Mathematical Analysis of Evolution, Information, and Complexity

Edited by Wolfgang Arendt and Wolfgang P. Schleich



WILEY-VCH Verlag GmbH & Co. KGaA

Mathematical Analysis of Evolution, Information, and Complexity

Edited by Wolfgang Arendt and Wolfgang P. Schleich For additional information reagarding this topic, please refer also to the following publications

Bruß, D., Leuchs, G. (eds.)

Lectures on Quantum Information

2007 ISBN 978-3-527-40527-5

Audretsch, J. (ed.)

Entangled World The Fascination of Quantum Information and Computation

2006 ISBN 978-3-527-40470-4

Stolze, J., Suter, D.

Quantum Computing A Short Course from Theory to Experiment

2004 ISBN 978-3-527-40438-4

Mathematical Analysis of Evolution, Information, and Complexity

Edited by Wolfgang Arendt and Wolfgang P. Schleich



WILEY-VCH Verlag GmbH & Co. KGaA

The Editors

Prof. Dr. Wolfgang Arendt

University of Ulm Institute of Applied Analysis wolfgang.arendt@uni-ulm.de

Prof. Dr. Wolfgang P. Schleich

University of UIm Dept. of Quantum Physics Wolfgang.Schleich@uni-ulm.de

Cover picture

Taken from: Bernd Mohring, Coherent Manipulation and Transport of Matter Waves Verlag Dr. Hut ISBN-10: 3899634810 By cortesy of Bernd Mohring All books published by Wiley-VCH are carefully produced. Nevertheless, authors, editors, and publisher do not warrant the information contained in these books, including this book, to be free of errors. Readers are advised to keep in mind that statements, data, illustrations, procedural details or other items may inadvertently be inaccurate.

Library of Congress Card No.: applied for

British Library Cataloguing-in-Publication Data: A catalogue record for this book is available from the British Library.

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.dnb.de.

© 2009 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

All rights reserved (including those of translation into other languages). No part of this book may be reproduced in any form by photoprinting, microfilm, or any other means nor transmitted or translated into a machine language without written permission from the publishers. Registered names, trademarks, etc. used in this book, even when not specifically marked as such, are not to be considered unprotected by law.

Typesetting le-tex publishing services oHG, Leipzig

Printingbetz-druck GmbH, DarmstadtBindingLitges & Dopf GmbH, Heppenheim

Printed in the Federal Republic of Germany Printed on acid-free paper

ISBN: 978-3-527-40830-6

Contents

Preface XV

List of Contributors XIX

Prologue XXIII Wolfgang Arendt, Delio Mugnolo and Wolfgang Schleich

1 Weyl's Law 1

Wolfgang Arendt, Robin Nittka, Wolfgang Peter, Frank Steiner

۱v

- 1.1 Introduction 1
- 1.2 A Brief History of Weyl's Law 2
- 1.2.1 Weyl's Seminal Work in 1911–1915 2
- 1.2.2 The Conjecture of Sommerfeld (1910) 5
- 1.2.3 The Conjecture of Lorentz (1910) 7
- 1.2.4 Black Body Radiation: From Kirchhoff to Wien's Law 8
- 1.2.5 Black Body Radiation: Rayleigh's Law 10
- 1.2.6 Black Body Radiation: Planck's Law and the Classical Limit 12
- 1.2.7 Black Body Radiation: The Rayleigh–Einstein–Jeans Law 14
- 1.2.8 From Acoustics to Weyl's Law and Kac's Question 18
- 1.3 Weyl's Law with Remainder Term. I 19
- 1.3.1 The Laplacian on the Flat Torus \mathbb{T}^2 19
- 1.3.2 The Classical Circle Problem of Gauss 20
- 1.3.3 The Formula of Hardy–Landau–Voronoï 21
- 1.3.4 The Trace Formula on the Torus \mathbb{T}^2 and the Leading Weyl Term 22
- 1.3.5Spectral Geometry: Interpretation of the Trace Formula
on the Torus \mathbb{T}^2 in Terms of Periodic Orbits24
- 1.3.6 The Trace of the Heat Kernel on *d*-Dimensional Tori and Weyl's Law 25
- 1.3.7 Going Beyond Weyl's Law: One can Hear the Periodic Orbits of the Geodesic Flow on the Torus \mathbb{T}^2 27
- 1.3.8 The Spectral Zeta Function on the Torus \mathbb{T}^2 28
- 1.3.9An Explicit Formula for the Remainder Term in Weyl's Law
on the Torus \mathbb{T}^2 and for the Circle Problem29

