



**IAS/PARK CITY
MATHEMATICS SERIES**

Volume 10

Computational Complexity Theory

**Steven Rudich
Avi Wigderson
Editors**



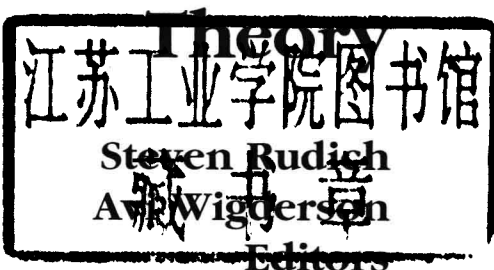
**American Mathematical Society
Institute for Advanced Study**



**IAS/PARK CITY
MATHEMATICS SERIES**

Volume 10

Computational Complexity



**American Mathematical Society
Institute for Advanced Study**

IAS/Park City Mathematics Institute runs mathematics education programs that bring together high school mathematics teachers, researchers in mathematics and mathematics education, undergraduate mathematics faculty, graduate students, and undergraduates to participate in distinct but overlapping programs of research and education. This volume contains the lecture notes from the Graduate Summer School program on Computational Complexity Theory held in Princeton in the summer of 2000.

2000 *Mathematics Subject Classification*. Primary 68Qxx; Secondary 03D15.

Library of Congress Cataloging-in-Publication Data

Computational complexity theory / Steven Rudich, Avi Wigderson, editors.

p. cm. — (IAS/Park City mathematics series, ISSN 1079-5634 ; v. 10)

“Volume contains the lecture notes from the Graduate Summer School program on Computational Complexity Theory held in Princeton in the summer of 2000”—T.p. verso.

Includes bibliographical references.

ISBN 0-8218-2872-X (hardcover : acid-free paper)

I. Computational complexity. I. Rudich, Steven. II. Wigderson, Avi. III. Series.

QA267.7.C685 2004
511.3'52—dc22

2004049026

Copying and reprinting. Material in this book may be reproduced by any means for educational and scientific purposes without fee or permission with the exception of reproduction by services that collect fees for delivery of documents and provided that the customary acknowledgment of the source is given. This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to reprint-permission@ams.org.

Excluded from these provisions is material in articles for which the author holds copyright. In such cases, requests for permission to use or reprint should be addressed directly to the author(s). (Copyright ownership is indicated in the notice in the lower right-hand corner of the first page of each article.)

© 2004 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights
except those granted to the United States Government.

Printed in the United States of America.

⊗ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.

Visit the AMS home page at <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 09 08 07 06 05 04

Computational Complexity Theory

Preface

The IAS/Park City Mathematics Institute (PCMI) was founded in 1991 as part of the “Regional Geometry Institute” initiative of the National Science Foundation. In mid 1993 the program found an institutional home at the Institute for Advanced Study (IAS) in Princeton, New Jersey. The PCMI now holds its summer programs either in Park City or in Princeton.

The IAS/Park City Mathematics Institute encourages both research and education in mathematics and fosters interaction between the two. The three-week summer institute offers programs for researchers and postdoctoral scholars, graduate students, undergraduate students, high school teachers, mathematics education researchers, and undergraduate faculty. One of PCMI’s main goals is to make all of the participants aware of the total spectrum of activities that occur in mathematics education and research: we wish to involve professional mathematicians in education and to bring modern concepts in mathematics to the attention of educators. To that end the summer institute features general sessions designed to encourage interaction among the various groups. In-year activities at sites around the country form an integral part of the High School Teacher Program.

