomology sheaves in the derived category of constructible sheaves of  $\mathbf{Q}$ -vector spaces on  $T$ .

In the particular case  $S = \text{Spec}(k)$  the (weak)  $K(\pi, 1)$ -conjecture says that  $\mathcal{H}_{\mathbf{Q}}(S)$  is the Hopf algebra of functions on a proalgebraic group  $\text{Gal}_{\mathcal{M}, \mathbf{Q}}(k)$  (in particular it sits entirely in grading zero). This group is called the motivic Galois group of  $k$ . The category  $DM^{lc}(S, \mathbf{Q})$  is in this case equivalent to the whole category  $DM(S, \mathbf{Q})$  and the equivalence of the derived categories mentioned above becomes the known hypothetical correspondence between motives and representations of the motivic Galois group [15]. This wonderful picture whose origins go back to Grothendieck's idea of motives ([7], [12], [15]) must have an analog for integral homotopy types. All my attempts to find such an analog even in the case when  $S$  is the spectrum of an algebraically closed field of characteristic zero so far failed. We have a lot of knowledge about torsion effects in the motivic category and this knowledge does not want to fit into any nice scheme.

## REFERENCES

- [1] J. F. Adams. *Stable homotopy and generalized homology*. University of Chicago Press, 1974.
- [2] S. Bloch. Algebraic cycles and higher K-theory. *Adv. in Math.*, 61:267–304, 1986.

- [3] S. Bloch. The moving lemma for higher Chow groups. *J. Algebr. Geom.*, 3(3):537–568, Feb. 1994.
- [4] A. Dold and R. Thom. Quasifaserungen und unendliche symmetrische Produkte. *Ann. of Math.*, 67:230–281, 1956.
- [5] E. M. Friedlander and V. Voevodsky. Bivariant cycle cohomology. <http://www.uiuc.edu/K-theory>, (75), 1995.
- [6] S. I. Gelfand and Yu. I. Manin. *Methods of homological algebra*. Springer-Verlag, Berlin, 1996.
- [7] A. Grothendieck. Standard conjectures on algebraic cycles. In *Algebraic geometry. International Colloq., Tata Inst., Bombay 1968*, pages 193–199. Oxford Univ. Press, London, 1969.
- [8] M. Hovey, B. Shipley, and J. Smith. Symmetric spectra. <http://hopf.math.purdue.edu/pub/Hovey-Shipley-Smith/>, 1998.
- [9] J.F. Jardine. Algebraic homotopy theory. *Canadian J. Math.*, 33(2):302–319, 1981.
- [10] J.F. Jardine. Algebraic homotopy theory and some homotopy groups of algebraic groups. *C. R. Math. Rep. Acad. Sci. Canada*, 3(4):191–196, 1981.
- [11] S. MacLane. *Categories for working mathematician*, volume 5 of *Graduate texts in Mathematics*. Springer-Verlag, 1971.
- [12] Yu. Manin. Motifs and monoidal transformations. *Math. of the USSR - Sbornik*, 6(4):439–470, 1968.
- [13] J.S. Milne. *Etale Cohomology*. Princeton Univ. Press, Princeton, NJ, 1980.
- [14] F. Morel and V. Voevodsky.  $\mathbf{A}^1$ -homotopy theory of schemes. *Preprint*, 1998.
- [15] *Motives*, volume 54-55 of *Proc. of Symp. in Pure Math.* AMS, 1994.
- [16] A. Neeman. The Grothendieck duality theorem via Bousfield’s techniques and Brown representability. *J. Amer. Math. Soc.*, 9(1):205–236, 1996.
- [17] A. Neeman. On a theorem of Brown and Adams. *Topology*, 36(3):619–645, 1997.
- [18] A. Neeman. Brown representability for the dual. *Inv. Math.*, 133(1):97–105, 1998.
- [19] J. Smith. Private communication. 1998.
- [20] M. Spivakovsky. A solution to Hironaka’s polyhedra game. In *Arithmetic and Geometry*, volume 2, pages 419–432. Birkhauser, Boston, 1983.
- [21] A. Suslin and V. Voevodsky. Singular homology of abstract algebraic varieties. *Inv. Math.*, 123(1):61–94, 1992.

- [22] A. Suslin and V. Voevodsky. Relative cycles and Chow sheaves. <http://www.math.uiuc.edu/K-theory>, (35), 1994.
- [23] R. Thomason and T. Trobaugh. Higher algebraic K-theory of schemes and of derived categories. In *The Grothendieck festchrift*, volume 3, pages 247–436. Birkhauser, Boston, 1990.
- [24] V. Voevodsky. Homology of schemes II. <http://www.math.uiuc.edu/K-theory>, (34), 1994.
- [25] V. Voevodsky. Triangulated categories of motives over a field. <http://www.math.uiuc.edu/K-theory>, (74), 1995.
- [26] V. Voevodsky. The Milnor Conjecture. *Max-Planck Inst. preprint series or* <http://www.math.uiuc.edu/K-theory> (170), 1996.
- [27] C. Weibel. Homotopy K-theory. In *Algebraic K-theory and algebraic number theory*, volume 83 of *Contemp. Math.*, pages 461–488. AMS, Providence, 1989.

Vladimir Voevodsky  
Department of Mathematics  
Northwestern University  
Evanston IL USA  
vladimir@math.nwu.edu

## WHAT IS MOONSHINE?

RICHARD E. BORCHERDS<sup>1</sup>

This is an informal write up of my talk at the ICM in Berlin. It gives some background to Goddard's talk [Go] about the moonshine conjectures. For other survey talks about similar topics see [B94], [B98], [LZ], [J], [Ge], [Y].

The classification of finite simple groups shows that every finite simple group either fits into one of about 20 infinite families, or is one of 26 exceptions, called sporadic simple groups. The monster simple group is the largest of the sporadic finite simple groups, and was discovered by Fischer and Griess [G]. Its order is

$$\begin{aligned} & 8080, 17424, 79451, 28758, 86459, 90496, 17107, 57005, 75436, 80000, 00000 \\ = & 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \end{aligned}$$

(which is roughly the number of elementary particles in the earth). The smallest irreducible representations have dimensions 1, 196883, 21296876,  $\dots$ . The elliptic modular function  $j(\tau)$  has the power series expansion

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots,$$

where  $q = e^{2\pi i\tau}$ , and is in some sense the simplest nonconstant function satisfying the functional equations  $j(\tau) = j(\tau + 1) = j(-1/\tau)$ . John McKay noticed some rather weird relations between coefficients of the elliptic modular function and the representations of the monster as follows:

$$\begin{aligned} 1 &= 1, \\ 196884 &= 196883 + 1, \\ 21493760 &= 21296876 + 196883 + 1, \end{aligned}$$

where the numbers on the left are coefficients of  $j(\tau)$  and the numbers on the right are dimensions of irreducible representations of the monster. At the time he discovered these relations, several people thought it so unlikely that there could be a relation between the monster and the elliptic modular function that they politely told McKay that he was talking nonsense. The term "monstrous moonshine" (coined by Conway) refers to various extensions of McKay's observation, and in particular to relations between sporadic simple groups and modular functions.

For the benefit of readers who are not native English speakers, I had better point out that "moonshine" is not a poetic terms referring to light from the moon. It means foolish or crazy ideas. (Quatsch in German.) A typical example of its

---

<sup>1</sup>Supported by a Royal Society professorship.

use is the following quotation from E. Rutherford (the discoverer of the nucleus of the atom): “The energy produced by the breaking down of the atom is a very poor kind of thing. Anyone who expects a source of power from the transformations of these atoms is talking moonshine.” (Moonshine is also a name for corn whiskey, especially if it has been smuggled or distilled illegally.)

We recall the definition of the elliptic modular function  $j(\tau)$ . The group  $SL_2(\mathbf{Z})$  acts on the upper half plane  $H$  by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}.$$

A modular function (of level 1) is a function  $f$  on  $H$  such that  $f((a\tau + b)/(c\tau + d)) = f(\tau)$  for all  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ . It is sufficient to assume that  $f$  is invariant under the generators  $\tau \mapsto \tau + 1$  and  $\tau \mapsto -1/\tau$  of  $SL_2(\mathbf{Z})$ . The elliptic modular function  $j$  is the simplest nonconstant example, in the sense that any other modular function can be written as a function of  $j$ . It can be defined as follows:

$$\begin{aligned} j(\tau) &= \frac{E_4(\tau)^3}{\Delta(\tau)} \\ &= q^{-1} + 744 + 196884q + 21493760q^2 + \dots, \end{aligned}$$

$$\begin{aligned} E_4(\tau) &= 1 + 240 \sum_{n>0} \sigma_3(n)q^n \\ &= 1 + 240q + 2160q^2 + \dots \\ (\sigma_3(n) &= \sum_{d|n} d^3), \end{aligned}$$

$$\begin{aligned} \Delta(\tau) &= q \prod_{n>0} (1 - q^n)^{24} \\ &= q - 24q + 252q^2 + \dots. \end{aligned}$$

A modular form of weight  $k$  is a holomorphic function

$$f(\tau) = \sum_{n \geq 0} c(n)q^n$$

on the upper half plane satisfying the functional equation  $f((a\tau + b)/(c\tau + d)) = (c\tau + d)^k f(\tau)$  for all  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ . The function  $E_4(\tau)$  is an Eisenstein series and is a modular form of weight 4, while  $\Delta(\tau)$  is a modular form of weight 12.

The function  $j(\tau)$  is an isomorphism from the quotient  $SL_2(\mathbf{Z}) \backslash H$  to  $\mathbf{C}$ , and is uniquely defined by this up to multiplication by a constant or addition of a constant. In particular any other modular function is a function of  $j$ , so  $j$  is in some sense the simplest nonconstant modular function.

An amusing property of  $j$  (which so far seems to have no relation with moonshine) is that  $j(\tau)$  is an algebraic integer whenever  $\tau$  is an imaginary quadratic

irrational number. A well known consequence of this is that

$$\exp(\pi\sqrt{163}) = 262537412640768743.99999999999925\dots$$

is very nearly an integer. The explanation of this is that  $j((1+i\sqrt{163})/2)$  is exactly the integer

$$-262537412640768000 = -2^{18}3^35^323^329^3,$$

and

$$\begin{aligned} j((1+i\sqrt{163})/2) &= q^{-1} + 744 + 196884q + \dots \\ &= -e^{\pi\sqrt{163}} + 744 + (\text{something very small}). \end{aligned}$$

McKay and Thompson suggested that there should be a graded representation  $V = \bigoplus_{n \in \mathbf{Z}} V_n$  of the monster, such that  $\dim(V_n) = c(n-1)$ , where  $j(\tau) - 744 = \sum_n c(n)q^n = q^{-1} + 196884q + \dots$ . Obviously this is a vacuous statement if interpreted literally, as we could for example just take each  $V_n$  to be a trivial representation. To characterize  $V$ , Thompson suggested looking at the McKay-Thompson series

$$T_g(\tau) = \sum_n \text{Tr}(g|V_n)q^{n-1}$$

for each element  $g$  of the monster. For example,  $T_1(\tau)$  should be the elliptic modular function. Conway and Norton [C-N] calculated the first few terms of each McKay-Thompson series by making a reasonable guess for the decomposition of the first few  $V_n$ 's into irreducible representations of the monster. They discovered the astonishing fact that all the McKay-Thompson series appeared to be Hauptmoduls for certain genus 0 subgroups of  $SL_2(\mathbf{R})$ . (A Hauptmodul for a subgroup  $\Gamma$  is an isomorphism from  $\Gamma \backslash H$  to  $\mathbf{C}$ , normalized so that its Fourier series expansion starts off  $q^{-1} + O(1)$ .)

As an example of some Hauptmoduls of elements of the monster, we will look at the elements of order 2. There are 2 conjugacy classes of elements of order 2, usually called the elements of types  $2A$  and  $2B$ . The corresponding McKay-Thompson series start off

$$\begin{aligned} T_{2B}(\tau) &= q^{-1} + 276q - 2048q^2 + \dots && \text{Hauptmodul for } \Gamma_0(2) \\ T_{2A}(\tau) &= q^{-1} + 4372q + 96256q^2 + \dots && \text{Hauptmodul for } \Gamma_0(2)+ \end{aligned}$$

The group  $\Gamma_0(2)$  is  $\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) \mid c \text{ is even} \}$ , and the group  $\Gamma_0(2)+$  is the normalizer of  $\Gamma_0(2)$  in  $SL_2(\mathbf{R})$ . Ogg had earlier commented on the fact that the full normalizer  $\Gamma_0(p)+$  of  $\Gamma_0(p)$  for  $p$  prime is a genus 0 group if and only if  $p$  is one of the primes 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, or 71 dividing the order of the monster.

Conway and Norton's conjectures were soon proved by A. O. L. Atkin, P. Fong, and S. D. Smith. The point is that to prove something is a virtual character of a finite group it is only necessary to prove a finite number of congruences. In the case of the moonshine module  $V$ , proving the existence of an infinite dimensional representation of the monster whose McKay-Thompson series are give

Hauptmoduls requires checking a finite number of congruences and positivity conditions for modular functions, which can be done by computer.

This does not give an explicit construction of  $V$ , or an explanation about why the conjectures are true. Frenkel, Lepowsky, and Meurman managed to find an explicit construction of a monster representation  $V = \bigoplus V_n$ , such that  $\dim(V_n) = c(n-1)$ , and this module had the advantage that it came with some extra algebraic structure preserved by the monster. However it was not obvious that  $V$  satisfied the Conway-Norton conjectures. So the main problem in moonshine was to show that the monster modules constructed by Frenkel, Lepowsky and Meurman on the one hand, and by Atkin, Fong, and Smith on the other hand, were in fact the same representation of the monster.

Peter Goddard [Go] has given a description of the proof of this in his talk in this volume, so I will only give a quick sketch of this. The main steps of the proof are as follows:

- 1. The module  $V$  constructed by Frenkel, Lepowsky, and Meurman has an algebraic structure making it into a “vertex algebra”. A detailed proof of this is given in [F-L-M].
- 2. Use the vertex algebra structure on  $V$  and the Goddard-Thorn no-ghost theorem [G-T] from string theory to construct a Lie algebra acted on by the monster, called the monster Lie algebra.
- 3. The monster Lie algebra is a “generalized Kac-Moody algebra” ([K90]); use the (twisted) Weyl-Kac denominator formula to show that  $T_g(\tau)$  is a “completely replicable function”.
- 4. Y. Martin [M], C. Cummins, and T. Gannon [C-G] proved several theorems showing that completely replicable functions were modular functions of Hauptmoduls for genus 0 groups. By using these theorems it follows that  $T_g$  is a Hauptmodul for a genus 0 subgroup of  $SL_2(\mathbf{Z})$ , and hence  $V$  satisfies the moonshine conjectures. (The original proof used an earlier result by Koike [Ko] showing that the appropriate Hauptmoduls were completely replicable, together with a boring case by case check and the fact that a completely replicable function is characterized by its first few coefficients.)

We will now give a brief description of some of the terms above, starting with vertex algebras. The best reference for finding out more about vertex algebras is Kac’s book [K]. In this paragraph we give a rather vague description. Suppose that  $V$  is a commutative ring acted on by a group  $G$ . We can form expressions like

$$u(x)v(y)w(z),$$

where  $u, v, w \in V$  and  $x, y, z \in G$ , and the action of  $x \in G$  on  $u \in V$  is denoted rather confusingly by  $u(x)$ . (This is not a misprint for  $x(u)$ ; the reason for this strange notation is to make the formulas compatible with those in quantum field theory, where  $u$  would be a quantum field and  $x$  a point of space-time.) For each fixed  $u, v, \dots \in V$ , we can think of  $u(x)v(y) \cdots$  as a function from  $G^n$  to  $V$ . We

can rewrite the axioms for a commutative ring acted on by  $G$  in terms of these functions. We can now think of a vertex algebra roughly as follows: we are given lots of functions from  $G^n$  to  $V$  satisfying the axioms mentioned above, with the difference that these functions are allowed to have certain sorts of singularities. In other words a vertex algebra is a sort of commutative ring acted on by a group  $G$ , except that the multiplication is not defined everywhere but has singularities. In particular we cannot recover an underlying ring by defining the product of  $u$  and  $v$  to be  $u(0)v(0)$ , because the function  $u(x)v(y)$  might happen to have a singularity at  $u = v = 0$ .

It is easy to write down examples of vertex algebras: any commutative ring acted on by a group  $G$  is an example. (Actually this is not quite correct: for technical reasons we should use a formal group  $\hat{G}$  instead of a group  $G$ .) Conversely any vertex algebra “without singularities” can be constructed in this way. Unfortunately there are no easy examples of vertex algebras that are not really commutative rings. One reason for this is that nontrivial vertex algebras must be infinite dimensional; the point is that if a vertex algebra has a nontrivial singularity, then by differentiating it we can make the singularity worse and worse, so we must have an infinite dimensional space of singularities. This is only possible if the vertex algebra is infinite dimensional. However there are plenty of important infinite dimensional examples; see for example Kac’s book for a construction of the most important examples, and [FLM] for a construction of the monster vertex algebra.

Next we give a brief description of generalized Kac-Moody algebras. The best way to think of these is as infinite dimensional Lie algebras which have most of the good properties of finite dimensional reductive Lie algebras. Consider a typical finite dimensional reductive Lie algebra  $G$ , (for example the Lie algebra  $G = M_n(\mathbf{R})$  of  $n \times n$  real matrices). This has the following properties:

- 1.  $G$  has an invariant symmetric bilinear form  $(,)$  (for example  $(a, b) = -Tr(a, b)$ ).
- 2.  $G$  has a (Cartan) involution  $\omega$  (for example,  $\omega(a) = -a^t$ ).
- 3.  $G$  is graded as  $G = \bigoplus_{n \in \mathbf{Z}} G_n$  with  $G_n$  finite dimensional and with  $\omega$  acting as  $-1$  on the “Cartan subalgebra”  $G_0$ . (For example, we could put the basis element  $e_{i,j}$  of  $M_n(\mathbf{R})$  in  $G_{i-j}$ .)
- 4.  $(a, \omega(a)) > 0$  if  $g \in G_n, g \neq 0$ .

Conversely any Lie algebra satisfying the conditions above is essentially a sum of finite dimensional and affine Lie algebras. Generalized Kac-Moody algebras are defined by the same conditions with one small change: we replace condition 4 by

- 4'.  $(a, \omega(a)) > 0$  if  $g \in G_n, g \neq 0$  and  $n \neq 0$ .

This has the effect of allowing an enormous number of new examples, such as all Kac-Moody algebras and the Heisenberg Lie algebra (which behaves like a sort of degenerate affine Lie algebra). Generalized Kac-Moody algebras have many of the properties of finite dimensional semisimple Lie algebras, and in particular they



have an analogue of the Weyl character formula for some of their representations, and an analogue of the Weyl denominator formula. An example of the Weyl-Kac denominator formula for the algebra  $G = SL_2[z, z^{-1}]$  is

$$\prod_{n>0} (1 - q^{2n})(1 - q^{2n-1}z)(1 - q^{2n-1}z^{-1}) = \sum_{n \in \mathbf{Z}} (-1)^n q^{n^2} z^n.$$

This is the Jacobi triple product identity, and is also the Macdonald identity for the affine Lie root system corresponding to  $A_1$ .

Dyson described Macdonald's discovery of the Macdonald identities in [D]. Dyson found identities for  $\eta(\tau)^m = q^{m/24} \prod_{n>0} (1 - q^n)^m$  for the following values of  $m$ :

$$3, 8, 10, 14, 15, 21, 24, 26, 28, \dots$$

and wondered where this strange sequence of numbers came from. (The case  $m = 3$  is just the Jacobi triple product identity with  $z = 1$ .) Macdonald found his identities corresponding to affine root systems, which gave an explanation for the sequence above: with one exception, the numbers are the dimensions of simple finite dimensional complex Lie algebras. The exception is the number 26 (found by Atkin), which as far as I know has not been explained in terms of Lie algebras. It seems possible that it is somehow related to the fake monster Lie algebra and the special dimension 26 in string theory.

Next we give a quick explanation of "completely replicable" functions. A function is called completely replicable if its coefficients satisfy certain relations. As an example of a completely replicable function, we will look at the elliptic modular function  $j(\tau) - 744 = \sum c(n)q^n$ . This satisfies the identity

$$j(\sigma) - j(\tau) = p^{-1} \prod_{\substack{m>0 \\ n \in \mathbf{Z}}} (1 - p^m q^n)^{c(mn)},$$

where  $p = e^{2\pi i\sigma}$ ,  $q = e^{2\pi i\tau}$ . (This formula was proved independently in the 80's by Koike, Norton, and Zagier, none of whom seem to have published their proofs.) Comparing coefficients of  $p^m q^n$  on both sides gives many relations between the coefficients of  $j$  whenever we have a solution of  $m_1 n_1 = m_2 n_2$  in positive integers, which are more or less the relations needed to show that  $j$  is completely replicable. For example, from the relation  $2 \times 2 = 1 \times 4$  we get the relation

$$c(4) = c(3) + \frac{c(1)^2 - c(1)}{2},$$

or equivalently

$$20245856256 = 864299970 + \frac{196884^2 - 196884}{2}.$$

In the rest of this paper we will discuss various extensions of the original moonshine conjectures, some of which are still unproved. The first are Norton's "generalized moonshine" conjectures [N]. If we look at the Hauptmodul  $T_{2A}(\tau) = q^{-1} + 4372q + \dots$  we notice that one of the coefficients is almost the same as the

dimension 4371 of the smallest non-trivial irreducible representation of the baby monster simple group, and the centralizer of an element of type 2A in the monster is a double cover of the baby monster. Similar things happen for other elements of the monster, suggesting that for each element  $g$  of the monster there should be some sort of graded moonshine module  $V_g = \bigoplus_n V_{g,n}$  acted on by a central extension of the centralizer  $Z_M(g)$ . In particular we would get series  $T_{g,h}(\tau) = \sum_n \text{Tr}(h|V_{g,n})q^n$  satisfying certain conditions. Some progress has been made on this by Dong, Li, and Mason [D-L-M], who proved the generalized moonshine conjectures in the case when  $g$  and  $h$  generate a cyclic group by reducing to the case when  $g = 1$  (the ordinary moonshine conjectures). G. Höhn [H] has made some progress in the harder case when  $g$  and  $h$  do not generate a cyclic group by constructing the required modules for the baby monster (when  $g$  is of type 2A). It seems likely that his methods would also work for the Fischer group  $Fi_{24}$ , but it is not clear how to go further than this. There might be some relation to elliptic cohomology (see [Hi] for more discussion of this), as this also involves pairs of commuting elements in a finite group and modular forms.

The space  $V_g$  mentioned above does not always have an invariant vertex algebra structure on it. Ryba discovered that a vertex algebra structure sometimes magically reappears when we reduce  $V_g$  modulo the prime  $p$  equal to the order of  $g$ . In fact  $V_g/pV_g$  can often be described as the Tate cohomology group  $\hat{H}^0(g, V)$  for a suitable integral form  $V$  of the monster vertex algebra. This gives natural examples of vertex algebras over finite fields which do not lift naturally to characteristic 0. (Note that most books and papers on vertex algebras make the assumption that we work over a field of characteristic 0; this assumption is often unnecessary and excludes many interesting examples such as the one above.)

We will finish by describing some more of McKay's observations about the monster, which so far are completely unexplained. The monster has 9 conjugacy classes of elements that can be written as the product of two involutions of type 2A, and their orders are 1, 2, 3, 4, 5, 6, 2, 3, 4. McKay pointed out that these are exactly the numbers appearing on an affine  $E_8$  Dynkin diagram giving the linear relation between the simple roots. They are also the degrees of the irreducible representations of the binary icosahedral group. A similar thing happens for the baby monster: this time there are 5 classes of elements that are the product of two involutions of type 2A and their orders are 2, 4, 3, 2, 1. (This is connected with the fact that the baby monster is a "3,4-transposition group".) These are the numbers on an affine  $F_4$  Dynkin diagram, and if we take the "double cover" of an  $F_4$  Dynkin diagram we get an  $E_7$  Dynkin diagram. The number on an  $E_7$  Dynkin diagram are 1, 1, 2, 2, 3, 3, 4, 2 which are the dimensions of the irreducible representations of the binary octahedral group. The double cover of the baby monster is the centralizer of an element of order 2 in the monster. Finally a similar thing happens for  $Fi_{24}:2$ : this time there are 3 classes of elements that are the product of two involutions of type 2A and their orders are 2, 3, 1. (This is connected with the fact that  $F_{24}:2$  is a "3-transposition group".) These are the numbers on an affine  $G_2$  Dynkin diagram, and if we take the "triple cover" of an  $G_2$  Dynkin diagram we get an  $E_6$  Dynkin diagram. The number on an  $E_6$  Dynkin diagram are 1, 1, 1, 2, 2, 3, which are the dimensions of the irreducible

representations of the binary tetrahedral group. The triple cover of  $Fi_{24}.2$  is the centralizer of an element of order 3 in the monster.

The connection between Dynkin diagrams and 3-dimensional rotation groups is well understood (and is called the McKay correspondence), but there is no known explanation for the connection with the monster.

## REFERENCES

- [B94] R. E. Borcherds, *Simple groups and string theory*, First European congress of mathematics, Paris July 1992, Ed. A. Joseph and others, vol. 1 p. 411-421, Birkhauser 1994.
- [B98] R. E. Borcherds, *Automorphic forms and Lie algebras*. Current developments in mathematics 1996, to be published by international press, 1998. Also available from [www.dpmms.cam.ac.uk/~reb](http://www.dpmms.cam.ac.uk/~reb).
- [C-G] C. J. Cummins, T. Gannon, *Modular equations and the genus zero property of moonshine functions*. Invent. Math. 129 (1997), no. 3, 413-443.
- [C-N] J. H. Conway, S. Norton, *Monstrous moonshine*, Bull. London. Math. Soc. 11 (1979) 308-339.
- [D] F. J. Dyson, *Missed opportunities*. Bull. Amer. Math. Soc. 78 (1972), 635-652.
- [D-L-M] C. Dong, H. Li, G. Mason, *Modular invariance of trace functions in orbifold theory*, preprint q-alg/9703016.
- [F-L-M] I. B. Frenkel, J. Lepowsky, A. Meurman, *Vertex operator algebras and the monster*, Academic press 1988. (Also see the announcement A natural representation of the Fischer-Griess monster with the modular function  $J$  as character, Proc. Natl. Acad. Sci. USA 81 (1984), 3256-3260.)
- [Ge] R. W. Gebert, *Introduction to vertex algebras, Borcherds algebras and the monster Lie algebra*, Internat. J. Modern Physics A8 (1993) no 31, 5441-5503.
- [Go] The Work of R. E. Borcherds, this volume, p. 99.
- [G-T] P. Goddard and C. B. Thorn, *Compatibility of the dual Pomeron with unitarity and the absence of ghosts in the dual resonance model*, Phys. Lett., B 40, No. 2 (1972), 235-238.
- [G] R. L. Griess, *The friendly giant*. Invent. Math. 69 (1982), no. 1, 1-102.
- [Hi] F. Hirzebruch, T. Berger, R. Jung, *Manifolds and modular forms*. Aspects of Mathematics, E20. Friedr. Vieweg & Sohn, Braunschweig, 1992. ISBN: 3-528-06414-5

- [H] G. Höhn, *Selbstduale Vertexoperatorsuperalgebren und das Babymonster*. [Self-dual vertex-operator superalgebras and the Baby Monster] Dissertation, Rheinische Friedrich-Wilhelms-Universität Bonn, Bonn, 1995. Bonner Mathematische Schriften 286. Universität Bonn, Mathematisches Institut, Bonn, 1996.
- [J] E. Jurisich, *Generalized Kac-Moody Lie algebras, free Lie algebras and the structure of the Monster Lie algebra*. J. Pure Appl. Algebra 126 (1998), no. 1-3, 233–266.
- [K90] V. G. Kac, *Infinite dimensional Lie algebras*, third edition, Cambridge University Press, 1990. (The first and second editions (Birkhauser, Basel, 1983, and C.U.P., 1985) do not contain the material on generalized Kac-Moody algebras.)
- [Ko] M. Koike, *On Replication Formula and Hecke Operators*, Nagoya University preprint.
- [LZ] B. Lian, G. Zuckerman, *New perspectives on the BRST-algebraic structure in string theory*, hep-th/921107, Communications in Mathematical Physics 154, (1993) 613-64, and *Moonshine cohomology*, q-alg/ 950101 Finite groups and Vertex Operator Algebras, RIMS publication (1995) 87-11.
- [M] Y. Martin, *On modular invariance of completely replicable functions. Moonshine, the Monster, and related topics* (South Hadley, MA, 1994), 263–286, Contemp. Math., 193, Amer. Math. Soc., Providence, RI, 1996.
- [N] S. P. Norton, Appendix to G. Mason's paper in *The Arcata Conference on Representations of Finite Groups* (Arcata, Calif., 1986), 181–210, Proc. Sympos. Pure Math., 47, Part 1, Amer. Math. Soc., Providence, RI, 1987.

Richard E. Borcherds  
D.P.M.M.S.  
16 Mill Lane,  
Cambridge CB2 1SB  
England  
reb@dpmms.cam.ac.uk  
www.dpmms.cam.ac.uk/~reb



## FOURIER ANALYSIS AND SZEMERÉDI'S THEOREM

W. T. GOWERS

ABSTRACT. The famous theorem of Szemerédi asserts that for every positive integer  $k$  and every positive real number  $\delta > 0$  there is a positive integer  $N$  such that every subset of  $\{1, 2, \dots, N\}$  of cardinality at least  $\delta N$  contains an arithmetic progression of length  $k$ . A second proof of the theorem was given by Furstenberg using ergodic theory, but neither this proof nor Szemerédi's gave anything other than extremely weak information about the dependence of  $N$  on  $k$  and  $\delta$ . In this article we describe a new, more quantitative approach to Szemerédi's theorem which greatly improves the best known bound when  $k = 4$ , and which will probably do the same for general  $k$ .

1991 Mathematics Subject Classification: 11P99

Keywords and Phrases: Arithmetic progressions, Fourier analysis

## §1. INTRODUCTION.

A well known result of van der Waerden [vdW], published in 1927, is the following.

THEOREM 1A. *Let the natural numbers be partitioned into finitely many sets. Then one of the sets contains arbitrarily long arithmetic progressions.*

A straightforward compactness argument allows this statement to be rephrased as follows.

THEOREM 1B. *For every pair of positive integers  $k, r$  there exists a positive integer  $M$  such that, whenever the set  $\{1, 2, \dots, M\}$  is partitioned into  $r$  subsets  $C_1, \dots, C_r$ , at least one of the subsets contains an arithmetic progression of length  $k$ .*

This is one of the classic results of Ramsey theory: it is customary to call the cells of the partition *colours*, the partition itself an  *$r$ -colouring* and the resulting arithmetic progression *monochromatic*.

Let us define  $M(k, r)$  to be the minimal  $M$  for which the conclusion of Theorem 1B holds. A compactness argument proves that  $M(k, r)$  is finite but does not give any bound for it. As it happens, though, van der Waerden proved the second version of his theorem directly, and it is possible to extract from his proof an explicit estimate for  $M(k, r)$ . However, the estimate is enormously large, as we shall see later, and barely qualifies as a quantitative bound.

