

Contents

About this book	page	xiii
Acknowledgments		xvii
Introduction		xix
0 Notational conventions		1
0.1 Representing objects as strings		2
0.2 Decision problems/languages		3
0.3 Big-oh notation		3
EXERCISES		4
PART ONE: BASIC COMPLEXITY CLASSES		7
1 The computational model—and why it doesn't matter		9
1.1 Modeling computation: What you really need to know		10
1.2 The Turing machine		11
1.3 Efficiency and running time		15
1.4 Machines as strings and the universal Turing machine		19
1.5 Uncomputability: An introduction		21
1.6 The Class P		24
1.7 Proof of Theorem 1.9: Universal simulation in $O(T \log T)$ -time		29
CHAPTER NOTES AND HISTORY		32
EXERCISES		34
2 NP and NP completeness		38
2.1 The Class NP		39
2.2 Reducibility and NP-completeness		42
2.3 The Cook-Levin Theorem: Computation is local		44
2.4 The web of reductions		50
2.5 Decision versus search		54
2.6 coNP, EXP, and NEXP		55
2.7 More thoughts about P, NP , and all that		57
CHAPTER NOTES AND HISTORY		62
EXERCISES		63
		vii

Diagonalization	68
3.1 Time Hierarchy Theorem	69
3.2 Nondeterministic Time Hierarchy Theorem	69
3.3 Ladner's Theorem: Existence of NP -intermediate problems	71
3.4 Oracle machines and the limits of diagonalization	72
CHAPTER NOTES AND HISTORY	76
EXERCISES	77
Space complexity	78
4.1 Definition of space-bounded computation	78
4.2 PSPACE completeness	83
4.3 NL completeness	87
CHAPTER NOTES AND HISTORY	93
EXERCISES	93
The polynomial hierarchy and alternations	95
5.1 The Class Σ_2^P	96
5.2 The polynomial hierarchy	97
5.3 Alternating Turing machines	99
5.4 Time versus alternations: Time-space tradeoffs for SAT	101
5.5 Defining the hierarchy via oracle machines	102
CHAPTER NOTES AND HISTORY	104
EXERCISES	104
Boolean circuits	106
6.1 Boolean circuits and P_{poly}	107
6.2 Uniformly generated circuits	111
6.3 Turing machines that take advice	112
6.4 P_{poly} and NP	113
6.5 Circuit lower bounds	115
6.6 Nonuniform Hierarchy Theorem	116
6.7 Finer gradations among circuit classes	116
6.8 Circuits of exponential size	119
CHAPTER NOTES AND HISTORY	120
EXERCISES	121
Randomized computation	123
7.1 Probabilistic Turing machines	124
7.2 Some examples of PTMs	126
7.3 One-sided and "zero-sided" error: RP , coRP , ZPP	131
7.4 The robustness of our definitions	132
7.5 Relationship between BPP and other classes	135
7.6 Randomized reductions	138
7.7 Randomized space-bounded computation	139
CHAPTER NOTES AND HISTORY	140
EXERCISES	141

8 Interactive proofs	143
8.1 Interactive proofs: Some variations	144
8.2 Public coins and AM	150
8.3 IP = PSPACE	157
8.4 The power of the prover	162
8.5 Multiprover interactive proofs (MIP)	163
8.6 Program checking	164
8.7 Interactive proof for the permanent	167
CHAPTER NOTES AND HISTORY	169
EXERCISES	170
9 Cryptography	172
9.1 Perfect secrecy and its limitations	173
9.2 Computational security, one-way functions, and pseudorandom generators	175
9.3 Pseudorandom generators from one-way permutations	180
9.4 Zero knowledge	186
9.5 Some applications	189
CHAPTER NOTES AND HISTORY	194
EXERCISES	197
10 Quantum computation	201
10.1 Quantum weirdness: The two-slit experiment	202
10.2 Quantum superposition and qubits	204
10.3 Definition of quantum computation and BQP	209
10.4 Grover's search algorithm	216
10.5 Simon's algorithm	219
10.6 Shor's algorithm: Integer factorization using quantum computers	221
10.7 BQP and classical complexity classes	230
CHAPTER NOTES AND HISTORY	232
EXERCISES	234
11 PCP theorem and hardness of approximation: An introduction	237
11.1 Motivation: Approximate solutions to NP -hard optimization problems	238
11.2 Two views of the PCP Theorem	240
11.3 Equivalence of the two views	244
11.4 Hardness of approximation for vertex cover and independent set	247
11.5 NP \subseteq PCP (poly(n), 1): PCP from the Walsh-Hadamard code	249
CHAPTER NOTES AND HISTORY	254
EXERCISES	255
PART TWO: LOWER BOUNDS FOR CONCRETE COMPUTATIONAL MODELS	257
12 Decision trees	259
12.1 Decision trees and decision tree complexity	259
12.2 Certificate complexity	262
12.3 Randomized decision trees	263

