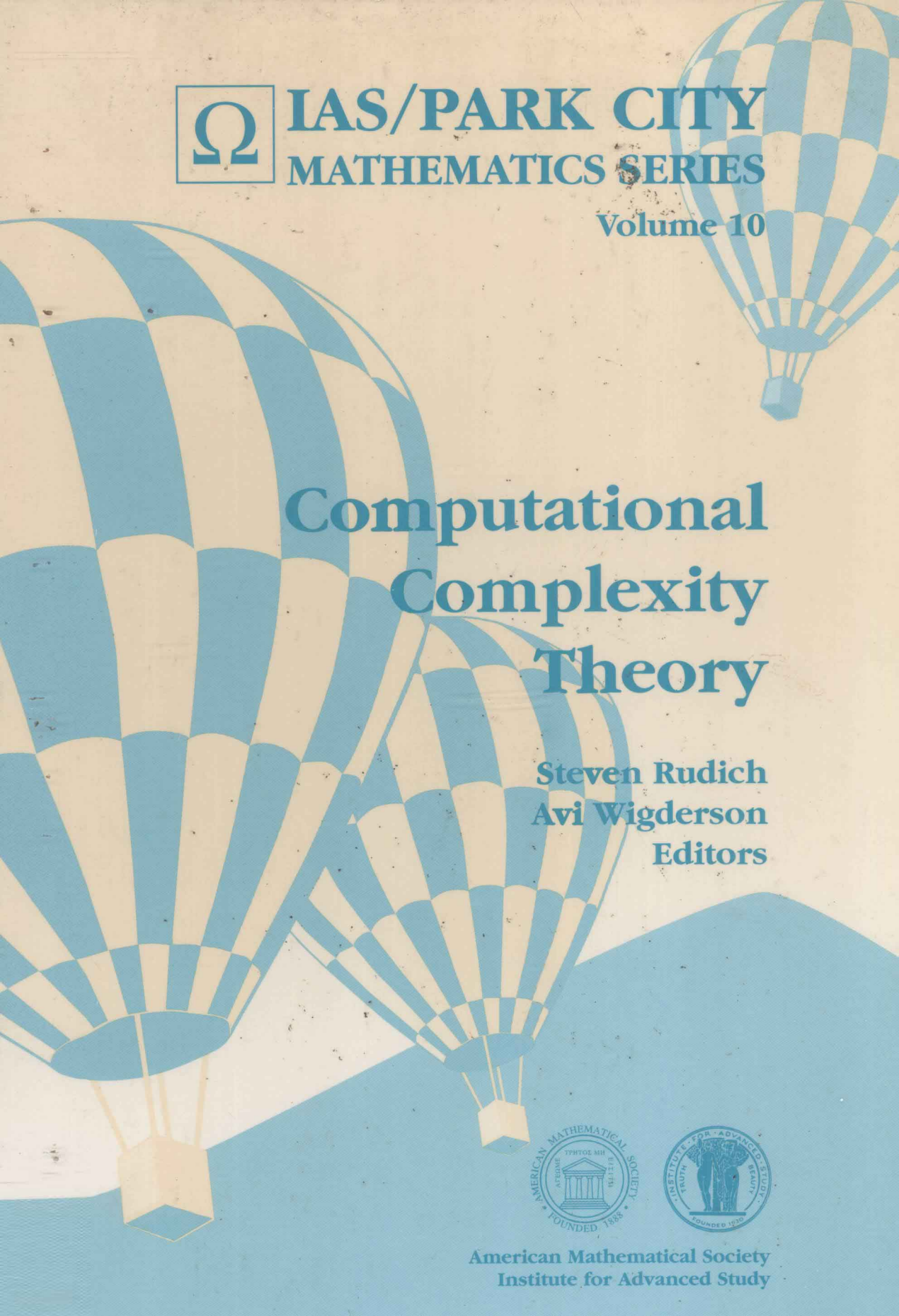


IAS/PARK CITY
MATHEMATICS SERIES
Volume 10

Computational Complexity Theory

Steven Rudich
Avi Wigderson
Editors

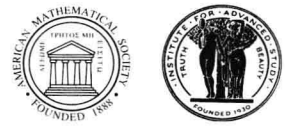
American Mathematical Society
Institute for Advanced Study

IAS/PARK CITY MATHEMATICS SERIES

Volume 10

Computational Complexity Theory

Steven Rudich
Avi Wigderson
Editors



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

QA267.7 .C685 2004
511.3'52—dc22 20040490026

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

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 give 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