In 1936, Erdős and Turán [ET] made a conjecture which significantly strengthened van der Waerden's theorem. It soon became clear that their conjecture was

very difficult, and it took almost forty years before it was solved, by Szemerédi [Sz2]. The statement is the following.

**THEOREM 2A.** *Any subset of the natural numbers with positive upper density contains arithmetic progressions of arbitrary length.*

Again, there is a finite version.

**THEOREM 2B.** *For every natural number  $k$  and positive real number  $\delta$  there exists a natural number  $N$  such that every subset of  $\{1, 2, \dots, N\}$  of cardinality at least  $\delta N$  contains an arithmetic progression of length  $k$ .*

This certainly implies van der Waerden's theorem, as one can take  $\delta = r^{-1}$  and consider the most frequently occurring colour. For this reason, the result is often called the *density version* of van der Waerden's theorem (as opposed to the *colouring version*).

It is interesting to consider why Erdős and Turán made their conjecture, and to compare it with other results in Ramsey theory. Ramsey's theorem itself states that for every  $k$  and  $r$  there exists  $N$  such that if the edges of the complete graph on  $N$  vertices are coloured with  $r$  colours, then a complete subgraph on  $k$  vertices can be found with all its edges the same colour. However, it is absolutely not true that one can do this with the most frequently occurring colour. (For example, consider a complete bipartite graph on two sets of equal size.) A theorem of Schur states that if  $N$  is sufficiently large and the set  $\{1, 2, \dots, N\}$  is coloured with  $r$  colours, then one of the colours contains a triple  $(x, y, z)$  with  $x + y = z$ . Again, there is no density version of the statement – just consider the set of all odd numbers less than  $N$ . The most important difference between van der Waerden's theorem and Schur's theorem in this respect is that van der Waerden's theorem is affine-invariant. This property rules out simple counterexamples such as the set of all integers satisfying some congruence.

This shows why the conjecture had a chance of being true, but the motivation for it was stronger than that. In particular, it was reasonable to think that it would not be possible to prove the conjecture using the sorts of inefficient combinatorial arguments that yielded poor bounds for van der Waerden's theorem. In that case, a proof of the conjecture would give new quantitative information even for the colouring statement. Moreover, if the bounds turned out to be good enough, one could obtain an important number-theoretic result purely combinatorially. To be precise, Erdős went on to give the following conjecture, which was possibly his favourite of all problems.

**CONJECTURE 3.** *Let  $A$  be a set of natural numbers such that  $\sum_{n \in A} n^{-1} = \infty$ . Then  $A$  contains arithmetic progressions of arbitrary length.*

This conjecture, if true, would imply that the primes contained arbitrarily long arithmetic progressions, and the proof would use very little about the distribution of primes – Chebyshev's theorem would suffice. However, Szemerédi's proof used van der Waerden's theorem, so, although it was a major breakthrough, it did not after all provide improved bounds, and indeed Conjecture 3 is still wide open, even for progressions of length three.

A different sort of breakthrough was made by Furstenberg [Fu] in 1977, who gave a second proof of Szemerédi's theorem, which used ergodic theory (much of which was new, fascinating and specially developed by Furstenberg for the purpose). Furstenberg's methods have since been extended, and there are now several purely combinatorial results for which the only known proofs use ergodic theory. Some of these will be discussed later in this paper. However, the ergodic theory method as it stands does not give any estimates and so in particular gives no information about Conjecture 3.

Let us now consider in more detail the best known bounds for this class of problems. In order to state them, it will be necessary to remind the reader of the *Ackermann hierarchy* of rapidly-growing functions, defined as follows. Let  $A_1(n) = 2 + n$ ,  $A_2(n) = 2n$  and  $A_3(n) = 2^n$ . In general one obtains  $A_k(n)$  by starting with the number 2 and applying the function  $A_{k-1}$   $n - 1$  times. In other words, each function iterates the previous one. A concise definition is

$$A_1(n) = 2 + n; \quad A_k(1) = 2 \quad (k > 1); \quad A_k(n) = A_{k-1}(A_k(n-1)) \quad (n > 1).$$

Note in particular that  $A_4(n)$  is given by a tower of twos of height  $n$ , while  $A_5(n)$  is given by a tower of twos of height  $A_5(n-1)$ .

The *Ackermann function* itself is defined as  $A(n) \equiv A_n(n)$ . Thus, it grows faster than any individual function  $A_k$ . In fact, it is known to grow faster than any primitive recursive function, which very roughly means any function that can be defined starting with the successor function and using a finite sequence of single inductive definitions (rather than the double induction we needed above). Nevertheless, this function does from time to time appear naturally (for a very good example see Ron Graham's account in this volume of the work of Peter Shor) and was the upper bound obtained by van der Waerden for the function  $M(k, 2)$ , that is, the smallest  $M$  such that every 2-colouring of  $\{1, 2, \dots, M\}$  yields a monochromatic arithmetic progression of length  $k$ . (One might reasonably suppose that this was about the worst bound that could arise from *any* sensible proof of a natural combinatorial statement. If you believe this, then see [PH] or [GRS Section 6.3].) This remained the best known upper bound until 1987, by which time some people had even been tempted to wonder whether there was a comparable lower bound, although the best known lower bound was only exponential in  $k$ . Then Shelah [Sh] found a primitive recursive upper bound for  $M(k, 2)$  of  $A_5(k)$ . To everybody's surprise, his argument was very natural, not especially difficult and in much the same spirit as that of van der Waerden. This, needless to say, did not stop it being highly ingenious.

Since Szemerédi used van der Waerden's theorem in the middle of an inductive step, one can guess that his argument, when combined with Shelah's later bound, gave an upper bound for  $N(k, \delta)$  of the general form of  $A_6(k)$  (for fixed  $\delta$ ), but this has not been checked. Despite this bound being a huge improvement on the Ackermann function, it still had the flavour of a bound that just happened to come out of a not particularly quantitative argument. Moreover, to improve it, it was clear that a substantially new proof would be necessary, one which avoided the use of van der Waerden's theorem. (Another important tool in Szemerédi's proof, his so-called uniformity lemma, also makes a big contribution. See [G1] for a proof



that the function  $A_4$  can occur in nature.)

Fortunately, there was one result in the area which was undeniably quantitative, a proof in 1953 by Roth [R1] that  $N(3, \delta)$  is at most  $\exp \exp(C/\delta)$  for some absolute constant  $C$ . This result was proved using Fourier analysis, and the proof will be sketched below. On the other hand, the argument did not seem to generalize to progressions of length greater than three, for reasons which will also be sketched below. Indeed, Szemerédi was able to make further progress only after he had found a different proof for progressions of length three. Even so, the existence of Roth's proof suggested that Fourier analysis (or exponential sums – they are the same in this context) ought to be used as the basis for any significant improvement to the bounds in Szemerédi's theorem. In this paper, we shall indicate how to use it for progressions of length four. More details can be found in [G2]. (It should be remarked that Roth [R2], using ideas of Szemerédi, found a proof in this case which used exponential sums, but this proof was not purely analytic. In particular it still required van der Waerden's theorem.)

## §2. ROTH'S ARGUMENT.

Let  $N$  be a prime (for convenience) and write  $\mathbb{Z}_N$  for  $\mathbb{Z}/N\mathbb{Z}$ , the integers mod  $N$ . Let  $\omega$  be the primitive  $N^{\text{th}}$  root of unity  $\exp(2\pi i/N)$ . Given a function  $f : \mathbb{Z}_N \rightarrow \mathbb{C}$ , one can define a discrete Fourier transform  $\tilde{f}$  by the formula

$$\tilde{f}(r) = \sum_{s \in \mathbb{Z}_N} f(s) \omega^{-rs} .$$

One then has the inversion formula

$$f(s) = N^{-1} \sum_{r \in \mathbb{Z}_N} \tilde{f}(r) \omega^{rs} ,$$

while Parseval's identity takes the form

$$\sum_{r \in \mathbb{Z}_N} |\tilde{f}(r)|^2 = N \sum_{s \in \mathbb{Z}_N} |f(s)|^2 .$$

Since the Fourier transform is in some sense measuring periodicity, it is not surprising that it should be useful for problems to do with arithmetic progressions. Roth's argument starts with the observation (standard to analytic number theorists) that it gives a neat way of counting arithmetic progressions of length three. Consider three subsets  $A, B, C$  of  $\mathbb{Z}_N$ , and identify these sets with their characteristic functions. Then the number of triples  $(x, y, z)$  such that  $x \in A$ ,  $y \in B$ ,  $z \in C$  and  $x + z = 2y$  (this last condition states that  $(x, y, z)$  is an arithmetic progression mod  $N$ ) is

$$N^{-1} \sum_r \sum_{x, y, z} A(x) B(y) C(z) \omega^{-r(x-2y+z)} .$$

(Here, and from now on, all sums where the range is unspecified are over the whole of  $\mathbb{Z}_N$ .) To see this, notice that  $\sum_r \omega^{-r(x-2y+z)}$  is zero when  $x - 2y + z \neq 0$ , and

otherwise  $N$ , while  $A(x)B(y)C(z)$  is 1 if  $x \in A$ ,  $y \in B$  and  $z \in C$ , and otherwise zero.

Now  $\omega^{-r(x-2y+z)} = \omega^{-rx}\omega^{2ry}\omega^{-rz}$ , so the expression above is nothing other than

$$N^{-1} \sum_r \tilde{A}(r)\tilde{B}(-2r)\tilde{C}(r) .$$

Notice that  $\tilde{A}(0)$  is just the cardinality of the set  $A$ , and similarly for  $B$  and  $C$ , so we can split this up as

$$N^{-1}|A||B||C| + \sum_{r \neq 0} \tilde{A}(r)\tilde{B}(-2r)\tilde{C}(r) . \quad (*)$$

If  $A$ ,  $B$  and  $C$  have cardinalities  $\alpha N$ ,  $\beta N$  and  $\gamma N$  respectively, then the first term equals  $\alpha\beta\gamma N^2$ . Notice that this is exactly the number of triples one would expect to have satisfying the conditions above if the sets  $A$ ,  $B$  and  $C$  had been chosen randomly with their given cardinalities, since there are  $N^2$  triples  $(x, y, z)$  in arithmetic progression mod  $N$ , and the probability that an individual one lies in  $A \times B \times C$  is  $\alpha\beta\gamma$ . Of course, in general  $A$ ,  $B$  and  $C$  are not chosen randomly, and  $A \times B \times C$  may well contain no arithmetic progression mod  $N$ , but this can happen only if the first term is cancelled out by the second, and *this* can happen only if some of the non-zero Fourier coefficients of  $A$ ,  $B$  and  $C$  are large.

One applies this argument as follows. Let  $A \subset \{0, 1, 2, \dots, N-1\}$  be a set of cardinality  $\alpha N$  containing no arithmetic progression of length three. Let  $B$  and  $C$  both equal  $\{x \in A : N/3 < x < 2N/3\}$ . Now regard  $A$ ,  $B$  and  $C$  as subsets of  $\mathbb{Z}_N$  in the obvious way. Notice that if  $(x, y, z) \in A \times B \times C$  and  $x+z = 2y \pmod N$ , then either  $x = y = z$  or  $(x, y, z)$  corresponds to an arithmetic progression in the original set  $A$  when it was *not* regarded as a subset of  $\mathbb{Z}_N$ . As explained in the previous paragraph, the fact that  $A \times B \times C$  contains no arithmetic progressions mod  $N$  (apart from the degenerate ones of the form  $(x, x, x)$ , but there are too few of these to be significant) implies that  $A$ ,  $B$  and  $C$  have large non-zero Fourier coefficients. More precisely, it is not hard to deduce from (\*) that if  $B = C$  has cardinality at least  $\alpha N/4$ , then there must exist a non-zero  $r$  such that  $|\tilde{A}(r)| \geq \alpha^2 N/20$ . (If  $|B| < \alpha N/4$ , then  $A$  is not uniformly distributed inside  $\mathbb{Z}_N$ , and a similar but stronger conclusion is true.)

A good way to view the argument so far is to regard the size of the largest non-zero Fourier coefficient of  $A$  as a measure of non-randomness. Then what we have shown (or rather sketched) is that either  $A$  is random, in which case it contains plenty of arithmetic progressions of length three, just as one would expect, or it is non-random, in which case it has a non-zero Fourier coefficient which is large, where "large" means exceeding  $\gamma N$  for some constant  $\gamma > 0$  that depends only on the density  $\alpha$  of the set  $A$ .

We must now deal with the second case, so suppose that  $r \neq 0$  and  $|\tilde{A}(r)| \geq \gamma N$ . Let  $m$  be a sufficiently large integer (depending on  $\alpha$  only) and define, for  $1 \leq j \leq m$ , the set  $P_j$  to be  $\{s \in \mathbb{Z}_N : (j-1)N/m \leq rs < jN/m\}$ . The sets  $P_j$  have been chosen so that the function  $s \mapsto \omega^{-rs}$  is roughly constant on each  $P_j$ .

Let  $s_j$  be an arbitrary element of  $P_j$ . Then

$$\tilde{A}(r) = \sum_s A(s)\omega^{-rs} = \sum_{j=1}^m \sum_{s \in P_j} A(s)\omega^{-rs}$$

is well approximated by

$$\sum_{j=1}^m \sum_{s \in P_j} A(s)\omega^{-rs_j} = \sum_{j=1}^m |A \cap P_j| \omega^{-rs_j}.$$

Since the numbers  $\omega^{-rs_j}$  are evenly spread around the unit circle, this sum cannot be large unless the sets  $|A \cap P_j|$  have widely differing sizes, and because we know that  $\sum_{j=1}^m |A \cap P_j| = \alpha N$ , this implies that there exists  $j$  such that  $|A \cap P_j| \geq (\alpha + \gamma')|P_j|$ , where  $\gamma'$  again depends on  $\alpha$  only.

Now  $P_j$  is nothing other than an arithmetic progression mod  $N$  with common difference  $r^{-1}$ . If the argument above is done carefully, then the size of  $P_j$  can be made proportional to  $N$  (with a constant depending on  $\alpha$  only) and  $|A \cap P_j| \geq (\alpha + c\alpha^2)|P_j|$ , where  $c$  is an absolute constant. The final ingredient is a simple and standard argument, based on Dirichlet's pigeonhole principle, which shows that the set  $P_j$  can be partitioned into  $r$  sets, with  $r$  proportional to  $\sqrt{N}$ , which are not only arithmetic progressions mod  $N$  but are still arithmetic progressions when regarded as subsets of  $\{0, 1, \dots, N-1\}$ . Then, by an averaging argument, we can find one of these,  $Q$  say, such that  $|A \cap Q| \geq (\alpha + c\alpha^2)|Q|$  and  $Q$  has size proportional to  $\sqrt{N}$ .

The proof is now over, because we have managed to find a subprogression of  $\{0, 1, \dots, N-1\}$  inside which the density of the set  $A$  has gone up from  $\alpha$  to  $\alpha(1 + c\alpha)$ . We can then repeat the argument. A small calculation shows that we cannot repeat it more than  $C/\alpha$  times, where  $C$  is another absolute constant, and another small calculation gives the bound  $N(3, \delta) \leq \exp \exp(C/\delta)$ , the double exponential coming from the fact that at each iteration we are taking the square root of  $N$ .

### §3. PROGRESSIONS OF LENGTH FOUR.

One could summarize Roth's proof as follows. If a set  $A \subset \mathbb{Z}_N$  (or more accurately its characteristic function) has no large non-trivial Fourier coefficients, then it behaves randomly in a useful sense. In particular, it contains roughly the right number of arithmetic progressions of length three. On the other hand, if it has a large non-trivial Fourier coefficient, then it is not uniformly distributed inside mod- $N$  arithmetic progressions of size proportional to  $N$ . It follows by a pigeonhole argument that there is a genuine arithmetic progression  $P$  of size proportional to  $\sqrt{N}$  such that the density of  $A \cap P$  inside  $P$  is significantly larger than the density of  $A$  inside  $\mathbb{Z}_N$ . This allows us to iterate.

It is now natural to wonder whether the "random behaviour" of the set  $A$  implies anything about the number of arithmetic progressions it contains of length four. However, it turns out that merely having small Fourier coefficients is not

enough. An example to illustrate this is the set  $A = \{x \in \mathbb{Z}_N : -N/1000 < x^2 < N/1000\}$  (where, for the purposes of the inequality,  $x^2$  stands for the representative of  $x^2$  that lies between  $-N/2$  and  $N/2$ ). It can be shown, using estimates due to Weyl [We] for exponential sums involving quadratic functions, that all the non-zero Fourier coefficients of this set are very small. We now give a very rough argument (which can easily be made rigorous) to show that  $A$  contains more mod- $N$  arithmetic progressions of length four than one would expect. (If  $A$  has size  $\alpha N$  and is chosen randomly, then one expects about  $\alpha^4 N^2$  quadruples of the form  $(a, a+d, a+2d, a+3d)$  to belong to  $A^4$ .) Suppose we know that  $a-d$ ,  $a$  and  $a+d$  all belong to  $A$ . Then  $(a-d)^2$ ,  $a^2$  and  $(a+d)^2$  are all “small” mod  $N$ . Taking differences, this implies that  $2ad-d^2$  and  $2ad+d^2$  are both small, which implies that  $4ad$  and  $2d^2$  are both small. But then  $(a+2d)^2 = a^2 + 4ad + 2d^2$  must be small. In other words, once we have an arithmetic progression of length three in  $A$  (and of these we have about the expected number) there is a greater chance than there should be that the next term in the progression also belongs to  $A$ . Therefore  $A$  contains more progressions of length four than it should.

With a bit more effort, one can use similar ideas to construct a set  $A$  with small Fourier coefficients and *fewer* arithmetic progressions of length four than a random set of the same cardinality. This seems to indicate that, beautiful as Roth's argument is, there is a fundamental limitation to Fourier methods which stops it generalizing. On the other hand, it is difficult to find examples to illustrate this that are fundamentally different from the set  $A$  above. That is, they all seem to involve quadratic polynomials and work for basically the same reason. It turns out that this is *necessary*, and can be proved to be necessary using Fourier methods. We now give a very brief outline of the argument.

The first step is to define a stronger notion of randomness, which we call quadratic uniformity. Let us define a set  $A$  to be  $\delta$ -uniform if  $|\tilde{A}(r)| \leq \delta N$  for every non-zero  $r$ . Write  $A+k$  for  $\{x \in \mathbb{Z}_N : x-k \in A\}$ . Define  $A$  to be  $\delta$ -quadratically uniform if  $A \cap (A+k)$  is  $\delta$ -uniform for all but at most  $\delta N$  values of  $k$ . In loose terms,  $A$  is quadratically uniform if there are almost no translates of  $A$  (meaning sets of the form  $A+k$ ) for which the intersection  $A \cap (A+k)$  has a non-trivial large Fourier coefficient.

It can be shown that if  $A$  has size  $\alpha N$  and is  $\delta$ -quadratically uniform for sufficiently small  $\delta$  (depending on  $\alpha$  only) then  $A$  contains approximately the correct number of arithmetic progressions of length four, and in particular at least one such progression. (The proof is similar to the weak mixing case in Furstenberg's argument. I am grateful to Gil Kalai for pointing this out to me.) We therefore have an appropriate generalization of the first step of Roth's argument, and in fact it can be generalized further, without much difficulty, to deal with arithmetic progressions of arbitrary length.

However, it is not at all obvious what to do if  $A$  is *not* quadratically uniform. From the definition we can say that there is a set  $B \subset \mathbb{Z}_N$  of size at least  $\delta N$  and a function  $\phi : B \rightarrow \mathbb{Z}_N$  never taking the value zero such that  $|A \cap (A+k) \sim (\phi(k))| \geq \delta N$  for every  $k \in B$ , but this fact on its own does not seem particularly helpful. In order to get any further, it is useful to examine the set  $A = \{x \in \mathbb{Z}_N : -N/1000 < x^2 < N/1000\}$  mentioned earlier. This is an example of a set which is uniform but

not quadratically uniform. A number  $x$  belongs to  $A \cap (A+k)$  only if both  $x^2$  and  $(x-k)^2$  are small, which implies that  $2kx - k^2$  is small. It follows (from an easy calculation) that  $A \cap (A+k) \sim (2k)$  is large. Thus, the quadratic nature of the set  $A$  leads to linear behaviour of the function  $\phi$ .

This suggests that perhaps  $\phi$  cannot be an entirely arbitrary function, and the suggestion is correct. The rest of our proof consists in showing first that  $\phi$  must always have a certain weakish linearity property, and then (reversing the implication from quadratic to linear above) that the linearity of  $\phi$  implies some sort of quadratic bias to the set  $A$ . Finally, this quadratic bias implies (using Weyl's estimates for exponential sums mentioned earlier) the existence of an arithmetic progression  $P$  of size  $N^c$  such that  $|A \cap P| \geq (\alpha + \gamma)|P|$  (where  $c$  and  $\gamma$  depend on  $\alpha$  only).

The most interesting of the steps is finding the linearity of the function  $\phi$ , which is itself done in two stages. The first is a somewhat algebraic argument which shows that, for a constant  $\gamma$  depending on  $\alpha$  only,  $B^4$  contains  $\gamma N^3$  quadruples  $(a, b, c, d)$  such that  $a + b = c + d$  and  $\phi(a) + \phi(b) = \phi(c) + \phi(d)$ . Let us call such a quadruple  $\phi$ -additive. Notice that there are only  $N^3$  quadruples  $(a, b, c, d) \in \mathbb{Z}_N^4$  such that  $a + b = c + d$ , so this is potentially a strong restriction on the function  $\phi$ , and seems to put pressure on  $\phi$  to be linear, or at least to be linear when restricted to some large subset of  $B$ .

After a little thought, however, one realizes that there are definitely non-linear examples of functions  $\phi$  for which there are many  $\phi$ -additive quadruples. A typical one is the following. Let  $m$  be an integer much larger than 1 and much smaller than  $N$  and let  $B = \mathbb{Z}_N$ . Given  $0 \leq x < N$ , write it as  $qm + r$  with  $0 \leq r < m$ , and define  $\phi(x)$  to be  $r$ . It can be checked easily that there are many  $\phi$ -additive quadruples, and also that there is no large subset of  $\mathbb{Z}_N$  on which  $\phi$  is linear.

On the other hand, if one thinks of the numbers 1 and  $m$  as being something like a basis of  $\mathbb{Z}_N$ , then  $\phi$  is something like a linear function defined on a two-dimensional set. It turns out, and this is of enormous importance for the proof, that this sort of quasi-linear behaviour is typical. That is, if there are many  $\phi$ -additive quadruples, then there must be a large subset  $B'$  of  $B$  such that the restriction of  $\phi$  to  $B'$  resembles a linear function defined on a space of not too high a dimension. The proof of this fact is not at all easy, because it relies on a deep theorem of Freiman [F1,2] which we now describe, and in particular a recent proof of Freiman's theorem due to Ruzsa [Ru].

Let  $X$  be a subset of  $\mathbb{Z}$  of size  $n$ . The *sumset* of  $X$ , written  $X + X$ , is simply  $\{x + y : x, y \in X\}$ . Suppose that we know that the sumset of  $X$  has cardinality at most  $Cn$  (where we think of  $n$  as large and  $C$  as fixed). What does this tell us about the set  $X$ ? This question is not unlike the question we have just asked about  $\phi$ , and one can make similar remarks. The most obvious example of a set  $X$  with small sumset is an arithmetic progression. The next most obvious is a large subset of an arithmetic progression. However, these do not exhaust all possibilities. For example, if  $X = \{a_1 r_1 + a_2 r_2 : 0 \leq a_i < s_i\}$  then it is an easy exercise to show that  $|X + X| < 4|X|$ . Such a set is called, for obvious reasons, a *two-dimensional* arithmetic progression, and it is not hard to guess the definition of a  $d$ -dimensional arithmetic progression for arbitrary  $d$ . It is another (similar) easy exercise to show

that a large subset of a low-dimensional arithmetic progression will have a small sumset. Remarkably, the converse is also true, and this is Freiman's theorem.

**THEOREM 4.** *Let  $X$  be a subset of  $\mathbb{Z}$  such that  $|X + X| \leq C|X|$ . Then  $X$  is a subset of a  $d$ -dimensional arithmetic progression of size at most  $D|X|$ , where  $d$  and  $D$  depend on  $C$  only.*

To relate Freiman's theorem to our problem, we consider the graph of the function  $\phi$ , which we shall call  $\Gamma$ . This is a subset of  $\mathbb{Z}_N^2$  of size at most  $N$  which contains at least  $\gamma N^3$  quadruples  $(x, y, z, w)$  such that  $x + y = z + w$ . A theorem of Balog and Szemerédi [BS] now tells us that  $\Gamma$  contains a subset  $X$  of size at least  $\eta N$  such that  $|X + X| \leq C|X|$ , with  $\eta$  and  $C$  constants that depend on  $\gamma$  (and hence  $\alpha$ ) only. It is an easy exercise to formulate an appropriate version of Freiman's theorem for subsets of  $\mathbb{Z}^2$  (as we may regard  $X$ ) and prove that it is equivalent to Freiman's theorem in  $\mathbb{Z}$ . Applying such a version of Freiman's theorem to  $X$ , we find that  $X$  is a subset of a  $d$ -dimensional arithmetic progression  $P$  of size at most  $D|X|$ . An easy averaging argument shows that  $P$  must contain a one-dimensional arithmetic progression  $Q$  of size proportional to  $N^{1/d}$  such that  $|X \cap Q| \geq D^{-1}|Q|$ . Now  $X$  is the graph of the restriction of  $\phi$  to some subset  $B'$  of  $B$ , and  $Q$  is the restriction of a linear function  $\psi$  to an arithmetic progression  $R \subset \mathbb{Z}$  (of size proportional to  $N^{1/d}$ ). The estimate for  $|X \cap Q|$  tells us that  $\phi(x) = \psi(x)$  for at least  $D^{-1}|R|$  values of  $x \in R$ . We have shown that  $\phi$  has at least some linear behaviour, and it turns out to be enough.

We shall now be even more brief. (The reader wishing for more details of the proof should consult [G2].) The linear behaviour of  $\phi$  implies the existence of an arithmetic progression  $S$  of size proportional to  $N^{1/d}$  and a quadratic function  $q$  such that, writing  $f(s)$  for  $A(s) - \alpha$ , we have the inequality

$$\sum_{s \in S} f(s) + \left| \sum_{s \in S} f(s) \omega^{q(s)} \right| \geq \zeta |S|$$

with  $\zeta$  depending on  $\alpha$  only. It can be shown, using Weyl's estimates again, that  $S$  can be partitioned into arithmetic progressions  $T_1, \dots, T_m$  with  $m \leq N^{1-\epsilon}$  such that the restriction of  $\omega^{q(s)}$  to any  $T_j$  is approximately constant. (For Roth's theorem we needed the corresponding result for linear functions, which is much easier.) When this is done, we have that

$$\left| \sum_{s \in S} f(s) \omega^{q(s)} \right| \leq \sum_{j=1}^m \left| \sum_{s \in T_j} f(s) \omega^{q(s)} \right| \approx \sum_{j=1}^m \left| \sum_{s \in T_j} f(s) \right|.$$

An averaging argument then yields some  $j$  such that  $|T_j| \geq N^\epsilon$  and  $\sum_{s \in T_j} f(s) \geq \zeta' |T_j|$ . The second condition is equivalent to the statement that  $|A \cap T_j| \geq (\alpha + \zeta') |T_j|$ . Finally, we can iterate, just as in the proof of Roth's theorem.

A small modification of the above argument (which uses Ruzsa's proof of Freiman's theorem rather than quoting the theorem directly) leads to an upper bound of  $\exp \exp(\delta^{-C})$  for  $N(4, \delta)$ . Equivalently, if  $A \subset \{1, 2, \dots, N\}$  has cardinality at least  $N(\log \log N)^{-c}$ , then it must contain an arithmetic progression of length four. Here,  $C$  and  $c$  are absolute constants. Let us state this result formally.

THEOREM 5. Let  $\delta > 0$  and let  $N$  be a natural number greater than or equal to  $\exp \exp(\delta^{-C})$ , where  $C$  is an absolute constant. Then every subset of the set  $\{1, 2, \dots, N\}$  of size at least  $\delta N$  contains an arithmetic progression of length four.

COROLLARY 6. Let  $r$  and  $N$  be natural numbers such that  $N \geq \exp \exp(r^C)$ , where  $C$  is an absolute constant. Then, however the set  $\{1, 2, \dots, N\}$  is coloured with  $r$  colours, there is a monochromatic arithmetic progression of length four.

In terms of our previous notation, Corollary 6 states that  $M(4, r) \leq \exp \exp(r^C)$ . The bound given by Shelah's argument is more like  $A_4(A_4(r))$ , or in other words a tower of twos of height a tower of twos of height  $r$ . The previous best known bound for Theorem 5 was even larger, since the full strength of van der Waerden's theorem was used by Szemerédi even in this special case [Sz1]. So, as we remarked earlier, the bound was probably something like  $A_6(\delta^{-1})$ .

#### §4. FURTHER RESULTS AND QUESTIONS.

The first question to deal with is whether the above argument generalizes to progressions of arbitrary length. The answer is that most of it does with no difficulty at all. However, one part involves significant extra difficulty. Let us define a set  $A$  to be  $\delta$ -cubically uniform if the intersection

$$A \cap (A + k) \cap (A + l) \cap (A + k + l)$$

is  $\delta$ -uniform for all but at most  $\delta N^2$  pairs  $(k, l)$ . Then if  $A$  is *not*  $\delta$ -cubically uniform, one obtains a set  $B \subset \mathbb{Z}_N^2$  of cardinality at least  $\delta N^2$  and a function  $\phi : B \rightarrow \mathbb{Z}_N$ , such that, for every  $(k, l) \in B$ , the Fourier coefficient of the above intersection at  $\phi(k, l)$  has size at least  $(k, l)$ . The arguments for progressions of length four tell us a great deal about the behaviour of  $\phi$  in each variable separately, but to prove results for longer progressions one must relate these restrictions in order to show that  $\phi$  has some sort of *bilinear* property, and this is not easy to do. At the time of writing, I have a long preprint which deals with the general case and which is still being checked thoroughly. If it stands up to scrutiny, it will give an upper bound for  $N(k, \delta)$  of  $\exp \exp(\delta^{-\exp \exp(k+10)})$ .

This estimate is still far from best possible. In fact, for fixed  $k$ , the best known lower bound for  $N(k, \delta)$  is  $\exp(c(\log(1/\delta))^2)$  [Be]. (This bound may seem unimpressive, but it demonstrates the interesting fact that randomly chosen sets are not the worst, and thereby partly explains the difficulty of Szemerédi's theorem.) The main obstacle to further progress on bounds is that progressions of length three are not fully understood. There is now a development of Roth's argument due to Heath-Brown [H-B] and Szemerédi [Sz3], which gives an upper bound for  $N(3, \delta)$  of  $\exp(\delta^{-C})$ , but this still greatly exceeds the lower bound just mentioned. In particular, the value of  $C$  that comes from the argument exceeds 1, which means that it does not prove the first non-trivial case of Conjecture 3. Finding the correct asymptotic behaviour of  $N(3, \delta)$  is a fascinating problem, not just for its own sake, but because any methods used to solve it are almost certain to have important further applications.

