

Contents

<i>List of Figures</i>	page xiii
<i>Preface</i>	xv
<i>Organization and Chapter Summaries</i>	xvii
<i>Acknowledgments</i>	xxiii
1 Introduction and Preliminaries	1
1.1 Introduction	1
1.1.1 A Brief Overview of Complexity Theory	2
1.1.2 Characteristics of Complexity Theory	6
1.1.3 Contents of This Book	8
1.1.4 Approach and Style of This Book	12
1.1.5 Standard Notations and Other Conventions	16
1.2 Computational Tasks and Models	17
1.2.1 Representation	18
1.2.2 Computational Tasks	18
1.2.3 Uniform Models (Algorithms)	20
1.2.4 Non-uniform Models (Circuits and Advice)	36
1.2.5 Complexity Classes	42
Chapter Notes	43
2 P, NP, and NP-Completeness	44
2.1 The P Versus NP Question	46
2.1.1 The Search Version: Finding Versus Checking	47
2.1.2 The Decision Version: Proving Versus Verifying	50
2.1.3 Equivalence of the Two Formulations	54
2.1.4 Two Technical Comments Regarding NP	55
2.1.5 The Traditional Definition of NP	55
2.1.6 In Support of P Different from NP	57
2.1.7 Philosophical Meditations	58
2.2 Polynomial-Time Reductions	58
2.2.1 The General Notion of a Reduction	59
2.2.2 Reducing Optimization Problems to Search Problems	61
2.2.3 Self-Reducibility of Search Problems	63
2.2.4 Digest and General Perspective	67

CONTENTS

2.3	NP-Completeness	67
2.3.1	Definitions	68
2.3.2	The Existence of NP-Complete Problems	69
2.3.3	Some Natural NP-Complete Problems	71
2.3.4	NP Sets That Are Neither in P nor NP-Complete	81
2.3.5	Reflections on Complete Problems	85
2.4	Three Relatively Advanced Topics	87
2.4.1	Promise Problems	87
2.4.2	Optimal Search Algorithms for NP	92
2.4.3	The Class coNP and Its Intersection with NP	94
	Chapter Notes	97
	Exercises	99
3	Variations on P and NP	108
3.1	Non-uniform Polynomial Time (P/poly)	108
3.1.1	Boolean Circuits	109
3.1.2	Machines That Take Advice	111
3.2	The Polynomial-Time Hierarchy (PH)	113
3.2.1	Alternation of Quantifiers	114
3.2.2	Non-deterministic Oracle Machines	117
3.2.3	The P/poly Versus NP Question and PH	119
	Chapter Notes	121
	Exercises	122
4	More Resources, More Power?	127
4.1	Non-uniform Complexity Hierarchies	128
4.2	Time Hierarchies and Gaps	129
4.2.1	Time Hierarchies	129
4.2.2	Time Gaps and Speedup	136
4.3	Space Hierarchies and Gaps	139
	Chapter Notes	139
	Exercises	140
5	Space Complexity	143
5.1	General Preliminaries and Issues	144
5.1.1	Important Conventions	144
5.1.2	On the Minimal Amount of Useful Computation Space	145
5.1.3	Time Versus Space	146
5.1.4	Circuit Evaluation	153
5.2	Logarithmic Space	153
5.2.1	The Class L	154
5.2.2	Log-Space Reductions	154
5.2.3	Log-Space Uniformity and Stronger Notions	155
5.2.4	Undirected Connectivity	155
5.3	Non-deterministic Space Complexity	162
5.3.1	Two Models	162
5.3.2	NL and Directed Connectivity	164
5.3.3	A Retrospective Discussion	171

CONTENTS

5.4	PSPACE and Games	172
	Chapter Notes	175
	Exercises	175
6	Randomness and Counting	184
6.1	Probabilistic Polynomial Time	185
6.1.1	Basic Modeling Issues	186
6.1.2	Two-Sided Error: The Complexity Class BPP	189
6.1.3	One-Sided Error: The Complexity Classes RP and coRP	193
6.1.4	Zero-Sided Error: The Complexity Class ZPP	199
6.1.5	Randomized Log-Space	199
6.2	Counting	202
6.2.1	Exact Counting	202
6.2.2	Approximate Counting	211
6.2.3	Searching for Unique Solutions	217
6.2.4	Uniform Generation of Solutions	220
	Chapter Notes	227
	Exercises	230
7	The Bright Side of Hardness	241
7.1	One-Way Functions	242
7.1.1	Generating Hard Instances and One-Way Functions	243
7.1.2	Amplification of Weak One-Way Functions	245
7.1.3	Hard-Core Predicates	250
7.1.4	Reflections on Hardness Amplification	255
7.2	Hard Problems in E	255
7.2.1	Amplification with Respect to Polynomial-Size Circuits	257
7.2.2	Amplification with Respect to Exponential-Size Circuits	270
	Chapter Notes	277
	Exercises	278
8	Pseudorandom Generators	284
	Introduction	285
8.1	The General Paradigm	288
8.2	General-Purpose Pseudorandom Generators	290
8.2.1	The Basic Definition	291
8.2.2	The Archetypical Application	292
8.2.3	Computational Indistinguishability	295
8.2.4	Amplifying the Stretch Function	299
8.2.5	Constructions	301
8.2.6	Non-uniformly Strong Pseudorandom Generators	304
8.2.7	Stronger Notions and Conceptual Reflections	305
8.3	Derandomization of Time-Complexity Classes	307
8.3.1	Defining Canonical Derandomizers	308
8.3.2	Constructing Canonical Derandomizers	310
8.3.3	Technical Variations and Conceptual Reflections	313
8.4	Space-Bounded Distinguishers	315
8.4.1	Definitional Issues	316

