

Texts in Theoretical Computer Science

An EATCS Series

Editors: W. Brauer G. Rozenberg A. Salomaa
On behalf of the European Association
for Theoretical Computer Science (EATCS)

Advisory Board: G. Ausiello M. Broy S. Even
J. Hartmanis N. Jones T. Leighton M. Nivat
C. Papadimitriou D. Scott

Springer-Verlag Berlin Heidelberg GmbH

Lane A. Hemaspaandra • Mitsunori Ogihara

The Complexity Theory Companion

With 43 Figures



Springer

Authors

Prof. Dr. Lane A. Hemaspaandra
Prof. Dr. Mitsunori Ogihara
Department of Computer Science
Rochester, NY 14627
USA
{lane,ogihara}@cs.rochester.edu

Series Editors

Prof. Dr. Wilfried Brauer
Institut für Informatik
Technische Universität München
Arcisstrasse 21, 80333 München, Germany
brauer@informatik.tu-muenchen.de

Prof. Dr. Grzegorz Rozenberg
Leiden Institute of Advanced Computer Science
University of Leiden
Niels Bohrweg 1, 2333 CA Leiden, The Netherlands
rozenber@liacs.nl

Prof. Dr. Arto Salomaa
Data City
Turku Centre for Computer Science
20 500 Turku, Finland
asalomaa@utu.fi

Library of Congress Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Hemaspaandra, Lane A.:

The complexity theory companion/Lane A. Hemaspaandra; Mitsunori Ogihara. –
Berlin; Heidelberg; New York; Barcelona; Hong Kong; London; Milan;
Paris; Tokyo: Springer, 2002
(Texts in theoretical computer science)

ACM Computing Classification (1998): F.1, F.2.2, F.4

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

ISBN 978-3-642-08684-7 ISBN 978-3-662-04880-1 (eBook)

DOI 10.1007/978-3-662-04880-1

© Springer-Verlag Berlin Heidelberg 2002

Originally published by Springer-Verlag Berlin Heidelberg New York in 2002.

Softcover reprint of the hardcover 1st edition 2002

The use of general descriptive names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Cover Design: KünkelLopka, Heidelberg

Typesetting: Camera-ready by the authors

Printed on acid-free paper SPIN 10723529 45/3142SR – 5 4 3 2 1 0

This book is dedicated to our families—the best of companions.

Preface

Invitation

Secret 1 *Algorithms are at the heart of complexity theory.*

That is the dark secret of complexity theory. It is recognized by complexity theorists, but would be literally incredible to most others. In this book, we hope to make this secret credible. In fact, the real secret is even more dramatic.

Secret 2 *Simple algorithms are at the heart of complexity theory.*

A corollary of Secret 2 is that every practitioner of computer science or student of computer science already possesses the ability required to understand, enjoy, and employ complexity theory.

We realize that these secrets fly in the face of conventional wisdom. Most people view complexity theory as an arcane realm populated by pointy-hatted (if not indeed pointy-headed) sorcerers stirring cauldrons of recursion theory with wands of combinatorics, while chanting incantations involving complexity classes whose very names contain hundreds of characters and sear the tongues of mere mortals. This stereotype has sprung up in part due to the small amount of esoteric research that fits this bill, but the stereotype is more strongly attributable to the failure of complexity theorists to communicate in expository forums the central role that algorithms play in complexity theory.

Throughout this book—from the tree-pruning and interval-pruning algorithms that shape the first chapter to the query simulation procedures that dominate the last chapter—we will see that proofs in complexity theory usually employ algorithms as their central tools. In fact, to more clearly highlight the role of algorithmic techniques in complexity theory, *this book is organized by technique rather than by topic*. That is, in contrast to the organization of other books on complexity theory, each chapter of this book focuses on one technique—what it is, and what results and applications it has yielded.

The most thrilling times in complexity theory are when a new technique is introduced and sweeps like fire over the field. In addition to highlighting the centrality of algorithms in the proof arsenal of complexity theory, we feel that our technique-based approach more vividly conveys to the reader the flavor and excitement of such conflagrations. We invite the reader to come

with us as we present nine techniques, usually simple and algorithmic, that burned away some of the field's ignorance and helped form the landscape of modern complexity theory.

Usage

We intend this book as a companion for students and professionals who seek an accessible, algorithmically oriented, research-centered, up-to-date guide to some of the most interesting techniques of complexity theory. The authors and their colleague Joel Seiferas have test-driven the book's approach in two different courses at the University of Rochester. We have used this technique-based approach in Rochester's one-semester basic complexity theory course, which is taken by all first-year computer science graduate students and also by those undergraduates specializing or specially interested in theoretical computer science, and in our second course on complexity theory, which is taken by all second-year graduate students as their theory "breadth" course.

We found in both these course settings that the technique-based approach allowed us to impart to students a significant amount of the feel and experience of complexity theory research and led to more student interest and involvement than occurred in earlier course incarnations using other texts. We expect that this will not only benefit the complexity theory students in the courses, but will also help all the course's students become prepared to do work that is theoretically aware, informed, and well-grounded.