As mentioned in the introduction, several generalizations of Szemerédi's theorem have been proved using ergodic theory and do not (yet) have any other proofs.

Thus, the question of obtaining *any* bounds for them, not just reasonable ones, is open. We mention three such results. The first is the density version, due to Furstenberg, of a theorem of Gallai.

**THEOREM 7.** *Let  $X \subset \mathbb{Z}^d$  and let  $\delta > 0$ . If  $N$  is sufficiently large then every set  $A \subset \{1, 2, \dots, N\}^d$  of size at least  $\delta N^d$  has a subset homothetic to  $X$ .*

It seems likely that our methods can be used to give a quantitative version of Theorem 7, but so far this has not been done.

The next result is the density version of the Hales-Jewett theorem, which itself is one of the central results of Ramsey theory. To state it, we need a small amount of notation. Let  $Q(k, N)$  be the  $N$ -dimensional grid  $\{1, 2, \dots, k\}^N$ . (One can think of elements of  $Q(k, N)$  as words of length  $N$  in the alphabet  $\{1, 2, \dots, k\}$ .) Given  $x = (x_1, \dots, x_N) \in Q(k, N)$ ,  $r \in \{1, 2, \dots, k\}$  and a set  $W \subset \{1, 2, \dots, N\}$ , define  $x \oplus rW$  to be the sequence obtained from  $x$  by replacing  $x_j$  by  $r$  whenever  $j \in W$  and otherwise leaving it unchanged. A *Hales-Jewett line* in  $Q(k, N)$  is a set of the form  $\{x \oplus rW : 1 \leq r \leq k\}$ . The density version of the Hales-Jewett theorem, proved by Furstenberg and Katznelson [FK], is the following result. (The original theorem of Hales and Jewett [HJ] is of course the colouring version.)

**THEOREM 8.** *Let  $\delta > 0$  and  $k \in \mathbb{N}$ . If  $N$  is sufficiently large, then every set  $A \subset Q(k, N)$  of cardinality at least  $\delta k^N$  contains a Hales-Jewett line.*

One can easily deduce Szemerédi's theorem by projecting  $Q(k, N)$  to  $\mathbb{Z}$  in a sensible way. Even the case  $k = 3$  of the Furstenberg-Katznelson theorem is very hard and was open for a long time. In fact, unlike with Szemerédi's theorem, the case  $k = 2$  is not quite obvious either, but it follows easily from a lemma of Sperner [Sp].

Because of the difficulty of the case  $k = 3$ , there seems to be no immediate prospect of a quantitative version of Theorem 8. If one could somehow find a reasonably simple analytic argument when  $k = 3$ , then our methods might conceivably suggest a way of extending this to the general case. I would guess, however, that the problem will remain open for a long time.

Finally, we mention a beautiful generalization of Szemerédi's theorem due to Bergelson and Leibman [BL], which solved a problem that had attracted a great deal of interest for several years.

**THEOREM 9.** *Let  $\delta > 0$  and let  $p_1, \dots, p_k$  be polynomials with integer coefficients such that  $p_i(0) = 0$  for every  $i$ . If  $N$  is sufficiently large, then for every set  $A \subset \{1, 2, \dots, N\}$  of size at least  $\delta N$  there exist integers  $a$  and  $d$  (with  $d \neq 0$ ) such that  $a + p_i(d) \in A$  for every  $i$ .*

Interestingly, the main obstacle for Bergelson and Leibman was obtaining a proof of the colouring version of Theorem 6. They could then use Furstenberg's methods to deduce the density version. Their proof of the colouring version also used ergodic theory, but it can be done purely combinatorially (see [M] or [W]).

The most elementary case of Theorem 9 that does not follow from Szemerédi's theorem is when  $k = 2$ ,  $p_1(x) = 0$  and  $p_2(x) = x^2$ . Then the result states that  $A$  contains a pair of the form  $(a, a + d^2)$ . This result was first proved by Furstenberg [Fu] and Sárközy [S]. Sárközy's argument used exponential sums and



gave a sensible bound, which has subsequently been improved by Pintz, Steiger and Szemerédi [PSS] so that it is now known that a density of  $C(\log N)^{-c(N)}$  will suffice, where  $c(N) = \log \log \log \log N/12$ . (It is still not known whether one can get away with a density of  $N^{-\epsilon}$  for some  $\epsilon > 0$ .) It is quite possible, therefore, that some sort of mixture of our methods and other existing methods would give a quantitative version of Theorem 9. This would undoubtedly be a difficult project to carry out, not least because the methods to be mixed are all individually complicated. However, I expect it will be done by somebody in the next ten or fifteen years, if not sooner.

Let me close by saying that in this paper I have concentrated on my recent work because most of the rest is described in the proceedings of the 1994 Congress [G3], and also by Bollobás in this volume.

#### REFERENCES

- [BS] A. Balog and E. Szemerédi, *A statistical theorem of set addition*, *Combinatorica* 14 (1994), 263-268.
- [Be] F. A. Behrend, *On sets of integers which contain no three in arithmetic progression*, *Proc. Nat. Acad. Sci.* 23 (1946), 331-332.
- [BL] V. Bergelson and A. Leibman, *Polynomial extensions of van der Waerden and Szemerédi theorems*, *J. Amer. Math. Soc.* 9 (1996), 725-753.
- [ET] P. Erdős and P. Turán, *On some sequences of integers*, *J. London Math. Soc.* 11 (1936), 261-264.
- [F1] G. R. Freiman, *Foundations of a Structural Theory of Set Addition*, (in Russian), Kazan Gos. Ped. Inst., Kazan (1966).
- [F2] G. R. Freiman, *Foundations of a Structural Theory of Set Addition*, *Translations of Mathematical Monographs* 37, Amer. Math. Soc., Providence, R. I., USA.
- [Fu] H. Furstenberg, *Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, *J. Anal. Math.* 31 (1977), 204-256.
- [FK] H. Furstenberg and Y. Katznelson, *A density version of the Hales-Jewett theorem*, *J. Anal. Math.* 57 (1991), 64-119.
- [G1] W. T. Gowers, *Lower bounds of tower type for Szemerédi's uniformity lemma*, *GAFSA, Geom. Funct. Anal.* 7 (1997), 322-337.
- [G2] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, *GAFSA, Geom. Funct. Anal.* 8 (1998), 529-551.
- [G3] W. T. Gowers, *Recent results in the theory of infinite-dimensional Banach spaces*, *Proc. I.C.M. Zürich 1994*, Birkhäuser Verlag, Basel, Switzerland 1995.
- [GRS] R. L. Graham, B. L. Rothschild and J. H. Spencer, *Ramsey Theory*, *Wiley Interscience* (2nd ed. 1990).
- [HJ] A. W. Hales and R. I. Jewett, *Regularity and positional games*, *Trans. Amer. Math. Soc.* 106 (1963), 222-229.

- [H-B] D. R. Heath-Brown, *Integer sets containing no arithmetic progressions*, J. London Math. Soc. (2) 35 (1987), 385-394.
- [M] R. McCutcheon, *Elemental methods in ergodic Ramsey theory* (to appear).
- [PH] J. Paris and L. Harrington, *A mathematical incompleteness in Peano arithmetic*, in Handbook of Mathematical Logic (J. Barwise ed.), North-Holland (1977), 1133-1142.
- [PSS] J. Pintz, W. L. Steiger and E. Szemerédi, *On sets of natural numbers whose difference set contains no squares*, J. London Math. Soc. (2) 37 (1988), 219-231.
- [R1] K. F. Roth, *On certain sets of integers*, J. London Math. Soc. 28 (1953), 245-252.
- [R2] K. F. Roth, *Irregularities of sequences relative to arithmetic progressions, IV*, Period. math. Hungar. 2 (1972), 301-326.
- [Ru] I. Ruzsa, *Generalized arithmetic progressions and sumsets*, Acta Math. Hungar. 65 (1994), 379-388.
- [S] A. Sárközy, *On difference sets of integers I*, Acta Math. Acad. Sci. Hungar. 31 (1978), 125-149.
- [Sh] S. Shelah, *Primitive recursive bounds for van der Waerden numbers*, J. Amer. Math. Soc. 1 (1988), 683-697.
- [Sp] E. Sperner, *Ein Satz über Untermengen einer endlichen Menge*, Math. Z. 27 (1928), 544-548.
- [Sz1] E. Szemerédi, *On sets of integers containing no four elements in arithmetic progression*, Acta Math. Acad. Sci. Hungar. 20 (1969), 89-104.
- [Sz2] E. Szemerédi, *On sets of integers containing no  $k$  elements in arithmetic progression*, Acta Arith. 27 (1975), 299-345.
- [Sz3] E. Szemerédi, *Integer sets containing no arithmetic progressions*, Acta Math. Hungar. 56 (1990), 155-158.
- [vdW] B. L. van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw Arch. Wisk. 15 (1927), 212-216.
- [W] M. J. Walters, *Combinatorial proofs of the polynomial van der Waerden theorem and the polynomial Hales-Jewett theorem*, J. London Math. Soc., (to appear).
- [We] H. Weyl, *Über die Gleichverteilung von Zahlen mod Eins*, Math. Annalen 77 (1913), 313-352.

W. T. Gowers  
University of Cambridge  
Department of Pure Mathematics  
and Mathematical Statistics  
16 Mill Lane  
Cambridge CB2 1SB  
England  
wtg10@dpmmms.cam.ac.uk

## EDITOR'S REMARK:

Due to a failure of the printing device, Figure 1 in the article of Curtis T. McMullen on page 841 of Volume II of these Proceedings is slightly scrambled. We therefore reproduce it here in correct form:

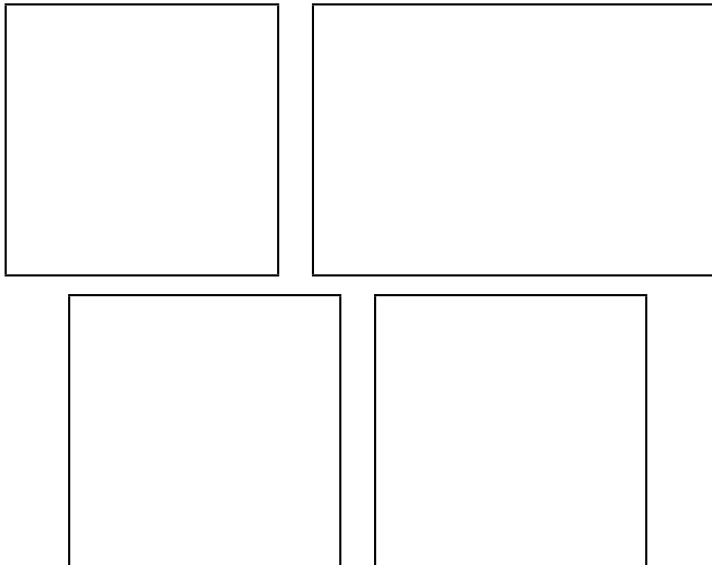


Figure 1. Dynamical systems with deep points: a totally degenerate Kleinian group, the Feigenbaum polynomial, a critical circle map and the golden mean Siegel disk.

## RIGIDITY AND INFLEXIBILITY IN CONFORMAL DYNAMICS

CURTIS T. MCMULLEN<sup>1</sup>

## 1 INTRODUCTION

This paper presents a connection between the rigidity of hyperbolic 3-manifolds and universal scaling phenomena in dynamics.

We begin by stating an inflexibility theorem for 3-manifolds of infinite volume, generalizing Mostow rigidity (§2). We then connect this inflexibility to dynamics and discuss:

- The geometrization of 3-manifolds which fiber over the circle (§2);
- The renormalization of unimodal maps  $f : [0, 1] \rightarrow [0, 1]$  (§4),
- Real-analytic circle homeomorphisms with critical points (§5), and
- The self-similarity of Siegel disks (§6).

Chaotic sets for these four examples are shown in Figure 1. The snowflake in the first frame is the limit set  $\Lambda$  of a Kleinian group  $\Gamma$  acting on the Riemann sphere  $S_\infty^2 = \partial\mathbb{H}^3$ . Its center  $c$  is a *deep point* of  $\Lambda$ , meaning the limit set is very dense at microscopic scales near  $c$ . Because of the inflexibility and combinatorial periodicity of  $M = \mathbb{H}^3/\Gamma$ , the limit set is also self-similar at  $c$  with a universal scaling factor.

The remaining three frames show deep points of the (filled) Julia set for other conformal dynamical systems: the Feigenbaum polynomial, a critical circle map and the golden ratio Siegel disk. Our goal is to explain an inflexibility theory that leads to universal scaling factors and convergence of renormalization for these examples as well.

The qualitative theory of dynamical systems, initiated by Poincaré in his study of celestial mechanics, seeks to model and classify stable regimes, where the topological form of the dynamics is locally constant. In the late 1970s physicists discovered a rich, universal structure in the onset of instability. One-dimensional dynamical systems emerged as elementary models for critical phenomena, phase transitions and renormalization.

In pure mathematics, Mostow and others have developed a rigidity theory for compact manifolds  $M^n$  of constant negative curvature,  $n \geq 3$ , and other quotients of symmetric spaces. This theory shows  $M$  is determined up to isometry by  $\pi_1(M)$

---

<sup>1</sup>Research supported in part by the NSF.

1991 Mathematics Subject Classification: 30D05, 30F40, 58F11, 58F23

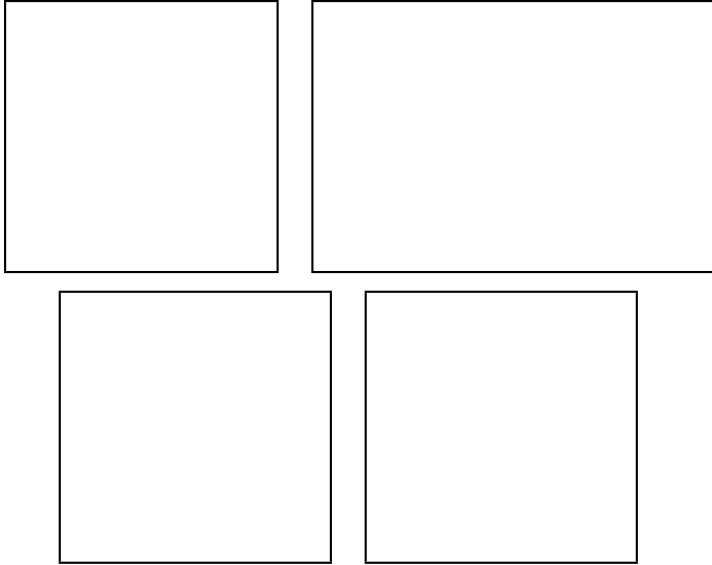


Figure 1. Dynamical systems with deep points: a totally degenerate Kleinian group, the Feigenbaum polynomial, a critical circle map and the golden mean Siegel disk.

as an abstract, finitely-presented group. Remarkably, rigidity of  $M$  is established via the ergodic theory of  $\pi_1(M)$  acting on the boundary of the universal cover of  $M$ .

In our case,  $M = \mathbb{H}^3/\Gamma$  is a hyperbolic 3-manifold, the boundary of its universal cover  $\mathbb{H}^3$  is isomorphic to  $S^2$ , and the action of  $\pi_1(M) \subset \text{Isom}^+(\mathbb{H}^3) = PSL_2(\mathbb{C})$  on  $S^2$  is conformal. Similarly, upon complexification, 1-dimensional dynamical systems give rise to holomorphic maps on the Riemann sphere  $\widehat{\mathbb{C}} \cong S^2$ . Hyperbolic space  $\mathbb{H}^3$  enters the dynamical picture as a means to organize *geometric limits* under rescaling (§3). The universality observed by physicists can then be understood, as in the case of 3-manifolds, in terms of rigidity of these geometric limits.

We conclude with progress towards the classification of hyperbolic manifolds (§7), where geometric limits also play a central role.

## 2 HYPERBOLIC 3-MANIFOLDS AND FIBRATIONS

A *hyperbolic manifold* is a complete Riemannian manifold with a metric of constant curvature  $-1$ . Mostow rigidity states that any two closed, homotopy equivalent hyperbolic 3-manifolds are actually isometric.

In this section we discuss a remnant of rigidity for *open* manifolds. Let  $\text{core}(M) \subset M$  denote the *convex core* of  $M$ , defined as the closure of the set of geodesic loops in  $M$ . The manifold  $M$  satisfies  *$[r, R]$ -injectivity bounds*,  $r > 0$ , if for any  $p \in \text{core}(M)$ , the largest embedded ball  $B(p, s) \subset M$  has radius  $s \in [r, R]$ .

Let  $f : M \rightarrow N$  be a homotopy equivalence between a pair of hyperbolic 3-manifolds. Then  $f$  is a  $K$ -quasi-isometry if, when lifted to the universal covers,

$$\begin{aligned} \text{diam}(\tilde{f}(B)) &\leq K(\text{diam } B + 1) \quad \forall B \subset \tilde{M}, \quad \text{and} \\ \text{diam}(\tilde{f}^{-1}(B)) &\leq K(\text{diam } B + 1) \quad \forall B \subset \tilde{N}. \end{aligned}$$

A diffeomorphism  $f : M \rightarrow N$  is an *asymptotic isometry* if  $f$  is exponentially close to an isometry deep in the convex core. That is, there is an  $A > 1$  such that for any nonzero vector  $v \in T_p M$ ,  $p \in \text{core}(M)$ , we have

$$\left| \log \frac{|Df(v)|}{|v|} \right| \leq CA^{-d(p, \partial \text{core}(M))}.$$

In [Mc2] we show:

**THEOREM 2.1 (GEOMETRIC INFLEXIBILITY)** *Let  $M$  and  $N$  be quasi-isometric hyperbolic 3-manifolds with injectivity bounds. Then  $M$  and  $N$  are asymptotically isometric.*

Mostow rigidity is a special case: if  $M$  and  $N$  are closed, then any homotopy equivalence  $M \sim N$  is a quasi-isometry, injectivity bounds are automatic, and  $\partial \text{core}(M) = \emptyset$ , so an asymptotic isometry is an isometry.

To sketch the proof of Theorem 2.1, recall any hyperbolic 3-manifold  $M$  determines a conformal dynamical system, namely the action of its fundamental group  $\pi_1(M)$  on the sphere at infinity  $S_\infty^2 = \partial \mathbb{H}^3$  for the universal cover  $\tilde{M} \cong \mathbb{H}^3$ . The *limit set*  $\Lambda \subset S_\infty^2$  is the chaotic locus for this action; its convex hull covers the core of  $M$ . The action is properly discontinuously on the rest of the sphere, and the quotient  $\partial M = (S_\infty^2 - \Lambda)/\pi_1(M)$  gives a natural Riemann surface at infinity for  $M$ .



Figure 2. An observer deep in the convex core sees a kaleidoscopic view of  $\partial M$ .

A quasi-isometric deformation of  $M$  determines a quasiconformal deformation  $v$  of  $\partial M$ , which in turn admits a (harmonic) visual extension  $V$  to an equivalent deformation of  $M$ . The strain  $SV(p)$  is the average of the ellipse field  $Sv = \bar{\partial}v$  over all visual rays  $\gamma$  from  $p$  to  $\partial M$ . By our injectivity bounds,  $\gamma$  corkscrews chaotically before exiting the convex core. Thus the ellipses of  $Sv$  on  $\partial M$  appear in random orientations as seen from  $p$  (Figure 2). This randomness provides abundant cancellation in the visual average, and we find the metric distortion

$\|SV(p)\|$  is exponentially small compared to  $\|Sv\|_\infty$ . Thus  $V$  is an infinitesimal asymptotic isometry.

In dimension 3, any two quasi-isometric hyperbolic manifolds are connected by a smooth path in the deformation space, so the global theorem follows from the infinitesimal version.

Inflexibility is also manifest on the sphere at infinity. Let us say a local homeomorphism  $\phi$  on  $S_\infty^2 \cong \widehat{\mathbb{C}}$  is  $C^{1+\alpha}$ -conformal at  $z$  if the complex derivative  $\phi'(z)$  exists and

$$\phi(z + t) = \phi(z) + \phi'(z) \cdot t + O(|t|^{1+\alpha}).$$

We say  $x \in \Lambda \subset S_\infty^2$  is a *deep point* if  $\Lambda$  is so dense at  $x$  that for some  $\beta > 0$ ,

$$B(y, s) \subset B(x, r) - \Lambda \implies s = O(r^{1+\beta}).$$

It is easy to see that a geodesic ray  $\gamma \subset \mathbb{H}^3$  terminating at a deep point in the limit set penetrates the convex hull of  $\Lambda$  at a linear rate. From the inflexibility theorem we find:

**COROLLARY 2.2** *Let  $M$  and  $N$  satisfy injectivity bounds, and let  $\phi : S_\infty^2 \rightarrow S_\infty^2$  be a quasiconformal conjugacy between  $\pi_1(M)$  and  $\pi_1(N)$ . Then  $\phi$  is  $C^{1+\alpha}$ -conformal at every deep point of the limit set of  $\pi_1(M)$ .*

The inflexibility theorem is motivated by the following application to 3-manifolds that fiber over the circle. Let  $S$  be a closed surface of genus  $g \geq 2$  and let  $\psi \in \text{Mod}(S)$  be a pseudo-Anosov mapping class. Let

$$T_\psi = S \times [0, 1] / \{(x, 0) \sim (\psi(x), 1)\}$$

be the 3-manifold fibering over the circle with fiber  $S$  and monodromy  $\psi$ . By a deep theorem of Thurston,  $T_\psi$  is hyperbolic. To find its hyperbolic structure, let  $V(S)$  denote the variety of representations  $\rho : \pi_1(S) \rightarrow \text{Isom}(\mathbb{H}^3)$ , and define

$$\mathcal{R} : V(S) \rightarrow V(S)$$

by  $\mathcal{R}(\rho) = \rho \circ \psi_*^{-1}$ . We refer to  $\mathcal{R}$  as a *renormalization operator*, because it does not change the group action on  $\mathbb{H}^3$ , only its marking by  $\pi_1(S)$ .

Let  $QF(S) \stackrel{Q}{\cong} \text{Teich}(S) \times \text{Teich}(\overline{S}) \subset V(S)$  denote the space of quasifuchsian groups, and define

$$M(X, \psi) = \lim_{n \rightarrow \infty} Q(X, \psi^{-n}Y), \quad \text{for any } (X, Y) \in \text{Teich}(S) \times \text{Teich}(\overline{S}).$$

Then  $M = M(X, \psi)$  has injectivity bounds, its convex core is homeomorphic to  $S \times [0, \infty)$ , and the manifolds  $M$  and  $\mathcal{R}(M)$  are quasi-isometric. By the inflexibility theorem there is an asymptotic isometry  $\Psi : M \rightarrow M$  in the homotopy class of  $\psi$ , so the convex core of  $M$  is asymptotically periodic. As  $n$  tends to  $\infty$ , the marking of  $\mathcal{R}^n(M)$  moves into the convex core at a linear rate, and we find:

**THEOREM 2.3** *The renormalizations  $\mathcal{R}^n(M(X, \psi))$  converge exponentially fast to a fixed-point  $M_\psi$  of  $\mathcal{R}$ .*

Since  $\mathcal{R}(M_\psi) = M_\psi$ , the map  $\psi$  is realized by an isometry  $\alpha$  on  $M_\psi$ , and the quotient  $T_\psi = M_\psi/\langle\alpha\rangle$  gives the desired hyperbolic structure on the mapping cylinder of  $\psi$ .

This iterative construction of  $T_\psi$  hints at a dynamical theory of the action of  $\text{Mod}(S)$  on the variety  $V(S)$ , as does the following result [Kap]:

**THEOREM 2.4 (KAPOVICH)** *The derivative  $D\mathcal{R}_\psi$  is hyperbolic on the tangent space to  $V(S)$  at  $M_\psi$  for all pseudo-Anosov mapping classes on closed surfaces.*

The snowflake in the first frame of Figure 1 is a concrete example of the limit set  $\Lambda$  for a Kleinian group  $\Gamma = \pi_1(M(X, \psi))$  as above. In this example  $S$  is a torus, made hyperbolic by introducing a single orbifold point  $p \in S$  of order 3; and  $\psi = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \in SL_2(\mathbb{Z}) \cong \text{Mod}(S)$  is the simplest pseudo-Anosov map. The suspension of  $p \in S$  gives a singular geodesic  $\gamma \subset T_\psi$  forming the orbifold locus of the mapping torus of  $\psi$ .

The picture is centered at a deep point  $c \in \Lambda$  fixed by an elliptic element of order 3 in  $\Gamma$ . The limit set  $\Lambda$  is a nowhere dense but very furry tree, with six limbs meeting at  $c$ . By general results,  $\Lambda$  is a locally connected dendrite, with Hausdorff dimension two but measure zero [CaTh], [Th1, Ch. 8], [Sul1], [BJ1]; in fact by [BJ2] we have  $0 < \mu_h(\Lambda) < \infty$  for the gauge function  $h(r) = r^2 |\log r \log \log r|^{1/2}$ .

One can easily construct a quasiconformal automorphism  $\phi$  of  $\Gamma$ , with  $\phi(c) = c$  and  $\phi \circ \gamma = \psi_*(\gamma) \circ \phi$  for all  $\gamma \in \Gamma$ . By Corollary 2.2,  $\phi$  is  $C^{1+\alpha}$ -conformal at  $c$ , and we find:

**THEOREM 2.5** *The limit set  $\Lambda$  is self-similar at each elliptic fixed-point in  $\Lambda$ , with scaling factor  $\phi'(c) = e^L$ . Here  $L$  is the complex length of the singular geodesic  $\gamma$  on  $T_\psi$ .*

In particular the self-similarity factor  $e^L$  is inherited from the geometry of the rigid manifold  $T_\psi$ , and it is universal across all manifolds  $M(X, \psi)$  attracted to  $M_\psi$  under renormalization.

### 3 GEOMETRIC LIMITS IN DYNAMICS

In this section we extend the inflexibility of Kleinian groups and their limit sets to certain other conformal dynamical systems  $\mathcal{F}$  and their Julia sets  $J$ , where we will find:

*The conformal structure at the deep points of  $J$  is determined by the topological dynamics of  $\mathcal{F}$ .*

Consider the space  $\mathcal{H}$  of all holomorphic maps  $f : U(f) \rightarrow V(f)$  between domains in  $\widehat{\mathbb{C}}$ . Introduce a (non-Hausdorff) topology on  $\mathcal{H}$  such that  $f_n \rightarrow f$  if



for any compact  $K \subset U(f)$ , we have  $K \subset U(f_n)$  for all  $n \gg 0$  and  $f_n|K \rightarrow f|K$  uniformly.

A *holomorphic dynamical system* is a subset  $\mathcal{F} \subset \mathcal{H}$ . Given a sequence of dynamical systems  $\mathcal{F}_n \subset \mathcal{H}$ , the *geometric limit*  $\mathcal{F} = \limsup \mathcal{F}_n$  consists of all maps  $f = \lim f_{n_i}$  obtained as limits of subsequences  $f_{n_i} \in \mathcal{F}_{n_i}$ .

To bring hyperbolic space into the picture, identify  $\widehat{\mathbb{C}}$  with the boundary of the Poincaré ball model for  $\mathbb{H}^3$ , let  $\text{F}\mathbb{H}^3$  be its frame bundle, and let  $\omega_0 \in \text{F}\mathbb{H}^3$  be a standard frame at the center of the ball. Given any other  $\omega \in \text{F}\mathbb{H}^3$ , there is a unique Möbius transformation  $g$  sending  $\omega_0$  to  $\omega$ , and we define

$$(\mathcal{F}, \omega) = g^*(\mathcal{F}) = \{g^{-1} \circ f \circ g : f \in \mathcal{F}\}.$$

In other words,  $(\mathcal{F}, \omega)$  is  $\mathcal{F}$  as ‘seen from’  $\omega$ .

We say  $\mathcal{F}$  is *twisting* if it is essentially nonlinear — for example, if there exists an  $f \in \mathcal{F}$  with a critical point, or if  $\mathcal{F}$  contains a free group of Möbius transformations.

Given a closed set  $J \subset \widehat{\mathbb{C}}$ , we say  $(\mathcal{F}, J)$  is *uniformly twisting* if  $\limsup(\mathcal{F}, \omega_n)$  is twisting for any sequence  $\omega_n \in \text{F}(\text{hull}(J))$ , the frame bundle over the convex hull of  $J$  in  $\mathbb{H}^3$ . Informally, uniform twisting means  $\mathcal{F}$  is quite nonlinear at every scale around every point of  $J$ .

For a Kleinian group, the pair  $(\Gamma, \Lambda(\Gamma))$  is uniformly twisting iff  $M = \mathbb{H}^3/\Gamma$  has injectivity bounds. Thus geometric inflexibility, Corollary 2.2, is a special case of [Mc2]:

**THEOREM 3.1 (DYNAMIC INFLEXIBILITY)** *Let  $(\mathcal{F}, J)$  be uniformly twisting, and let  $\phi$  be a quasiconformal conjugacy from  $\mathcal{F}$  to another holomorphic dynamical system  $\mathcal{F}'$ . Then  $\phi$  is  $C^{1+\alpha}$ -conformal at all deep points of  $J$ .*

The next three sections illustrate how such inflexibility helps explain universal scaling in dynamics.

#### 4 RENORMALIZATION OF INTERVAL MAPS

Let  $f : I \rightarrow I$  be a real-analytic map on an interval. The map  $f$  is *quadratic-like* if  $f(\partial I) \subset \partial I$  and  $f$  has a single quadratic critical point  $c_0(f) \in \text{int}(I)$ . The basic example is  $f(x) = x^2 + c$  on  $[-a, a]$  with  $f(a) = a$ . We implicitly identify maps that are linearly conjugate.

If an iterate  $f^p|L$  is also quadratic-like for some interval  $L$ , with  $c_0(f) \in L \subset I$ , then we can take the least such  $p > 1$  and define the *renormalization* of  $f$  by

$$\mathcal{R}(f) = f^p|L.$$

The order of the intervals  $L, f(L), \dots, f^p(L) = L \subset I$  determines a permutation  $\sigma(f)$  on  $p$  symbols.

The map  $f$  is *infinitely renormalizable* if the sequence  $\mathcal{R}^n(f)$  is defined for all  $n > 0$ . The *combinatorics* of  $f$  is then recorded by the sequence of permutations  $\tau(f) = \langle \sigma(\mathcal{R}^n(f)) \rangle$ . We say  $f$  has *bounded combinatorics* if only finitely many permutations occur, and *periodic combinatorics* if  $\tau(\mathcal{R}^q f) = \tau(f)$  for some  $q \geq 1$ .