CONTENTS

8.4.2	Two Constructions	318
8.5	Special-Purpose Generators	325
8.5.1	Pairwise Independence Generators	326
8.5.2	Small-Bias Generators	329
8.5.3	Random Walks on Expanders	332
	Chapter Notes	334
	Exercises	337
9	Probabilistic Proof Systems	349
	Introduction and Preliminaries	350
9.1	Interactive Proof Systems	352
9.1.1	Motivation and Perspective	352
9.1.2	Definition	354
9.1.3	The Power of Interactive Proofs	357
9.1.4	Variants and Finer Structure: An Overview	363
9.1.5	On Computationally Bounded Provers: An Overview	366
9.2	Zero-Knowledge Proof Systems	368
9.2.1	Definitional Issues	369
9.2.2	The Power of Zero-Knowledge	372
9.2.3	Proofs of Knowledge – A Parenthetical Subsection	378
9.3	Probabilistically Checkable Proof Systems	380
9.3.1	Definition	381
9.3.2	The Power of Probabilistically Checkable Proofs	383
9.3.3	PCP and Approximation	398
9.3.4	More on PCP Itself: An Overview	401
	Chapter Notes	404
	Exercises	406
10	Relaxing the Requirements	416
10.1	Approximation	417
10.1.1	Search or Optimization	418
10.1.2	Decision or Property Testing	423
10.2	Average-Case Complexity	428
10.2.1	The Basic Theory	430
10.2.2	Ramifications	442
	Chapter Notes	451
	Exercises	453
	Epilogue	461
	Appendix A: Glossary of Complexity Classes	463
A.1	Preliminaries	463
A.2	Algorithm-Based Classes	464
A.2.1	Time Complexity Classes	464
A.2.2	Space Complexity Classes	467
A.3	Circuit-Based Classes	467
	Appendix B: On the Quest for Lower Bounds	469
B.1	Preliminaries	469

CONTENTS

B.2	Boolean Circuit Complexity	471
B.2.1	Basic Results and Questions	472
B.2.2	Monotone Circuits	473
B.2.3	Bounded-Depth Circuits	473
B.2.4	Formula Size	474
B.3	Arithmetic Circuits	475
B.3.1	Univariate Polynomials	476
B.3.2	Multivariate Polynomials	476
B.4	Proof Complexity	478
B.4.1	Logical Proof Systems	480
B.4.2	Algebraic Proof Systems	480
B.4.3	Geometric Proof Systems	481
Appendix C: On the Foundations of Modern Cryptography		482
C.1	Introduction and Preliminaries	482
C.1.1	The Underlying Principles	483
C.1.2	The Computational Model	485
C.1.3	Organization and Beyond	486
C.2	Computational Difficulty	487
C.2.1	One-Way Functions	487
C.2.2	Hard-Core Predicates	489
C.3	Pseudorandomness	490
C.3.1	Computational Indistinguishability	490
C.3.2	Pseudorandom Generators	491
C.3.3	Pseudorandom Functions	492
C.4	Zero-Knowledge	494
C.4.1	The Simulation Paradigm	494
C.4.2	The Actual Definition	494
C.4.3	A General Result and a Generic Application	495
C.4.4	Definitional Variations and Related Notions	497
C.5	Encryption Schemes	500
C.5.1	Definitions	502
C.5.2	Constructions	504
C.5.3	Beyond Eavesdropping Security	505
C.6	Signatures and Message Authentication	507
C.6.1	Definitions	508
C.6.2	Constructions	509
C.7	General Cryptographic Protocols	511
C.7.1	The Definitional Approach and Some Models	512
C.7.2	Some Known Results	517
C.7.3	Construction Paradigms and Two Simple Protocols	517
C.7.4	Concluding Remarks	522
Appendix D: Probabilistic Preliminaries and Advanced Topics in Randomization		523
D.1	Probabilistic Preliminaries	523
D.1.1	Notational Conventions	523
D.1.2	Three Inequalities	524

CONTENTS

D.2	Hashing	528
D.2.1	Definitions	528
D.2.2	Constructions	529
D.2.3	The Leftover Hash Lemma	529
D.3	Sampling	533
D.3.1	Formal Setting	533
D.3.2	Known Results	534
D.3.3	Hitters	535
D.4	Randomness Extractors	536
D.4.1	Definitions and Various Perspectives	537
D.4.2	Constructions	541
Appendix E: Explicit Constructions		545
E.1	Error-Correcting Codes	546
E.1.1	Basic Notions	546
E.1.2	A Few Popular Codes	547
E.1.3	Two Additional Computational Problems	551
E.1.4	A List-Decoding Bound	553
E.2	Expander Graphs	554
E.2.1	Definitions and Properties	555
E.2.2	Constructions	561
Appendix F: Some Omitted Proofs		566
F.1	Proving That \mathcal{PH} Reduces to $\#\mathcal{P}$	566
F.2	Proving That $\mathcal{IP}(f) \subseteq \mathcal{AM}(O(f)) \subseteq \mathcal{AM}(f)$	572
F.2.1	Emulating General Interactive Proofs by AM-Games	572
F.2.2	Linear Speedup for \mathcal{AM}	578
Appendix G: Some Computational Problems		583
G.1	Graphs	583
G.2	Boolean Formulae	585
G.3	Finite Fields, Polynomials, and Vector Spaces	586
G.4	The Determinant and the Permanent	587
G.5	Primes and Composite Numbers	587
<i>Bibliography</i>		589
<i>Index</i>		601