At times, we stop the flow of a proof or discussion with a "Pause to Ponder." These are places at which we encourage the reader to pause for a moment and find his or her own solution to the issue raised. Even an unsuccessful attempt to craft a solution will usually make the proof/discussion that follows clearer and more valuable, as the reader will better understand the challenges posed by the hurdle that the proof/discussion overcomes.

With some exceptions due to result dependencies, the non-appendix chapters are generally ordered to put the easier chapters near the start of the book and the more demanding chapters near the end of the book.

Acknowledgments

We are extraordinarily indebted to the following people, who proofread one or more chapters, for their invaluable help, suggestions, corrections, and insights: Eric Allender, Russell Bent, Alina Beygelzimer, Matthew Boutell, Samuel Chen, Yin-He Cheng, Louis Deaett, Gregory Goldstein, Fred Green, Ulrich Hertrampf, Chris Homan, Gabriel Istrate, Jason Ku, David Lagakos, Andrew Learn, Tao Li, Ioan Macarie, Proshanto Mukherji, Kenneth Regan, William Scherer III, Alan Selman, D. Sivakumar, Howard Straubing, Robert Swier,

Mayur Thakur, Jonathan Tomer, Jacobo Torán, Leen Torenvliet, Dieter van Melkebeek, Heribert Vollmer, Julie Zhong, and Marius Zimand. We also thank the many other people who have helped us with advice, comments, corrections, literature pointers, most-recent-version information, and suggestions: Andris Ambainis, Vikraman Arvind, Richard Beigel, Nate Blaylock, Daniel Bovet, Jin-Yi Cai, Diane Cass, Stephen Fenner, Lance Fortnow, William Gasarch, Viliam Geffert, Oded Goldreich, Juris Hartmanis, Edith Hemaspaandra, Paul Ilardi, Sven Kosub, Richard Lipton, Alexis Maciel, Wolfgang Merkle, Christos Papadimitriou, Thanos Papathanasiou, Eduardo Pinheiro, Robert Rettinger, Jörg Rothe, Alex Samorodnitsky, Marcus Schaefer, Michael Shear, Uwe Schöning, Joel Seiferas, Samik Sengupta, Carl Smith, Scott Stoness, Madhu Sudan, Chunqiang Tang, Jun Tarui, Thomas Thierauf, Luca Trevisan, Chris Umans, Osamu Watanabe, Chee Yap, and Stathis Zachos. Any remaining errors are the responsibility of the authors.

We thank our thesis advisors, Juris Hartmanis and Kojiro Kobayashi; their insightful, dedicated, joyous approach to research has been a continuing inspiration to us.

We appreciate the grants—NSF-CCR-8957604, NSF-INT-9116781/JSPS-ENGR-207, NSF-CCR-9322513, NSF-INT-9513368/DAAD-315-PRO-fo-ab, NSF-CCR-9701911, NSF-CCR-9725021, NSF-INT-9726724, NSF-INT-9815095/DAAD-315-PPP-gü-ab NSF-DUE-9980943, DARPA-F30602-98-2-0133, NIA-R01-AG18231—that have supported our research programs during the planning and writing of this book.

For generous advice, help, and support, we thank the Springer-Verlag series editors and staff, namely, Wilfried Brauer, Grzegorz Rozenberg, Arto Salomaa, Alfred Hofmann, Frank Holzwarth, Ingeborg Mayer, Sherryl Sundell, and Hans Wössner. Our own department's technical and secretarial staff—especially Jill Forster, Elaine Heberle, and Jim Roche—was invaluable in keeping our computers up and our manuscript copied and circulating, and we much appreciate their help.

We are grateful to those colleagues—Peter van Emde Boas, Harald Hempel, Jörg Rothe, Alan Selman, Seinosuke Toda, Leen Torenvliet, Heribert Vollmer, Klaus Wagner, Osamu Watanabe, and Gerd Wechsung—who have generously hosted our research visits during the planning and writing of this book, and to the many colleagues, as cited in the Bibliographic Notes sections, who have collaborated with us on the research described in some sections of this book.

Above all, we thank Edith, Ellen, Emi, and Erica for their advice, love, and support.