Each summer a different topic is chosen as the focus of the Research Program and Graduate Summer School. Activities in the Undergraduate Program deal with this topic as well. Lecture notes from the Graduate Summer School are being published each year in this series. The first ten volumes are:

- Volume 1: *Geometry and Quantum Field Theory* (1991)
- Volume 2: *Nonlinear Partial Differential Equations in Differential Geometry* (1992)
- Volume 3: *Complex Algebraic Geometry* (1993)
- Volume 4: *Gauge Theory and Four-Manifolds* (1994)
- Volume 5: *Hyperbolic Equations and Frequency Interactions* (1995)
- Volume 6: *Probability Theory and Applications* (1996)
- Volume 7: *Symplectic Geometry and Topology* (1997)
- Volume 8: *Representation Theory of Lie Groups* (1998)
- Volume 9: *Arithmetic Algebraic Geometry* (1999)
- Volume 10: *Computational Complexity Theory* (2000)

Future volumes from the 2001 Summer School on *Quantum Field Theory, Supersymmetry and Enumerative Geometry* and from the 2002 Summer School on *Automorphic Forms and Applications* are in preparation. The 2003 Research Program

and Graduate Summer School topic is *Harmonic Analysis and Partial Differential Equations*.

Some material from the Undergraduate Program is published as part of the Student Mathematical Library series of the American Mathematical Society. We hope to publish material from other parts of the IAS/Park City Mathematics Institute in the future. This will include material from the High School Teacher Program and publications documenting the interactive activities which are a primary focus of the PCMI. At the summer institute late afternoons are devoted to seminars of common interest to all participants. Many deal with current issues in education; others treat mathematical topics at a level which encourages broad participation. The PCMI has also spawned interactions between universities and high schools at a local level. We hope to share these activities with a wider audience in future volumes.

David R. Morrison, Series Editor
March, 2003

Contents

Preface	xiii
Introduction	1
Week One:	
COMPLEXITY THEORY: FROM GÖDEL TO FEYNMAN	3
Steven Rudich, Complexity Theory: From Gödel to Feynman	5
Lecture 1. History and Basic Concepts	7
1.1. History	7
1.2. The Turing Machine	8
1.3. Some Basic Definitions	11
1.4. The Church-Turing Thesis	12
1.5. Computational Resources	12
1.6. Gödel's Letter	13
1.7. The Modern Day Version of $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$	13
1.8. Appendix	17
Lecture 2. Resources, Reductions and P vs. NP	19
2.1. Time and Space	19
2.2. Polynomial Time	19
2.3. Non-Deterministic Turing Machines	20
2.4. Consequences of $\mathbf{P} = \mathbf{NP}$	22
2.5. Reducibility	23
2.6. Completeness	24
2.7. Cook-Levin Theorem	25
2.8. Other \mathbf{NP} -complete Problems	27
2.9. What Gödel Missed	27
Lecture 3. Probabilistic and Quantum Computation	29
3.1. Schwartz-Zippel Theorem	29
3.2. Verifying Arithmetic	30
3.3. Probabilistic Complexity Classes	30
3.4. Quantum Computation	32
3.5. Conclusion	33

Lecture 4. Complexity Classes	35
4.1. Simulation	35
4.2. Hierarchy Theorems	37
4.3. Ladner's Theorem	38
4.4. Relativization	39
4.5. Relations Between Some Complexity Classes	40
4.6. Co-classes	41
Lecture 5. Space Complexity and Circuit Complexity	45
5.1. Savitch's Theorem	45
5.2. The Immerman-Szelepcsényi Theorem	46
5.3. PSPACE -Completeness	48
5.4. Boolean Circuits	49
5.5. Circuit Complexity Classes	51
5.6. Non-Uniform Circuits and Advice Turing Machines	52
Lecture 6. Oracles and the Polynomial Time Hierarchy	55
6.1. Complexity Classes Relative to an Oracle	55
6.2. Polynomial Hierarchy	56
6.3. Placing BPP in the World Picture	60
6.4. Karp-Lipton Theorem	62
Lecture 7. Circuit Lower Bounds	65
7.1. Circuit Complexity and Low Degree Polynomials	65
7.2. Approximation Method	66
Lecture 8. "Natural" Proofs of Lower Bounds	75
8.1. How to Reason That a Problem is Hard	75
8.2. An Old "Stumbling Block": Relativization	75
8.3. A New Direction: Non-Uniform Lower Bounds	76
8.4. A New "Stumbling Block": Natural Proofs	76
8.5. Natural Proofs of Lower Bounds for AC ₀	77
8.6. Generalizing Our Definitions	79
8.7. "Naturalizing" Smolensky's Proof	79
8.8. What's "Bad" About a Natural Proof?	81
8.9. Why Do Natural Proofs Arise?	83
8.10. Unnatural Circuit Lower Bounds	83
8.11. The Big Picture	83
Bibliography	85
Avi Wigderson, Average Case Complexity	89
Lecture 1. Average Case Complexity	91
1.1. Introduction	91
1.2. Levin's Theory of Average-Case Complexity	91
1.3. A "Generic" Dist-NP Complete Problem	94
1.4. Converting Worst-Case Hardness into Average-Case Hardness	95
1.5. Five Possible Worlds	96
Bibliography	99