**THEOREM 4.1** *Let  $f : I \rightarrow I$  be infinitely renormalizable, with combinatorics of period  $q$ . Then  $\mathcal{R}^{qn}(f) \rightarrow F$  exponentially fast as  $n \rightarrow \infty$ , where  $F$  is the unique fixed-point of the renormalization operator  $\mathcal{R}^q$  with the same combinatorics as  $f$ .*

For example, the Feigenbaum polynomial  $f(x) = x^2 - 1.4101155 \dots$ , arising at the end of the cascade of period doublings in the quadratic family, has  $\tau(f) = \langle (12), (12), (12), \dots \rangle$ . Under renormalization,  $\mathcal{R}^n(f)$  converges exponentially fast to a solution of the functional equation

$$F \circ F(x) = \alpha^{-1}F(\alpha x).$$

To formulate the speed of convergence more completely, extend  $f : I \rightarrow I$  to a complex analytic map on a neighborhood of  $I \subset \mathbb{C}$ , and let  $F : W \rightarrow \mathbb{C}$  denote the maximal analytic continuation of the renormalization fixed-point. Then we find there is an  $A > 1$  such that for any compact  $K \subset W$ , we have

$$\sup_{z \in K} |\mathcal{R}^n(f)(z) - F(z)| = O(A^{-n}),$$

where  $\mathcal{R}^n(f)$  is suitably rescaled.

Now suppose only that  $f$  has bounded combinatorics. Under iteration of  $f$ , all but countably many points in  $I$  are attracted to the postcritical Cantor set

$$P(f) = \overline{\bigcup_{n>0} f^n(c_0(f))} \subset I.$$

**THEOREM 4.2** *Let  $f$  and  $g$  be infinitely renormalizable maps with the same bounded combinatorics. Then  $f|P(f)$  and  $g|P(g)$  are  $C^{1+\alpha}$ -conjugate.*

Thus quantitative features of the attractor  $P(f)$  (such as its Hausdorff dimension) are determined by the combinatorics  $\tau(f)$ .

These universal properties of quadratic-like maps were observed experimentally and linked to renormalization by Feigenbaum and Coullet-Tresser in the late 1970s. A program for applying complex quadratic-like maps to renormalization was formulated by Douady and Hubbard in the early 1980s. Sullivan introduced a wealth of new ideas and established the convergence  $\mathcal{R}^{nq}(f) \rightarrow F$  [Sul3], [Sul4]. The inflexibility theory gives a new proof yielding, in addition, exponential speed of convergence and  $C^{1+\alpha}$ -smoothness of conjugacies.

Our approach to renormalization is via *towers* [Mc2]. For simplicity we treat the case of the Feigenbaum polynomial  $f$ . By Sullivan's *a priori* bounds, the sequence of renormalizations  $\langle \mathcal{R}^n(f) \rangle$  is compact, and all limits are complex quadratic-like maps with definite moduli. Passing to a subsequence we can arrange that  $\mathcal{R}^{n+i}(f) \rightarrow f_i$  and obtain a tower

$$\mathcal{T} = \langle f_i : i \in \mathbb{Z} \rangle \quad \text{such that } f_{i+1} = f_i \circ f_i \forall i.$$

The Julia set  $J(\mathcal{T}) = \bigcup J(f_i)$  is dense in  $\mathbb{C}$ , and we deduce that  $\mathcal{T}$  is rigid — it admits no quasiconformal deformations. Convergence of renormalization,  $\mathcal{R}^n(f) \rightarrow F$ , then easily follows.

The rapid speed of convergence of renormalization comes from inflexibility of the one-sided tower  $\mathcal{T} = \langle f, f^2, f^4, \dots \rangle$ . To establish this inflexibility, we first show the full dynamical system  $\mathcal{F}(f) = \{f^{-i} \circ f^j\}$  contains copies of  $f^{2^n}$  near every  $z \in J(f)$  and at every scale. Thus  $(\mathcal{F}(f), J(f))$  is *uniformly twisting*. Next we use expansion in the hyperbolic metric on  $\mathbb{C} - P(f)$  to show  $c_0(f)$  is a *deep point* of  $J(f)$ . Finally by Theorem 3.1, a quasiconformal conjugacy  $\phi$  from  $f$  to  $\mathcal{R}(f) = f \circ f$  is actually  $C^{1+\alpha}$ -conformal at the critical point. At small scales  $\phi$  provides a nearly linear conjugacy from  $\mathcal{R}^n(f)$  to  $\mathcal{R}^{n+1}(f)$ , and exponential convergence follows.

The second frame of Figure 1 depicts the Julia set of the infinitely renormalizable Feigenbaum polynomial  $f$ , centered at its critical point. The Julia set  $J(f)$  is locally connected [JH], [LS]; it is still unknown if  $\text{area}(J(f)) = 0$ .

Milnor has observed that the Mandelbrot set  $M$  is quite dense at the Feigenbaum point  $c = -1.4101155\dots \in \partial M$  and at other fixed-points of tuning [Mil], and it is reasonable to expect that  $c$  is a deep point of  $M$ . Lyubich has recently given an elegant proof of the hyperbolicity of renormalization at its fixed-points, including a new proof of exponential convergence of  $\mathcal{R}^n(f)$  via the Banach space Schwarz lemma, and a proof of Milnor's conjecture that blowups of  $M$  around the Feigenbaum point converge to the whole plane in the Hausdorff topology [Lyu].

## 5 CRITICAL CIRCLE MAPS

A *critical circle map*  $f : S^1 \rightarrow S^1$  is a real-analytic homeomorphism with a single cubic critical point  $c_0(f) \in S^1$ . A typical example is the *standard map*

$$f(x) = x + \Omega + K \sin(x), \quad x \in \mathbb{R}/2\pi\mathbb{Z}, \quad \Omega \in \mathbb{R}$$

with  $K = -1$  and  $c_0 = 0$ . These maps arise in KAM theory and model the disappearance of invariant circles [FKS], [Lan], [Rand], [Mak], [DGK]. Another class of examples are the rational maps

$$f(z) = \lambda z^2 \frac{z-3}{1-3z}, \quad |\lambda| = 1, \quad (5.1)$$

acting on  $S^1 = \{z : |z| = 1\}$  with  $c_0(f) = 1$ .

If  $f : S^1 \rightarrow S^1$  has no periodic points, then it is topologically conjugate to a rigid rotation by angle  $2\pi\rho(f)$ , where the *rotation number*  $\rho(f)$  is irrational [Y]. The behavior of  $f$  is strongly influenced by the continued fraction of its rotation number,

$$\rho(f) = 1/(a_1 + 1/(a_2 + 1/(a_3 + \dots))), \quad a_i \in \mathbb{N}.$$

By truncating the continued fraction we obtain rational numbers  $p_n/q_n \rightarrow \rho(f)$ . We say  $\rho(f)$  is of *bounded type* if  $\sup a_i < \infty$ .

**THEOREM 5.1 (DE FARIA-DE MELO)** *Let  $f_1, f_2$  be two critical circle maps with equal irrational rotation numbers of bounded type. Then  $f_1$  and  $f_2$  are  $C^{1+\alpha}$ -conjugate.*

We sketch the proof from [dFdM]. Consider a complex analytic extension of  $f(z)$  to a neighborhood of  $S^1$ . Let the *Julia set*  $J(f)$  be the closure of the set of periodic points of  $f$ . As for maps of the interval, one finds the critical point  $c_0(f)$  is a *deep point* of  $J(f)$ , and the full dynamical system  $(\mathcal{F}(f), J(f))$  is *uniformly twisting*. Because of the good arithmetic of  $\rho(f)$ , the forward orbit of the critical point is spread evenly along  $S^1$ , so in fact the Julia set is deep at *every* point on the circle. To complete the proof, one constructs a quasiconformal conjugacy between  $f_1$  and  $f_2$ , and then applies the inflexibility Theorem 3.1 to deduce that  $\phi|_{S^1}$  is  $C^{1+\alpha}$ .

To bring renormalization into the picture, it is useful to work on the universal cover  $\mathbb{R}$  of  $S^1 = \mathbb{R}/2\pi\mathbb{Z}$ . One can then treat the lifted map  $f : \mathbb{R} \rightarrow \mathbb{R}$  and the deck transformation  $g(x) = x + 2\pi$  on an equal footing. The maps  $(f, g)$  form a basis for a subgroup  $\mathbb{Z}^2 \subset \text{Diff}(\mathbb{R})$ , and any matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$  determines a *renormalization operator* by

$$\mathcal{R}(f, g) = (f^a g^b, f^c g^d).$$

When the continued fraction of  $\rho(f)$  is periodic, one can choose  $\mathcal{R}$  such that  $\mathcal{R}^n(f, g)$  converges exponentially fast to a fixed-point of renormalization  $(F, G)$ . For the more general case where  $\rho(f)$  is of bounded type, a finite number of renormalization operators suffice to relate any two adjacent levels of the tower  $\mathcal{T} = \langle f^{q_n} \rangle$ .

The third frame in Figure 1 depicts the Julia set of the rational map  $f(z)$  given by equation (5.1), with  $\lambda \approx -0.7557 - 0.6549i$  chosen so  $\rho(f)$  is the golden ratio. The picture is centered at the deep point  $c_0(f) \in J(f)$ . Petersen has shown  $J(f)$  is locally connected [Pet]; it is an open problem to determine if  $\text{area}(J(f)) = 0$ .

Levin has proposed a similar theory for critical circle *endomorphisms* such as  $f(z) = \lambda z^3(z - 2)/(1 - 2z)$  [Lev].

## 6 THE GOLDEN-RATIO SIEGEL DISK

Let  $f(z) = \lambda z + z^2$ , where  $\lambda = e^{2\pi i\theta}$ .

Siegel showed that  $f$  is analytically conjugate to the rotation  $z \mapsto \lambda z$  on a neighborhood of the origin when  $\theta$  is Diophantine ( $|\theta - p/q| > C/q^n$ ). The *Siegel disk*  $D$  for  $f$  is the maximal domain on which  $f$  can be linearized. For  $\theta$  of bounded type, Herman and Świątek proved that  $\partial D$  is a quasicircle passing through the critical point  $c_0(f) = -\lambda/2$  [Dou1], [Sw]. In particular, the critical point provides the only obstruction to linearization.

Now suppose  $\theta$  is a quadratic rational such as the golden ratio:

$$\theta = \frac{\sqrt{5}-1}{2} = 1/(1 + 1/(1 + 1/(1 + \dots))).$$

Then the continued fraction of  $\theta$  is preperiodic; there is an  $s > 0$  such that  $a_{n+s} = a_n$  for all  $n \gg 0$ . Experimentally, a universal structure emerges at the transition from linear to nonlinear behavior at  $\partial D$  [MN] [Wid]. In [Mc4] we prove:

THEOREM 6.1 *If  $\theta$  is a quadratic irrational, then the boundary of the Siegel disk  $D$  for  $f$  is self-similar about the critical point  $c_0(f) \in \partial D$ .*

More precisely, there is a map  $\phi : (\overline{D}, c_0) \rightarrow (\overline{D}, c_0)$  which is a  $C^{1+\alpha}$ -conformal contraction at the critical point, and locally conjugates  $f^{q_n}$  to  $f^{q_{n+s}}$ .

THEOREM 6.2 *Let  $f$  and  $g$  be quadratic-like maps with Siegel disks having the same rotation number of bounded type. Then  $f|_{\overline{D}_f}$  and  $g|_{\overline{D}_g}$  are  $C^{1+\alpha}$  conjugate.*

For instance, let  $D_a$  be the Siegel disk for  $f_a(z) = \lambda z + z^2 + az^3$ . Then the Hausdorff dimension of  $\partial D_a$  is constant for small values of  $a$ . As for the Julia set we have:

THEOREM 6.3 *If  $\theta$  has bounded type, then the Hausdorff dimension of the Julia set of  $f(z) = e^{2\pi i\theta}z + z^2$  is strictly less than two.*

A blowup of the golden ratio Siegel disk, centered at the critical point  $c_0(f) \in \partial D$ , is shown in the final frame of Figure 1. The picture is self-similar with a universal scaling factor 1.8166... depending only on the rotation number. The Julia set of  $f$  is locally connected [Pet]. Recently Buff and Henriksen have shown that the golden Siegel disk contains a Euclidean triangle with vertex resting on the critical point [BH]; empirically, an angle of approximately  $120^\circ$  will fit.

The mechanism of rigidity for Siegel disks is visible in the geometry of the filled Julia set  $K(f) = \{z : f^n(z) \text{ remains bounded for all } n > 0\}$ . Under iteration, every point in the interior of  $K(f)$  eventually lands in the Siegel disk, and  $\partial K(f) = J(f)$ . The gray cauliflower forming the interior of  $K(f)$  in Figure 1 is visibly dense at the critical point. In fact  $c_0(f)$  is a measurable deep point of  $K(f)$ , meaning

$$\frac{\text{area}(K(f) \cap B(c_0, r))}{\text{area}(B(c_0, r))} = 1 - O(r^\beta), \quad \beta > 0. \quad (6.1)$$

For the proof of Theorem 6.2, one starts with a quasiconformal conjugacy  $\phi$  from  $f$  to  $g$  furnished by the theory of polynomial-like maps [DH]. Since  $f$  and  $g$  have the same linearization on their Siegel disks, we can assume  $\phi$  is conformal on  $D_f$ . But then  $\phi$  is conformal throughout  $\text{int } K(f)$ . By (6.1) the conformal behavior dominates near  $c_0(f)$ , and we conclude  $\phi$  is  $C^{1+\alpha}$ -conformal at the critical point. This smoothness is spread to all points of  $\partial D_f$  using the good arithmetic of  $\theta$ .

The self-similarity of  $\partial D$  is established similarly, using a conjugacy from  $f^{q_n}$  to  $f^{q_{n+s}}$ .

THE DICTIONARY. Table 3 summarizes the parallels which emerge between hyperbolic manifolds, quadratic-like maps on the interval, critical circle maps and Siegel disks. This table can be seen as a contribution to Sullivan's dictionary between conformal dynamical systems [Sul2], [Mc1].

## 7 SURFACE GROUPS AND THEIR GEOMETRIC LIMITS

For a complete classification of conformal dynamical systems, one must go beyond the bounded geometry of the preceding examples, and confront short geodesics,

HYPERBOLIC MANIFOLDS	INTERVAL MAPS	SIEGEL DISKS/ CIRCLE MAPS
Discrete surface group $\Gamma \subset PSL_2(\mathbb{C})$ $M = \mathbb{H}^3/\Gamma$	$\mathbb{R}$ -quadratic polynomial $f(z) = z^2 + c$	Nonlinear rotation $f(z) = \lambda z + z^2$ or $\lambda z^2(z - 3)/(1 - 3z)$
Representation $\rho : \pi_1(S) \rightarrow \Gamma$	Quadratic-like map $f : U \rightarrow V$	Holomorphic commuting pair $(f, g)$
Ending lamination $\epsilon(M) \in \mathcal{GL}(S)$	Tuning invariant $\tau(f) = \langle \sigma(\mathcal{R}^n(f)) \rangle$	Continued fraction $\theta = [a_1, a_2, \dots], \lambda = e^{2\pi i\theta}$
Inj. radius $(M) > r > 0$	Bounded combinatorics	Bounded type
Cut points in $\Lambda$ $= \bigcup_1^\infty$ (Cantor sets)	Postcritical set $P(f) = \overline{\bigcup f^n(c)}, f'(c) = 0$ $=$ (Cantor set) $=$ (circle or quasi-circle)	
$(\mathbb{R}$ -tree of $\epsilon(M), \pi_1(S)$ )	$(\text{proj lim } \mathbb{Z}/p_i, x \mapsto x + 1)$	$(\mathbb{R}/\mathbb{Z}, x \mapsto x + \theta)$
$\Lambda(\Gamma)$ is locally connected	$J(f)$ is locally connected	$J(f)$ is locally connected
area $\Lambda(\Gamma) = 0$	area $(J(f)) = 0?$	
Inj. radius $\in [r, R]$ in core $(M)$	$(\mathcal{F}(f), J(f))$ is uniformly twisting	
Mapping class $\psi \in \text{Mod}(S)$	Kneading permutation	Automorphism $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of $\mathbb{Z}^2$
Renormalization Operators		
$\mathcal{R}(\rho) = \rho \circ \psi^{-1}$	$\mathcal{R}(f) = f^p(z)$	$\mathcal{R}(f, g) = (f^a g^b, f^c g^d)$
Stable Manifold of Renormalization		
$M =$ asymptotic fiber	$f =$ limit of doublings	$\theta =$ golden ratio
Elliptic points deep in $\Lambda(\Gamma)$	Critical point $c_0(f)$ deep in $J(f)$ or $K(f)$	
$\rho \circ \psi^{-n}, n = 1, 2, 3, \dots$	$f^n, n = 1, 2, 4, 8, 16, \dots$	$f^n, n = 1, 2, 3, 5, 8, \dots$
Geometric limit of $\mathcal{R}^n(\rho)$	Quadratic-like tower $\langle f_i : i \in \mathbb{Z} \rangle; f_{i+1} = f_i \circ f_i$	Tower of commuting pairs
Hyperbolic 3-manifold $S \times [0, 1]/\psi$ fibering over the circle	Fixed-points of Renormalization	
Conformal structure is $C^{1+\alpha}$ -rigid at deep points $\implies$ Renormalization converges exponentially fast		
$M$ is asymptotically rigid	$J(f)$ is self-similar at the critical point $c_0(f)$	

Table 3.

unbounded renormalization periods and Liouville rotation numbers. We conclude with an example of such a complete classification in the setting of hyperbolic geometry.

Let  $S$  be the compact surface obtained by removing a disk from a torus. Let  $AH(S) \subset V(S)$  be the set of discrete faithful representations such that  $\rho(\pi_1(\partial S))$  is parabolic. A representation  $\rho : \pi_1(S) \rightarrow \Gamma$  in  $AH(S)$  gives a hyperbolic manifold  $M = \mathbb{H}^3/\Gamma$  homeomorphic to  $\text{int}(S) \times \mathbb{R}$ . To each end of  $M$  one can associate an *end invariant*

$$E^\pm(M) = \begin{cases} \partial^\pm(M) \in \text{Teich}(S) & \text{or} \\ \epsilon^\pm(M) \in \mathbb{PML}(S). \end{cases}$$

In the first case the end is naturally completed by a hyperbolic punctured torus  $\partial^\pm(M)$ ; in the second case the end is pinched along a simple curve or lamination  $\epsilon^\pm(M)$ .

Identifying  $\text{Teich}(S) \cup \mathbb{PML}(S)$  with  $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{R} \cup \infty$ , we may now state:

**THEOREM 7.1 (MINSKY)** *The pair of end invariants establishes a bijection*

$$E : AH(S) \rightarrow \overline{\mathbb{H}} \times \overline{\mathbb{H}} - \overline{\mathbb{R}} \times \overline{\mathbb{R}}$$

with  $E^{-1}$  continuous.

**COROLLARY 7.2** *Each Bers' slice of  $AH(S)$  is bounded by a Jordan curve naturally parameterized by  $\mathbb{R} \cup \infty$ , with rational points corresponding to cusps.*

**COROLLARY 7.3** *Geometrically finite manifolds are dense in  $AH(S)$ .*

Theorem 7.1 establishes a special case of Thurston's *ending lamination conjecture* [Mc1, §4]. We remark that  $E$  is *not* a homeomorphism, and indeed  $AH(S)$  is not even a topological manifold with boundary [Mc3, Appendix].

The proof of Theorem 7.1 from [Min] can be illustrated in the case  $E(M) = (\tau, \lambda)$ , with  $\tau \in \mathbb{H}$  and  $\lambda \in \mathbb{R}$  an irrational number with continued fraction  $[a_1, a_2, \dots]$ . By rigidity of manifolds in  $\partial AH(S)$ , it suffices to construct a quasi-isometry

$$\phi : M \rightarrow M(a_1, a_2, \dots)$$

from  $M$  to a model Riemannian manifold explicitly constructed from the ending invariant. The quasi-isometry is constructed piece by piece, over blocks  $M_i$  of  $M$  corresponding to terms  $a_i$  in the continued fraction.

The construction yields a description not only of manifolds in  $AH(S)$ , but also of their geometric limits, which we formulate as follows.

**THEOREM 7.4** *Every geometric limit  $M = \lim M_n$ ,  $M_n \in AH(S)$ , is determined up to isometry by a sequence  $\langle a_i, i \in I \rangle$ , where*

- $I \subset \mathbb{Z}$  is a possibly infinite interval,
- $a_i \in \text{Teich}(S) \cup \{*\}$  if  $i$  is an endpoint of  $I$ ; and
- $a_i \in \{1, 2, 3, \dots, \infty\}$  otherwise.

Here  $\langle a_i \rangle$  should be thought of as a generalized continued fraction, augmented by Riemann surface data for the geometrically finite ends of  $M$ . (The special point  $\{*\}$  is used for the triply-punctured sphere.)

For example, the sequence  $\langle a_i \rangle = \langle \dots, \infty, \infty, \infty, \dots \rangle$  determines the periodic manifold

$$M_\infty \cong \text{int}(S) \times \mathbb{R} - \left( \bigcup_{\mathbb{Z}} \gamma_i \times \{i\} \right),$$

where  $\gamma_i \subset S$  are simple closed curves and  $i(\gamma_i, \gamma_{i+1}) = 1$ . These curves enumerate the rank two cusps of  $M_\infty$ . Geometrically,  $M_\infty$  is obtained from the Borromean rings complement  $S^3 - B$  (itself a hyperbolic manifold) by taking the  $\mathbb{Z}$ -covering induced by the linking number with one component of  $B$ .

In general the coefficients  $\langle a_i \rangle$  in Theorem 7.4 specify how to obtain  $M$  by Dehn filling the cusps of  $M_\infty$ . Compare [Th2, §7].

Corollaries 7.2 and 7.3 are reminiscent of two open conjectures in dynamics: the local connectivity of the Mandelbrot set, and the density of hyperbolicity for complex quadratic polynomials.

Quadratic polynomials, however, present an infinite variety of parabolic bifurcations, in contrast to the single basic type occurring for punctured tori. This extra diversity is reflected in the topological complexity of the boundary of the Mandelbrot set, versus the simple Jordan curve bounding a Bers slice.

Parabolic bifurcations can be analyzed by Ecalle cylinders [Dou2] and parabolic towers [Hin], both instances of geometric limits as in §3. A complete understanding of complex quadratic polynomials will likely entail a classification of all their geometric limits as well.

#### REFERENCES

- [BJ1] C. J. Bishop and P. W. Jones. Hausdorff dimension and Kleinian groups. *Acta Math.* 179(1997), 1–39.
- [BJ2] C. J. Bishop and P. W. Jones. The law of the iterated logarithm for Kleinian groups. In *Lipa's Legacy (New York, 1995)*, volume 211 of *Contemp. Math.*, pages 17–50. Amer. Math. Soc., 1997.
- [BH] X. Buff and C. Henriksen. Scaling ratios and triangles in Siegel disks. *Preprint, Cornell, 1998*.
- [CaTh] J. W. Cannon and W. P. Thurston. Group invariant Peano curves. *Preprint, Princeton, 1985*.
- [dFdM] E. de Faria and W. de Melo. Rigidity of critical circle mappings I, II. *SUNY IMS Preprints 1997/16,17*.
- [DGK] T. W. Dixon, T. Gherghetta, and B. G. Kenny. Universality in the quasiperiodic route to chaos. *Chaos* 6(1996), 32–42.



- [Dou1] A. Douady. Disques de Siegel et anneaux de Herman. In *Séminaire Bourbaki, 1986/87*, pages 151–172. Astérisque, volume 152-153, 1987.
- [Dou2] A. Douady. Does a Julia set depend continuously on the polynomial? In R. Devaney, editor, *Complex Analytic Dynamics*. AMS Proc. Symp. Appl. Math. 49, 1994.
- [DH] A. Douady and J. Hubbard. On the dynamics of polynomial-like mappings. *Ann. Sci. Éc. Norm. Sup.* 18(1985), 287–344.
- [Hin] B. Hinkle. Parabolic limits of renormalization. *SUNY IMS Preprint 1997/7*.
- [Lan] O. E. Lanford III. Renormalization group methods for circle mappings with general rotation number. In *VIIIth International Congress on Mathematics Physics (Marseille, 1986)*, pages 532–536. World Scientific, 1987.
- [JH] Y. Jiang and J. Hu. The Julia set of the Feigenbaum quadratic polynomial is locally connected. *Preprint, 1993*.
- [Kap] M. Kapovich. On dynamics of pseudo-Anosov homeomorphisms on the representation variety of surface groups. *Ann. Acad. Sci. Fenn. Math.* 23(1998), 83–100.
- [Lev] G. Levin. Bounds for maps of an interval with one reflecting critical point. I. *Fund. Math., To appear*.
- [LS] G. Levin and S. van Strien. Local connectivity of the Julia set of real polynomials. *SUNY IMS Preprint 1995/5; Annals of Math., To appear*.
- [Lyu] M. Lyubich. Feigenbaum-Coulet-Tresser universality and Milnor’s hairiness conjecture. *Annals of Math., To appear*.
- [FKS] L. P. Kadanoff M. J. Feigenbaum and S. J. Shenker. Quasiperiodicity in dissipative systems: a renormalization group analysis. *Phys. D* 5(1982), 370–386.
- [Mak] R. S. MacKay. *Renormalisation in Area-Preserving Maps*. World Scientific, 1993.
- [MN] N. S. Manton and M. Nauenberg. Universal scaling behavior for iterated maps in the complex plane. *Commun. Math. Phys.* 89(1983), 555–570.
- [Mc1] C. McMullen. The classification of conformal dynamical systems. In *Current Developments in Mathematics, 1995*, pages 323–360. International Press, 1995.
- [Mc2] C. McMullen. *Renormalization and 3-Manifolds which Fiber over the Circle*. Annals of Math Studies 142, Princeton University Press, 1996.
- [Mc3] C. McMullen. Complex earthquakes and Teichmüller theory. *J. Amer. Math. Soc.* 11(1998), 283–320.

- [Mc4] C. McMullen. Self-similarity of Siegel disks and the Hausdorff dimension of Julia sets. *Acta Math.*, To appear, 1998.
- [Mil] J. Milnor. Self-similarity and hairiness in the Mandelbrot set. In M. C. Tangora, editor, *Computers in Geometry and Topology*, Lect. Notes Pure Appl. Math., pages 211–259. Dekker, 1989.
- [Min] Y. Minsky. The classification of punctured torus groups. *SUNY IMS Preprint 1997/6*; *Annals of Math.*, To appear.
- [Pet] C. L. Petersen. Local connectivity of some Julia sets containing a circle with an irrational rotation. *Acta Math.* 177(1996), 163–224.
- [Rand] D. Rand. Universality and renormalisation in dynamical systems. In *New Directions in Dynamical Systems*, pages 1–56. Cambridge University Press, 1988.
- [Sul1] D. Sullivan. Growth of positive harmonic functions and Kleinian group limit sets of zero planar measure and Hausdorff dimension two. In *Geometry at Utrecht*, Lecture Notes in Math. 894, pages 127–144. Springer-Verlag, 1981.
- [Sul2] D. Sullivan. Conformal dynamical systems. In *Geometric Dynamics*, Lecture Notes in Math 1007, pages 725–752. Springer-Verlag, 1983.
- [Sul3] D. Sullivan. Quasiconformal homeomorphisms in dynamics, topology and geometry. In *Proceedings of the International Conference of Mathematicians*, pages 1216–1228. Amer. Math. Soc., 1986.
- [Sul4] D. Sullivan. Bounds, quadratic differentials and renormalization conjectures. In F. Browder, editor, *Mathematics into the Twenty-first Century: 1988 Centennial Symposium, August 8-12*, pages 417–466. Amer. Math. Soc., 1992.
- [Sw] G. Świątek. On critical circle homeomorphisms. *Preprint*, 1997.
- [Th1] W. P. Thurston. *Geometry and Topology of Three-Manifolds*. Lecture Notes, Princeton University, 1979.
- [Th2] W. P. Thurston. Hyperbolic structures on 3-manifolds II: Surface groups and 3-manifolds which fiber over the circle. *Preprint*.
- [Wid] M. Widom. Renormalization group analysis of quasi-periodicity in analytic maps. *Commun. Math. Phys.* 92(1983), 121–136.
- [Y] J.-C. Yoccoz. Il n’y a pas de contre-exemple de Denjoy analytique. *C. R. Acad. Sci. Paris Sér. I Math.* 298(1984), 141–144.

Curtis T. McMullen  
Mathematics Department  
Harvard University  
1 Oxford St  
Cambridge, MA 02138



## QUANTUM COMPUTING

PETER W. SHOR

ABSTRACT. The Church-Turing thesis says that a digital computer is a universal computational device; that is, it is able to simulate any physically realizable computational device. It has generally been believed that this simulation can be made efficient so that it entails at most a polynomial increase in computation time. This may not be true if quantum mechanics is taken into consideration. A quantum computer is a hypothetical machine based on quantum mechanics. We explain quantum computing, and give an algorithm for prime factorization on a quantum computer that runs asymptotically much faster than the best known algorithm on a digital computer. It is not clear whether it will ever be possible to build large-scale quantum computers. One of the main difficulties is in manipulating coherent quantum states without introducing errors or losing coherence. We discuss quantum error-correcting codes and fault-tolerant quantum computing, which can guarantee highly reliable quantum computation, given only moderately reliable quantum computing hardware.

1991 Mathematics Subject Classification: Primary 68Q05; Secondary 11Y05, 81P99.

Keywords and Phrases: Quantum computer, computational complexity, prime factorization.

## 1 INTRODUCTION.

Quantum computers are hypothetical machines that use principles of quantum mechanics for their basic operations. They will be very difficult to build; currently experimental physicists are working on two- and three-bit quantum computers, and useful quantum computers would require hundreds to thousands of bits. However, there seem to be no fundamental physical laws that would preclude their construction. In 1994, I showed that a quantum computer could factor large numbers in time polynomial in the length of the numbers, a nearly exponential speed-up over classical algorithms. This factoring result was surprising for a number of different reasons. First, the connection of quantum mechanics with number theory was itself surprising. For cryptographers, the result was surprising because the difficulty of factoring is the basis of the RSA cryptosystem [27], and nobody had anticipated the possibility of an attack via quantum physics. For many theoretical computer

scientists, it was surprising because they had more or less convinced themselves that no type of computing machine could offer this large a speed-up over a classical digital computer. In retrospect, several results [7, 30] should have led them to question this; however, not much attention was paid to these results until they led to the development of the factoring algorithm,

A question that has generated much discussion is where the extra power of quantum computers comes from. There are a number of differences between quantum and classical computers, and most appear to be required for the extra power. In particular, quantum interference is needed; one high-level way to describe the quantum factoring algorithm is that the computation is arranged so that computational paths giving the wrong answer interfere to cancel each other out, leaving a high probability of obtaining the right answer. Another property of quantum systems that plays a crucial role is entanglement, or non-classical correlation, between quantum systems. Many non-quantum physical systems such as waves exhibit interference, but none of these systems exhibits entanglement, and they do not appear usable for quantum computation. Finally, a third property required is the high dimensionality of quantum systems; the dimension of the joint quantum state space of  $n$  objects grows exponentially with  $n$ , whereas classically the dimension of the joint state space of  $n$  objects only grows linearly. The factoring algorithm makes critical use of this extra dimensionality.