VI Contents

1.3.10	The Value Distribution of the Remainder Term
	in the Circle Problem 32
1.3.11	A Conjecture on the Value Distribution of the Remainder Term
	in Weyl's Law for Integrable and Chaotic Systems 34
1.4	Weyl's Law with Remainder Term. II 38
1.4.1	The Laplace–Beltrami Operator on <i>d</i> -Dimensional Compact Riemann
	Manifolds \mathcal{M}^d and the Pre-Trace Formula 38
1.4.2	The Sum Rule for the Automorphic Eigenfunctions on \mathcal{M}^d 39
1.4.3	Weyl's Law on \mathcal{M}^d and its Generalization by Carleman 40
1.4.4	The Selberg Trace Formula and Weyl's Law 42
1.4.5	The Trace of the Heat Kernel on \mathcal{M}^2 44
1.4.6	The Trace of the Resolvent on \mathcal{M}^2 and Selberg's Zeta Function 45
1.4.7	The Functional Equation for Selberg's Zeta Function $Z(s)$ 48
1.4.8	An Explicit Formula for the Remainder Term in Weyl's Law on \mathcal{M}^2
	and the Hilbert–Polya Conjecture on the Riemann Zeros 49
1.4.9	The Prime Number Theorem
	vs. the Prime Geodesic Theorem on \mathcal{M}^2 51
1.5	Generalizations of Weyl's Law 52
1.5.1	Weyl's Law for Robin Boundary Conditions 52
1.5.2	Weyl's Law for Unbounded Quantum Billiards 53
1.6	A Proof of Weyl's Formula 54
1.7	Can One Hear the Shape of a Drum? 59
10	
1.8	Does Diffusion Determine the Domain? 63
1.8	References 64
1.8 2	
	References 64
	References 64 Solutions of Systems of Linear Ordinary Differential Equations 73
2	References 64 Solutions of Systems of Linear Ordinary Differential Equations 73 Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng
2 2.1	References 64 Solutions of Systems of Linear Ordinary Differential Equations 73 Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng 73 Introduction 73
2 2.1 2.2	References64Solutions of Systems of Linear Ordinary Differential Equations73Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng73Introduction73The Exponential Ansatz of Magnus76
2 2.1 2.2	References 64 Solutions of Systems of Linear Ordinary Differential Equations 73 <i>Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng</i> Introduction 73 The Exponential Ansatz of Magnus 76 The Feynman–Dyson Series,
2 2.1 2.2 2.3	References 64 Solutions of Systems of Linear Ordinary Differential Equations 73 <i>Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng</i> Introduction 73 The Exponential Ansatz of Magnus 76 The Feynman–Dyson Series, and More General Perturbation Techniques 78
2 2.1 2.2 2.3 2.4	References 64 Solutions of Systems of Linear Ordinary Differential Equations 73 <i>Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng</i> Introduction 73 The Exponential Ansatz of Magnus 76 The Feynman–Dyson Series, and More General Perturbation Techniques 78 Power Series Methods 80
2 2.1 2.2 2.3 2.4 2.4.1	 References 64 Solutions of Systems of Linear Ordinary Differential Equations 73 Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng Introduction 73 The Exponential Ansatz of Magnus 76 The Feynman–Dyson Series, and More General Perturbation Techniques 78 Power Series Methods 80 Regular Points 80 Singularities of the First Kind 81 Singularities of Second Kind 82
2 2.1 2.2 2.3 2.4 2.4.1 2.4.2 2.4.3 2.5	References 64 Solutions of Systems of Linear Ordinary Differential Equations 73 <i>Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng</i> Introduction 73 The Exponential Ansatz of Magnus 76 The Feynman–Dyson Series, and More General Perturbation Techniques 78 Power Series Methods 80 Regular Points 80 Singularities of the First Kind 81 Singularities of Second Kind 82 Multi-Summability of Formal Power Series 84
2 2.1 2.2 2.3 2.4 2.4.1 2.4.2 2.4.3	References 64 Solutions of Systems of Linear Ordinary Differential Equations 73 <i>Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng</i> Introduction 73 The Exponential Ansatz of Magnus 76 The Feynman–Dyson Series, and More General Perturbation Techniques 78 Power Series Methods 80 Regular Points 80 Singularities of the First Kind 81 Singularities of Second Kind 82 Multi-Summability of Formal Power Series 84 Asymptotic Power Series Expansions 84
2 2.1 2.2 2.3 2.4 2.4.1 2.4.2 2.4.3 2.5	References 64 Solutions of Systems of Linear Ordinary Differential Equations 73 <i>Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng</i> Introduction 73 The Exponential Ansatz of Magnus 76 The Feynman–Dyson Series, and More General Perturbation Techniques 78 Power Series Methods 80 Regular Points 80 Singularities of the First Kind 81 Singularities of Second Kind 82 Multi-Summability of Formal Power Series 84
2 2.1 2.2 2.3 2.4 2.4.1 2.4.2 2.4.3 2.5 2.5.1 2.5.2 2.5.3	References64Solutions of Systems of Linear Ordinary Differential Equations73Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng73Introduction73The Exponential Ansatz of Magnus76The Feynman–Dyson Series,78and More General Perturbation Techniques78Power Series Methods80Regular Points80Singularities of the First Kind81Singularities of Second Kind82Multi-Summability of Formal Power Series84Asymptotic Power Series Expansions84Gevrey Asymptotics85Asymptotic Existence Theorems85
2 2.1 2.2 2.3 2.4 2.4.1 2.4.2 2.4.3 2.5 2.5.1 2.5.2 2.5.3 2.5.4	References64Solutions of Systems of Linear Ordinary Differential Equations73Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng73Introduction73The Exponential Ansatz of Magnus76The Feynman–Dyson Series,78and More General Perturbation Techniques78Power Series Methods80Regular Points80Singularities of the First Kind81Singularities of Second Kind82Multi-Summability of Formal Power Series84Asymptotic Power Series Expansions84Gevrey Asymptotics85Asymptotic Existence Theorems85k-Summability86
2 2.1 2.2 2.3 2.4 2.4.1 2.4.2 2.4.3 2.5 2.5.1 2.5.2 2.5.3 2.5.4 2.5.5	References 64 Solutions of Systems of Linear Ordinary Differential Equations 73 <i>Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng</i> Introduction 73 The Exponential Ansatz of Magnus 76 The Feynman–Dyson Series, and More General Perturbation Techniques 78 Power Series Methods 80 Regular Points 80 Singularities of the First Kind 81 Singularities of Second Kind 82 Multi-Summability of Formal Power Series 84 Asymptotic Power Series Expansions 84 Gevrey Asymptotics 85 Asymptotic Existence Theorems 85 k-Summability 86 Multi-Summability 89
2 2.1 2.2 2.3 2.4 2.4.1 2.4.2 2.4.3 2.5 2.5.1 2.5.2 2.5.3 2.5.4 2.5.5 2.5.6	References 64 Solutions of Systems of Linear Ordinary Differential Equations 73 <i>Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng</i> Introduction 73 The Exponential Ansatz of Magnus 76 The Feynman–Dyson Series, and More General Perturbation Techniques 78 Power Series Methods 80 Regular Points 80 Singularities of the First Kind 81 Singularities of Second Kind 82 Multi-Summability of Formal Power Series 84 Asymptotic Power Series Expansions 84 Gevrey Asymptotics 85 Asymptotic Existence Theorems 85 k-Summability 86 Multi-Summability 89 Applications to PDE 90
2 2.1 2.2 2.3 2.4 2.4.1 2.4.2 2.4.3 2.5 2.5.1 2.5.2 2.5.3 2.5.4 2.5.5 2.5.6 2.5.7	References 64 Solutions of Systems of Linear Ordinary Differential Equations 73 <i>Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng</i> Introduction 73 The Exponential Ansatz of Magnus 76 The Feynman–Dyson Series, and More General Perturbation Techniques 78 Power Series Methods 80 Regular Points 80 Singularities of the First Kind 81 Singularities of Second Kind 82 Multi-Summability of Formal Power Series 84 Asymptotic Power Series Expansions 84 Gevrey Asymptotics 85 Asymptotic Existence Theorems 85 k-Summability 86 Multi-Summability 89 Applications to PDE 90 Perturbed Ordinary Differential Equations 91
2 2.1 2.2 2.3 2.4 2.4.1 2.4.2 2.4.3 2.5 2.5.1 2.5.2 2.5.3 2.5.4 2.5.5 2.5.6	References 64 Solutions of Systems of Linear Ordinary Differential Equations 73 <i>Werner Balser, Claudia Röscheisen, Frank Steiner, Eric Sträng</i> Introduction 73 The Exponential Ansatz of Magnus 76 The Feynman–Dyson Series, and More General Perturbation Techniques 78 Power Series Methods 80 Regular Points 80 Singularities of the First Kind 81 Singularities of Second Kind 82 Multi-Summability of Formal Power Series 84 Asymptotic Power Series Expansions 84 Gevrey Asymptotics 85 Asymptotic Existence Theorems 85 k-Summability 86 Multi-Summability 89 Applications to PDE 90

- 2.6.2 The Mathieu Equation 93
- 2.6.3 The Whittaker–Hill Formula 93
- 2.6.4 Calculating the Determinant 94
- 2.6.5 Applications to PDE 94 References 95

3 A Scalar–Tensor Theory of Gravity with a Higgs Potential 99

Nils Manuel Bezares-Roder, Frank Steiner

- 3.1 Introduction 99
- 3.1.1 General Relativity and the Standard Model of Particle Physics 99
- 3.1.2 Alternative Theories of Gravity and Historical Overview 111
- 3.2 Scalar-Tensor Theory with Higgs Potential 115
- 3.2.1 Lagrange Density and Models 115
- 3.2.2 The Field Equations 118
- 3.2.3 Field Equations After Symmetry Breakdown 119
- 3.2.4 Outlook 124
 - References 131
- 4 Relating Simulation and Modeling of Neural Networks 137

Stefano Cardanobile, Heiner Markert, Delio Mugnolo, Günther Palm, Friedhelm Schwenker

- 4.1 Introduction 137
- 4.2 Voltage-Based Models 138
- 4.3 Changing Paradigm From Biological Networks of Neurons to Artificial Neural Networks 142
- 4.4 Numerical Simulation of Neural Networks 143
- 4.5 Population-Based Simulation of Large Spiking Networks 148
- 4.6 Synaptic Plasticity and Developing Neural Networks 152 References 153
- 5 Boolean Networks for Modeling Gene Regulation 157