Sanjeev Arora, Exploring Complexity through Reductions	101
Introduction	103
Lecture 1. PCP Theorem and Hardness of Computing Approximate Solutions	105
1. Approximation Algorithms	105
2. Probabilistically Checkable Proofs	106
3. Håstad's PCP and Inapproximability of MAX-3SAT	108
4. Inapproximability of MAX-3SAT(13)	108
5. Inapproximability of MAX-INDEP-SET	109
6. Inapproximability of Other Problems	110
7. History	111
Lecture 2. Which Problems Have Strongly Exponential Complexity?	113
1. SERF-Reductions	113
2. The Main Theorem	114
Lecture 3. Toda's Theorem: $PH \subseteq P^{\#P}$	119
1. Classes $\#P$ and $\oplus P$	119
2. The Main Lemma	121
3. Proof of Theorem 21	122
4. Open Problems	123
Bibliography	125
Ran Raz, Quantum Computation	127
Lecture 1. Introduction	129
1.1. Classical Deterministic Machines	130
1.2. Classical Probabilistic Machines	131
1.3. Quantum Systems	132
1.4. Dirac's Ket Notation	133
1.5. Quantum Measurement	134
1.6. Transition Matrix and Interference	134
1.7. Measurement According to a Different Base	135
1.8. The Polarizers Experiment	136
1.9. Historical Background	137
Lecture 2. Bipartite Quantum Systems	139
2.1. The Quantum Register	139
2.2. Bipartite Quantum Systems	140
2.3. Tensor Product of Vectors	140
2.4. Tensor Product of Matrices	141
2.5. Partial Measurements	142
2.6. The EPR Paradox	142
2.7. Entanglement and Interference	143
2.8. The No-Cloning Theorem	144
Lecture 3. Quantum Circuits and Shor's Factoring Algorithm	147
3.1. Quantum Circuit Complexity	147
3.2. Quantum Simulation of Classical Computations	149

3.3. Quantum Parallelization	150
3.4. Quantum Fourier Transform	150
3.5. Finding the Period of a Vector	151
3.6. Finding Order modulo N	152
Bibliography	155
Week Two:	
LOWER BOUNDS	157
Ran Raz, Circuit and Communication Complexity	159
Lecture 1. Communication Complexity	161
1.1. Basic Model and Some Examples	161
1.2. Deterministic versus Probabilistic Complexity	162
1.3. Communication Complexity of Equality	163
1.4. Input Matrix and Monochromatic Covers	164
1.5. The Rank Lower Bound	165
Lecture 2. Lower Bounds for Probabilistic Communication Complexity	167
2.1. Probabilistic Protocols and Unbalanced Rectangles	167
2.2. Lower Bound for Inner-Product	168
2.3. Lower Bound for Set Disjointness	171
2.4. The 3-Distinctness Problem	172
Lecture 3. Communication Complexity and Circuit Depth	175
3.1. Karchmer - Wigderson Games	175
3.2. Monotone Complexity	178
3.3. Monotone Karchmer-Wigderson Games	180
3.4. Lower Bound for Matching	182
Lecture 4. Lower Bound for Directed st -Connectivity	185
4.1. The <i>FORK</i> Game	185
4.2. Restricted <i>FORK</i> Protocols	187
4.3. Trivial Lower Bound of $\Omega(\log(w))$	188
Lecture 5. Lower Bound for <i>FORK</i> (Continued)	191
5.1. Increasing the Density	191
5.2. Combinatorial Claim	192
5.3. Proof of The Main Lemma	192
Bibliography	197
Paul Beame, Proof Complexity	199
Lecture 1. An Introduction to Proof Complexity	201
1.1. Proof Systems	201
1.2. Examples of Propositional Proof Systems	203
1.3. Polynomial Calculus with Resolution - PCR	210
1.4. Proof System Hierarchy	213