Lane A. Hemaspaandra

Mitsunori Ogiwara

Rochester, NY
October 2001

Contents

Preface	vii
Invitation	vii
Usage	viii
1. The Self-Reducibility Technique	1
1.1 GEM: There Are No Sparse NP-Complete Sets Unless $P=NP$..	2
1.2 The Turing Case	18
1.3 The Case of Merely Putting Sparse Sets in $NP - P$: The Hartmanis–Immerman–Sewelson Encoding	22
1.4 OPEN ISSUE: Does the Disjunctive Case Hold?	26
1.5 Bibliographic Notes	26
2. The One-Way Function Technique	31
2.1 GEM: Characterizing the Existence of One-Way Functions ..	32
2.2 Unambiguous One-Way Functions Exist If and Only If Bounded-Ambiguity One-Way Functions Exist	35
2.3 Strong, Total, Commutative, Associative One-Way Functions Exist If and Only If One-Way Functions Exist	36
2.4 OPEN ISSUE: Low-Ambiguity, Commutative, Associative One-Way Functions?	42
2.5 Bibliographic Notes	43
3. The Tournament Divide and Conquer Technique	45
3.1 GEM: The Semi-feasible Sets Have Small Circuits	45
3.2 Optimal Advice for the Semi-feasible Sets	48
3.3 Unique Solutions Collapse the Polynomial Hierarchy	56
3.4 OPEN ISSUE: Are the Semi-feasible Sets in P/linear ?	63
3.5 Bibliographic Notes	63
4. The Isolation Technique	67
4.1 GEM: Isolating a Unique Solution	68
4.2 Toda’s Theorem: $PH \subseteq P^{PP}$	72
4.3 $NL/\text{poly} = UL/\text{poly}$	82

4.4	OPEN ISSUE: Do Ambiguous and Unambiguous Nondeterminism Coincide?	87
4.5	Bibliographic Notes	87
5.	The Witness Reduction Technique	91
5.1	Framing the Question: Is $\#P$ Closed Under Proper Subtraction?	91
5.2	GEM: A Complexity Theory for Feasible Closure Properties of $\#P$	93
5.3	Intermediate Potential Closure Properties	99
5.4	A Complexity Theory for Feasible Closure Properties of $\text{Opt}P$	103
5.5	OPEN ISSUE: Characterizing Closure Under Proper Decrement	105
5.6	Bibliographic Notes	106
6.	The Polynomial Interpolation Technique	109
6.1	GEM: Interactive Protocols for the Permanent	110
6.2	Enumerators for the Permanent	119
6.3	$IP = PSPACE$	122
6.4	$MIP = NEXP$	133
6.5	OPEN ISSUE: The Power of the Provers	163
6.6	Bibliographic Notes	163
7.	The Nonsolvable Group Technique	167
7.1	GEM: Width-5 Branching Programs Capture Nonuniform- NC^1	168
7.2	Width-5 Bottleneck Machines Capture $PSPACE$	176
7.3	Width-2 Bottleneck Computation	181
7.4	OPEN ISSUE: How Complex Is Majority-Based Probabilistic Symmetric Bottleneck Computation?	192
7.5	Bibliographic Notes	192
8.	The Random Restriction Technique	197
8.1	GEM: The Random Restriction Technique and a Polynomial-Size Lower Bound for Parity	197
8.2	An Exponential-Size Lower Bound for Parity	207
8.3	PH and $PSPACE$ Differ with Probability One	218
8.4	Oracles That Make the Polynomial Hierarchy Infinite	222
8.5	OPEN ISSUE: Is the Polynomial Hierarchy Infinite with Probability One?	231
8.6	Bibliographic Notes	231

9. The Polynomial Technique	235
9.1 GEM: The Polynomial Technique	236
9.2 Closure Properties of PP	241
9.3 The Probabilistic Logspace Hierarchy Collapses	252
9.4 OPEN ISSUE: Is PP Closed Under Polynomial-Time Turing Reductions?	259
9.5 Bibliographic Notes	260
 A. A Rogues' Gallery of Complexity Classes	263
A.1 P: Determinism	264
A.2 NP: Nondeterminism	266
A.3 Oracles and Relativized Worlds	268
A.4 The Polynomial Hierarchy and Polynomial Space: The Power of Quantifiers	270
A.5 E, NE, EXP, and NEXP	274
A.6 P/Poly: Small Circuits	276
A.7 L, NL, etc.: Logspace Classes	277
A.8 NC, AC, LOGCFL: Circuit Classes	279
A.9 UP, FewP, and US: Ambiguity-Bounded Computation and Unique Computation	281
A.10 #P: Counting Solutions	286
A.11 ZPP, RP, coRP, and BPP: Error-Bounded Probabilism	288
A.12 PP, $C = P$, and SPP: Counting Classes	290
A.13 FP, NPSV, and NPMV: Deterministic and Nondeterministic Functions	291
A.14 P-Sel: Semi-feasible Computation	294
A.15 $\oplus P$, $\text{Mod}_k P$: Modulo-Based Computation	297
A.16 SpanP, OptP: Output-Cardinality and Optimization Function Classes	297
A.17 IP and MIP: Interactive Proof Classes	299
A.18 PBP, SF, SSF: Branching Programs and Bottleneck Computation	300
 B. A Rogues' Gallery of Reductions	305
B.1 Reduction Definitions: \leq_m^p , \leq_T^p ,	305
B.2 Shorthands: R and E	307
B.3 Facts about Reductions	307
B.4 Circuit-Based Reductions: NC^k and AC^k	308
B.5 Bibliographic Notes	308
 References	309
 Index	335