Christian Wawra, Michael Kühl, Hans A. Kestler

- 5.1 Introduction 157
- 5.2 Biological Background 158
- 5.3 Aims of Modeling 160
- 5.4 Modeling Techniques 161
- 5.5 Modeling GRNs with Boolean Networks 162
- 5.6 Dynamic Behavior of Large Random Networks 165
- 5.7 Inference of Gene Regulatory Networks from Real Data 169
- 5.7.1 Problem Definition 170
- 5.7.2 Identifying Algorithms 170
- 5.7.3 Noisy Data and the Data First Approach 171
- 5.7.4 An Information Theoretical Approach 174
- 5.7.5 Using the Chi-Square Test
 - to Find Relationships Among Genes 175
- 5.8 Conclusion 175

References 177

6	Symmetries in Quantum Graphs 181
	Jens Bolte, Stefano Cardanobile, Delio Mugnolo, Robin Nittka
6.1	Symmetries 181
6.2	Quantum Graphs 185
6.3	Energy Methods for Schrödinger Equations 186
6.4	Symmetries in Quantum Graphs 190
6.5	Schrödinger Equation with Potentials 192
6.6	Concluding Remarks and Open Problems 193
	References 195
7	Distributed Architecture for Speech-Controlled Systems
	Based on Associative Memories 197
	Zöhre Kara Kayikci, Dmitry Zaykovskiy, Heiner Markert, Wolfgang Minker,
	Günther Palm
7.1	Introduction 197
7.2	System Architecture 199
7.3	Feature Extraction on Mobile Devices 202
7.3.1	ETSI DSR Front-End 202
7.3.1.1	Feature Extraction 202
7.3.1.2	Feature Compression 203
7.3.2	Implementation of the Front-End on Mobile Phones 204
7.3.2.1	Multi-Threading 204
7.3.2.2	Fixed-Point Arithmetic 204
7.3.2.3	Processing Time on Real Devices 205
7.4	Speech Recognition Systems Based on Associative Memory 205
7.4.1	Features to Subword Units Conversion using HMMs 206
7.4.1.1	Acoustic Models 206
7.4.1.2	Language Model and Dictionary 207
7.4.2	Subword Units to Words Conversion
	using Neural Associative Memory 207
7.4.2.1	Neural Associative Memories 207
7.4.2.2	The Neural Associative Memory-Based Architecture
	for Word Recognition 209
7.4.2.3	The Functionality of the Architecture 210
7.4.2.4	Learning of New Words 211
7.5	Words to Semantics Conversion using Associative Memory 211
7.5.1	Spoken Word Memory 212
7.5.2	Language Parser 213
7.5.3	Ambiguities 214
7.5.4	Learning of New Objects 215
7.6	Sample System/Experimental Results 215
7.7	Conclusion 216
	References 217

- 8 Machine Learning for Categorization of Speech Utterances 219
 - Amparo Albalate, David Suendermann, Roberto Pieraccini, Wolfgang Minker
- 8.1 Introduction 219
- 8.2 An Overview of Pattern Recognition 222
- 8.3 Utterance Classification as a Text-Classification Problem 224
- 8.4 Utterance Corpus Description 225
- 8.5 Utterance Preprocessing 226
- 8.6 Feature Extraction Based on Term Clustering 227
- 8.6.1 Term Vector of Lexical Co-occurrences 228
- 8.6.2 Hard Term Clustering 229
- 8.6.2.1 Disambiguation 230
- 8.6.3 Fuzzy Term Clustering 231
- 8.6.4 Pole-Based Overlapping Clustering 231
- 8.6.4.1 PoBOC with Fuzzy C-medoids 232
- 8.6.4.2 Utterance Feature Vector 232
- 8.6.5 Utterance Categorization 232
- 8.7 Supervised Methods for Utterance Categorization 233
- 8.7.1 Naïve Bayes Classifier 233
- 8.7.2 Vector Model with Term Weighting for Utterance Classification 233
- 8.7.2.1 Term Frequency 234
- 8.7.2.2 IDF, RIDF and ISCF Scores 234
- 8.8 Evaluation Methods and Results 235
- 8.8.1 Classification with One Labeled Utterance and Feature Extraction 235
- 8.8.2 Classification Based on F Samples per Category 236
- 8.9 Summary and Conclusion 239 References 239
- 9 Semi-Supervised Clustering in Functional Genomics 243
 - Johann M. Kraus, Günther Palm, Friedhelm Schwenker, Hans A. Kestler
- 9.1 Introduction 243
- 9.2 Biological Background 244
- 9.2.1 Functional Genomics 244
- 9.2.2 DNA Microarray Technology 244
- 9.3 Cluster Analysis 245
- 9.3.1 Clustering Microarray Data 246
- 9.3.2 Cluster Methods 248
- 9.3.2.1 Hierarchical Clustering 248
- 9.3.2.2 Partitional Clustering 250
- 9.3.2.3 Incremental Updates 252
- 9.3.2.4 Model-Based Clustering 253
- 9.3.2.5 Spectral Clustering and Other Graph-Based Methods 254
- 9.3.2.6 Biclustering 255
- 9.3.3 Cluster Validation 257

X Contents

9.4	Semi-Supervised Clustering 259
9.4.1	Modeling Background Knowledge 261
9.4.2	Results 262
9.4.3	Challenges 263
9.5	Summary 264
<i></i>	References 266
	References 200
10	luces December and Frature Franchise from a December
10	Image Processing and Feature Extraction from a Perspective
	of Computer Vision and Physical Cosmology 273
	Holger Stefan Janzer, Florian Raudies, Heiko Neumann, Frank Steiner
10.1	Introduction 273
10.1.1	
10.2	Background from Computer Vision 275
10.3	Background from Physical Cosmology 275
10.4	Image Formation and Characterization 277
10.4.1	Generation and Representation of 2D Images 278
10.4.1.1	Perspective Projection 278
10.4.1.2	Stereographic Projection 279
10.4.1.3	Mollweide Projection 279
10.4.2	Image Properties 280
10.4.2.1	Quantization Property 280
	Spatial Resolution Property 281
	Scale Space Property 281
10.4.3	
	Histogram 282
	Covariance and Correlation 282
	Joint Histogram 283
	Co-occurrence 284
	Fourier Transformation of One Observation of an RF 284
	Fourier Transformation of a Common Distribution Function 285
	Two-Point Correlation Function and Power Spectrum 285
10.4.4	
	Data Term 288
	Smoothness Term 289
	Constraint Term 289
10.5	Methods of Image Processing 289
10.5.1	Filtering Process 290
10.5.2	Linear and Space-Invariant Filters 290
	Gaussian 290
	First-Order Derivative 291
	Second-Order Derivative and Laplacian of Gaussian (LoG) 292
	Gabor Filter 292
10.5.2.5	Gabor Filter Bank 293
10.5.3	1 0 0
10.5.4	Extraction of Image Structures 295