In the rest of the paper, I describe these results in more detail. In section 2, I start by discussing Church's thesis, which still appears to hold, and an extension of it, to which quantum computers now appear to be a counterexample. In the following section, I describe the quantum circuit model for quantum computation. This is not laid out particularly well anywhere else, so I spend a reasonable amount of space on it. In section 4, I describe the differences between the quantum circuit model and possible physical realizations of quantum computers, and say a little about why the model appears to give the right definition of what is efficiently computable using quantum mechanics. Section 5 describes the factoring algorithm. Section 6 discusses error-correcting codes and fault-tolerant quantum computing. In the final section, I mention some related results.

## 2 THE POLYNOMIAL CHURCH'S THESIS.

Church's thesis says that any computable function can be computed on a Turing machine, which is essentially a mathematical abstraction of a digital computer. This thesis arose in the 1930's, and was motivated by the realization that three apparently quite distinct definitions of computable functions were all equivalent. It is well known that Church's thesis is not a theorem, because it does not specify a rigorous mathematical definition of "computable"; specifying such a definition would lead to a provable theorem (and in many cases has), but would also detract from the generality of the thesis. What is somewhat less commonly realized is that this thesis can be viewed as a statement about the laws of physics, simply by interpreting computable to mean computable in the physical world. For this interpretation, if the laws of physics are computable by a Turing machine, then Church's thesis is true.

The development of digital computers rendered the distinction between computable and uncomputable functions too coarse in practice, as it does not take into account the time required for computation. What was needed for the theory of computation was some characterization of efficiently computable functions. In the early 1970's, theoretical computer scientists reached a good compromise between theory and practice with the definition of polynomial-time computable functions. These are functions whose value can be computed in a number of steps polynomial in the input size. The corresponding set of languages—functions whose range is  $\{0, 1\}$ —is known as P (or PTIME). While nobody claims that a function computable in time  $n^{100}$  is efficiently computable in practice, the set of polynomial time computable functions is structurally nice enough to use in proofs, and for functions arising in practice it appears to include most of the efficiently computable ones and exclude most of those not efficiently computable. This definition naturally gave rise to a “folk thesis,” the polynomial Church's thesis, which says that any function physically computable in time  $t$  on some machine  $X$  can be computed on a Turing machine in time  $p(t)$ , where  $p$  is a polynomial depending only on the machine  $X$ .

Is this folk thesis valid? One good place to start looking for counterexamples is with physical systems which seem to require large amounts of computer time to simulate. Two obvious such candidates are turbulence and quantum mechanics. I will have nothing further to say about turbulence, except that I think the computational complexity of turbulence is a question worthy of serious study. Richard Feynman, in 1982, was the first to consider the case of quantum mechanics [16]. He gave arguments for why quantum mechanical systems should inherently require an exponential overhead to simulate on digital computers. In a lengthy “side remark,” he proposed using quantum computers, operating on quantum mechanical principles, to circumvent this problem. David Deutsch [15] followed up on Feynman's proposal by defining quantum Turing machines, and suggesting that if quantum computers could solve quantum mechanical problems more quickly than digital computers, they might also solve classical problems more quickly. It currently appears that this is indeed the case. One piece of evidence for this is that quantum computers can solve certain “oracle problems” faster than classical computers [7, 30]; here an oracle problem is one where the computer is given a subroutine (oracle) which must be treated as a black box. The behavior of computational complexity with respect to oracles, however, has not proved a reliable guide to its true behavior. Another piece of evidence that quantum computers are a counterexample to the polynomial Church's thesis is that they can factor integers and find discrete logarithms in polynomial time, something which it is not known how to do on classical computers despite many years of study. The factorization algorithm is discussed later in this paper.

### 3 THE QUANTUM CIRCUIT MODEL.

In this section we discuss the *quantum circuit model* [32] for quantum computation. This is a rigorous mathematical model for a quantum computer. It is not the only mathematical model for quantum computation; there are also the *quantum Turing*

*machine model* [7, 32] and the *quantum cellular automata model*. All these models result in the same class of polynomial-time quantum computable functions. Of these, the quantum circuit model is possibly the simplest to describe. It is also easier to connect with possible physical implementations of quantum computers than the quantum Turing machine model. The disadvantage of this model is that it is not naturally a *uniform* model. Uniformity is a technical condition arising in complexity theory, and to make the quantum circuit model uniform, additional constraints must be imposed on it. This issue is discussed later in this section.

In analogy with a classical bit, a two-state quantum system is called a *qubit*, or quantum bit. Mathematically, a qubit takes a value in the vector space  $\mathbb{C}^2$ . We single out two orthogonal basis vectors in this space, and label these  $V_0$  and  $V_1$ . In “ket” notation, which is commonly used in this field, these are represented as  $|0\rangle$  and  $|1\rangle$ . More precisely, quantum states are invariant under multiplication by scalars, so a qubit lives in two-dimensional complex projective space; for simplicity, we work in complex Euclidean space  $\mathbb{C}^2$ . To conform with physics usage, we treat qubits as column vectors and operate on them by left multiplication.

One of the fundamental principles of quantum mechanics is that the joint quantum state space of two systems is the tensor product of their individual quantum state spaces. Thus, the quantum state space of  $n$  qubits is the space  $\mathbb{C}^{2^n}$ . The basis vectors of this space are parameterized by binary strings of length  $n$ . We make extensive use of the tensor decomposition of this space into  $n$  copies of  $\mathbb{C}^2$ , where  $V_{b_1 b_2 \dots b_n} = V_{b_1} \otimes V_{b_2} \otimes \dots \otimes V_{b_n}$ . Generally, we use position to distinguish the  $n$  different qubits. Occasionally we need some other notation for distinguishing them, in which case we denote the  $i$ 'th qubit by  $V^{[i]}$ . Since quantum states are invariant under multiplication by scalars, they can be normalized to be unit length vectors; except where otherwise noted, quantum states in this paper are normalized. Quantum computation takes place in the quantum state space of  $n$  qubits  $\mathbb{C}^{2^n}$ , and obtains extra computational power from its exponential dimensionality.

In a usable computer, we need some means of giving it the problem we want solved (input), some means of extracting the answer from it (output), and some means of manipulating the state of the computer to transform the input into the desired output (computation). We next briefly describe input and output for the quantum circuit model. We then take a brief detour to describe the classical circuit model; this will motivate the rules for performing the computation on a quantum computer.

Since we are comparing quantum computers to classical computers, the input to a quantum computer will be classical information. It can thus be expressed as a binary string  $S$  of some length  $k$ . We need to encode this in the initial quantum state of the computer, which must be a vector in  $\mathbb{C}^{2^n}$ . The way we do this is to concatenate the bit string  $S$  with  $n - k$  0's to obtain the length  $n$  string  $S0\dots 0$ . We then initialize the quantum computer in the state  $V_{S0\dots 0}$ . Note that the number of qubits is in general larger than the input. These extra qubits are often required as workspace in implementing quantum algorithms.

At the end of a computation, the quantum computer is in a state which is a unit vector in  $\mathbb{C}^{2^n}$ . This state can be written explicitly as  $W = \sum_s \alpha_s V_s$  where  $s$  ranges over binary strings of length  $n$ ,  $\alpha_s \in \mathbb{C}$ , and  $\sum_s |\alpha_s|^2 = 1$ . These  $\alpha_s$

Figure 1: Construction of a Toffoli gate using the classical gates AND, OR and NOT. The input is on the left and the output on the right.

are called *probability amplitudes*, and we say that  $W$  is a *superposition* of basis vectors  $V_s$ . In quantum mechanics, the Heisenberg uncertainty principle tells us that we cannot measure the complete quantum state of this system. There are a large number of permissible measurements; for example, any orthogonal basis of  $\mathbb{C}^{2^n}$  defines a measurement whose possible outcomes are the elements of this basis. However, we assume that the output is obtained by projecting each qubit onto the basis  $\{V_0, V_1\}$ . When applied to a state  $\sum_s \alpha_s V_s$ , this projection produces the string  $s$  with probability  $|\alpha_s|^2$ . The quantum measurement process is inherently probabilistic. Thus we do not require that the computation gives the right answer all the time; but that we obtain the right answer at least  $2/3$  of the time. Here, the probability  $2/3$  can be replaced by any number strictly between  $1/2$  and  $1$  without altering what can be computed in polynomial time by quantum computers—if the probability of obtaining the right answer is strictly larger than  $1/2$ , it can be amplified by running the computation several times and taking the majority vote of the results of these separate computations.

In order to motivate the rules for state manipulation in a quantum circuit, we now take a brief detour and describe the classical circuit model. Recall that a classical circuit can always be written solely with the three gates AND ( $\wedge$ ), OR ( $\vee$ ) and NOT ( $\neg$ ). These three gates are thus said to form a *universal* set of gates. Figure 1 gives an example circuit for a computation called a *Toffoli gate* using these three types of gates. Besides these three gates, note that we also need elements which duplicate the values on wires. These duplicating “gates” are not possible in the domain of quantum computing.

A quantum circuit is similarly built out of logical quantum wires carrying qubits, and quantum gates acting on these qubits. Each wire corresponds to one of the  $n$  qubits. We assume each gate acts on either one or two wires. The possible physical transformations of a quantum system are unitary transformations, so each quantum gate can be described by a unitary matrix. A quantum gate on one qubit is then described by a  $2 \times 2$  matrix, and a quantum gate on two qubits by a  $4 \times 4$  matrix. Note that since unitary matrices are invertible, the computation is



reversible; thus starting with the output and working backwards one obtains the input. Further note that for quantum gates, the dimension of the output space is equal to that of the input space, so at all times during the computation we have  $n$  qubits carried on  $n$  quantum wires. Figure 2 contains an example of a quantum circuit for computing a Toffoli gate.

Quantum gates acting on one or two qubits ( $\mathbb{C}^2$  or  $\mathbb{C}^4$ ) naturally induce a transformation on the state space of the entire quantum computer ( $\mathbb{C}^{2^n}$ ). For example, if  $A$  is a  $4 \times 4$  matrix acting on qubits  $i$  and  $j$ , the induced action on a basis vector of  $\mathbb{C}^{2^n}$  is

$$A^{[i,j]} V_{b_1 b_2 \dots b_n} = \sum_{s=0}^1 \sum_{t=0}^1 A_{b_i b_j st} V_{b_1 b_2 \dots b_{i-1} s b_{i+1} \dots b_{j-1} t b_{j+1} \dots b_n}. \quad (1)$$

This is a tensor product of  $A$  (acting on qubits  $i$  and  $j$ ) with the identity matrix (acting on the remaining qubits). When we multiply a general vector by a quantum gate, it can have negative and positive coefficients which cancel out, leading to quantum interference.

As there are for classical circuits, there are also universal sets of gates for quantum circuits; such a universal set of gates is sufficient to build circuits for any quantum computation. One particularly useful universal set of gates is the set of all one-bit gates and a specific two-bit gate called the Controlled NOT (CNOT). These gates can efficiently simulate any quantum circuits whose gates act on only a constant number of qubits [2]. On basis vectors, the CNOT gate negates the second (target) qubit if and only if the first (control) qubit is 1. In other words, it takes  $V_{XY}$  to  $V_{XZ}$  where  $Z = X + Y \pmod{2}$ . This corresponds to the unitary matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (2)$$

Note that the CNOT is a classical reversible gate. To obtain a universal set of classical reversible gates, you need at least one reversible three-bit gate, such as a Toffoli gate; otherwise you can only perform linear Boolean computations. A Toffoli gate is a doubly controlled NOT, which negates the 3rd bit if and only if the first two are both 1. By itself the Toffoli gate is universal for reversible classical computation, as it can simulate both AND and NOT gates [17]. Thus, if you can make a Toffoli gate, you can perform any reversible classical computation. Further, as long as the input is not erased, any classical computation can be efficiently performed reversibly [3], and thus implemented efficiently by Toffoli gates.

Because of the extra possibilities allowed by quantum interference, for quantum circuits the CNOT together with all quantum one-bit gates forms a universal set of gates. Figure 2 gives a construction of a Toffoli gate out of CNOT gates and one-bit gates [2], showing that this set is at least universal for classical computation. This particular construction does not result in a Toffoli gate with all positive

Figure 2: Construction of a Toffoli gate using quantum gates. The gates represented by  $\oplus$  are CNOT's, where the circle identifies the target qubit. The gate  $R$  is  $\begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$ , and  $R^\dagger$  is the Hermitian transpose of  $R$ . In this construction, the phase on  $V_{101}$  is  $-1$ , and all the other phases are  $+1$ ; the phases can all be made  $+1$  by a somewhat more complicated quantum circuit.

phases—multiplying the corresponding matrices in Figure 2 produces the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{3}$$

which is the classical Toffoli gate with a phase of  $-1$  on one of its outcomes. This still acts classically as a Toffoli gate, since phases are irrelevant to classical computation. In quantum computation, however, we must keep careful track of phases. A more complicated circuit can be constructed which eliminates this phase of  $-1$  [2].

We now define the complexity class BQP, which stands for bounded-error quantum polynomial time. This is the class of languages which can be computed on a quantum computer in polynomial time, with the computer giving the correct answer at least  $2/3$  of the time. To give a rigorous definition of this complexity class using quantum circuits, we need to consider uniformity conditions. Any specific quantum circuit can only compute a function whose domain (input) is binary strings of a specific length. To use the quantum circuit model to implement functions taking arbitrary length binary strings as input, we take a family of quantum circuits, containing one circuit for inputs of each length. Without any further conditions on the family of circuits, the designer of this circuit family could hide an uncomputable function in the design of the circuits for each input length.

This definition would thus result in the unfortunate inclusion of uncomputable functions in the complexity class BQP. To exclude this possibility, we require *uniformity* conditions on the circuit family. The easiest way of doing this is to require a classical Turing machine that on input  $n$  outputs a description of the circuit for length  $n$  inputs, and which runs in time polynomial in  $n$ . For quantum computing, we need an additional uniformity condition on the circuits. It would be possible for the circuit designer to hide uncomputable (or hard-to-compute) information in the unitary matrices corresponding to quantum gates. We thus require that the  $k$ 'th digit of the entries of these matrices can be computed by a second Turing machine in time polynomial in  $k$ . Although we do not have space to discuss this fully, the power of the machines designing the circuit family can actually be varied over a wide range; this helps us convince ourselves that we have the right definition of BQP.

The definition of polynomial time computable functions on a quantum computer is thus those functions computable by a *uniform* family of circuits whose size (number of gates) is polynomial in the length of the input, and which for any input gives the right answer at least  $2/3$  of the time. The corresponding set of languages (functions with values in  $\{0, 1\}$ ) is called BQP.

#### 4 RELATION OF THE MODEL TO QUANTUM PHYSICS.

The quantum circuit model of the previous section is much simplified from the realities of quantum physics. There are operations possible in physical quantum systems which do not correspond to any simple operation allowable in the quantum circuit model, and complexities that occur when performing experiments that are not reflected in the quantum circuit model. This section contains a brief discussion of these issues, some of which are discussed more thoroughly in [7].

In everyday life, objects behave very classically, and on large scales we do not see any quantum mechanical behavior. This is due to a phenomenon called decoherence, which makes superpositions of states decay, and makes large-scale superpositions of states decay very quickly. A thorough discussion of decoherence can be found in [35]; one reason it occurs is that we are dealing with open systems rather than closed ones. Although closed systems quantum mechanically undergo unitary evolution, open systems need not. They are subsystems of systems undergoing unitary evolution, and the process of taking subsystems does not preserve unitarity.

However hard we may try to isolate quantum computers from the environment, they will still undergo some decoherence and errors. We need to know that these processes do not fundamentally change their behavior. Using no error correction, if each gate results in an amount of decoherence and error of order  $1/t$ , then  $O(t)$  operations can be performed before the quantum state becomes so noisy as to usually give the wrong answer [7]. Active error correction can improve this situation substantially, and is discussed in section 6.

In some proposed physical architectures for quantum computers, there are restrictions that are more severe than the quantum computing model. Many of these restrictions do not change the class BQP. For example, it could easily be

the case that a gate could only be applied to a pair of *adjacent* qubits. We can still operate on a pair of arbitrary qubits: by repeatedly exchanging one of these qubits with a neighbor we can bring this pair together. If there are  $n$  qubits in the computer, this can only increase the computation time by a factor of  $n$ , preserving the complexity class BQP.

The quantum circuit model described in the previous section postpones all measurements to the end, and assumes that we are not allowed to use probabilistic steps. Both of these possibilities are allowed in general by quantum mechanics, but neither possibility makes the complexity class BQP larger [7]. For fault-tolerant quantum computing, however, it is very useful to permit measurements in the middle of the computation, in order to measure and correct errors.

The quantum circuit model also assumes that we only operate on a constant number of qubits at a time. In general quantum systems, all the qubits evolve simultaneously according to some Hamiltonian describing the system. This simultaneous evolution of many qubits cannot be described by a single gate in our model, which only operates on two qubits at once. In a realistic model of quantum computation, we cannot allow general Hamiltonians, since they are not experimentally realizable. Some Hamiltonians that act on all the qubits at once, however, are experimentally realizable. It would be nice to know that even though these Hamiltonians cannot be directly described by our model, they cannot be used to compute functions not in BQP in polynomial time. This could be accomplished by showing that systems with such Hamiltonians can be efficiently simulated by a quantum computer. Some work has been done on simulating Hamiltonians on quantum computers [1, 24, 33], but I do not believe this question has been completely addressed yet.

An important aspect of quantum mechanics not used in the quantum circuit model is that identical particles are indistinguishable; in general they must obey either Fermi-Dirac or Einstein-Bose statistics when they are interchanged. Particle statistics do not appear to add any power to the quantum computing model, but I do not believe this has been rigorously proved.

From the view of the current state of experimental physics, quantum computers appear to be extremely difficult to build, but do not seem to violate any fundamental physical laws. As qubits, we need to use quantum systems which are relatively stable, which interact strongly with each other (to carry out quantum gates quickly), but which interact weakly with everything else (to avoid errors caused by interaction with the environment). Since the discovery of the factoring algorithm, a variety of proposals for experimental implementation of quantum computers have been made. One of these proposals is to use the electronic states of ions in an electromagnetic ion trap as the qubits, to manipulate them using lasers, and to communicate between different ions using a vibrational mode of the ions, or *phonon* [12]. Another is to use nuclear spins of atoms in a complex molecule as the qubits, and to manipulate them using nuclear magnetic resonance spectroscopy [14, 18]. A quite recent proposal is to use nuclear spins of impurities embedded in a silicon chip as the qubits, and to manipulate them using electronics on the same chip [23]. None of these proposals has been experimentally realized for more than a handful of qubits, but they all have proponents who believe that

they may be scaled up to obtain much larger working quantum computers.

## 5 THE FACTORING ALGORITHM.

For factoring an  $L$ -bit number  $N$ , the best classical algorithm known is the number field sieve, which asymptotically takes time  $O(\exp(cL^{1/3} \log^{2/3} L))$ . On a quantum computer, the quantum factoring algorithm takes asymptotically  $O(L^2 \log L \log \log L)$  steps. The key idea of the quantum factoring algorithm is the use of a Fourier transform to find the period of the sequence  $u_i = x^i \pmod{N}$ , from which period a factorization of  $N$  can be obtained. The period of this sequence is exponential in  $L$ , so this approach is not practical on a digital computer. On a quantum computer, however, we can find the period in polynomial time by exploiting the  $2^{2L}$ -dimensional state space of  $2L$  qubits, and taking a Fourier transform over this space. The exponential dimensionality of this space permits us to take the Fourier transform of an exponential length sequence. How this works should be clearer from the following sketch of the algorithm, the full details of which are in [28], along with a quantum algorithm for finding discrete logarithms.

The idea behind all the fast factoring algorithms (classical or quantum) is fairly simple. To factor  $N$ , find two residues mod  $N$  such that

$$s^2 \equiv t^2 \pmod{N} \quad (4)$$

but  $s \not\equiv \pm t \pmod{N}$ . We now have

$$(s+t)(s-t) \equiv 0 \pmod{N} \quad (5)$$

and neither of these two factors is  $0 \pmod{N}$ . Thus,  $s+t$  must contain one factor of  $N$  (and  $s-t$  another). We can extract this factor by finding the greatest common divisor of  $s+t$  and  $N$ ; this computation can be done in polynomial time using Euclid's algorithm.

In the quantum factoring algorithm, we find the multiplicative period  $r$  of a residue  $x \pmod{N}$ . This period  $r$  satisfies  $x^r \equiv 1 \pmod{N}$ ; if we are lucky then  $r$  is even, so both sides of this congruence are squares, and we can try the above factorization method. If we have just a little bit more luck, then  $x^{r/2} \not\equiv -1 \pmod{N}$ , so we obtain a factor by computing  $\gcd(x^{r/2} + 1, N)$ . It is a fairly simple exercise in number theory to show that for large  $N$  with two or more prime factors, at least half the residues  $x \pmod{N}$  produce prime factors using this technique, and that for most large  $N$ , the fraction of good residues  $x$  is much higher; thus, if we try several different values for  $x$ , we have to be particularly unlucky not to obtain a factorization using this method.

We now need to explain what the quantum Fourier transform is. The quantum Fourier transform on  $k$  qubits maps the state  $V_a$ , where  $a$  is considered as an integer between 0 and  $2^k - 1$ , to a superposition of the states  $V_b$  as follows:

$$V_a \rightarrow \frac{1}{2^{k/2}} \sum_{b=0}^{2^k-1} \exp(2\pi i ab/2^k) V_b \quad (6)$$

It is easy to check that this transformation defines a unitary matrix. It is not as straightforward to implement this Fourier transform as a sequence of one- and two-bit quantum gates. However, an adaption of the Cooley-Tukey algorithm decomposes this transformation into a sequence of  $k(k - 1)/2$  one- and two-bit gates. More generally, the discrete Fourier transform over any product  $Q$  of small primes (of size at most  $\log Q$ ) can be performed in polynomial time on a quantum computer.

We are now ready to give the quantum algorithm for factoring. What we do is design a polynomial-size circuit which starts in the quantum state  $V_{00\dots 0}$  and whose output, with reasonable probability, lets us factor an  $L$ -bit number  $N$  in polynomial time using a digital computer. This circuit has two main registers, the first of which is composed of  $2L$  qubits and the second of  $L$  qubits. It also requires a few extra qubits of work space, which we do not mention in the summary below but which are required for implementing the step (8) below.

We start by putting the computer into the state representing the superposition of all possible values of the first register:

$$\frac{1}{2^L} \sum_{a=0}^{2^L-1} V_a \otimes V_0. \tag{7}$$

This can easily be done using  $2L$  gates by putting each of the qubits in the first register into the state  $\frac{1}{\sqrt{2}}(V_0 + V_1)$ .

We next use the value of  $a$  in the first register to compute the value  $x^a \pmod N$  in the second register. This can be done using a reversible classical circuit for computing  $x^a \pmod N$  from  $a$ . Computing  $x^a \pmod N$  using repeated squaring takes asymptotically  $O(L^3)$  quantum gates using the grade school multiplication algorithm, and  $O(L^2 \log L \log \log L)$  gates using fast integer multiplication (which is actually faster only for relatively large values of  $L$ ). This leaves the computer in the state

$$\frac{1}{2^L} \sum_{a=0}^{2^L-1} V_a \otimes V_{x^a \pmod N}. \tag{8}$$

The next step is to take the discrete Fourier transform of the first register, as in Equation (6). This puts the computer into the state

$$\frac{1}{2^{2L}} \sum_{a=0}^{2^L-1} \sum_{b=0}^{2^L-1} \exp(2\pi iab/2^{2L}) V_b \otimes V_{x^a \pmod N}. \tag{9}$$

Finally, we measure the state. This will give the output  $V_b \otimes V_{x^j \pmod N}$  with probability equal to the square of the coefficient on this vector in the sum (9). Since many values of  $x^a \pmod N$  are equal, many terms in this sum contribute to each coefficient. Explicitly, this probability is:

$$\frac{1}{2^{4L}} \left| \sum_{\substack{a \equiv j \pmod r \\ 0 \leq a < 2^{2L}}} \sum_{b=0}^{2^L-1} \exp(2\pi iab/2^{2L}) \right|^2. \tag{10}$$

This is a geometric sum, and it is straightforward to check that this sum is very small except when

$$rb \approx d2^{2L} \tag{11}$$

for some integer  $d$ . We thus are likely to observe only values of  $b$  satisfying (11). Rewriting this equation, we obtain

$$\frac{b}{2^{2L}} \approx \frac{d}{r}. \tag{12}$$

We know  $b$  and  $2^{2L}$ , and we want to find  $r$ . We chose  $2L$  as the size of the first register in order to make  $d/r$  likely to be the closest fraction to  $b/2^{2L}$  with denominator at most  $N$ . Thus, all we need do to find  $r$  is to round  $b/2^{2L}$  to a fraction with denominator less than  $N$ . This can be done in polynomial time using a continued fraction expansion.

More details of this algorithm can be found in [28]. Recently, Zalka [34] has analyzed the resources required by this algorithm much more thoroughly, improving upon their original values in many respects. For example, he shows that you can use only  $3L + o(L)$  qubits, whereas the original algorithm required  $2L$  extra qubits for workspace, giving a total of  $5L$  qubits. He also shows how to efficiently parallelize the algorithm to run on a parallel quantum computer.

## 6 QUANTUM ERROR CORRECTING CODES.

One of the reactions to the quantum factoring paper was that quantum computers would be impossible to build because it would be impossible to reduce decoherence and errors to levels low enough to ensure reliable quantum computation. Indeed, without error correction, it would probably be an impossible task to build quantum computers large enough to factor 100-digit numbers—factoring such a number requires billions of steps, so each step would need to be accurate to better than one part in a billion, a virtually impossible challenge in experimental physics. Fortunately, it is possible to design fault-tolerant circuits for quantum computers, which allow computations of arbitrary length to be performed with gates having accuracy of only some constant  $c$ . Current estimates using known methods for constructing fault-tolerant quantum circuits put this constant in the range of  $10^{-4}$  [25]; improved techniques could increase this value.

For some time after the factoring algorithm was discovered, however, it was believed that making quantum computers fault-tolerant was impossible. There were a number of plausible arguments for why this should be true. One argument for the impossibility of quantum error correction was based on the theorem, related to the Heisenberg uncertainty principle, that an unknown quantum state cannot be duplicated. The argument was that since you cannot duplicate quantum information, you cannot have more than one copy of a qubit around at any given time, and thus that it was impossible to protect a qubit from errors. Indeed, the simplest classical error correcting code is the 3-repetition code, which triplicates each bit, and other classical error correcting codes also appear to be based on repetition. Despite this pessimistic argument, quantum error correcting codes do exist, and

are generalizations of classical error-correcting codes. The codes protect quantum information from error and decoherence not by duplicating it, but by hiding it in subspaces of  $\mathbb{C}^{2^n}$  which are affected very little by decoherence and errors that act on only one qubit, or only a small number of qubits.

Before we discuss quantum error correcting codes in detail, we need to say more about the measurement process. For every set of orthogonal subspaces of  $\mathbb{C}^{2^n}$  which span the entire space, there is a measurement which outputs one of these subspaces as classical data, and which projects the original quantum state onto this subspace. For example, if our quantum state is  $\sum_{s=0}^{2^n-1} \alpha_s V_s$  and we measure the first qubit, we obtain the (not normalized) quantum state

$$\sum_{s'=0}^{2^{n-1}-1} \alpha_{0s'} V_{0s'} \quad \text{with probability} \quad \sum_{s'=0}^{2^{n-1}-1} |\alpha_{0s'}|^2, \tag{13}$$

and the state

$$\sum_{s'=0}^{2^{n-1}-1} \alpha_{1s'} V_{1s'} \quad \text{with probability} \quad \sum_{s'=0}^{2^{n-1}-1} |\alpha_{1s'}|^2. \tag{14}$$

This measurement corresponds to the partition of  $\mathbb{C}^{2^n}$  into the two subspaces generated by  $\{V_{0s'}\}$  and by  $\{V_{1s'}\}$ .

To illustrate how quantum error correcting codes work, we first explain what goes wrong when we try to extend the straightforward repetition code to the quantum realm. The obvious thing to do is to take

$$\begin{aligned} V_0 &\rightarrow V_{000} \\ V_1 &\rightarrow V_{111} \end{aligned} \tag{15}$$

This indeed does protect against value errors in our qubits. Suppose we apply the error transformation  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  to the first qubit. Then the encodings of  $V_0$  and  $V_1$  get taken to the states  $V_{100}$  and  $V_{011}$ , respectively. The subspace generated by these two quantum states is orthogonal to that generated by the original codewords  $V_{000}$  and  $V_{111}$ . We can thus make a measurement which reveals that there was a bit flip in the first qubit without measuring (and thus disturbing) the encoded quantum state. It is easily seen that bit flips applied to each of the three qubits create subspaces that are orthogonal to each other, so there is a quantum measurement which identifies on which qubit a bit flip error occurred without disturbing the encoded state. It is then straightforward to fix the bit flip error by applying a quantum gate to the qubit in error.

However, a phase error on one of the qubits is disastrous in this code. What happens when the error transformation  $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$  is applied to one of the qubit is that it takes an encoded  $V_0$  to an encoded  $V_0$ , and takes an encoded  $V_1$  to an encoded  $e^{i\phi} V_1$ . Thus, a phase error on *any* of the three qubits translates to a phase error on the encoded qubit, making the encoding three times as vulnerable to phase errors.



We now explain the above difficulty another way which illuminates the construction of quantum error-correcting codes. We consider phase flip errors, which are phase errors with  $\phi = \pi$ . There is a transformation that takes phase flips to bit flips and vice versa. This is the Hadamard transform, which is

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (16)$$

When this is applied to all the qubits in the code above, as well as the encoded qubits, we get the code

$$\begin{aligned} V_0 &\rightarrow \frac{1}{2}(V_{000} + V_{110} + V_{101} + V_{011}) \\ V_1 &\rightarrow \frac{1}{2}(V_{111} + V_{001} + V_{010} + V_{100}) \end{aligned} \quad (17)$$

Notice that for this code, a single bit flip interchanges  $V_0$  and  $V_1$ , so this code cannot correct bit flips, again showing that code (15) cannot correct phase flips.

What we need to make a good quantum error correcting code is a code having the property that bit flips can be corrected both before and after the application of the Hadamard transformation. Such a code can be found by generalizing the codes (15) and (17), and it was discovered independently by two groups [11, 31]. It is based on the classical 7-bit Hamming code, and is defined as follows:

$$\begin{aligned} V_0 &\rightarrow \frac{1}{\sqrt{8}}(V_{0000000} + V_{1110100} + V_{0111010} + V_{0011101} \\ &\quad + V_{1001110} + V_{0100111} + V_{1010011} + V_{1101001}) \\ V_1 &\rightarrow \frac{1}{\sqrt{8}}(V_{1111111} + V_{0001011} + V_{1000101} + V_{1100010} \\ &\quad + V_{0110001} + V_{1011000} + V_{0101100} + V_{0010110}). \end{aligned} \quad (18)$$

The indices of the basis vectors in the support of the encoded states are exactly the classical 7-bit Hamming code. The fact that the classical Hamming code corrects one error means this code can correct one bit flip. This quantum code is taken to itself under the application of the Hadamard transform (16) both to the encoded qubit and to each encoding qubit, showing that it is also able to correct one phase flip. In fact, it can correct a simultaneous bit flip and phase flip.