12.4	Some techniques for proving decision tree lower bounds	264	18	Average case complexity: Levin's theory	361
CHAPTER NOTES AND HISTORY		268	18.1	Distributional problems and distP	362
EXERCISES		269	18.2	Formalization of "real-life distributions"	365
Communication complexity		270	18.3	distnp and its complete problems	365
13.1	Definition of two-party communication complexity	271	18.4	Philosophical and practical implications	369
13.2	Lower bound methods	272	CHAPTER NOTES AND HISTORY		371
13.3	Multipart communication complexity	278	EXERCISES		371
13.4	Overview of other communication models	280	19	Hardness amplification and error-correcting codes	373
CHAPTER NOTES AND HISTORY		282	19.1	Mild to strong hardness: Yao's XOR lemma	375
EXERCISES		283	19.2	Tool: Error-correcting codes	379
Circuit lower bounds: Complexity theory's Waterloo		286	19.3	Efficient decoding	385
14.1	AC^0 and Håstad's Switching Lemma	286	19.4	Local decoding and hardness amplification	386
14.2	Circuits with "counters": ACC	291	19.5	List decoding	392
14.3	Lower bounds for monotone circuits	293	19.6	Local list decoding: Getting to $BPP = P$	394
14.4	Circuit complexity: The frontier	297	CHAPTER NOTES AND HISTORY		398
14.5	Approaches using communication complexity	300	EXERCISES		399
CHAPTER NOTES AND HISTORY		304	20	Derandomization	402
EXERCISES		305	20.1	Pseudorandom generators and derandomization	403
Proof complexity		307	20.2	Proof of Theorem 20.6: Nisan-Wigderson Construction	407
15.1	Some examples	307	20.3	Derandomization under uniform assumptions	413
15.2	Propositional calculus and resolution	309	20.4	Derandomization requires circuit lower bounds	415
15.3	Other proof systems: A tour d'horizon	313	CHAPTER NOTES AND HISTORY		418
15.4	Metamathematical musings	315	EXERCISES		419
CHAPTER NOTES AND HISTORY		316	21	Pseudorandom constructions: Expanders and extractors	421
EXERCISES		317	21.1	Random walks and eigenvalues	422
Algebraic computation models		318	21.2	Expander graphs	426
16.1	Algebraic straight-line programs and algebraic circuits	319	21.3	Explicit construction of expander graphs	434
16.2	Algebraic computation trees	326	21.4	Deterministic logspace algorithm for undirected connectivity	440
16.3	The Blum-Shub-Smale model	331	21.5	Weak random sources and extractors	442
CHAPTER NOTES AND HISTORY		334	21.6	Pseudorandom generators for space-bounded computation	449
EXERCISES		336	CHAPTER NOTES AND HISTORY		454
PART THREE: ADVANCED TOPICS		339	EXERCISES		456
Complexity of counting		341	22	Proofs of PCP theorems and the Fourier transform technique	460
17.1	Examples of counting problems	342	22.1	Constraint satisfaction problems with nonbinary alphabet	461
17.2	The Class #P	344	22.2	Proof of the PCP theorem	461
17.3	#P completeness	345	22.3	Hardness of $2CSP_W$: Tradeoff between gap and alphabet size	472
17.4	Toda's theorem: $\#P \subseteq P^{\#SAT}$	352	22.4	Håstad's 3-bit PCP Theorem and hardness of MAX-3SAT	474
17.5	Open problems	358	22.5	Tool: The Fourier transform technique	475
CHAPTER NOTES AND HISTORY		359	22.6	Coordinate functions, long Code, and its testing	480
EXERCISES		359	22.7	Proof of Theorem 22.16	481
		359	22.8	Hardness of approximating SET-COVER	486
		359	22.9	Other PCP theorems: A survey	488
		359	22.A	Transforming $qCSP$ instances into "nice" instances	491
		359	CHAPTER NOTES AND HISTORY		493
		359	EXERCISES		495

23 Why are circuit lower bounds so difficult?	498
23.1 Definition of natural proofs	499
23.2 What's so natural about natural proofs?	500
23.3 Proof of Theorem 23.1	503
23.4 An "unnatural" lower bound	504
23.5 A philosophical view	505
CHAPTER NOTES AND HISTORY	506
EXERCISES	507
Appendix: Mathematical background	508
A.1 Sets, functions, pairs, strings, graphs, logic	509
A.2 Probability theory	510
A.3 Number theory and groups	517
A.4 Finite fields	521
A.5 Basic facts from linear Algebra	522
A.6 Polynomials	527
Hints and selected exercises	531
Main theorems and definitions	545
Bibliography	549
Index	575
Complexity class index	579