- 10.6 Invariant Features of Images 296
- 10.6.1 Statistical Moments and Fourier Descriptors 297
- 10.6.1.1 Statistical Joint Central Moments 297
- 10.6.1.2 Fourier Descriptors 297
- 10.6.2 Stereography and Topology 298
- 10.6.2.1 Stereography 298
- 10.6.2.2 Topology 299
- 10.6.3 Minkowski Functionals and Minkowski Valuations 301
- 10.6.3.1 Stochastic Geometry 301
- 10.6.3.2 Integral Geometry 302
- 10.6.3.3 Applications 303
- 10.7 Concluding Remarks 307 References 309
- 11 Boosting Ensembles of Weak Classifiers in High Dimensional Input Spaces 311 Ludwig Lausser, Friedhelm Schwenker, Hans A. Kestler
- 11.1 Introduction 311
- 11.2 Hypothesis Boosting Problem 312
- 11.3 Learn 313
- 11.4 Boosting by Majority 315
- 11.5 AdaBoost 316
- 11.5.1 Training Sample Error 317
- 11.5.2 Generalization Error 318
- 11.5.3 AdaBoost on Noisy Data 319
- 11.6 BrownBoost 320
- 11.7 AdaBoost for Feature Selection 323
- 11.8 Conclusion 325 References 331
- 12 The Sampling Theorem in Theory and Practice 333 Wolfgang Arendt, Michal Chovanec, Jürgen Lindner, Robin Nittka
- 12.1 Introduction and History 333
- 12.2 The Sampling Theorem in Applications 334
- 12.2.1 Applications in Theory 334
- 12.2.2 Applications in Practice 335
- 12.2.3 Special Case: Applications in the Field of Information Transmission 336
- 12.3 Mathematical Formulation of the Sampling Theorem 339
- 12.3.1 Notation 339
- 12.3.2 The Sampling Theorem 340
- 12.3.3 Efficient Proof 341
- 12.3.3.1 Dirichlet's Theorem 341
- 12.3.3.2 A First Attempt of a Proof 342
- 12.3.3.3 The Efficient Proof 343
- 12.3.4 Conventional Proof 344

- XII Contents
 - 12.3.4.1 Tempered Distributions 344
 - 12.3.4.2 Fourier Transformation 345
 - 12.3.4.3 Inversion Theorem 346
 - 12.3.4.4 Examples 347
 - 12.3.4.5 Convolution 348
 - 12.3.4.6 The Conventional Proof 350
 - 12.3.4.7 A Convolution Theorem for a Specific Function 352 References 353

13 Coding and Decoding of Algebraic–Geometric Codes 355

- Martin Bossert, Werner Lütkebohmert, Jörg Marhenke
- 13.1 Introduction 355
- 13.2 Introduction to Linear Codes 355
- 13.3 Introduction to Forward Error Correction 357
- 13.3.1 Binary Symmetric Channel, BSC 358
- 13.3.2 Additive White Gaussian Noise Channel, AWGN 358
- 13.3.3 Maximum A Posteriori (MAP)
- and Maximum Likelihood (ML) Decoding 359
- 13.3.4 Hard- and Soft-Decision Decoding 360
- 13.3.5 Bounded Distance Decoding 360
- 13.4 Algebraic–Geometric Codes 360
- 13.5Computation of Riemann–Roch Spaces363
- 13.6 Decoding up to Half the Minimum Distance 365
- 13.7 Interpolation-Based Decoding 368
- 13.8 Power Decoding of Low Rate Reed–Solomon Codes 372
- 13.9 Interpolation-Based Soft-Decision Decoding 373
- 13.10 Soft-Decision Decoding with the Dorsch Algorithm 376 References 377
- Investigation of Input–Output Gain in Dynamical Systems for Neural Information Processing 379
 Stefano Cardanobile, Michael Cohen, Silvia Corchs, Delio Mugnolo,

Stefano Caraanobue, Michael Conen, Suvia Corchs, Deuo Mugnolo, Heiko Neumann

- 14.1 Overview 379
- 14.2 Introduction 379
- 14.3 The Basic Unit: Analytical Study of the Dipole 383
- 14.3.1 Well-Posedness Results 384
- 14.3.2 Linearization 385
- 14.4 The Basic Unit: Numerical Analysis of the Dipole 388
- 14.5 Model of a Recurrent Network 389
- 14.6 Discussion and Conclusions 391 References 392
- 15 Wave Packet Dynamics and Factorization 395
 - Rüdiger Mack, Wolfgang P. Schleich, Daniel Haase, Helmut Maier
- 15.1 Introduction 395

- 15.1.1 Central Ideas 395
- 15.1.2 Outline of the Article 396
- 15.2 How to Factor Numbers 398
- 15.2.1 Prime Numbers, a Primality Test and a Naive Approach to Factorization *399*
- 15.2.2 A More Sophisticated Algorithm 400
- 15.2.3 Problems with this Algorithm and Probability of Success 400
- 15.3 How to Find the Period of a Function: The Magic Role of Entanglement 401
- 15.3.1 Encoding in Quantum Systems 401
- 15.3.2 Mapping of Periodicity 403
- 15.3.3 Projection 404
- 15.3.4 Phase State 404
- 15.3.5 Subtleties 405
- 15.4 Analogy with Atom Optics 406
- 15.4.1 Scattering Atoms off a Standing Wave 406
- 15.4.2 Method of Stationary Phase 407
- 15.4.3 Interference in Phase Space 408
- 15.5 Exponential Growth of Hilbert Spaceas a Resource of Exponential Speedup 409
- 15.6 Conclusions 410
- 15.A Modular Arithmetic 411
- 15.A.1 Basic Idea 411
- 15.A.2 Modular Multiplication 412
- 15.A.3 Modular Exponentiation 412
- 15.A.3.1 Recurrence Relation 413
- 15.A.3.2 Periodicity 413
- 15.B Chinese Remainder Theorem 414
- 15.B.1 Residues Represented as a Matrix 414
- 15.B.2 Modular Multiplication 416
- 15.B.3 Period of Function from Chinese Remainder Theorem 416
- 15.C Euler's Function 417
- 15.C.1 Definition 417
- 15.C.2 Multiplicative Property 418
- 15.C.3 A Compact Formula for ϕ 418
- 15.D Euclidean Algorithm 420
- 15.E Primitive Root 420
- 15.E.1 Definition 421
- 15.E.2 Periods for Prime Numbers 421
- 15.F Probability for Lucky Choice 423
- 15.F.1 Expression for the Period 423
- 15.F.2 Analysis of Different Cases 424
- 15.G Elements of Atom Optics 425
- 15.G.1 Quantum State of Motion in Raman-Nath Approximation 426
- 15.G.2 Momentum Distribution 426

Contents

15.G.3	Discreteness	of Momentum	due to	Interference	427
--------	--------------	-------------	--------	--------------	-----

- 15.H Factorization with a Gauss Sum due to its Periodicity 429 References 430
- 16 Isomorphism and Factorization -Classical and Quantum Algorithms 433
 - Sebastian Dörn, Daniel Haase, Jacobo Torán, Fabian Wagner
- 16.1 Introduction 433
- 16.2 Factorization of Integers: Classical Algorithms 434
- 16.3 Graph Isomorphism: Classical Algorithms 435
- 16.4 Quantum Algorithms for Integer Factorization 436
- 16.4.1 The Quantum Fourier Transform and Period Finding 437
- 16.4.2 Generalization of the Period-Finding Algorithm 439
- 16.5 Quantum Approach to Graph Isomorphism 443
- 16.5.1 The Hidden-Subgroup Problem and Graph Isomorphism 443
- 16.5.2 The Quantum Query Model and Graph Isomorphism 444
- 16.5.3 Quantum Walks and the Fix-Automorphism Problem 445
- 16.6 Reductions of Integer Factorization and Graph Isomorphism to Ring Isomorphism 447
- 16.6.1 Factoring Integers and Finding Ring Automorphisms 448
- 16.6.2 Graph Isomorphism and Ring Isomorphism 449 References 451
- 17 **QuickSort from an Information Theoretic View** 455
 - Beatrice List, Markus Maucher, Uwe Schöning, Rainer Schuler
- 17.1 Introduction 455
- 17.1.1 Recursion for the Expected Number of Comparisons 457
- 17.2 An Upper Bound 458
- 17.3 A Lower Bound 459
- 17.4 The δ -Random Source 462
- 17.5 Conclusion 464 References 464 Further Reading 464