Lecture 2. Lower Bounds in Proof Complexity	215
2.1. The Pigeonhole Principle	215
2.2. Width vs. Size of Resolution Proofs	218
2.3. Resolution Proofs Based on the Width-Size Relationship	220
2.4. Nullstellensatz and Polynomial Calculus Lower Bounds	223
Lecture 3. Automatizability and Interpolation	227
3.1. Automatizability	227
3.2. Interpolation	228
3.3. Lower Bounds Using Interpolation	229
3.4. Limitations	231
Lecture 4. The Restriction Method	233
4.1. Decision Trees	234
4.2. Restriction Method in Circuit Complexity	235
4.3. Restriction Method in Proof Complexity	236
Lecture 5. Other Research and Open Problems	241
Bibliography	243
Week Three:	
RANDOMNESS IN COMPUTATION	247
Preface to “Week Three: RANDOMNESS IN COMPUTATION”	249
Oded Goldreich, Pseudorandomness – Part I	253
Preface	255
Lecture 1. Computational Indistinguishability	257
1.1. Introduction	257
1.2. The Notion of Pseudorandom Generators	258
1.3. The Definition of Computational Indistinguishability	259
1.4. Relation to Statistical Closeness	259
1.5. Indistinguishability by Repeated Experiments	261
Lecture 2. Pseudorandom Generators	265
2.1. Basic Definition and Initial Discussion	265
2.2. Amplifying the Stretch Function	266
2.3. How to Construct Pseudorandom Generators	267
Lecture 3. Pseudorandom Functions and Concluding Remarks	273
3.1. Definition and Construction of Pseudorandom Functions	273
3.2. Applications of Pseudorandom Functions	274
3.3. Concluding Remarks	276
Appendix	279
Proof of Theorem 2.7	279
Bibliography	283

Luca Trevisan, Pseudorandomness – Part II	287
Introduction	289
Lecture 1. Deterministic Simulation of Randomized Algorithms	291
1. Probabilistic Algorithms versus Deterministic Algorithms	291
2. De-randomization Under Complexity Assumptions	293
Lecture 2. The Nisan-Wigderson Generator	297
1. Pseudorandom Generators	297
2. The Two Main Theorems	298
3. Error-Correcting Codes and Worst-Case to Average-Case Reductions	299
4. The Nisan-Wigderson Construction	300
Lecture 3. Analysis of the Nisan-Wigderson Generator	305
Lecture 4. Randomness Extractors	309
1. Use of Weak Random Sources	309
2. Extractors	310
3. Applications	310
4. An Extractor from Nisan-Wigderson	311
Bibliography	313
Salil Vadhan, Probabilistic Proof Systems — Part I	315
Lecture 1. Interactive Proofs	317
1.1. Definitions	318
1.2. Graph Nonisomorphism	319
1.3. co-NP and More	321
1.4. Additional Topics	325
1.5. Exercises	327
Lecture 2. Zero-Knowledge Proofs	331
2.1. Definition	331
2.2. Zero-Knowledge Proofs for NP	332
2.3. Additional Topics	338
2.4. Exercises	341
Suggestions for Further Reading	343
Bibliography	345
Madhu Sudan, Probabilistically Checkable Proofs	349
Lecture 1. Introduction to PCPs	351
1. Overview	351
2. Definitions and Formal Statement of Results	352
3. Broad Skeleton of the Proof	356
4. Gap Problems and Polynomial Constraint Satisfaction	356
5. Low-Degree Testing	358
6. Self-Correction of Polynomials	359