We now have a seven bit code that can corrects a phase and/or a bit flip applied to one of its qubits. This is by no means the complete set of possible quantum mechanical errors on one qubit; this set is parameterized by several continuous variables. However, the ability of a quantum code to correct the following set of four one-bit errors confers on it the ability to correct any possible one-bit quantum error:

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \quad (19)$$

These four errors correspond to no error, a bit flip, a phase flip, and a simultaneous bit and phase flip, respectively. We do not have enough space to explain this in

detail, but the fact that these form a basis for the set of  $2 \times 2$  matrices is enough to imply they can correct any one-bit quantum error. The rigorous details of this implication are in [11]; a more intuitive explanation is in [6].

This quantum Hamming code is the smallest nontrivial example of a set of codes based on linear binary codes named CSS codes after their discoverers [11, 31], and which contains codes that are much more efficient than this first one. For fault tolerance, which will be discussed next, we only need to use CSS codes. However, a more general framework that includes these codes was discovered simultaneously by two groups [19, 20, 10]. Substantial work on quantum error correcting codes has occurred since their discovery, much of it referenced in [10].

In classical computers, error correcting codes have been found to be very useful for storing and transmitting information, but not for providing fault-tolerant computing. It is difficult to perform gates on encoded qubits, and once the qubits have been decoded, they are no longer protected from error. Theoretically, the best way to provide high levels of fault tolerance for classical circuits was discovered by von Neumann, who discovered it after reasoning that some means of protection from error had to exist in biological systems. This method involves the use of massive redundancy. If you plan to run your computer for  $t$  steps, you make  $c \log t$  copies of every bit, and during the computation, you continually compare them in order to catch any errors you have made. The drawback of this method is that it requires  $c \log t$  overhead, which is too expensive for use in practice, given the remarkably low levels of error obtainable by current computer hardware. On the other hand, it can be shown that if you must use unreliable gates,  $O(\log t)$  overhead is required to achieve reliable computation, so von Neumann's construction is up to a constant factor best possible.

As in classical computers, quantum error correcting codes should work well for protecting qubits while they are being stored and transmitted. However, because quantum data cannot be cloned, fault tolerance using massive redundancy cannot work in quantum computers. We thus need another method. The methods currently known for providing fault tolerance in quantum computers are based on quantum error correcting codes [25, 29]. To use quantum error correcting codes for reliable computation, we need to show how to do two additional things with them, neither of which is at first glance obviously possible. These are:

1. correct errors using noisy gates so that errors are corrected faster than new errors are introduced;
2. perform quantum gates on encoded bits without decoding them, while making sure that any errors cannot propagate too widely during the computation.

We do not have much space to discuss how to accomplish these tasks, so we say nothing about the first task, and give only a very broad sketch of how the second task can be accomplished.

In order to compute on encoded qubits without decoding, we need fault-tolerant implementations of a universal set of quantum gates on the encoded qubits. What we need are circuits having the property that if errors occur in only a few quantum gates, or are present in a few of the inputs, these errors cannot affect too many of the qubits in the output of the gate (otherwise, there will

Figure 3: Implementation of a CNOT gate on qubits encoded using the quantum Hamming code (18). This circuit can be used in fault-tolerant quantum circuits, since an error in the  $i$ 'th wire of an encoded qubit (or in the  $i$ 'th gate) can only propagate to the  $i$ 'th wire of each of the output qubits. Gates that are implementable on encoded qubits in this fashion are called *transversal* gates.

be more errors than the quantum error-correcting codes we are using can correct). It turns out that certain gates are easy to implement this way. Figure 3 shows how to perform a CNOT on two encoded qubits by performing it on each pair of encoding wires. Similarly, if a Hadamard gate (16) is applied to each quantum wire, a Hadamard gate is performed on the encoded qubit. Implementations of this type are called transversal gates, and these do not form a universal set of quantum gates. We need to supplement the set of transversal gates with an extra gate implemented using another method. It was shown how to perform the Toffoli gate fault-tolerantly on encoded qubits in [29], and the set of transversal gates augmented by this gate is a universal set of gates.

To implement a circuit of size  $t$  fault-tolerantly, the techniques of [29] required gates with error rate at most  $O(1/(\log t)^c)$ . To obtain fault tolerance using gates with constant error rate requires a further idea: the use of concatenated codes. These are nested codes, where each layer catches most of the errors missed by the previous layer. Judicious use of concatenated codes and careful analysis shows that gates with some constant error rate are able to produce fault-tolerant quantum circuits; this constant is currently estimated at around  $10^{-4}$ . For more details, see the excellent survey of fault-tolerance in quantum computing [25].

## 7 OTHER WORK.

This section discusses areas related to quantum computing; it is not intended to be a complete survey, but a somewhat idiosyncratic view of some results I find interesting. I have tried to mention survey articles when they exist, so the interested reader can find pointers to the literature. One excellent resource is the quant-ph

preprint archive, at <http://xxx.lanl.gov/>, containing preprints of many recent research articles in this field. John Preskill, at Caltech, recently taught a course on quantum computing and quantum information, and his excellent set of lecture notes is available on the web [26].

As Feynman suggested, it appears that quantum computing is good at computing simulations of quantum mechanical dynamics. Some work has already appeared showing this [1, 24, 33], but much remains to be done.

A significant algorithm in quantum computing is L. K. Grover's search algorithm, which searches an unordered list of  $N$  items (or the range of an efficiently computable function) for a specific item in time  $O(\sqrt{N})$ , an improvement on the optimal classical algorithm, which must look at  $N/2$  items on average before finding a specific item [21]. The technique used in this algorithm can be applied to a number of other problems to also obtain a square root speed-up [22].

One of the earliest applications of quantum mechanics to areas related to computing is quantum cryptography, more specifically quantum key distribution. Consider two people trying to share some secret information which they can then use as a key for a cryptosystem. If they can only communicate over a phone line possibly open to eavesdroppers, they have no choice but to use public key cryptography [27], which may be open to attack by a quantum computer or (say) discovery of a fast factoring algorithm on a classical computer. However, if they in addition have access to an optical fiber which they can use to transmit quantum states, they can use quantum cryptography [4]. One of them (the sender) transmits states chosen at random from a set of non-orthogonal quantum states (e.g.  $V_0$ ,  $V_1$ ,  $\frac{1}{\sqrt{2}}(V_0 + V_1)$ ,  $\frac{1}{\sqrt{2}}(V_0 - V_1)$ ) The receiver then reads the states in either the basis  $\{V_0, V_1\}$  or  $\{\frac{1}{\sqrt{2}}(V_0 \pm V_1)\}$ , again chosen at random. Communicating over a classical channel using a special protocol, they can figure out the states for which they agree on the measurement basis; they should agree on about half the states, each of which supplies a bit towards a secret key. If an eavesdropper was listening, she cannot have gained too much information—since she does not know in which basis the states were transmitted, any information she gains must cause a disturbance in the states, which the sender and receiver can detect by measuring some of their states instead of using them for the secret key. They can also further sacrifice some of their bits to ensure that the eavesdropper gains virtually no information about the remaining bits of their key, and that they agree on all the bits of this key. Since the original quantum cryptography papers, there have been many articles either proposing other schemes or working towards rigorous proofs that the scheme is secure against all possible quantum attacks (i.e., when the eavesdropper has access to a quantum computer). A good bibliography on quantum cryptography is [8].

Quantum cryptography is but one aspect of a rapidly burgeoning subject, quantum information theory. A startling result in this field, the interest in which helped contribute to its recent rapid growth, was the discovery of quantum teleportation [5]. It is not possible to transmit an unknown quantum state using only classical information (say, over a telephone line). However, if two people share an EPR pair, such as the quantum state  $\frac{1}{\sqrt{2}}(V_{01} - V_{10})$ , with the sender holding

the first qubit and the receiver holding the second, then they can transmit an unknown quantum bit using a classical channel. The sender performs a combined measurement on the unknown state and the EPR pair, and transmits the classical two-bit outcome to the receiver, who then uses this information to reconstruct the unknown state from his half of the EPR pair. The act of teleportation thus uses up the resource of *entanglement* between the sender and the receiver, which is present in the EPR pair. One research direction in quantum information theory is quantifying the amount of entanglement in a quantum state. Another direction is measuring the classical and the quantum capacities of a quantum channel. More information on quantum information theory can be found in Preskill's course notes [26] and in the survey article [6].

Another recent development is the study of quantum communication complexity. If two people share quantum entanglement, as well as a classical communications channel, this permits them to send each other qubits, but does not reduce the number of bits required for transmission of classical information. However, if they both have some classical data, and they wish to compute some classical function of this data, shared quantum entanglement may help reduce the amount of purely classical communication required to compute this function. This was first shown by Cleve and Burhman [13]. More results on communication complexity have since been shown, and some of these were recently used to give lower bounds on the power of quantum computers in the black-box (oracle) model [9].

There has been a substantial amount of recent work on both quantum error correcting codes and quantum fault tolerance. Many results on quantum error correcting codes are reviewed in [10], and Preskill has written an excellent survey of fault tolerant quantum computing [25].

## REFERENCES

- [1] D. S. Abrams and S. Lloyd, Simulation of many-body Fermi systems on a universal quantum computer, *Phys. Rev. Lett.* 79 (1997), 2586–2589.
- [2] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Elementary gates for quantum computation, *Phys. Rev. A* 52 (1995), 3457–3467.
- [3] C. H. Bennett, Logical reversibility of computation, *IBM J. Res. Develop.* 17 (1973), 525–532.
- [4] C. H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (1984) 175–179.
- [5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, *Phys. Rev. Lett.* 70 (1993), 1895–1898.
- [6] C. H. Bennett and P. W. Shor, Quantum information theory, *IEEE Transactions on Information Theory* (1998), to appear.

- [7] E. Bernstein and U. Vazirani, Quantum complexity theory, *SIAM J. Computing* 26 (1997), 1411–1473.
- [8] G. Brassard, Quantum cryptography: a bibliography, *SIGACT News* 24:3 (1993), 16–20. A more recent version is online at:  
<http://www.iro.umontreal.ca/~crepeau/Biblio-QC.html>.
- [9] H. Burhman, R. Cleve and A. Wigderson, Quantum vs. classical communication and computation, in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, ACM Press, New York (1998), 63–69.
- [10] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over  $GF(4)$ , *IEEE Transactions on Information Theory* 44 (1998), 1369–1387.
- [11] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, *Phys. Rev. A* 54 (1995) 1098–1106.
- [12] J. I. Cirac and P. Zoller, Quantum computations with cold trapped ions, *Phys. Rev. Lett.* 74 (1995), 4091–4094.
- [13] R. Cleve and H. Burhman, Substituting quantum entanglement for communication, *Phys. Rev. A* 56 (1997), 1201–1204.
- [14] D. G. Cory, A. F. Fahmy and T. F. Havel, Ensemble quantum computing by nuclear magnetic resonance spectroscopy, *Proc. Nat. Acad. Sci.* 94 (1997), 1634–1639.
- [15] D. Deutsch, Quantum theory, the Church–Turing principle and the universal quantum computer, *Proc. Roy. Soc. London Ser. A* 400 (1985) 96–117.
- [16] R. Feynman, Simulating physics with computers, *Internat. J. Theoret. Phys.* 21 (1982), 467–488.
- [17] E. Fredkin and T. Toffoli, Conservative logic, *Internat. J. Theoret. Phys.* 21 (1982), 219–253.
- [18] N. A. Gershenfeld and I. L. Chuang, Bulk spin resonance quantum computation *Science* 275 (1997), 350–356.
- [19] D. Gottesman, A class of quantum error-correcting codes saturating the quantum Hamming bound, *Phys. Rev. A* 54 (1996), 1862–1868.
- [20] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*, Ph.D. Thesis, California Institute of Technology (1997). Also LANL e-print <http://xxx.lanl.gov/> quant-ph/9705052, available online at <http://xxx.lanl.gov/>.
- [21] L. K. Grover, Quantum mechanics helps in searching for a needle in a haystack, *Phys. Rev. Lett.* 78 (1997), 325–328.

- [22] L. K. Grover, A framework for fast quantum mechanical algorithms, in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, ACM Press, New York (1998), 53–62.
- [23] B. E. Kane, A silicon-based nuclear spin quantum computer, *Nature* 393 (1998), 133–137.
- [24] S. Lloyd, Universal quantum simulators, *Science* 273 (1996), 1073–1078.
- [25] J. Preskill, Fault-tolerant quantum computation, to appear in *Introduction to Quantum Computation*, H.-K. Lo, S Popescu and T. P. Spiller, eds. (1998). Also LANL e-print quant-ph/9712048, available online at <http://xxx.lanl.gov/>.
- [26] J. Preskill, Lecture notes for Physics 229 (1998), available online at <http://www.theory.caltech.edu/people/preskill/ph229/>.
- [27] R. L. Rivest, A. Shamir and L. Adleman, A method of obtaining digital signatures and public-key cryptosystems, *Comm. Assoc. Comput. Mach.* 21 (1978), 120–126.
- [28] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Computing* 26 (1997), 1484–1509.
- [29] P. W. Shor, Fault-tolerant quantum computation, in *Proc. 37th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos, CA (1996), 56–65.
- [30] D. R. Simon, On the power of quantum computation, *SIAM J. Computing* 26 (1997), 1474–1483.
- [31] A. Steane, Multiple particle interference and quantum error correction, *Proc. Roy. Soc. London Ser. A* 452 (1996), 2551–2577.
- [32] A. Yao, Quantum circuit complexity, in *Proceedings of the 34th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos, CA (1993), 352–361.
- [33] C. Zalka, Efficient simulation of quantum systems by quantum computers, *Proc. Roy. Soc. London Ser. A* 454 (1998), 313–322.
- [34] C. Zalka, Fast versions of Shor’s quantum factoring algorithm, LANL e-print quant-ph/9806084 (1998), available online at <http://xxx.lanl.gov/>.
- [35] W. H. Zurek, Decoherence and the transition from quantum to classical, *Physics Today* 44 (1991) 36–44.

Peter W. Shor  
AT&T Labs – Research  
180 Park Ave.  
Florham Park, NJ 07932 USA  
[shor@research.att.com](mailto:shor@research.att.com)

## SECTION 1. LOGIC

## O-MINIMALITY

A. J. WILKIE

In the paper [11] Tarski makes the following *observation*: every subset of the set of real numbers  $\mathbb{R}$  definable in the ordered ring  $\langle \mathbb{R}; +, \cdot, 0, 1, < \rangle$  (which I shall henceforth denote by  $\bar{\mathbb{R}}$ ) is a finite union of open intervals and points. This is certainly an easy consequence of his famous quantifier elimination theorem ([12]) - that every subset of  $\mathbb{R}^n$  definable in  $\bar{\mathbb{R}}$  is semi-algebraic, i.e. definable by a *quantifier free* formula - and must have seemed a relatively unimportant one at the time. However, it turned out to be a remarkable insight. For in the 1980's van den Dries showed that most of the qualitative geometric and topological finiteness properties enjoyed by the class of semi-algebraic sets actually follow from this observation alone. Indeed, many such properties, e.g. finite cell-decomposition theorems in the continuous category, do not even require the ring structure, although some do, e.g. finite cell-decomposition theorems in the differentiable category and finite triangulation theorems.

The property described in Tarski's observation is now known as *o-minimality* and, as was shown by Knight, Pillay and Steinhorn in [7] and [10], it can be fruitfully considered in quite general situations: a structure  $\mathcal{M} = \langle M, <, \dots \rangle$ , where  $<$  is a dense, linear order (without endpoints) of the domain  $M$ , is called *o-minimal* if every definable (without parameters) subset of  $M$  is a finite union of points and open intervals (with endpoints in  $M \cup \{\pm\infty\}$ ).

It is a suprising and non-obvious fact that o-minimality is preserved under elementary equivalence. This is one of the main results of [7] and is typical of the "uniformity-in-parameters" that crops up frequently in this subject: it is equivalent to the statement that for any formula  $\phi(x_1, \dots, x_n, y)$  of the language of  $\mathcal{M}$ , there is a natural number  $N$  depending only on  $\phi$  such that the set  $\{b \in M : \mathcal{M} \models \phi[a_1, \dots, a_n, b]\}$  is the union of at most  $N$  open intervals and points for any choice of parameters  $a_1, \dots, a_n \in M$ .

More generally, one can also deduce from the assumption of o-minimality that there are only finitely many homeomorphism types amongst sets of the form  $\langle < b_1, \dots, b_r > \in M^r : \mathcal{M} \models \psi[a_1, \dots, a_n, b_1, \dots, b_r] \rangle$  as  $\langle a_1, \dots, a_n \rangle$  varies over  $M^n$ , where  $\psi(x_1, \dots, x_n, y_1, \dots, y_r)$  is a formula of the language of  $\mathcal{M}$ . (Here,  $M^r$  is equipped with the product topology and  $M$  with the order topology.) Similar



results and, indeed, a definitive account of the foundations of the general theory of o-minimality can be found in van den Dries' recent book [3].

Of course, this general theory is only worthwhile if there are interesting examples (other than  $\mathbb{R}$  and its reducts) and it is my main aim in this short note to state a result that provides a rich source of o-minimal expansions of  $\mathbb{R}$ .

Let  $\tilde{\mathbb{R}}$  be any expansion of the real ordered field  $\bar{\mathbb{R}}$  with language  $\tilde{L}$  say. Call a formula  $\psi$  of  $\tilde{L}$  *tame* if there exists a natural number  $N$  (depending only on  $\psi$ ) such that whenever the free variables of  $\psi$  are partitioned into two classes, say  $\psi = \psi(x_1, \dots, x_m, y_1, \dots, y_r)$ , then the set  $\{ \langle b_1, \dots, b_r \rangle \in \mathbb{R}^r : \mathcal{M} \models \psi[a_1, \dots, a_m, b_1, \dots, b_r] \}$  has at most  $N$  connected components for any choice of  $\langle a_1, \dots, a_m \rangle \in \mathbb{R}^m$ . Then I know of no counterexample to the following

CONJECTURE

With  $\tilde{\mathbb{R}}$  as above, if every quantifier free formula of  $\tilde{L}$  is tame then  $\tilde{\mathbb{R}}$  is o-minimal (which, in fact, implies that every formula of  $\tilde{L}$  is tame - see [7] again).

I am, however, rather sceptical.

In order to state my result in this direction it is convenient to introduce a unary connective, denoted  $C$ , to our language, with truth condition:-

$\tilde{\mathbb{R}} \models (C\phi)[a_1, \dots, a_n]$  if and only if  $\langle a_1, \dots, a_n \rangle$  lies in the closure (in  $\mathbb{R}^n$ ) of the set  $\{ \langle b_1, \dots, b_n \rangle \in \mathbb{R}^n : \tilde{\mathbb{R}} \models \phi[b_1, \dots, b_n] \}$ .

Clearly  $C$  is already definable in  $\tilde{L}$  (for interpretations expanding  $\bar{\mathbb{R}}$ ) but the point is that we have the following

THEOREM (Wilkie, [14]).

Let  $\tilde{\mathbb{R}}$  be as above and suppose that every quantifier free formula is tame. Then so is any formula that can be obtained from quantifier free formulas by finitely many applications of conjunction, disjunction, existential quantification and the connective  $C$ . Further, if we also assume that  $\tilde{\mathbb{R}}$  has the form  $\langle \bar{\mathbb{R}}, \mathcal{F} \rangle$  where  $\mathcal{F}$  is a collection of infinitely differentiable functions from  $\mathbb{R}^n$  to  $\mathbb{R}$  (for various  $n$ 's), then *any* formula of  $\tilde{L}$  is equivalent (in  $\tilde{\mathbb{R}}$ ) to one of this type, and hence (since a connected subset of  $\mathbb{R}$  is an interval)  $\tilde{\mathbb{R}}$  is o-minimal.

The reason for proving a theorem of this type was that the tameness condition on the quantifier free definable sets was established for a wide class of examples through the work of Khovanskii ([6], but see also [5] in conjunction with [8]). He showed that it holds for structures of the form  $\langle \mathbb{R}, f_1, \dots, f_p \rangle$  where  $f_1, \dots, f_p : \mathbb{R}^n \rightarrow \mathbb{R}$  are infinitely differentiable functions (actually, the following implies they are analytic) satisfying a system of partial differential equations of the form

$$\frac{\partial f_i}{\partial x_j} = P_{i,j}(x_1, \dots, x_n, f_1, \dots, f_i), \quad 1 \leq i \leq p, 1 \leq j \leq p,$$

where each  $P_{i,j}(x_1, \dots, x_n, y_1, \dots, y_i)$  is a polynomial with real coefficients. (The sequence  $f_1, \dots, f_p$  is then called a *Pfaffian chain* on  $\mathbb{R}^n$ ).

Thus, by the theorem, these structures are o-minimal.

In particular,  $\langle \bar{\mathbb{R}}, \exp \rangle$  is o-minimal, where  $\exp(x) = e^x$  is the exponential function (take  $p = n = 1, P_{1,1}(x_1, y_1) = y_1$ ). In fact, this result appears in [1] although some of the arguments in that paper are, to my mind, incomplete. However, the main idea there is fundamentally sound and was studied extensively by my student S. Maxwell (see[9]) before I finally adapted it to establish the theorem above. Perhaps I should also mention that in the case of  $\langle \bar{\mathbb{R}}, \exp \rangle$  we now have better information (see[13]): every definable set is *existentially* definable (from which o-minimality follows very easily from Khovanskii's result). However, nothing like this is known for expansion of  $\bar{\mathbb{R}}$  by general Pfaffian chains.

I conclude with an application of the general uniformity result mentioned earlier. Clearly, if we take  $\mathcal{M} = \bar{\mathbb{R}}$  then we can deduce that for any  $n, k$  there is  $N = N(n, k)$  such that there are at most  $N$  homeomorphism types of sets of the form  $P^{-1}(0)$  where  $P : \mathbb{R}^n \rightarrow \mathbb{R}$  is a real polynomial of total degree at most  $k$ . This was actually proved by Hardt (see[4]) before o-minimality came on the scene. Now van den Dries noticed that if we take  $\mathcal{M} = \langle \bar{\mathbb{R}}, \exp \rangle$  then Hardt's result may be improved by using a trick of Khovanskii's. Namely, we take the *exponents* of the variables in  $P$ , as well as the coefficients, as *parameters* - which we can do as long as we bound the number of monomial terms in  $P$ . We then obtain the result that for any  $n, k$  there is  $N = N(n, k)$  such that there are at most  $N$  homeomorphism types of sets of the forms  $P^{-1}(0)$  where  $P : \mathbb{R}^n \rightarrow \mathbb{R}$  is a real polynomial (of arbitrary degree but) which is the sum of at most  $k$  monomials (i.e. terms of the form  $ax_1^{q_1} \cdots x_n^{q_n}$  for  $a \in \mathbb{R}$  and  $q_1, \dots, q_n \in \mathbb{N}$ , although, in fact, we could also allow  $q_1, \dots, q_n \in \mathbb{R}$ ). (Remark: for  $n = 1$  this is usually attributed to Descartes).

More recently Coste ([2]) has proved a uniformity result for the homeomorphism types of definable *functions* in o-minimal structures and this gives a corresponding result for the homeomorphism types of polynomials with a restricted number of monomial terms.

#### REFERENCES

- [1] J.-Y. Charbonnel, 'Sur certains sous-ensembles de l'espace euclidien', Ann. Inst. Fourier. Grenoble 41, 3 (1991), 679–717.
- [2] M. Coste, 'Topological types of fewnomials', Preprint 96–39 (1996), University of Rennes.
- [3] L. van den Dries, 'Tame topology and o-minimal structures', LMS Lecture Note Series 248, CUP, (1998)
- [4] R. Hardt, 'Semi-algebraic local triviality in semi-algebraic mappings', Amer.J. Maths. 102 (1980), 291–302.

- [5] A. G. Khovanskii, 'On a class of systems of transcendental equations', *Soviet Math. Dokl.* 22 (1980), 762–765.
- [6] —, 'Fewnomials', *AMS Translations No. 88*, (1991).
- [7] J. F. Knight, A. Pillay and C. Steinhorn, 'Definable sets in ordered structures', II, *Trans. Amer. Math. Soc.* 295 (1986), 593–605.
- [8] D. Marker, 'Khovanskii's Theorem, in 'Algebraic Model Theory', (B. T. Hart et al. (eds), Toronto, ON). (1997), Kluwer 181–193.
- [9] S. Maxwell, 'A general model completeness result for expansions of the real ordered field', to appear in *Annals of Pure and Applied Logic*.
- [10] A. Pillay and C. Steinhorn, 'Definable sets and ordered structures, I', *Trans. Amer. Math. Soc.* 295 (1986), 565–592.
- [11] A. Tarski, 'Sur le ensembles definissables de nombres reels', *Fund. Math.* 17 (1931), 210–239.
- [12] —, 'A decision method for elementary algebra and geometry', Second edition revised, Rand Corporation, Berkley and Los Angeles, (1951).
- [13] A. J. Wilkie, 'Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function', *J. Amer. Math. Soc.* 9, No. 4, (1996), 1051–1094.
- [14] —, 'A general theorem of the complement and some new o-minimal structures'. (Submitted).

A. J. Wilkie  
Mathematical Institute  
University of Oxford  
24-29 St. Giles  
OX1 3LB Oxford  
England

## SECTION 12. PROBABILITY AND STATISTICS

LATTICE POINT PROBLEMS  
AND THE CENTRAL LIMIT THEOREM  
IN EUCLIDEAN SPACES

cf. Vol. III, p. 245–255

F. GÖTZE

## ERRATA

- 1) Replace in formula (1.2)  $\exp\{-\frac{v}{2}\}$  by  $\Gamma(\frac{d}{2} + 1)(\frac{v}{2})^{\frac{d}{2}} \exp\{-\frac{v}{2}\}$ .
- 2) On the same page replace line 14–16 from bottom by:  
... values in the interval  $[0, n - 1]$  with probability  $c > \chi(1)/2$ ,  $n > n_0$ . Thus there exists an integer  $j$  such that

$$\mathbf{P}\{T_n = j n^{-1}\} \geq c n^{-1}.$$

- 3) In the display formula after (5.6) replace  $\kappa = c_2 \delta^{-4/d}$  by  $\kappa = c_2 \delta^{4/d}$ .

Friedrich Götze  
Fakultät für Mathematik  
Universität Bielefeld  
Postfach 100131  
33501 Bielefeld  
Germany  
goetze@mathematik.Uni-Bielefeld.DE

## SECTION 10. PARTIAL DIFFERENTIAL EQUATIONS

ESTIMATES NEAR THE BOUNDARY FOR SOLUTIONS  
OF SECOND ORDER PARABOLIC EQUATIONS

MIKHAIL SAFONOV

ABSTRACT. We discuss different forms of the Harnack inequality for second order, linear, uniformly parabolic differential equations, and their applications to the estimates of solutions near the boundary. These applications include some Gaussian estimates and doubling properties for the caloric measure, and estimates for the quotient of two positive solutions vanishing on a portion of the boundary of a Lipschitz cylinder. A general approach to all these problems is demonstrated, which works for both the divergence and non-divergence equations and is based only on the "standard" Harnack inequality and elementary comparison arguments.

1991 Mathematics Subject Classification: Primary 35K

Keywords and Phrases: Harnack inequality, Caloric measure, Doubling property

## 1 INTRODUCTION. PRELIMINARY RESULTS

In this paper, we deal with the estimates of solutions to second order parabolic equations, which do not depend on the smoothness of coefficients. Such estimates have many important applications, especially in the theory of nonlinear equations (see [K], [LSU], [T], [PE]). Here we treat simultaneously the equations in the *divergence* form

$$Lu = \sum_{i,j=1}^n D_i(a_{ij}D_ju) - u_t = 0, \quad (D)$$

and in the *non-divergence* form

$$Lu = \sum_{i,j=1}^n a_{ij}D_{ij}u - u_t = 0, \quad (ND)$$

where  $D_j = \partial/\partial x_j$ ,  $D_{ij} = D_i D_j$ . We assume that the functions  $u = u(X)$  and the coefficients  $a_{ij} = a_{ij}(X)$  are defined and smooth for all  $X = (x, t) \in \mathbb{R}^{n+1}$ , and the operators  $L$  are uniformly parabolic, i.e.  $a_{ij}$  satisfy

$$\nu|\xi|^2 \leq \sum_{i,j} a_{ij} \xi_i \xi_j \quad \text{for all } \xi = (\xi_1, \dots, \xi_n) \in \mathbb{R}^n, \quad \max_{i,j} |a_{ij}(X)| \leq \nu^{-1}, \quad (1.1)$$

with a constant  $\nu \in (0, 1]$ . However, our estimates do not depend on the extra smoothness of  $u$  and  $a_{ij}$ , and by standard approximation procedures, they are extended to measurable  $a_{ij}$  in the divergence case (D) and to continuous  $a_{ij}$  in the non-divergence case (ND).

At present, the equation (D) are investigated much better than (ND). For example, under natural boundary conditions, the solution  $u$  of the equations (D) with measurable  $a_{ij}$  are well approximated by the solutions  $u^\varepsilon$  of equations with smooth  $a_{ij}^\varepsilon \rightarrow a_{ij}$  as  $\varepsilon \rightarrow 0$  (a.e.). A recent striking example by Nicolai Nadirashvili [N] (see also [S]) shows that this procedure fails to give a unique solution even for elliptic equations  $\sum a_{ij} D_{ij} u = 0$  with measurable  $a_{ij}$  in the unit ball  $B_1 \subset \mathbb{R}^n$ ,  $n \geq 3$ : different subsequences  $\{u^{\varepsilon_k}\}$  may converge to different functions.

Nevertheless, some properties of solutions look similar for the equations (D) and (ND), though their proofs are essentially different in these two cases. It turns out that two such statements, the *comparison principle* (Theorem 1.1) and the *interior Harnack inequality* (Theorem 1.2), provide the background for many others. From this “unifying” point of view, we present different versions of the Harnack inequality, estimates of quotients of positive solutions, doubling properties for  $L$ -caloric measure, and other related results. The proofs of these results are very “compressed”, for some statements we only give an outline of the main ideas. In the elliptic case, i.e. when  $a_{ij}$  and  $u$  in (D) or (ND) do not depend on  $t$ , most of these results are known from [CFMS], [B], [FGMS]. They were extended to the parabolic equation with time-independent coefficients in [S], [G], [FGS], and to general parabolic equations (D), (ND) in recent papers [FS], [FSY], [SY].