Index 465

Traveller, there are no paths. Paths are made by walking. Antonio Machado (1875–1939)

Preface

The present book is devoted to the mathematical analysis of evolution, information and complexity. The time evolution of systems or processes is a central question in science and covers a broad range of problems including diffusion processes, neural networks, quantum theory and cosmology. Analysis of information is needed in data compression, channel encoding, cryptography and often in the analysis of information processing in the computer or in the brain. Finally, the analysis of complexity is important for computer science, in particular algorithms, but more generally also for the investigation of complex and chaotic systems.

Since 2004 the University of Ulm has operated a graduate school dedicated to the field of *Mathematical Analysis of Evolution, Information and Complexity.* This program brings together scientists from the disciplines of mathematics, electrical engineering, computer science and physics. Our rather unique school addresses topics that need a unified and highly interdisciplinary approach. The common thread of these problems is mathematical analysis demonstrating once more the newly emerging notion of mathematics as technology.

Our book highlights some of the scientific achievements of our school and therefore bears its name *Mathematical Analysis of Evolution, Information and Complexity*. In order to introduce the reader to the subject we give elementary and thus accessible introductions to timely themes taken from different parts of science and technology such as information theory, neuro-informatics and mathematical physics.

Each article in the book was prepared by a team in which at least two different disciplines were represented. In this way mathematicians have collaborated on a chapter with physicists, or physicists have worked with electrical engineers and so on. Moreover, we have installed the rule that with every senior scientist there would be a graduate student working on this article. We hope that this rule has led to easily understandable contributions.

Mathematical Analysis of Evolution, Information and Complexity does not only represent the program of our school and has become the title of the book but has also served as the guiding principle for its organization. Indeed, we have chosen the three pillars "evolution", "information" and "complexity" of the school as titles for the three parts of the book. For each one we have identified one or two major themes as shown in Table 0.1.

XVI Preface

 Table 0.1 Organization of the book outlining its three pillars with their themes. The number above each topic indicates the chapter.

Evo	lution	Information		Complexity	
Spectral analysis	Networks	Pattern recognition	Signal analysis	Algorithms	
1 Weyl's law	4 biological neural networks	7 speech recognition: remote access	12 Shannon's theorem	15 Shor algorithm	
2 differential equations	5 gene regulation	8 speech recognition: machine learning	13 codes	16 quantum and classical algorithms	
3 cosmology	6 quantum graphs	9 cluster analysis in genomics	14 signal processing in the brain	17 sorting algorithms	
		10 image analysis in computer science and cosmology			
		11 data analysis and learning			

We have taken the liberty to assign each article to one of these themes. However, in many instances the contributions could have also been attributed to another theme. This feature is certainly a trade mark of an interdisciplinary article. These articles form the individual chapters of the book.

The topics addressed in each pillar range from quantum physics via bioinformatics to computer science and electrical engineering. The common element linking all chapters is mathematical analysis. To quote Galileo Galilei:

"Egli [il libro che è l'universo] è scritto in lingua matematica." ("The book which is the universe is written in mathematical language.")

In order to bring out most clearly the interconnections between the chapters of the book, we now briefly summarize the essential ideas of each contribution. We start with the pillar "evolution" consisting of the two themes of spectral analysis and networks.

Weyl's law describes the asymptotic distribution of the eigenvalues of the Laplacian. It has played an important role in the development of quantum theory. Chapter 1 gives a comprehensive summary of the history of Weyl's law, its generalization based on trace formulae, its application in quantum chaos, as well as a modern proof. A review and comparison of different methods of solving systems of linear ordinary differential equations is the topic of Chapter 2. Applications and extensions to partial differential equations such as the heat equation or the Schrödinger equation are given. The theme on evolution concludes in Chapter 3 with an introduction into general relativity with an alternative approach based on the scalartensor theory and the Higgs potential.

The theme of evolution in networks addresses biological neural networks, gene regulation and quantum graphs. For example, Chapter 4 provides an overview over models describing biological and computational neural networks. Here the central topic is the specific model developed in Ulm using neural populations as associative memories. Another example of a network of signalling compounds within the kernel of a cell is summarized in Chapter 5. The mathematical model of Boolean networks describes the gene regulation in living organisms. Quantum graphs, the topic of Chapter 6, represent yet another network. They are a toy model for a Schrödinger operator on a thin, quasi-one-dimensional network. The article studies the symmetries that emerge in such quantum networks.

A major portion of the book is dedicated to the mathematical analysis of information. Here the topics range from speech recognition via cluster analysis to signal processing in the brain. Usually speech recognition is implemented on powerful computers. In Chapter 7 tools are developed which allow remote access, for example, using cellular phones. Here, the Ulm technology of associative memories plays an important role. Spoken language dialogue systems are interactive, voicebased interfaces between humans and computers. They allow humans to carry out tasks of diverse complexity such as the reservation of tickets or the performance of bank transactions. Chapter 8 describes different appproaches for the categorization of caller utterances in the framescope of a technical support dialog system, with special focus on categorizers using small amounts of labeled examples. Functional genomics aim to provide links between genomic information and biological functions. One example is the connection between gene patterns and tumor status. Cluster analysis generates a structure of data solely exploring distances or similarities. A special feature of Chapter 9 is the demonstration that already sparse additional information leads to stable structures which are less susceptible to minor changes. Image analysis tries to detect complex structures in high-dimensional data. Chapter 10 compares and contrasts approaches developed in computer vision and cosmology. We conclude the theme of pattern recognition by discussing in Chapter 11 the fundamental method of classification in data analysis. Unfortunately, the true concept of classification is often not known. A method of combining several such concepts, called boosting, which leads to highly accurate classifiers, is described here.

Another important theme in the part on information is represented by signal analysis covering the topics of Shannon's sampling theorem, codes and signal processing in the brain. The sampling theorem shows how a signal can be reproduced by a finite number of measurements. Chapter 12 gives a historical overview and provides two proofs. Coding theory tells us how, by adding redundancy and correcting errors, information can be transmitted accurately. An overview of codes with emphasis on algebraic geometric codes is given in Chapter 13. This section concludes with Chapter 14 describing a model of how the human cortex processes its sensor signals. Mathematically this model consists of a system of coupled nonlinear ordinary differential equations whose long time behavior is discussed.

The last part addresses the topic of complexity focusing on classical as well as quantum algorithms. A central task in computer science is to find efficient algorithms. Chapter 15 lays the foundation of this chapter by explaining the famous Shor algorithm to factor numbers from a physics point of view. In the same vein Chapter 16 describes the state of the art of two famous problems, integer factorization and the graph isomorphism problem. It points out similarities and differences between these two problems when approached by classical or quantum computing. The QuickSort algorithm is a most efficient sorting method. It relies on dividing the sequence into parts of smaller lengths. In Chapter 17 the complexity of the method is studied with a special emphasis on varying the random source which governs the division.

