

Contents

Preface	ix
I Tools and Techniques	1
1 Introduction	3
1.1 A Min-Cut Algorithm	7
1.2 Las Vegas and Monte Carlo	9
1.3 Binary Planar Partitions	10
1.4 A Probabilistic Recurrence	15
1.5 Computation Model and Complexity Classes	16
Notes	23
Problems	25
2 Game-Theoretic Techniques	28
2.1 Game Tree Evaluation	28
2.2 The Minimax Principle	31
2.3 Randomness and Non-uniformity	38
Notes	40
Problems	41
3 Moments and Deviations	43
3.1 Occupancy Problems	43
3.2 The Markov and Chebyshev Inequalities	45
3.3 Randomized Selection	47
3.4 Two-Point Sampling	51
3.5 The Stable Marriage Problem	53
3.6 The Coupon Collector's Problem	57
Notes	63
Problems	64
4 Tail Inequalities	67
4.1 The Chernoff Bound	67

CONTENTS

4.2	Routing in a Parallel Computer	74
4.3	A Wiring Problem	79
4.4	Martingales	83
	Notes	96
	Problems	97
5	The Probabilistic Method	101
5.1	Overview of the Method	101
5.2	Maximum Satisfiability	104
5.3	Expanding Graphs	108
5.4	Oblivious Routing Revisited	112
5.5	The Lovász Local Lemma	115
5.6	The Method of Conditional Probabilities	120
	Notes	122
	Problems	124
6	Markov Chains and Random Walks	127
6.1	A 2-SAT Example	128
6.2	Markov Chains	129
6.3	Random Walks on Graphs	132
6.4	Electrical Networks	135
6.5	Cover Times	137
6.6	Graph Connectivity	139
6.7	Expanders and Rapidly Mixing Random Walks	143
6.8	Probability Amplification by Random Walks on Expanders	151
	Notes	155
	Problems	156
7	Algebraic Techniques	161
7.1	Fingerprinting and Freivalds' Technique	162
7.2	Verifying Polynomial Identities	163
7.3	Perfect Matchings in Graphs	167
7.4	Verifying Equality of Strings	168
7.5	A Comparison of Fingerprinting Techniques	169
7.6	Pattern Matching	170
7.7	Interactive Proof Systems	172
7.8	PCP and Efficient Proof Verification	180
	Notes	186
	Problems	188
II	Applications	195
8	Data Structures	197
8.1	The Fundamental Data-structuring Problem	197

CONTENTS

8.2	Random Treaps	201
8.3	Skip Lists	209
8.4	Hash Tables	213
8.5	Hashing with $O(1)$ Search Time	221
	Notes	228
	Problems	229
9	Geometric Algorithms and Linear Programming	234
9.1	Randomized Incremental Construction	234
9.2	Convex Hulls in the Plane	236
9.3	Duality	239
9.4	Half-space Intersections	241
9.5	Delaunay Triangulations	245
9.6	Trapezoidal Decompositions	248
9.7	Binary Space Partitions	252
9.8	The Diameter of a Point Set	256
9.9	Random Sampling	258
9.10	Linear Programming	262
	Notes	273
	Problems	275
10	Graph Algorithms	278
10.1	All-pairs Shortest Paths	278
10.2	The Min-Cut Problem	289
10.3	Minimum Spanning Trees	296
	Notes	302
	Problems	304
11	Approximate Counting	306
11.1	Randomized Approximation Schemes	308
11.2	The DNF Counting Problem	310
11.3	Approximating the Permanent	315
11.4	Volume Estimation	329
	Notes	331
	Problems	333
12	Parallel and Distributed Algorithms	335
12.1	The PRAM Model	335
12.2	Sorting on a PRAM	337
12.3	Maximal Independent Sets	341
12.4	Perfect Matchings	347
12.5	The Choice Coordination Problem	355
12.6	Byzantine Agreement	358
	Notes	361
	Problems	363

CONTENTS

13 Online Algorithms	368
13.1 The Online Paging Problem	369
13.2 Adversary Models	372
13.3 Paging against an Oblivious Adversary	374
13.4 Relating the Adversaries	377
13.5 The Adaptive Online Adversary	381
13.6 The k -Server Problem	384
Notes	387
Problems	389
14 Number Theory and Algebra	392
14.1 Preliminaries	392
14.2 Groups and Fields	395
14.3 Quadratic Residues	402
14.4 The RSA Cryptosystem	410
14.5 Polynomial Roots and Factors	412
14.6 Primality Testing	417
Notes	426
Problems	427
<i>Appendix A</i> Notational Index	429
<i>Appendix B</i> Mathematical Background	433
<i>Appendix C</i> Basic Probability Theory	438
References	447
Index	467