7. Obtaining a Non-trivial PCP	359
Lecture 2. NP-Hardness of PCS	361
1. Multivariate Polynomials	361
2. Hardness of Gap-PCS	363
3. Low-Degree Testing	367
4. Self-Correction	367
Lecture 3. A Couple of Digressions	369
1. A 3-Prover MIP for NP	370
2. $\text{NP} \subseteq \text{PCP}[\text{poly}, O(1)]$	372
Lecture 4. Proof Composition and the PCP Theorem	379
1. Where Are We?	379
2. Composing the Verifiers	379
3. The PCP Theorem	382
4. Towards Optimal PCPs	383
5. Roadmap to the Optimal PCP	384
Bibliography	387

Introduction

Computational Complexity Theory is a major research area of Computer Science. Its aim is to set the formal mathematical foundations of efficient computation. As such, it postulates that all agents/machines involved in performing a computational task have limited resources (such as time, memory, communication, etc.), and asks which tasks can be performed under such limitations.

There has been significant development in the nature and scope of the field in the last 30 years. Traditionally it studied the computation of well-defined functions on a completely specified input by a single, deterministic machine. While this continues to be a focus, the field evolved to also study a very broad variety of computational tasks by a diverse set of computational models, such as randomized, interactive, distributed, and parallel computation. These models may include many computers, which may behave cooperatively or adversarially.

Moreover, it became clear that the limits on the computational resources naturally lead to a fundamentally new and important way of understanding many central notions beyond computation itself, e.g., proof, knowledge, randomness, cryptography, and more. Indeed, the field is riddled with basic results and open problems which have deep conceptual meaning, and thus their significance can be readily understood by non-experts.

Complexity theory also quickly developed close connections with other fields, most notably Mathematics: first and most naturally with areas in Discrete Mathematics, but more recently with Algebra, Analysis, Geometry, and Number Theory. These connections, which often benefit both sides, keep increasing in quantity and depth. Other connections are developing with Physics, Biology, Economics, and other sciences.

The field has been lucky to continuously draw into it excellent students in the last decades. This period witnessed exciting development in creating new directions of study and understanding their inner relations with the basic problems of the field.

While mature in many ways, the most fundamental problems of the field are still wide open. We still have no clue if $P = NP$ or not, nor why it seems so difficult to prove any nontrivial resource lower bound on natural computational tasks. We still have no clue if randomness indeed is such a powerful aid for computation, or if there is always an efficient deterministic way around the coin-flips (as was discovered very recently for testing primality). But we do have a rich and intricate theory regarding these fundamental problems, which in particular ties them together in a deep and unexpected way.

This exciting state of the field seemed perfect for a Park City summer school. We have gathered some of the best researchers and teachers of the field to give diverse sets of lectures, aiming to introduce newcomers to the field. The organization of the courses was designed to start at a very basic level and lead up to the state of the art in some of the most active research areas in complexity. These were given over 3 weeks to more than 150 graduate students, postdocs, and scholars with different backgrounds who gathered on the IAS campus in Princeton during the summer of 2000.

The first week of lectures was devoted to a general introduction to the field. The main set of lectures, entitled “Complexity Theory: from Gödel to Feynman” was given by Steven Rudich, describing basic models, techniques, results and open problems. These were accompanied by lectures by Avi Wigderson on average-case complexity, by Sanjeev Arora on exploring complexity through reductions, and by Ran Raz on quantum computation.

The second week was devoted to lower bounds on concrete models. Ran Raz lectured on communication and circuit complexity, Michael Ben-Or lectured on arithmetic and algebraic complexity (notes missing from this volume), and Paul Beame lectured on proof complexity.

The third week of lectures was devoted to randomness in computation. Oded Goldreich and Luca Trevisan gave two series of lectures on different notions of pseudorandomness. Salil Vadhan lectured on interactive proof systems and zero knowledge, and Madhu Sudan lectured on the probabilistically checkable proofs (PCPs).

It is our pleasure to thank all speakers for this unique and exciting educational experience. We hope that the lecture notes they have provided, collected in this volume, will serve to welcome and introduce many more students and researchers to the wonderful field of Computational Complexity.

Steven Rudich and Avi Wigderson, Volume Editors
Graduate Summer School Organizers
September, 2002

Week One

**COMPLEXITY THEORY: FROM
GÖDEL TO FEYNMAN**

**Steven Rudich, Avi Wigderson, Sanjeev Arora,
and Ran Raz**