We would like to take the opportunity to thank the authors for their contributions, enthusiasm and reliability in producing this volume. Moreover, we are most grateful to Robin Nittka for his competent help in putting this book together. Finally, we appreciate the support of the Ministerium für Wissenschaft, Forschung und Kunst, Baden-Württemberg in the framework of the Promotionskolleg *Mathematical Analysis of Evolution, Information and Complexity.*

Ulm, August 2008

Wolfgang Arendt Wolfgang Schleich

List of Contributors

Amparo Albalate

University of Ulm Institute of Information Technology 89069 Ulm Germany amparo.albalate@uni-ulm.de

Wolfgang Arendt

University of Ulm Institute of Applied Analysis 89069 Ulm Germany wolfgang.arendt@uni-ulm.de

Werner Balser

University of Ulm Institute of Applied Analysis 89069 Ulm Germany werner.balser@uni-ulm.de

Nils Bezares-Roder

University of Ulm Institute of Theoretical Physics 89069 Ulm Germany nils.bezares@uni-ulm.de

Jens Bolte

Department of Mathematics Royal Holloway College, University of London Egham, TW20 0EX, United Kingdom jens.bolte@rhul.ac.uk

Martin Bossert

University of Ulm Institute of Telecommunications and Applied Information Theory 89069 Ulm Germany martin.bossert@uni-ulm.de

Stefano Cardanobile

Bernstein Center for Computational Neuroscience Albert-Ludwigs-Universität 79104 Freiburg i. Br. Germany stefano.cardanobile@bccn.uni-freiburg.de

Michal Chovanec

University of Ulm, Helmholtzstraße 18 Institute of Applied Analysis 89069 Ulm Germany michal.chovanec@uni-ulm.de

Michael Cohen

Boston University Department of Cognitive and Neural Systems 677 Beacon Street, Boston, MA 02215 USA mike@cns.bu.edu

Silvia Corchs

University of Ulm Institute of Neural Information Processing 89069 Ulm Germany silvia.corchs@uni-ulm.de

X List of Contributors

Sebastian Dörn

University of Ulm Institute of Theoretical Computer Science 89069 Ulm Germany sebastian.doern@uni-ulm.de

Daniel Haase

University of Ulm Institute of Number Theory and Probability Theory 89069 Ulm Germany daniel.haase@uni-ulm.de

Holger Stefan Janzer

University of Ulm Institute of Theoretical Physics 89069 Ulm Germany holger.janzer@uni-ulm.de

Zöhre Kara Kayikci

University of Ulm Institute of Neural Information Processing 89069 Ulm Germany zoehre.kara@uni-ulm.de

Hans A. Kestler

University of Ulm Clinic for Internal Medicine I and Institute of Neural Information Processing 89069 Ulm Germany hans.kestler@uni-ulm.de

Johann Kraus

University of Ulm Institute of Neural Information Processing 89069 Ulm Germany johann.kraus@uni-ulm.de

Michael Kühl

University of Ulm Institute of Biochemistry 89069 Ulm Germany michael.kuehl@uni-ulm.de

Ludwig Lausser

University of Ulm Institute of Neural Information Processing, Internal Medicine I 89069 Ulm Germany Iudwig.lausser@uni-ulm.de

Jürgen Lindner

University of Ulm Institute of Information Technology 89069 Ulm Germany juergen.lindner@uni-ulm.de

Beatrice List

LS telcom AG Im Gewerbegebiet 31–33 77839 Lichtenau Germany beatrice.list@gmx.de

Werner Lütkebohmert

University of Ulm Institute of Pure Mathematics 89069 Ulm Germany werner.luetkebohmert@uni-ulm.de

Rüdiger Mack

University of Ulm Institute of Quantum Physics 89069 Ulm Germany ruediger.mack@uni-ulm.de

Helmut Maier

University of Ulm Institute of Number Theory and Probability Theory 89069 Ulm Germany helmut.maier@uni-ulm.de

Jörg Marhenke

University of Ulm Institute of Pure Mathematics 89069 Ulm Germany joerg.marhenke@uni-ulm.de

Heiner Markert

University of Ulm Institute of Neural Information Processing 89069 Ulm Germany heiner.markert@uni-ulm.de

Markus Maucher

University of Ulm Institute of Theoretical Computer Science 89069 Ulm Germany markus.maucher@uni-ulm.de

Wolfgang Minker

University of Ulm Institute of Information Technology 89069 Ulm Germany wolfgang.minker@uni-ulm.de

Delio Mugnolo

University of Ulm, Helmholtzstraße 18 Institute of Applied Analysis 89069 Ulm Germany delio.mugnolo@uni-ulm.de

Heiko Neumann

University of Ulm Institute of Neural Information Processing 89069 Ulm Germany heiko.neumann@uni-ulm.de

Robin Nittka

University of Ulm, Helmholtzstraße 18 Institute of Applied Analysis 89069 Ulm Germany robin.nittka@uni-ulm.de

Günther Palm

University of Ulm Institute of Neural Information Processing 89069 Ulm Germany guenther.palm@uni-ulm.de

Wolfgang Peter

University of Ulm Institute of Theoretical Physics 89069 Ulm Germany whmpeter@web.de

Roberto Pieraccini

SpeechCycle, Inc. 26 Broadway, 11th Floor New York, NY 10004 USA roberto@speechcycle.com

Florian Raudies

University of Ulm Institute of Neural Information Processing 89069 Ulm Germany florian.raudies@uni-ulm.de

Claudia Röscheisen

University of Ulm, Helmholtzstraße 18 Institute of Applied Analysis 89069 Ulm Germany claudia.roescheisen@uni-ulm.de

Wolfgang Schleich

University of Ulm Institute of Quantum Physics 89069 Ulm Germany wolfgang.schleich@uni-ulm.de

Uwe Schöning

University of Ulm Institute of Theoretical Computer Science 89069 Ulm Germany uwe.schoening@uni-ulm.de

Rainer Schuler

LogicLine EDV-SystemService GmbH Planiestrasse 10 71063 Sindelfingen Germany rschuler@logicline.de

XXII List of Contributors

Friedhelm Schwenker

University of Ulm Institute of Neural Information Processing 89069 Ulm Germany friedhelm.schwenker@uni-ulm.de

Frank Steiner

University of Ulm Institute of Theoretical Physics 89069 Ulm Germany frank.steiner@uni-ulm.de

Eric Sträng

University of Ulm Institute of Theoretical Physics 89069 Ulm Germany eric.straeng@uni-ulm.de

David Suendermann

SpeechCycle, Inc. 26 Broadway, 11th Floor New York, NY 10004 USA david@speechcycle.com

Jacobo Torán

University of Ulm Institute of Theoretical Computer Science 89069 Ulm Germany jacobo.toran@uni-ulm.de

Fabian Wagner

University of Ulm Institute of Theoretical Computer Science 89069 Ulm Germany fabian.wagner@uni-ulm.de

Christian Wawra

University of Ulm Internal Medicine I 89069 Ulm Germany christian.wawra@uni-ulm.de

Dmitry Zaykovskiy

University of Ulm Institute of Information Technology 89069 Ulm Germany dmitry.zaykovskiy@uni-ulm.de

Prologue

Milestones of Evolution, Information and Complexity

Wolfgang Arendt, Delio Mugnolo and Wolfgang Schleich

The modern world, our world of triumphant rationality, began on November 10, 1619, with a revelation and a nightmare. On that day, in a room in the small Bavarian village of Ulm, René Descartes, a Frenchman, twenty-three years old, crawled into a wall stove and, when he was well-warmed, had a vision. It was not a vision of God, or of the mother of God, or of the celestial chariots, or of the New Jerusalem. It was a vision of the unification of all science.