For an arbitrary domain  $V \subset \mathbb{R}^{n+1}$ , we define its *parabolic boundary*  $\partial_p V$  as the set of all the points  $Y = (y, s) \in \partial V$ , such that there is a continuous curve  $X(t) = (x(t), t)$  lying in  $V \cup \{Y\}$  with initial point  $Y$ , along which  $t$  is non-decreasing. In particular, for  $Q = \Omega \times (t_0, T)$  we have

$$\partial_p Q = \partial_x Q \cup \partial_t Q, \quad \text{where } \partial_x Q = \partial \Omega \times (t_0, T), \quad \partial_t Q = \bar{\Omega} \times \{t_0\}. \quad (1.2)$$

For  $y \in \mathbb{R}^n$ ,  $r > 0$ ,  $Y = (y, s)$ ,  $Q = \Omega \times (t_0, T)$ , and small  $\delta > 0$ , we denote

$$\begin{aligned} B_r &= B_r(y) = \{x \in \mathbb{R}^n : |x - y| < r\}, & C_r &= C_r(Y) = B_r(y) \times (s - r^2, s + r^2), \\ Q_r &= Q_r(Y) = Q \cap C_r(Y), & \Delta_r &= \Delta_r(Y) = (\partial_p Q) \cap C_r(Y), \\ \Omega^\delta &= \{x \in \Omega : \text{dist}(x, \partial \Omega) > \delta\}, & Q^\delta &= \Omega^\delta \times (t_0 + \delta^2, T). \end{aligned}$$

**THEOREM 1.** (*Comparison principle*). *Let  $V$  be a bounded domain in  $\mathbb{R}^{n+1}$ , functions  $u, v \in C^2(V) \cap C(\bar{V})$  and satisfy  $Lu \leq Lv$  in  $V$ ,  $u \geq v$  on  $\partial_p V$ . Then  $u \geq v$  on  $\bar{V}$ .*

This theorem is well-known and its proof is elementary. The next one is far from obvious. In the divergence case, it was discovered by Moser [M] in 1964. In the non-divergence case, it was proved in [KS] in 1978-79, see also [K], Chapter 4.

**THEOREM 2.** (*Interior Harnack inequality*). *Let  $u$  be a nonnegative solution of  $Lu = 0$  in a bounded cylinder  $Q = \Omega \times (t_0, T)$ , and let positive constants  $\delta, \lambda$  be such that  $\Omega^\delta$  is a connected set, and  $\text{diam } \Omega + \sqrt{T - t_0} \leq \lambda\delta$ . Then for all  $x, y \in \Omega^\delta$  and  $s, t$  satisfying  $t_0 + \delta^2 \leq s < s + \delta^2 \leq t < T$ , we have*

$$u(y, s) \leq Nu(x, t) \quad (1.3)$$

with a constant  $N = N(n, \nu, \lambda)$ .

From now on we assume that  $\Omega$  is a bounded domain in  $\mathbb{R}^n$  satisfying the following Lipschitz condition with some positive constants  $r_0, m$ : for each  $y \in \partial\Omega$ , there is an orthonormal coordinate system (centered at  $y$ ), with coordinates  $x = (x_1, \dots, x_{n-1}, x_n) = (x', x_n)$ , such that

$$\Omega \cap \{|x'| < r_0, |x_n| < (m+1)r_0\} = \{|x'| < r_0, \varphi(x') < x_n < (m+1)r_0\}, \quad (1.4)$$

and  $|\nabla\varphi| \leq m$  on the ball  $\{|x'| < r_0\} \subset \mathbb{R}^{n-1}$ . Then for any continuous function  $g$  on  $\mathbb{R}^{n+1}$ , there exists a unique solution  $u \in C^2(Q) \cap C(\bar{Q})$  of the boundary value problem

$$Lu = 0 \quad \text{in } Q = \Omega \times (t_0, T), \quad u = g \quad \text{on } \partial_p Q. \quad (1.5)$$

This is a well-known fact for smooth  $\Omega$ , and it is easily extended to Lipschitz domains  $\Omega$  by their approximation with smooth domains  $\Omega^j \searrow \Omega$ . From Theorem 1.1 it follows that  $g \rightarrow u(X)$  is a linear continuous functional on  $C(\partial_p Q)$ . By the Riesz representation theorem, there exists of a unique probability measure (*L-caloric measure*)  $\omega^X = \omega_Q^X$  on  $\partial_p Q$ , such that the solution of the problem (1.5) has the form

$$u(X) = u(x, t) = \int_{\partial_p Q} g(Y) d\omega^X(Y). \quad (1.6)$$

The above representation is also valid for unbounded domains  $Q$  under some natural restrictions on the growth of solutions for  $|x| \rightarrow \infty$ . For example, if the function  $g$  is bounded, we restrict ourselves to the bounded solutions  $u$ .

**LEMMA 3.** *Let  $\Omega$  be a bounded Lipschitz domain in  $\mathbb{R}^n$  with constants  $r_0$  and  $m$ , and let  $Q = \Omega \times (t_0, \infty)$ . Then for any  $Y = (y, s) \in \partial_x Q = \partial\Omega \times (t_0, \infty)$ , and  $r \in (0, r_0]$ , we have*

$$\omega^X(\Delta_r) \geq N^{-1} \quad \text{on } Q_{r/2} \quad (1.7)$$

with a constant  $N = N(n, \nu, m) > 1$ . If  $Y = (y, t_0) \in \partial_t Q = \bar{\Omega} \times \{t_0\}$ , then the estimate (1.7) holds for all  $r > 0$  with a constant  $N = N(n, \nu) > 1$ .

*Proof.* Without loss of generality, we may assume  $t_0 = 0$ . First we consider a simpler case  $Y = (y, 0) \in \partial_t Q$ . In this case,

$$C = C_r(Y) = B_r(y) \times (-r^2, r^2) \supset C^+ = B_r(y) \times (0, r^2) \supset Q_r = Q \cap C.$$

The function

$$u(X) = \omega_{C^+}^X(\partial_t C^+) \quad \text{on } C^+, \quad u \equiv 1 \quad \text{on } C \setminus C^+$$

can be treated as a solution of the problem (1.5) in the cylinder  $C$  with  $g \equiv 1$  for  $t \leq 0$ ,  $g \equiv 0$  for  $t > 0$ . Therefore, applying Theorem 1.1 in  $Q_r = Q \cap C$  and then Theorem 1.2 in  $C$ , we obtain the desired estimate with a constant  $N = N(n, \nu) > 1$ :

$$\omega^X(\Delta_r) \geq u(X) \geq N^{-1}u(y, -r^2/2) = N^{-1} \quad \text{on } Q_{r/2}.$$

Now it remains to consider the case  $Y = (y, s) \in \partial_x Q$ , i.e.  $y \in \partial\Omega$ ,  $s \in (t_0, \infty)$ . By the Lipschitz condition, the set  $B_r(y) \setminus \Omega$  contains a ball  $B_{\mu r}(z)$  with  $\mu = \mu(m) > 0$ . Then

$$Z = (z, s - r^2/2) \in C' = B_{\mu r}(z) \times (s - r^2, s + r^2) \subset C \setminus Q,$$

where  $C = C_r(Y)$ . We can apply Theorem 1.2 to the function  $u(X) = \omega_C^X(\partial_t C')$  in  $C$  and to  $u'(X) = \omega_{C'}^X(\partial_t C')$  in  $C'$  extended as  $u' \equiv 1$  across  $\partial_t C'$ . This gives us

$$\omega^X(\Delta_r) \geq u(X) \geq N_1^{-1}u(Z) \geq N_1^{-1}u'(Z) \geq N_2^{-1} \quad \text{on } Q_{r/2},$$

where the constants  $N_1$  and  $N_2$  depend only on  $n, \nu, m$ . Lemma 1.1 is proved.  $\square$

**COROLLARY 4.** *Let  $Lu = 0$ ,  $u > 0$  in  $Q$ , and  $u = 0$  on  $\Delta_R(Y) = (\partial_p Q) \cap C_R(Y)$  for some  $Y \in \partial_x Q$  and  $R \in (0, r_0]$ . Then*

$$\sup_{Q_{R/2}} u \leq \theta \sup_{Q_R} u, \tag{1.8}$$

$$\sup_{Q_r} u \leq (2r/R)^\alpha \sup_{Q_R} u \quad \text{for all } r \in (0, R] \tag{1.9}$$

with constant  $\theta = \theta(n, \nu, m) \in (0, 1)$ ,  $\alpha = -\log_2 \theta > 0$ . If  $Y \in \partial_t Q$ , then (1.8) and (1.9) hold for all  $R > 0$  with  $\theta, \alpha$  depending only on  $n, \nu$ .

*Proof.* Let  $\omega^X$  denote the  $L$ -caloric measure on  $\partial_p Q_R$ . Then

$$\omega^X((\partial_p Q_R) \setminus \Delta_R) = 1 - \omega^X(\Delta_R) \leq 1 - N^{-1} = \theta \quad \text{on } Q_{R/2},$$

and since  $u = 0$  on  $\Delta_R(Y)$ ,

$$\sup_{Q_{R/2}} u = \sup_{Q_{R/2}} \int_{\partial_p Q_R} u d\omega^X \leq \sup_{Q_{R/2}} \omega^X((\partial_p Q_R) \setminus \Delta_R) \cdot \sup_{\partial_p Q_R} u \leq \theta \sup_{Q_R} u.$$

The estimate (1.8) is proved. Iterating this estimate, we also get (1.9).  $\square$



2 GAUSSIAN ESTIMATES FOR  $L$ -CALORIC MEASURE

For given cylinder  $Q = \Omega \times (t_0, T) \subset \mathbb{R}^{n+1}$ , introduce the functions  $d(x) = \text{dist}(x, \partial\Omega)$  on  $\Omega$ , and

$$\rho(X) = \rho_Q(X) = \rho(x, t) = d(x)/\sqrt{t - t_0} \quad \text{on } Q, \tag{2.1}$$

**THEOREM 5.** *There exist positive constants  $N, \beta$ , depending only on  $n$  and  $\nu$ , such that*

$$\omega^X(\partial_x Q) \leq N e^{-\beta \rho^2(X)} \quad \text{on } Q. \tag{2.2}$$

*Proof.* We fix  $Y_0 = (0, 1) \in \mathbb{R}^{n+1}$ , and for  $\rho > 0$  define  $M(\rho) = \sup \omega_C^{Y_0}(\partial_x C)$ , where  $C = B_\rho(0) \times (0, 1)$ , and the supremum is taken with respect to all parabolic operators  $L$  with coefficients  $a_{ij}$  satisfying (1.1). It is easy to see that  $M(\rho)$  decreases on  $(0, \infty)$ , and moreover, applying Corollary 1.1 to  $u(X) = \omega_C^X(\partial_x C)$ , we have  $M(\rho) \searrow 0$  as  $\rho \nearrow \infty$ . This allows us to fix a constant  $A = A(n, \nu)$  such that  $M(A) \leq 1/3$ . By substitution  $x \rightarrow (x - y)/\sqrt{h}$ ,  $t \rightarrow 1 + (t - s)/h$ , we also have  $\omega_C^Y(\partial_x C) \leq M(\rho)$  for all  $Y = (y, s) \in \mathbb{R}^{n+1}$  and  $C = B_d(y) \times (s - h, s)$  with  $d/\sqrt{h} \geq \rho$ . If we take  $Y = X = (x, t) \in Q = \Omega \times (t_0, T)$ ,  $d = d(x)$ , and  $h = t - t_0$ , then  $C = B_d(x) \times (t_0, t) \subset Q$  and  $\partial_t C \subset \partial_t Q$ , hence

$$\omega_Q^X(\partial_x Q) \leq \omega_C^X(\partial_x C) \leq M(d/\sqrt{t - t_0}) = M(\rho(X)). \tag{2.3}$$

Further, for natural  $j \geq 5$ , set  $\rho_j = 4A\sqrt{j}$ ,  $\varepsilon_j = 2/\sqrt{j}$ ,  $M_j = M(\rho_j)$ , and consider the cylinders

$$Q_j = B_{\rho_j}(0) \times (0, 1) \supset Q'_j = B_{\varepsilon_j A}(0) \times (1 - \varepsilon_j^2, 1).$$

The function  $\rho = \rho(X) = \rho(x, t) = (\rho_j - |x|)/\sqrt{t}$  corresponds by the equality (2.1) to  $Q = Q_j$ . One can easily verify the inequalities  $\rho \geq \rho_{j-1}$  on  $\partial_x Q'_j$  and  $\rho \geq \rho_{j+1}$  on  $\partial_t Q'_j$ . Therefore, the caloric measure  $\omega^X$  for  $L$  in  $Q_j$  satisfies

$$\omega^X(\partial_x Q_j) = \int_{\partial_x Q'_j} \omega^Y(\partial_x Q_j) d\omega^X(Y) \leq M_{j-1} \cdot \omega^X(\partial_x Q'_j) + M_{j+1} \cdot \omega^X(\partial_t Q'_j)$$

for all  $X \in \overline{Q'_j}$ . By the choice of  $A$ , we have  $\omega^{Y_0}(\partial_x Q'_j) = 1 - \omega^{Y_0}(\partial_t Q'_j) \leq 1/3$ , and the previous estimate yields

$$\begin{aligned} M_j &\leq \frac{1}{3} M_{j-1} + \frac{2}{3} M_{j+1}, \\ M_j - M_{j+1} &\leq 2^{-1}(M_{j-1} - M_j) \leq \dots \leq 2^{5-j}(M_5 - M_6) \leq 2^{5-j}. \end{aligned}$$

For arbitrary  $\rho \geq \rho_5$ , we choose  $j \geq 5$  such that  $\rho_j \leq \rho < \rho_{j+1}$ , so that

$$M(\rho) \leq M(\rho_j) = M_j = \sum_{k \geq j} (M_k - M_{k+1}) \leq 2^{6-j} \leq N e^{-\beta \rho_{j+1}^2} \leq N e^{-\beta \rho^2},$$

by appropriate choice of constants  $N, \beta$ , depending only on  $n$  and  $\nu$ . If  $N$  is chosen large enough, the estimate  $M(\rho) \leq Ne^{-\beta\rho^2}$  also holds for  $0 < \rho < \rho_5$ . Together with (2.3), these estimates imply the desired estimate (2.2).  $\square$

REMARK 2.1. From Theorem 2.1 it follows immediately the uniqueness of the Cauchy problem

$$Lu = 0 \quad \text{in } \mathbb{R}^n \times (0, T), \quad u(x, 0) \equiv g(x) \quad (2.4)$$

in the class of functions satisfying  $|u(x, t)| \leq Ne^{N|x|^2}$ , and the proof does not depend on the structure (divergence or non-divergence) of the operator  $L$ . Using some arguments in the papers by Moser [M] and Aronson [A1], one can prove a stronger statement: there is at most one solution of the problem (2.4) satisfying a one-sided inequality  $u(x, t) \geq -Ne^{N|x|^2}$  for all  $(x, t) \in \mathbb{R}^n \times (0, T)$ .

REMARK 2.2. In the divergence case, from Moser's Harnack inequality it follows the Hölder continuity of solutions, which was proved earlier by Nash [Ns]. Aronson [A2] also essentially used the Harnack inequality in the proof of the Gaussian estimates for the fundamental solution  $\Gamma(x, t; y, s)$  of the divergence operator  $L$ : for  $s < t$ ,

$$\begin{aligned} \frac{1}{N}(t-s)^{-n/2} \exp\left(-\frac{N|x-y|^2}{t-s}\right) \\ \leq \Gamma(x, t; y, s) \leq N(t-s)^{-n/2} \exp\left(-\frac{|x-y|^2}{N(t-s)}\right), \end{aligned} \quad (2.5)$$

with a constant  $N = N(n, \nu)$ . Fabes and Stroock [FS] gave another proof of the estimates (2.5) which is based on some ideas of Nash instead of the Harnack inequality, and they also showed that the Harnack inequality follows easily from (2.5). Thus all these facts are mutually related.

### 3 HARNACK INEQUALITIES

As before, let  $\Omega$  be a bounded domain in  $\mathbb{R}^n$  satisfying the Lipschitz condition with constants  $r_0, m$ , and let  $Q = \Omega \times (t_0, \infty)$ . For  $y \in \bar{\Omega}$  and  $r \in (0, r_0]$ , the set  $\Omega_r(y) = \Omega \cap B_r(y)$  contains a ball  $B_{\mu r}(y_r)$ , where  $\mu = \mu(m) \in (0, 1/2]$ . We fix such  $y_r$  depending on  $y$  and  $r$ , and for  $Y = (y, s)$ , denote  $Y_r^\pm = (y_r, s \pm 2r^2)$ . The following result is often referred to as a *boundary Harnack inequality*, or *Carleson type estimate*. For parabolic equations, it was first proved by Salsa [S] (in the divergence case) and Garofalo [G] (in the non-divergence case), see also [FSY].

THEOREM 6. *Let  $Q = \Omega \times (t_0, \infty)$ ,  $Y \in \partial_p Q$ ,  $0 < r \leq r_0/2$ , and let  $u$  be a nonnegative solution of  $Lu = 0$  in  $Q$ , satisfying  $u = 0$  on  $\Delta_{2r}(Y) = (\partial_p Q) \cap C_{2r}(Y)$ . Then*

$$u \leq N(n, \nu, m)u(Y_r^+) \quad \text{on } Q_r = Q_r(Y). \quad (3.1)$$

In the elliptic case, when  $a_{ij}$  and  $u$  do not depend on  $t$ , the interior Harnack inequality (1.3) is equivalent to

$$\sup_{\Omega^\delta} u \leq N(n, \nu, \lambda) \inf_{\Omega^\delta} u, \tag{3.2}$$

provided  $u \geq 0$ ,  $Lu = 0$  in  $\Omega$ ,  $\Omega^\delta$  is a connected set, and  $(\text{diam } \Omega)/\delta \leq \lambda$ . An easy example of the function

$$u(x, t) = t^{-1/2} \exp[-(x - 2)^2/4t] \text{ for } t > 0, \quad u(x, t) \equiv 0 \text{ for } t \leq 0,$$

which satisfies  $u \geq 0$ ,  $Lu = u_{xx} - u_t = 0$  in  $Q = (-1, 1) \times (-1, 1)$ , shows that we cannot simply replace  $\Omega^\delta$  by  $Q^\delta$  in the parabolic case. However, this is possible under the additional assumption  $u = 0$  on  $\partial_x Q$ . As in [G], [FGS], Theorem 3.1 yields the following *interior elliptic-type Harnack inequality*.

**THEOREM 7.** *Let  $Lu = 0$ ,  $u > 0$  in  $Q = \Omega \times (t_0, T)$ ,  $u = 0$  on  $\partial_x Q = \partial\Omega \times (t_0, T)$ , and let positive constants  $\delta \in (0, r_0)$  and  $\lambda > 1$  be such that  $(\text{diam } \Omega + \sqrt{T - t_0})/\delta \leq \lambda$ . Then*

$$\sup_{Q^\delta} u \leq N(n, \nu, m, \lambda) \inf_{Q^\delta} u. \tag{3.3}$$

*Proof* follows from Theorems 1.2 and 3.1 and the maximum principle:

$$\sup_{Q^\delta} u \leq \sup_{x \in \Omega} u(x, \delta^2/4) \leq N_1 \sup_{x \in \Omega^{\mu\delta}} u(x, \delta^2/2) \leq N \inf_{Q^\delta} u,$$

where  $N_1 = N_1(n, \nu, m)$ ,  $\mu = \mu(m) > 0$ . □

The next theorem is called a *boundary elliptic-type Harnack inequality*, because the constant  $N$  in (3.4) does not depend on the distance between  $C_r(Y)$  and  $\partial_x Q$ . In equivalent forms, this result is contained in [FS], [FSY].

**THEOREM 8.** *Under the assumptions of the previous theorem, let  $Y = (y, s) \in Q$  and  $r > 0$  be such that  $s - t_0 \geq 4\delta^2 > 0$  and  $C_r(Y) \subset C_{2r}(Y) \subset Q$ . Then*

$$\sup_{C_r(Y)} u \leq N(n, \nu, m, \lambda) \inf_{C_r(Y)} u. \tag{3.4}$$

*Proof.* If  $r > \delta$ , from  $C_{2r}(Y) \subset Q$  it follows  $C_r = C_r(Y) \subset Q^\delta$ , and (3.4) follows from the previous theorem. Therefore, we may restrict ourselves to the case  $0 < r \leq \delta$ . Iterating the interior Harnack inequality, one can get the estimate

$$u(Y_R^-) \leq N_0(R/r)^\gamma \inf_{C_r} u \quad \text{for } 0 < r \leq R \leq \delta \tag{3.5}$$

with positive constants  $N_0, \gamma$ , depending only on  $n, \nu, m$ . We take

$$R = \max\{\rho : r \leq \rho \leq \delta, \sup_{C_r} u \leq (r/\rho)^\gamma \sup_{Q_\rho} u\},$$

where  $Q_\rho = Q_\rho(Y) = Q \cap C_\rho(Y)$ . By this choice of  $R$  and (3.5), the proof of the desired estimate (3.4) is now reduced to the following one:

$$M_R = \sup_{Q_R} u \leq Nu(Y_R^-). \tag{3.6}$$

For the proof of (3.6), we first consider the case  $R \leq \delta/K$ , where  $K = \text{const} \geq 2$ . Introduce the cylinders

$$C' = B_{KR}(y) \times (s - 4R^2, s + 4R^2) \subset C_{KR}(Y), \quad Q' = Q \cap C' \subset Q_{KR}.$$

By definition of  $R$ ,

$$\sup_{\partial_x Q'} u \leq M_{KR} < (KR/r)^\gamma M_r = K^\gamma M_R.$$

Moreover, by Theorem 2.1,  $\omega_{C'}^X(\partial_x Q') \leq K^{-\gamma}/2$  on  $Q_R$ , provided  $K = K(n, \nu, m)$  is large enough. Using the representation (1.6) in  $Q'$ , we have

$$M_R = \sup_{Q_R} \int_{\partial_p Q'} u d\omega^X \leq \sup_{\partial_x Q'} u \cdot \sup_{Q_R} \omega_{C'}^X(\partial_x Q') + \sup_{\partial_t Q'} u \leq \frac{1}{2} M_R + \sup_{\partial_t Q'} u,$$

and  $M_R \leq 2u(Z)$  for some point  $Z = (z, s - 4R^2) \in \partial_t Q'$ , which lies strictly below  $Y_R^-$ . By Theorems 1.2 and 3.1, we get the estimate (3.6) in the case  $R \leq \delta/K$ . If  $\delta/K < R \leq \delta$ , then by the maximum principle  $M_R \leq u(Z)$  for some point  $Z = (z, s - \delta^2)$ , and since  $\text{diam } \Omega \leq \lambda\delta < K\lambda R$ , the previous argument is still valid. Thus we have (3.6) in any case, and so Theorem 3.3 is proved. □

#### 4 ESTIMATES FOR QUOTIENTS OF SOLUTIONS

Let  $\Omega$  be a bounded Lipschitz domain, and let  $y \in \partial\Omega$  and  $Y = (y, s)$  be fixed. We will use a local coordinate system which provides the representation (1.4) of a portion of  $\Omega$  in  $r_0$ -neighborhood of  $y = 0$ . In this neighborhood, the distance function  $d = d(x) = \text{dist}\{x, \partial\Omega\}$  is equivalent to  $d' = d'(x) = d'(x', x_n) = x_n - \varphi(x')$ . For  $r \in (0, r_0]$  and  $K > 1$ , we introduce the sets

$$\begin{aligned} D_r &= \{x = (x', x_n) : |x'| < r, 0 < d'(x) < r\} \times (s - r^2, s + r^2), \\ S_r &= (\partial_p D_r) \cap \{d' = r\}, \quad \Gamma_r = (\partial_p D_r) \cap \{0 < d' < r\}, \\ D_r^+ &= D_r \cap \{d' \geq r/K\}, \quad D_r^- = D_r \cap \{0 < d' < r/K\}, \\ S'_r &= D_r \cap \{d' = r/K\}, \quad \Gamma'_r = (\partial_p D_r) \cap \{0 < d' < r/K\}. \end{aligned}$$

For  $K \gg 1$ ,  $S'_r$  is a “wide” portion of  $\partial_p D'_r$  lying in  $\{d' > 0\}$ ,  $\Gamma'_r$  is a “narrow” portion of  $\partial_p D'_r$ . Using Lemma 1.1 and Corollary 1.1, one can obtain the estimates

$$\inf_{D_{r/K}^+} \omega_{D_r^-}^X(S'_r) \geq p_K = \frac{1}{N} K^{-\gamma}, \quad \sup_{D_{r/K}^-} \omega_{D_r^-}^X(\Gamma'_r) \leq q_K = N e^{-\beta K} \tag{4.1}$$

with some positive constants  $N, \gamma, \beta$  depending only on  $n, \nu, m$ . The bounds  $p_K$  and  $q_K$  have different decay rates as  $K \rightarrow \infty$ , because one needs to apply the

estimate (1.7)  $O(\ln K)$  times in order to get the first inequality in (4.1), while the second one is obtained by application of the estimate (1.8)  $O(K)$  times. We will fix  $K = K(n, \nu, m) \geq 1$  large enough to guarantee the inequality  $p_K \geq 2q_K$ . These inequality helps to prove the following results.

LEMMA 9. *Let  $\omega^X$  be  $L$ -caloric measure in the domain  $D_{2r}$  for some  $r \in (0, r_0/2]$ . Then there exists a constant  $N = N(n, \nu, m) \geq 1$ , such that*

$$N^{-1}\omega^X(S_{2r}) \leq \omega^X(\Gamma_{2r}) \leq N\omega^X(S_{2r}) \quad \text{on } D_r. \tag{4.2}$$

THEOREM 10. *Let  $Q = \Omega \times (t_0, \infty)$  and  $Y = (y, s) \in \partial_x Q$  be fixed. Let  $u_1$  and  $u_2$  be two positive solutions of  $Lu = 0$  in  $Q$ , and  $u_1 = 0$  on  $\Delta_{4r}(Y) = (\partial_p Q) \cap C_{4r}(Y)$ , where  $0 < 4r \leq \min(r_0, \sqrt{s - t_0})$ . Then*

$$\frac{u_1}{u_2} \leq N(n, \nu, m) \frac{u_1(Y_r^+)}{u_2(Y_r^-)} \quad \text{on } Q_r = Q_r(Y). \tag{4.3}$$

If also  $u_2 = 0$  on  $\Delta_{4r}(Y)$ , we can interchange  $u_1$  and  $u_2$  in (4.3), and this yields a lower estimate for  $u_1/u_2$  on  $Q_r$ . If  $u_2 = 0$  on  $\partial_x Q$ , we can also use the elliptic-type Harnack inequality, which gives the estimate of oscillation and the Hölder continuity of  $u_1/u_2$ . For more details, see [FSY].

### 5 DOUBLING PROPERTIES

The following *doubling property* in the divergence case follows easily from Aronson's estimate (2.3). In the non-divergence case, this estimate is not valid. Our methods work for both the divergence and non-divergence cases.

THEOREM 11. *Let a constant  $\varepsilon \in (0, 1/2)$  be given. Then for all  $r > 0$ , we have*

$$\omega^X(\Delta_r) \leq N\omega^X(\Delta_{r/2}) \quad \text{on } P = \{\varepsilon|x|^2 \leq t\} \tag{5.1}$$

*with a constant  $N = N(n, \nu, \varepsilon)$ , where  $\Delta_r = B_r(0) \times \{0\} \subset \mathbb{R}^n \times \{0\}$ , and  $\omega^X$  is the  $L$ -caloric measure for  $Q = \mathbb{R}^n \times (0, \infty)$ .*

THEOREM 12. *Let  $Q = \Omega \times (t_0, \infty)$ ,  $Y = (y, s) \in \partial_p Q$ , and constants  $\varepsilon \in (0, 1/2)$ ,  $\lambda \geq 1$  be given. Then the estimate (5.1) holds for  $\Delta_r = \Delta_r(Y)$  for all  $r \in (0, \lambda r_0/4]$  and  $X = (x, t) \in Q$  satisfying  $\varepsilon|x - y|^2 \leq t - s$ ,  $4r \leq \sqrt{t - s} \leq \lambda r_0$ .*

These theorems are proved in [SY]. One of its applications is the *Fatou theorem* which states that any positive solution of  $Lu = 0$  in  $Q$  has finite non-tangential limits at almost every (with respect to the  $L$ -caloric measure) point  $Y \in \partial_p Q$ . In the time-independent case, this result was proved in [FGS].

## REFERENCES

- [A1] D. G. Aronson, *Uniqueness of positive weak solutions of second order parabolic equations*, Ann. Polon. Math, v. 16 (1965), 285–303.
- [A2] D. G. Aronson, *Non-negative solutions of linear parabolic equations*, Ann. Scuola Norm. Sup. Pisa, v. 22 (1968), 607–694.
- [B] P. E. Bauman, *Positive solutions of elliptic equations in non-divergence form and their adjoints*, Arkiv fur Matematik, v. 22 (1984), 153–173.
- [CFMS] L. A. Caffarelli, E. B. Fabes, S. Mortola and S. Salsa, *Boundary behavior of nonnegative solutions of elliptic operators in divergence form*, Indiana J. of Math., v. 30 (1981), 499–502.
- [FGMS] E. B. Fabes, N. Garofalo, S. Marín-Malave and S. Salsa, *Fatou theorems for some nonlinear elliptic equations*, Revista Math. Iberoamericana, v. 4 (1988), 227–251.
- [FGS] E. B. Fabes, N. Garofalo and S. Salsa, *A backward Harnack inequality and Fatou theorem for nonnegative solutions of parabolic equations*, Illinois J. of Math., v. 30 (1986), 536–565.
- [FS] E.B. Fabes and M.V. Safonov, *Behavior near the boundary of positive solutions of second order parabolic equations*, J. Fourier Anal. and Appl., Special Issue: Proceedings of the Conference El Escorial 96 (1998), 871–882
- [FSY] E.B. Fabes, M.V. Safonov and Yu Yuan, *Behavior near the boundary of positive solutions of second order parabolic equations. II*, to appear in Trans. Amer. Math. Soc.
- [FSt] E. B. Fabes and D. W. Stroock, *A new proof of Moser’s parabolic Harnack inequality using the old idea of Nash*, Arch. Rational Mech. Anal., v. 96, no.4 (1986), 327–338.
- [G] N. Garofalo, *Second order parabolic equations in nonvariational form: boundary Harnack principle and comparison theorems for nonnegative solutions*, Ann. Mat. Pura Appl., v. 138 (1984), 267–296.
- [K] N. V. Krylov, *Nonlinear elliptic and parabolic equations of second order*, Nauka, Moscow, 1985 in Russian; English transl.: Reidel, Dordrecht, 1987.
- [KS] N. V. Krylov and M. V. Safonov, *A certain property of solutions of parabolic equations with measurable coefficients*, Izvestia Akad. Nauk SSSR, ser. Matem., v. 44 (1980), 161–175 in Russian; English transl. in Math. USSR Izvestija, v. 16 (1981), 151–164.
- [LSU] O. A. Ladyzhenskaya, V. A. Solonnikov and N. N. Ural’tseva, *Linear and quasi-linear equations of parabolic type*, Nauka, Moscow, 1967 in Russian; English transl.: Amer. Math. Soc., Providence, RI, 1968.
- [M] J. Moser, *A Harnack inequality for parabolic differential equations*, Comm. Pure and Appl. Math., v. 17 (1964), 101–134; and correction in: Comm. Pure and Appl. Math., v. 20 (1967), 231–236.
- [Nd] N.S. Nadirashvili, *Nonuniqueness in the martingale problem and the Dirichlet problem for uniformly elliptic operators*, 1995, preprint.