Philip J. Davis and Reuben Hersh, *Descartes' Dream*, Penguin, London 1986

René Descartes laid the foundation of modern science not only by his natural philosophy, but also by his mathematical contributions. For example, he addressed the tangent problem, which was only solved in its entirety 50 years later by Leibniz and Newton. For this purpose both of them invented mathematical calculus. In 1637 Descartes in his essay *Discours de la méthode* brought to light the physics of diffraction. He was the first to explain the most beautiful spectral phenomenon, the rainbow.

Δ Δ Δ

Since then, spectral analysis has come a long way. It has developed into one of the most fruitful concepts in natural sciences and technology. The overtones of an instrument, such as a tambourine or an organ pipe, and even the bodywork of a Mercedes limousine, exhibit a spectrum. Also in the microscopic world the concept of spectrum is useful. For example, the energy levels of the electron in a hydrogen atom form a spectrum. This fact turned out to be a crucial stepping stone for the development of quantum theory (Chapter 1).

Cosmic microwave background radiation was discovered in 1965 by Arno Penzias and Robert Wilson. In accordance with the Big Bang Theory, it fills the whole universe and is currently considered to be the major evidence for an expanding universe. For this discovery, Penzias and Wilson received the Nobel Prize in Physics in 1978 (Chapter 10). Such a microwave radiation possesses a spectrum which is characteristic of a so-called *black body*. Black bodies have been first considered by Gustav Kirchhoff in 1859 when he laid the foundation of the theory of thermal radiation. Fourteen years earlier he had already introduced two famous laws describing the time evolution of voltages and currents in electric circuits. In this way Kirchhoff single-handedly established modern electrical engineering.

Black bodies have also played a central role in the creation of quantum mechanics. Indeed, motivated by the problem of designing efficient lightbulbs, Max Planck in 1900 discovered that the energy of oscillators is quantized. Building on Planck's insights, Albert Einstein, born in Ulm in 1879, could explain the photoelectric effect. This explanation together with his discovery of the momentum of the light quantum opened the door to the development of quantum mechanics. For these achievements he was awarded the Nobel Prize in 1921. Moreover, his groundbreaking work on relativity, deeply rooted in Riemann's geometric theory, completely changed our understanding of the time evolution of the universe and marked the birth of modern cosmology (Chapter 3).

$\Delta \quad \Delta \quad \Delta$

To a large degree today's electrical engineering lives off the spectral analysis of signals, for example, making cell phones work. It was Claude Shannon who in 1949 discovered that a finite number of samples suffices to capture a wave (Chapter 12). Here he could build on the concept of the Fourier transform, which was introduced by Joseph Fourier in 1822 in his *Théorie analytique de la chaleur*. Shannon's sampling theorem provides the basis for the technology of digitalising and eventually perfectly reconstructing a signal. Moreover, in the very same paper entitled *Communication theory of secrecy systems*, Shannon laid the mathematical foundation of cryptography.

Still, signal processing faces a major theoretical limitation: The shorter a pulse in time, the less well defined the frequency. Bounds of this kind are intimately related to Shannon's investigations collected in his seminal paper *A mathematical theory of communication* from 1948. In this article he introduced the concept of *information entropy*, a measure of the information contained in a random message. Today this article is commonly considered to have initiated information theory.

$\Delta \quad \Delta \quad \Delta$

Also at the end of the 1940s, Donald Hebb was completing his most influential study, *The organization of behavior*. Therein he proposed a quantitative approach to the process of learning, thus giving birth to modern neuropsychology. Hebb was the first to analytically investigate the dual nature of the brain – biological tissue as well as source of perception – combining traditional behavioral studies and modern electrophysiology. His theory of learning suggested that synaptic connections are strengthened or weakened in order to achieve more efficient apprehension. Hebb's work introduced the notion of *synaptic plasticity* and paved the road for the interpretation of the brain as an ever-changing computing system.

Shortly before, in 1943, the first artificial *neural networks* had been introduced by Warren McCulloch and Walter Pitts in their article entitled *A logical calculus of the ideas immanent in nervous activity*. It soon became clear that boolean logic could be implemented in these theoretical devices, thereby enabling them to perform complex computations. Unfortunately, the early neural networks lacked any form of adaptation or learning features. It was Hebb's research that filled this gap. Even today Hebb's laws in their mathematical formulation are among the favorite theoretical tools when setting up and tuning an artificial neural network (Chapters 4, 7 and 14). They allow one to translate learning phenomena into the time evolution of a system of differential or difference equations (Chapter 2).

Δ Δ Δ

The spectrum of a wave can be viewed as a band of eigenfrequencies determined by the Helmholtz equation. This distribution of eigenvalues provides us with a deeper insight into the behaviour of light and matter and is described by Weyl's law, proven by Hermann Weyl in 1911. Surprisingly, there is a close analogue in number theory. The prime numbers are intimately related to Riemann's ζ -function whose nontrivial zeros look very much like a spectrum encountered in atomic physics. In this context Marcus de Sautoy talks about *the music of primes*, which is the title of his book on the Riemann ζ -function. Much is known about the distribution of the primes but the related Riemann's hypothesis on the zeros of the ζ -function is still a mystery. First formulated by Bernhard Riemann in 1859, it is probably the biggest open problem in mathematics today – in fact, it has been dubbed a Millennium Problem, whose solution would be rewarded with a \$1 000 000 prize by the Clay Mathematics Institute (Chapter 1).

Prime numbers and their distribution have fascinated mathematicians for generations. Today they serve us as a mathematical technology in cryptography. A modern life necessity is to transmit secret data, for example, for online banking purposes. It is counterintuitive that encryption can be made safer and more efficient by the use of public keys. In fact, cryptographic keys had to be kept strictly secret until the 1970s. However, even codes based on secret keys are not secure. The most prominent example is the Enigma code used by the Germany military in World War II and broken by Alan Turing in 1943. *Public keys* constituted a breakthrough and a radical change of the paradigm of secrecy. They were first proposed in 1976 in a famous paper by Whitfield Diffie and Martin Hellman entitled New directions in cryptography. In Diffie's and Hellman's words, "each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user in such a way that only the intended receiver is able to decipher it." The actual realization of their project is due to Ronald Rivest, Adi Shamir, and Leonard Adleman, who in 1978 developed the RSA cryptographic system. This work won them the Turing Award in 2002. It is surprising that the long awaited solution of the most famous and originally thought to be useless problem, the proof of Fermat's Last Theorem by Andrew Wiles in the 1990s, also provided us with new tools for cryptography such as elliptic curves. In

fact, their use for enciphering and deciphering was already implicitly contained in the work of Diffie and Hellman (Chapter 16).

Efficient cryptography is just one problem of modern signal theory. Another one is to find a language which permits error-free transmission of information in a process called coding/encoding. And it is again number theory, but also Fourier analysis, that gives us the right tools to perform this task with enormous efficiency (Chapter 13). Again, Shannon's sampling theorem plays a decisive role in this context.