- [Ns] J. Nash, *Continuity of solutions of parabolic and elliptic equations*, Amer. J. Math., v. 80 (1958), 931–954.
- [PE] F.O. Porper and S.D. Eidelman, *Two-sided estimates of fundamental solutions of second-order parabolic equations, and some applications*, Uspekhi Mat. Nauk, v. 39, no. 3 (1984), 107–156 in Russian; English transl. in Russian Math. Surveys, v. 39, no. 3 (1984), 119–178.
- [S] M.V. Safonov, *Nonuniqueness for second order elliptic equations with measurable coefficients*, to appear in SIAM Journal on Mathematical Analysis.
- [SY] M.V. Safonov and Yu Yuan, *Doubling properties for second order parabolic equations*, to appear in Annals of Math.
- [SI] S. Salsa, *Some properties of nonnegative solutions of parabolic differential operators*, Ann. Mat. Pura Appl., v. 128 (1981), 193–206.
- [T] N.S. Trudinger, *Pointwise estimates and quasilinear parabolic equations*, Comm. Pure and Appl. Math., v. 21 (1968), 205–226.

Mikhail Safonov  
School of Mathematics  
University of Minnesota  
Minneapolis, MN 55455

## SECTION 16. APPLICATIONS

The Invited Speaker, Bonnie Berger, was not able to attend the Congress.

RECENT DEVELOPMENTS  
IN COMPUTATIONAL GENE RECOGNITION

SERAFIM BATZOGLOU, BONNIE BERGER, DANIEL J. KLEITMAN,  
ERIC S. LANDER, AND LIOR PACTER

ABSTRACT. We survey recent mathematical and computational work in the field of gene recognition, focusing on the techniques that have been developed to tackle the problem of identifying protein coding regions in genes. We also present a new approach to gene recognition which is based on a variety of tools we have developed.

## 1 INTRODUCTION

## 1.1 WHAT DO YOU DO WITH 100KB OF HUMAN GENOMIC DNA?

Recent advances in DNA sequencing technology have led to rapid progress in the Human Genome Project. Within a few years, the entire human genome will be sequenced. The rapid accumulation of data has opened up new possibilities for biologists, while at the same time unprecedented computational challenges have emerged due to the mass of data. The questions of what to do with all the new information, how to store it, retrieve it, and analyze it, have only begun to be tackled by researchers [11]. These problems are distinguished from classical problems in biology, in that their solution requires an understanding not only of biology, but also of mathematics and computer science. Of the many problems, it is clear that the following tasks are of importance:

- Finding genes in large regions of DNA.
- Identifying protein coding regions within these genes.
- Understanding the function of the proteins encoded by the genes.

The important third problem, namely understanding the function of a newly sequenced gene, requires the solution of the second problem, identification of critical subregions which code for protein. Protein coding regions have different statistical characteristics from noncoding regions, and it is primarily this feature which



Figure 1: A schematic view of the transcription-translation process: During translation the T nucleotide becomes a U (Uracil). In this example, the boxed UAA triplet is not a codon and therefore does not end translation. Rather, the in-frame codons are "...GAC GAG AUA...". These are translated into "...D E I..." (D=Aspartic Acid, E=Glutamic acid, I=Isoleucine). Splicing occurs before translation. The translated amino acid sequence is folded into a protein.

enables us to distinguish them. An important aspect of work on the problem is the need to characterize these statistical differences and possibly explain their biological underpinnings. This paper surveys recent mathematical and computational approaches to developing algorithms for identifying protein coding regions within genes, and discusses some new methods we have recently developed.

## 1.2 BIOLOGICAL BACKGROUND

For the purposes of our discussion, we will define a gene (see Figure 1) to be a single, contiguous region of genomic DNA that encodes for one protein (along with the 5' and 3' flanking regions that contain promoter signals, etc.) There are four different nucleotides that make up a sequence of DNA. These are ADENINE (A), CYTOSINE (C), GUANINE (G) and THYMINE (T). For our purposes, we will think of DNA as being a string on an alphabet of size 4 (A,C,G,T). When a gene is expressed, it is first copied in a process known as TRANSCRIPTION. This forms a product known as RNA, which is a working template from which a protein is produced in a process known as TRANSLATION. Before translation, the RNA undergoes a SPLICING operation [14] conducted by certain enzymes, which typically delete most of it, leaving certain blocks of the original strand of RNA intact. These blocks are called EXONS and the parts that are removed are called INTRONS. The result of this pruning is the "mature" RNA, which is used during translation to make the protein. The protein consists of a sequence of amino acids linked together. During translation, each amino acid is produced by a triplet of consecutive nucleotides, known as a CODON, according to a known map that is

called the GENETIC CODE. This defines the CODING FRAME of the gene.

The gene actually has a “start” translation signal (ATG) and a stop translation sequence (TAA, TAG or TGA) both within exons; the sequence within exons between these forms the coding part of the sequence which contains all the information used to make the protein. The rest of the gene consists of introns, initial and final “non-coding exons” (these are exons that are glued together with the coding exons, but that are not used for making protein), as well as flanking regions containing biological signals of various sorts.

The splicing process is partially understood, and various SnRNP’s (these are RNA-protein complexes involved in splicing) have been identified that are involved in the splicing mechanism. These SnRNP’s (or spliceosomes) recognize various DNA sequences during splicing, and information about the consensus sites they recognize can be used to identify splice sites. Unfortunately, the biology is not understood to an extent that makes gene recognition possible on this basis alone [4]. Indeed, one of the main challenges for mathematicians and computer scientists working on these problems is to help biologists learn about splicing by detecting biologically significant signals in genomic databases.

### 1.3 THE COMPUTATIONAL TASK

The computational task we are concerned with is that of determining from an experimentally determined sequence of nucleotides, of length on the order of 100,000, where the genes are, and what proteins these genes produce. This endeavor has two parts, though in practice one handles them together: determining where each gene is, and determining which parts of its sequence are exons and which are introns. Here we focus on the latter of these two problems.

Nature uses a variety of biological signals, many of which remain to be identified. Fortunately (in view of our ignorance of the actual biological mechanism), we are not restricted to using only biological signals used by the cell. First, we know quite a bit about the constitution of intergenic and intronic sequences in humans. On the order of 30 percent of these sequences consist of certain REPEATS of various standard patterns or variations thereof [15]. Thus there are several hundred thousand copies of one or another variation of a sequence of length about 300 called Alu in the human genome, and many copies of other sequences as well. Due to the migratory nature of these repeats, and the mechanisms by which they occur, they are rare in exons. Secondly, the codons (and consequently amino acids) that code for protein, are not uniformly distributed, and their distribution differs from that of triplets in introns. This can help in distinguishing introns from exons. Other restrictions such as consistency in coding frame between exons greatly reduces the number of possible parses in a given gene. Indeed, even though in principle the number of parses is exponential in the number of potential splice sites identified, in practice many genes exhibit only a few possible parses after these numerous constraints are introduced.

The data available to us comes from a number of data bases, which contain examples of various kinds of biological sequences, as follows:

- The protein data base; it contains proteins whose amino acid sequences have

been determined.

- The cDNA data base; it consists of what are essentially the DNA sequences of the exons of a gene only, and fragments thereof.
- Data bases of genes whose splicings into introns and exons are known.
- Data bases of genes of various species without such information.

There are numerous complications in this problem, perhaps the most significant of which is the unreliable nature of the annotated data. There are also examples of genes which have “alternate splicings” so that under different circumstances the same gene can produce different proteins by being spliced differently into introns and exons. Finally there are introns whose splice sites are very different from the common consensus, not to mention numerous other exceptions to “the rules.”

## 2 PREVIOUS WORK

Current methods can be broadly categorized as learning, or homology based. While we cannot attempt to discuss in detail the myriad of approaches available, we will briefly comment on two methods currently in use, namely the HMM (Hidden Markov Model) approach (used by GENSCAN [2], GENEMARK [12] and GENIE [10]) and the homology based method (e.g. PROCRUSTES [6] and AAT [9]).

### 2.1 LEARNING BASED METHODS

Many of the most popular learning methods are based on a Hidden Markov Model approach [13] (although there are some notable exceptions to this, for example the language based system used in GENLANG [5]). It is assumed that the gene structure of a certain organism can be modeled probabilistically, with certain probabilities associated with being in certain “states,” and transition probabilities associated with these states. The states usually model functional units of a gene, for example exons (in the three different reading frames), introns (sometimes also in three different flavors depending on the frame of the exon preceding them), as well as terminal and initial exons, etc. The exact true model to be used is “learned” from the data. Coding and non-coding exons are usually modeled using 3-periodic fifth-order Markov Models. The exact methods used to model the various other biological signals (splice sites, etc.) vary greatly between the different programs.

The main drawback of many of these approaches is that performance is very dependent on the learning sets used [7]. Generally, only a single data set, developed by Haussler, Kulp and Reese [8], has been used for training. Overtraining of the Markov Models leads to poor results when new genes are encountered. This is especially true in genomics because early sequencing efforts tended to focus on gene rich areas in the genome, leading to an overabundance of short, GC rich genes. Some programs such as GENSCAN have begun to deal with this issue by separately handling GC rich and GC poor gene candidates.

Another drawback to learning methods is that homology information is not used for the predictions (this is starting to change with the advent of homology integration in programs such as **GENIE**). The user of the program is responsible for performing his/her own homology searches using **BLAST** [1] or another program.

Despite these drawbacks, the utility of the programs mentioned cannot be overlooked. Indeed, the **GENSCAN** package is becoming increasingly popular amongst biologists, and other programs such as **GRAIL** [16] (based on neural networks) have been in use for years.

## 2.2 HOMOLOGY BASED METHODS

The **PROCRUSTES** program [6] approaches gene recognition in a new, interesting way. The basic idea is that given a protein that is a homolog of the protein produced by the gene to be solved, one can determine the best way to parse the gene so that the resulting translated union of coding exons most closely resembles the target protein. This procedure can effectively be carried out using dynamic programming. Of course, the method is useless unless one can find a “good” match to the gene in question in a protein database (the **PROCRUSTES** program requires the user to find this input). Recently, cDNA databases are being used in analogous ways [9]. Exact estimates of how often these methods can be employed on new genes vary. Guesses range from 30-50 percent, with optimists arguing that these numbers will improve as the size of the databases increases.

## 2.3 PREVIOUS RESULTS

The analysis and benchmarking of gene recognition tools has become a science in and of itself. Of the many articles addressing these issues, we mention the excellent surveys of Burset and Guigó [3, 7]. The non-homology based algorithms are not sufficiently accurate to be relied on. Accuracy claims range from 60-90 percent per nucleotide, and 30-80 percent per entire exon with exact numbers dependent on who is making the claim. In practice these numbers are probably very optimistic [7]. Indeed, on a new sequence set, the programs identified about 1 in 6 genes correctly and completely missed the exons in 25 percent of the sequences.

The alarming aspect of the current state of the field is that these programs perform much worse when tested on new data, namely genes that have been sequenced, whose intron/exon structure is known experimentally. This poor performance is probably due to a number of factors, the most significant of which is that current “learning” takes place on small data sets which are often filled with errors since they have been annotated by the very same programs that are learning from them!

In practice, those who find genes use a very different approach. They hope that the cDNA or protein (or a good part of these) that are produced by the gene lie in one of the corresponding data bases. They then submit their sequences to **BLAST** [1], a program that finds best matches to members of the data base. When it is possible to match parts of the gene with an entire protein, then one has the answer to our problem, either by examining the alignments by eye, or submitting the matches to a program such as **PROCRUSTES** [6]. As the databases grow, the

likelihood of good matches to new genes increases. When this approach fails, they turn to the algorithms mentioned, and seek consensus results from them. The process is tedious, time consuming and does not necessarily produce correct results.

### 3 INNOVATIONS

We have developed a program (unpublished manuscript) based on the following ideas:

- Use of larger data bases such as the protein data base as a data source not only for homology, but for methods based on frequencies of  $k$ -tuples of nucleotides and amino acids. This greatly extends the amount of data available, and therefore allows consideration of  $k$ -tuples of much greater length than have been used heretofore.
- Use of a dictionary approach for finding matches as well as computing  $k$ -tuple frequencies from the databases. The idea of a dictionary has potential applications that go well beyond this particular problem.
- Attempt to use many separate indicators to distinguish exons, rather than integrating them immediately into one overall statistic.
- Use of not necessarily consecutive subsequences of nucleotides in our analysis.
- Distinguishing relatively long and not necessarily consecutive sequences of nucleotides and amino acids that occur unusually often in introns or exons, but not both, as markers for the same.
- Use of frame differentiation as an indicator for exons.
- Development of a visual program, which allows a user to see and evaluate predicted introns and exons, and experiment with alternative splicings, as well as predictions based on homology.
- Use of expected number of hits, rank statistics and other indicators in place of single maximal likelihood estimates.
- Use of gene data bases for homology-based identification of exons.
- Integration of repeat masking into the gene recognition process.
- Integration of homology-based and statistical approaches in the same program.
- Fast predictions using the above techniques, allowing for multiple homologs to be used in an automated fashion.

We briefly elaborate on two of these ideas below.

### 3.1 A FRAME TEST

Exons can be distinguished from introns in several ways. First, the nature of the translation code along with the nature of most proteins implies that the three possible reading frames (the first, second or third positions among the triplets that go to produce an amino acid) exhibit behavior that is usually quite different from one another. That is, if one examines a sequence of length 3 or more of nucleotides, one often finds that this sequence occurs much more often in one frame than another. This phenomenon becomes much more pronounced as the length of the sequence increases. Thus, most sequences of length 12 seem to have a pronounced bias toward a particular frame. The reason for this bias has to do with the genetic code. Mutations in the third position of a codon have much less effect on the resulting amino acid than, say, a mutation in the first position. Furthermore, an exon that is subject to an insertion or deletion of a single nucleotide will be translated into a completely different protein. Such changes are usually for the worse because natural selection has selected against them. There is much less of such strict conservation in introns. A single deletion or insertion appears to have little effect in an intron on anything, unless it occurs in a rare crucial place that will prevent the enzymes from splicing the intron. Perhaps for such reasons, introns tend not to show the frame bias seen in exons. In consequence, examining the presence or absence of consistent frame bias provides a good first reading of where the larger exons of the gene are. Furthermore some DNA subsequences look much more like exons than introns or vice versa, and detecting the presence of such can also help distinguish introns from exons.

Indeed, the problem of determining the frame of an exon is essentially resolved using such frame differential methods. Using the above mentioned techniques, and examining rare subsequences, we can identify the frames of exons correctly 98 percent of the time.

Since the frame information is heavily dependent on the subsequence length used, the information becomes more definitive as the subsequence gets longer. It is valuable to use as large a data set as possible for determining which sequences look like what. The data sets usually used on this problem provide only enough data to consider 6-tuples of nucleotides, whose length is that of two amino acids in the resulting protein. The data has more intron information, and provides useful frequency data for sequences of length up to 9 in introns. Much larger data sets can be exploited by using protein and cDNA databases. We discuss this idea next.

### 3.2 DICTIONARY APPROACHES

The protein and cDNA data bases contain information derived exclusively from exons. However the latter is complicated because it contains both fragments of coding exons, and also fragments which include non-coding exons. The latter tend to look very different from the coding exons we wish to find, and in fact look much more like introns than like coding exons, in general. (As always there are exceptions.) The cDNA data base is also complicated by the fact that the gene can lie on either strand of the DNA, so that the cDNA can represent the reverse complement of the original DNA sequence (where complementation interchanges

C with G and T with A.) Our approach to utilizing these data bases is to compile dictionaries of fragments of protein script and of cDNA script. These differ from ordinary dictionaries since we really do not know how to distinguish words. This means we can define wordlets to be sequences of any kind we choose. Instead of giving the meaning of such wordlets, which we would dearly love to do, the dictionary provides for each wordlet in it, a list of all members of the corresponding data base that contain it. We have compiled such dictionaries, and it is not difficult to do so on not very expensive computing machines both for cDNA data bases and the protein data base. In the former we have done so for nucleotide sequences of length 11, and also for sequences having 11 significant places with every third place skipped (hence length 16.) In the protein data base we have constructed a dictionary of amino acid sequences of length 4. We have used these numbers because they are convenient; furthermore they permit conclusions to be drawn about longer sequences as well, so that we have not yet encountered a need for a dictionary with longer wordlets.

Such dictionaries have immediate application to finding homologies where they exist in these data bases, that is, to finding members of them which are the product of the gene in question or share one or more of its exons, or resemble the products of these exons. For by looking up each wordlet of appropriate kind that occurs in the gene under consideration, one can compute how many wordlets each entry in the data base shares with the gene in question. One can, furthermore, use the protein data base dictionary with wordlets of length 4 to find how many wordlets of length 5 or 6 or etc., each entry shares with the gene in question. In our case there is little noise for length 5, and by ordering the entries according to the number of wordlets of length 5 in common with our gene, and examining the top segment of the ordered list, we can see which proteins share exons with our gene, and can quickly identify any proteins homologous to any parts of it. The cDNA data base and appropriate dictionaries can be used for the same purpose. It is also possible to use the wordlet frequency information contained in the protein data base dictionary as an intron/exon indicator. We suggest ordering the wordlets according to frequency of occurrence in the data base, and summing the ranks in a moving window of 25 successive wordlets for each frame to indicate exons. Tests suggest that this method is an improvement over the use of raw frequency data. In particular, some false positive exon signals are removed. The use of ranks also limits the sensitivity of the prediction methods to the learning data.

#### 4 DISCUSSION

This problem we have discussed can be viewed, in part, as follows: we have a script that is written in interspersed parts in two “languages”; there are characteristic transitions between one and the other, and these are helpful for identification purposes, but only up to a point. (Subsequences that resemble transitions between intron and exon occur fairly often inside introns and sometimes inside exons). Our task is to distinguish the parts in each language. The natural hope is that one can identify introns by the mechanism through which they are spliced out in the process of protein making. These mechanisms involve enzymes which interact

with both end segments of the intron that is cut out. If we could understand how the RNA strand arranges itself in the presence of these enzymes, understanding of the splicing process could allow us to predict what will be spliced. However, while we can extract some clues as to how good a potential splice site looks, such clues are not enough to solve the problem. The major clues which seem to help the most come from recognizing which parts of the gene appear to be written in “exon script”. By “exon script” we mean subsequences that can be translated into sequences of amino acids which “make sense” as protein parts. As discussed in the previous section, various tests designed to extract distinguishing features can prove to be very useful. The dictionaries we have created also add a large range of sources from which we can obtain data for the various tests.

The dictionary idea has many potential applications in understanding protein secondary structure and function as well. Most approaches to understanding how proteins fold together and what they do have been based on global considerations. However, it is known that perhaps half of proteins on the average consist of certain specific structures, in particular alpha helices, beta sheets, loops, etc. We cannot expect to understand a paragraph merely by identifying the presence of words that we do not understand, and these may occur in paragraphs with entirely different meanings. Nevertheless linguists have obtained remarkable conclusions by examining word frequencies in texts (such as the claim that certain books of the bible were actually written by several different authors.) It may well be that protein wordlets that often occur in alpha helices, for example can provide clues as to the folding of other proteins that contain them, so that it may be possible after all to assign meaning to at least some of the wordlets in these dictionaries.

There is insufficient space left for us in this paper or on its margins, so that results will be reported elsewhere.

## 5 ACKNOWLEDGMENTS

We thank Eric Banks, William Beebee, John Dunagan, Nick Feamster, Aram Harrow, Julia Lipman, Valentin Spitkovsky, Tina Tyan and Bill Wallis for helping in countless ways with the implementation of the ideas outlined in this paper. This project has been supported by Merck. Pachter has been partially supported by an NIH training grant and a Program in Mathematics and Molecular Biology graduate fellowship.

## REFERENCES

- [1] S. F. Altschul, S. F. Gish, W. Miller, E. W. Myers, and D. J. Lipman. Basic local alignment search tool. *Journal of Molecular Biology*, 215:403–410, 1990.
- [2] C. Burge and S. Karlin. Prediction of complete gene structures in human genomic DNA. *Journal of Molecular Biology*, 268:78–94, 1997.
- [3] M. Burset and R. Guigó. Evaluation of gene structure prediction programs. *Genomics*, 34(3):353–367, 1996.



- [4] J. M. Claverie, O. Poirot, and F. Lopez. The difficulty of identifying genes in anonymous vertebrate sequences. *Computers and Chemistry*, 21(4):203–214, 1997.
- [5] S. Dong and D. B. Searls. Gene structure prediction by linguistic methods. *Genomics*, 23:540–551, 1994.
- [6] M. S. Gelfand, A. A. Mironov, and P. A. Pevzner. Gene recognition via spliced sequence alignment. *Proc. Natl. Acad. Sci. USA*, 93:9061–9066, 1996.
- [7] R. Guigo. Computational gene identification: an open problem. *Computers and Chemistry*, 21(4):215–222, 1997.
- [8] D. Haussler, D. Kulp, and M. Reese. A representative benchmark gene data set. <http://www-hgc.lbl.gov/inf/genesets.html>, 1996.
- [9] Xiaoqiu Huang, Mark D. Adams, Hao Zhou, and Anthony Kerlavage. A tool for analyzing and annotating genomic sequences. *Genomics*, 46:37–45, 1997.
- [10] D. Kulp, D. Haussler, M. G. Reese, and F. H. Eeckman. A generalized Hidden Markov Model for the recognition of human genes in DNA. *Proceedings of the 4th Conference on Intelligent Systems in Molecular Biology*, 1996.
- [11] E. S. Lander. The new genomics- global views of biology. *Science*, 274(5287):536–539, 1996.
- [12] Alexander V. Lukashin and Mark Borodovsky. GENEMARK.HMM: new solutions for gene finding. *Nucleic Acids Research*, 26(4):1107–1115, 1998.
- [13] L. R. Rabiner. A tutorial on hidden markov models and selected applications in speech recognition. *Proc. IEEE*, 77(2):257–285, 1989.
- [14] P. A. Sharp. Split genes and RNA splicing. *Cell*, 77(6):805–815, 1994.
- [15] A. F. A. Smit. Origin of interspersed repeats in the human genome. *Curr. Opin. Genet. Devel.*, 6(6):743–749, 1996.
- [16] Y. Xu, R. J. Mural, M. Shah, and E. C. Uberbacher. Recognizing exons in genomic sequences using GRAIL II. In Jane Setlow, editor, *Genetic Engineering: Principles and Methods*, volume 16. Penum Press, 1994.

Serafim Batzoglou  
 Laboratory for Computer Science  
 Massachusetts Institute  
 of Technology  
 Cambridge, MA 02139  
 USA

Bonnie Berger and Lior Pachter  
 Department of Mathematics and  
 Laboratory for Computer Science  
 Massachusetts Institute  
 of Technology  
 Cambridge, MA 02139  
 USA

Daniel J. Kleitman  
 Department of Mathematics  
 Massachusetts Institute  
 of Technology  
 Cambridge, MA 02139  
 USA

Eric S. Lander  
 Whitehead Institute and  
 Department of Biology  
 Massachusetts Institute  
 of Technology  
 Cambridge, MA 02139  
 USA

## AUTHOR INDEX FOR VOLUMES I, II, AND III

Ajtai, M. ....	III	421	Collet, P. ....	III	123
Aldous, D. J. ....	III	205	Colmez, P. ....	II	153
Anbil, R. ....	III	677	Cook, W. ....	III	645
Andrews, G. E. ....	III	719	Cornalba, M. ....	II	249
Andrzejak, A. ....	III	471	Dauben, J. W. ....	III	799
Applegate, D. ....	III	645	de Jong, A. J. ....	II	259
Arthur, J. ....	II	507	Deift, P. ....	III	491
Artigue, M. ....	III	723	Deninger, C. ....	I	163
Aspinwall, P. S. ....	II	229	Diaconis, P. ....	I	187
Astala, K. ....	II	617	Diederich, K. ....	II	703
Avellaneda, M. ....	III	545	Dijkgraaf, R. ....	III	133
Bartolini Bussi, M. G. ...	III	735	Donaldson, S. K. ....	II	309
Batyrev, V. V. ....	II	239	Dranishnikov, A. N. ....	II	423
Batzoglou, S. ....	I	649	Dress, A. ....	III	565
Berger, B. ....	I	649	Driscoll, T. A. ....	III	533
Berkovich, A. ....	III	163	Dubrovin, B. ....	II	315
Berkovich, V. G. ....	II	141	Duke, W. ....	II	163
Bernstein, J. ....	II	519	Dwyer, W. G. ....	II	433
Bethuel, F. ....	III	11	Eliashberg, Y. ....	II	327
Beylkin, G. ....	III	481	Eliasson, L. H. ....	II	779
Bismut, J. M. ....	I	143	Engquist, B. ....	III	503
Bixby, R. ....	III	645	Eskin, A. ....	II	539
Bogomolny, E. ....	III	99	Feigenbaum, J. ....	III	429
Bollobás, B. ....	III	333	Fintushel, R. ....	II	443
Bollobás, B. ....	I	109	Foreman, M. ....	II	11
Borcherds, R. E. ....	I	607	Forrest, J. J. ....	III	677
Bramson, M. ....	III	213	Frank, A. ....	III	343
Buchholz, D. ....	III	109	Freedman, M. H. ....	II	453
Burago, D. ....	II	289	Freidlin, M. I. ....	III	223
Byrd, R. H. ....	III	667	Friedlander, E. M. ....	II	55
Chayes, J. T. ....	III	113	Gallavotti, G. ....	I	205
Chemla, K. ....	III	789	Gallot, S. ....	II	339
Cherednik, I. ....	II	527	Ghosh, J. K. ....	III	237
Christ, M. ....	II	627	Giorgilli, A. ....	III	143
Chv'atal, V. ....	III	645	Goddard, P. ....	I	99
Colding, T. H. ....	II	299	Goemans, M. X. ....	III	657

Götze, F. .... III	245	Lander, E. S. .... I	649
Götze, F. .... I	648	Lascoux, A. .... III	355
Gowers, W. T. .... I	617	Le Gall, J. F. .... III	279
Grötschel, M. .... I	15	Lewis, D. J. .... III	763
Grabovsky, Y. .... III	623	Lindblad, H. .... III	39
Graf, G. M. .... III	153	Lohkamp, J. .... II	381
Graham, R. .... I	133	Macdonald, I. G. .... I	303
Gramain, F. .... II	173	Machedon, M. .... III	49
Gray, J. J. .... III	811	Mahowald, M. .... II	465
Green, M. L. .... II	267	Mallat, S. .... I	319
Greengard, L. .... III	575	Malle, G. .... II	87
Grenander, U. .... III	585	Matoušek, J. .... III	365
Guzmán, M. .... III	747	Mattila, P. .... II	657
Hackbusch, W. .... I	235	McCoy, B. M. .... III	163
Hall, P. .... III	257	McDuff, D. .... I	339
Håstad, J. .... III	441	McLaughlin, K. T. R. .... III	491
Hayashi, S. .... II	789	McMullen, C. T. .... II	841
Hélein, F. .... III	21	McMullen, C. T. .... I	630
Herman, M. .... II	797	Melo, W. .... II	765
Higson, N. .... II	637	Merel, L. .... II	183
Hjorth, G. .... II	23	Merle, F. .... III	57
Hodgson, B. R. .... III	747	Milman, V. .... II	665
Hofer, H. H. W. .... I	255	Milton, G. W. .... III	623
Hoppensteadt, F. .... III	593	Miwa, T. .... I	359
Hou, T. Y. .... III	601	Mochizuki, S. .... II	187
Hrushovski, E. .... I	281	Moser, J. .... I	381
Huiskens, G. .... II	349	Mozes, S. .... II	571
Iooss, G. .... III	611	Müller, D. .... II	679
Ivanov, S. V. .... II	67	Müller, S. .... II	691
Izhikevich, E. .... III	593	Newelski, L. .... II	33
Jaegermann, N. T. .... II	731	Niederreiter, H. .... III	377
Jensen, R. R. .... III	31	Niss, M. .... III	767
Johnstone, I. M. .... III	267	Nocedal, J. .... III	667
Joyce, D. .... II	361	Ohtsuki, T. .... II	473
Kantor, W. M. .... II	77	Okamoto, H. .... III	513
Kapranov, M. .... II	277	Oliver, B. .... II	483
Kifer, Y. .... II	809	Pachter, L. .... I	649
Kleitman, D. J. .... I	649	Papanicolaou, G. .... I	403
Kočvara, M. .... III	707	Pedit, F. .... II	389
Kottwitz, R. E. .... II	553	Peskin, C. S. .... III	633
Kriecherbauer, T. .... III	491	Pinchuk, S. .... II	703
Kuksin, S. B. .... II	819	Pinkall, U. .... II	389
Kuperberg, K. .... II	831	Pisier, G. .... I	429
Labourie, F. .... II	371	Pitassi, T. .... III	451
Lacey, M. T. .... II	647	Polterovich, L. .... II	401
Lafforgue, L. .... II	563	Ponce, G. .... III	67

Presnell, B. ....	III	257	Talagrand, M. ....	I	507
Pukhlikov, A. V. ....	II	97	Taubes, C. H. ....	II	493
Pulleyblank, W. R. ....	III	677	Taubes, C. H. ....	I	119
Reiten, I. ....	II	109	Terhalle, W. ....	III	565
Rickard, J. ....	II	121	Thas, J. A. ....	III	397
Robert, A. ....	III	747	Todorcevic, S. ....	II	43
Ruan, Y. ....	II	411	Trefethen, L. N. ....	III	533
Safonov, M. ....	I	637	Tsirelson, B. ....	III	311
Sarnak, P. ....	I	453	Tsuji, T. ....	II	207
Schlickewei, H. P. ....	II	197	Uhlmann, G. ....	III	77
Schonmann, R. H. ....	III	173	Vafa, C. ....	I	537
Schrijver, A. ....	III	687	Venakides, S. ....	III	491
Seip, K. ....	II	713	Viana, M. ....	I	557
Serganova, V. ....	II	583	Villani, V. ....	III	747
Shalev, A. ....	II	129	Vilonen, K. ....	II	595
Shor, P. W. ....	I	467	Voevodsky, V. ....	I	579
Siegmund, D. ....	III	291	Wainger, S. ....	II	743
Sigmund, K. ....	I	487	Wakimoto, M. ....	II	605
Sloane, N. J. A. ....	III	387	Welzl, E. ....	III	471
Smale, S. ....	I	127	Wilkie, A. J. ....	I	633
Smirnov, F. A. ....	III	183	Willems, J. C. ....	III	697
Smith, D. A. ....	III	777	Williams, R. J. ....	III	321
Smith, H. F. ....	II	723	Wolff, T. ....	II	755
Stern, R. J. ....	II	443	Xia, Z. ....	II	867
Strömberg, J. O. ....	III	523	Yafaev, D. ....	III	87
Sudan, M. ....	III	461	Yau, H. T. ....	III	193
Sun, X. ....	III	575	Zelevinsky, A. ....	III	409
Šverák, V. ....	II	691	Zhang, S. W. ....	II	217
Świątek, G. ....	II	857	Zhou, X. ....	III	491
Sznitman, A. S. ....	III	301	Zowe, J. ....	III	707