 $\Delta \quad \Delta \quad \Delta$

Quantum theory, even though formulated in a quite abstract mathematical language, has reached a state of broad technological applications. In 1965, Richard Feynman received the Nobel Prize in Physics for his work on quantum electrodynamics. Seventeen years later he was one of the first to recognize the potential of a *quantum computer*. In all digital computers, starting from the Zuse Z3 and the ENIAC of the early 1940s to modern miniaturised devices, the logic is based on memory devices which store either a 0 or a 1, forming a bit of information. In a quantum computer this on/off dichotomy is replaced by the possibility of a *quantum bit* being in a superposition state. Abecedarian forms of such a quantum device exist to date in research labs only. Nevertheless, they have already been studied extensively at a theoretical level.

Once available, a quantum computer would substantially simplify large data analysis. Applications known today include, but are not limited to, the determination of shortest paths in networks or even the factorization of large numbers, for instance, by means of the algorithm discovered by Peter Shor in 1994 (Chapter 15). For this work he was awarded the Gödel Prize in 1999. It is remarkable that Shor's algorithm, implemented on a reasonably large quantum computer, could easily break common cryptographic techniques, including both RSA and methods based on elliptic curves. Possible remedies are random number generators based on Riemann's ζ -function. A fascinating relation between elliptic curves and the ζ -function is suggested by the Birch and Swinnerton–Dyer conjecture, formulated in the 1960s. It is still open and represents another of the Millennium Problems named by the Clay Institute.

However, not even quantum computers have an infinite potential. They may be exponentially faster when confronted with certain tasks, but they are not inherently more powerful than today's computers. Whenever we have to solve a problem with the help of a machine, even an ideal one such as a *universal Turing machine*, we have to use an algorithm which should be optimized. To quantify the intrinsic efficiency of algorithms to be implemented on computers is the goal of *algorithmic complexity theory*, founded by Juris Hartmanis and Richard Stearns in 1965. Their paper *On the computational complexity of algorithms* earned them the Turing Award in 1993.

 $\Delta \quad \Delta \quad \Delta$

Obviously, to *determine* the explicit solution of a problem in a short time, such as factoring of a large number, or to *check* whether given data indeed solve the

problem, for example whether the product of a given set of primes yields the original large number, represent two different tasks. The problems which are solvable by a fast algorithm constitute the class *P*, whereas *NP* consists of those problems which allow for a fast algorithm that is able to check whether a given possible answer is indeed a solution of the problem. Here an algorithm is called *fast* if it can be performed in a time which grows at most polynomially with the input size.

While algorithms for finding prime numbers were already known to the ancient Greek, checking whether a given number is actually a prime seems to be demanding. Nevertheless, it is only a *P*-problem as shown by Manindra Agrawal in 2002 after his post-doc stay at the University of Ulm. This stunning discovery won him the Clay Research Award in the same year and the Gödel Prize (together with his coauthors) in 2006. Another example of the *P* vs. *NP* question is the prime factorization of large numbers (Chapters 15 and 16). Today most of the cryptography devices rely upon the belief that factorization into primes, which is clearly an *NP* problem, is not a *P* problem. Still, all attempts to prove this hypothesis have remained unsuccessful. In 1956, Gödel conjectured in a letter to von Neumann that, in general, it should be possible to replace trial and error approaches by efficient algorithms – as for example done for various problems in number theory – thus implicitly suggesting that *P* = *NP*. Still, more than fifty years later we do not yet know the answer to the *P* vs. *NP* problem.

While it is clear that each *P* problem is also *NP*, most computer scientists firmly believe that the converse is not true, that is $P \neq NP$. This question represents a major research field of theoretical computer science and is also one of the seven Millennium Problems of the Clay Institute.

Δ Δ Δ

Consider the task of coloring a geographical map under the constraint that no two adjacent countries can have the same color. To decide for a given map whether it is possible to complete this task using only three different colors is at least as difficult as any *NP* problem, whereas it is a *P* problem to find a four-coloring of the map. The latter task is closely related to the four-color-theorem, stating that each map can in fact be colored with a maximum of four colors. This theorem was first proposed as a conjecture in 1852 and proven only in 1976 by Kenneth Appel and Wolfgang Haken. Their proof is the first one ever to rely in an essential way upon computer aid, rather than human thought, and has therefore started an everlasting debate in the philosophy of science. The four-color-theorem represents the zenith of the interplay between mathematics, logic and theoretical computer science. In contrast, Kurt Gödel's incompleteness theorem from 1931 was this interplay's nadir. It was a great enlightment to the scientific community to learn from Gödel that no automatic, computer-based mathematics will ever be possible.

Coloring problems belong to *graph theory*, a field studying properties of discrete structures. Also based on graph theoretical objects is a recent proof of the long standing Horn conjecture on the distribution of eigenvalues of a sum of matrices. This question was addressed by Weyl in 1912 but was not proven until the 1990s.

One of the key elements of the proof are surprising connections between ideas from discrete and continuous mathematics as well as from quantum mechanics. For his contributions to the solution of the Horn conjecture, the Clay Research Award was assigned to Terence Tao in 2003. He was also awarded the Fields Medal in 2006 for his results in the arithmetic of prime numbers. It is remarkable that the once abstract graph theory has also found useful applications in algorithmic computer science, especially in data clustering (Chapters 8 and 9), sequencing (Chapter 5), classification (Chapter 11), and sorting (Chapter 17).

 $\Delta \quad \Delta \quad \Delta$

In spite of its limitations in large data analysis, the most efficient system for information processing and computing is still a natural one – the brain. Hermann von Helmholtz was the first to suggest and eventually prove in 1852 that thoughts – or rather neural transmissions – have a finite speed, in fact as slow as 30 m/s. In the year of von Helmholtz's discovery Santiago Ramón y Cajal, the father of modern neurobiology, was born. To him we owe the insight that the nervous system is a fine network consisting of neurons which communicate by means of synapses. For this work, based on a biochemical technique developed by Camillo Golgi, both Golgi and Ramón y Cajal were awarded the Nobel Prize in Medicine in 1906. In 1952 Alan Hodgkin and Andrew Huxley proposed a mathematical model for the propagation of electrical pulses inside individual neurons. They were able to show that the neural transmission happens by means of an ionic current, which can also be modeled as a diffusion process and propagates as a wave. Their model won them the Nobel Prize in Medicine in 1963 (Chapter 4).

The theory of diffusion was originated in 1822 by Fourier in his studies on heat conduction. Eventually, thirty-three years later Adolf Fick formulated the law of diffusion as a partial differential equation involving time as a variable. Such laws are called *evolution equations*. Already Fick recognized that his model was not limited to thermodynamics but had many more fields of application ranging from chemistry to finance. In fact, Fick's law also agrees up to nonlinear correction terms with Hodgkin's and Huxley's differential equations. Moreover, the signalling across synapses is a chemical phenomenon that is partially based on diffusion. Further Nobel Prizes in Medicine have been awarded for related discoveries in 1936, 1963, and 1970, in a *crescendo* that was made possible by the development of electron microscopy. A hundred years after Ramón y Cajal, diffusion processes still belong to the core of computational neuroscience – in a braid of chance, linear determinism, and chaos.

$\Delta \quad \Delta \quad \Delta$

In 1887, Henri Poincaré won a contest sponsored by the King of Sweden asking for the solution of the famous *three-body problem* in celestial mechanics. In fact, Poincaré did not present the solution, but rather indicated a major problem in the mainstream approach to celestial mechanics itself. He pointed out that even a perfect deterministic theory would not yield a useful result, since usually the initial