Contents

Figure Credits **xiii**

Preface **xv**

1 Prologue **1**
1.1 Crossing Bridges . . . 1
1.2 Intractable Itineraries . . . 5
1.3 Playing Chess With God . . . 8
1.4 What Lies Ahead . . . 10
Problems . . . 11
Notes . . . 13

2 The Basics **15**
2.1 Problems and Solutions . . . 15
2.2 Time, Space, and Scaling . . . 18
2.3 Intrinsic Complexity . . . 23
2.4 The Importance of Being Polynomial . . . 25
2.5 Tractability and Mathematical Insight . . . 29
Problems . . . 30
Notes . . . 35

3 Insights and Algorithms **41**
3.1 Recursion . . . 42
3.2 Divide and Conquer . . . 43
3.3 Dynamic Programming . . . 53
3.4 Getting There From Here . . . 59
3.5 When Greed is Good . . . 64
3.6 Finding a Better Flow . . . 68
3.7 Flows, Cuts, and Duality . . . 71
3.8 Transformations and Reductions . . . 74
Problems . . . 76
Notes . . . 89

4 Needles in a Haystack: the Class NP **95**
4.1 Needles and Haystacks . . . 96
4.2 A Tour of NP . . . 97
4.3 Search, Existence, and Nondeterminism . . . 109
4.4 Knots and Primes . . . 115
Problems . . . 121
Notes . . . 125

5 Who is the Hardest One of All? NP-Completeness **127**
5.1 When One Problem Captures Them All . . . 128
5.2 Circuits and Formulas . . . 129
5.3 Designing Reductions . . . 133
5.4 Completeness as a Surprise . . . 145
5.5 The Boundary Between Easy and Hard . . . 153
5.6 Finally, Hamiltonian Path . . . 160
Problems . . . 163
Notes . . . 168

6 The Deep Question: P vs. NP **173**
6.1 What if P=NP? . . . 174
6.2 Upper Bounds are Easy, Lower Bounds Are Hard . . . 181
6.3 Diagonalization and the Time Hierarchy . . . 184
6.4 Possible Worlds . . . 187
6.5 Natural Proofs . . . 191
6.6 Problems in the Gap . . . 196
6.7 Nonconstructive Proofs . . . 199
6.8 The Road Ahead . . . 210
Problems . . . 211
Notes . . . 218

7 The Grand Unified Theory of Computation **223**
7.1 Babbage's Vision and Hilbert's Dream . . . 224
7.2 Universality and Undecidability . . . 230
7.3 Building Blocks: Recursive Functions . . . 240
7.4 Form is Function: the λ-Calculus . . . 249
7.5 Turing's Applied Philosophy . . . 258
7.6 Computation Everywhere . . . 264
Problems . . . 284
Notes . . . 290

8 Memory, Paths, and Games **301**
8.1 Welcome to the State Space . . . 302
8.2 Show Me The Way . . . 306
8.3 L and NL-Completeness . . . 310

8.4 Middle-First Search and Nondeterministic Space . . . 314
8.5 You Can't Get There From Here . . . 317
8.6 PSPACE, Games, and Quantified SAT . . . 319
8.7 Games People Play . . . 328
8.8 Symmetric Space . . . 339
Problems . . . 341
Notes . . . 347

9 Optimization and Approximation **351**
9.1 Three Flavors of Optimization . . . 352
9.2 Approximations . . . 355
9.3 Inapproximability . . . 364
9.4 Jewels and Facets: Linear Programming . . . 370
9.5 Through the Looking-Glass: Duality . . . 382
9.6 Solving by Balloon: Interior Point Methods . . . 387
9.7 Hunting with Eggshells . . . 392
9.8 Algorithmic Cubism . . . 402
9.9 Trees, Tours, and Polytopes . . . 409
9.10 Solving Hard Problems in Practice . . . 414
Problems . . . 427
Notes . . . 442

10 Randomized Algorithms **451**
10.1 Foiling the Adversary . . . 452
10.2 The Smallest Cut . . . 454
10.3 The Satisfied Drunkard: WalkSAT . . . 457
10.4 Solving in Heaven, Projecting to Earth . . . 460
10.5 Games Against the Adversary . . . 465
10.6 Fingerprints, Hash Functions, and Uniqueness . . . 472
10.7 The Roots of Identity . . . 479
10.8 Primality . . . 482
10.9 Randomized Complexity Classes . . . 488
Problems . . . 491
Notes . . . 502

11 Interaction and Pseudorandomness **507**
11.1 The Tale of Arthur and Merlin . . . 508
11.2 The Fable of the Chess Master . . . 521
11.3 Probabilistically Checkable Proofs . . . 526
11.4 Pseudorandom Generators and Derandomization . . . 540
Problems . . . 553
Notes . . . 560

12 Random Walks and Rapid Mixing **563**
12.1 A Random Walk in Physics . . . 564
12.2 The Approach to Equilibrium . . . 568
12.3 Equilibrium Indicators . . . 573
12.4 Coupling . . . 576
12.5 Coloring a Graph, Randomly . . . 579
12.6 Burying Ancient History: Coupling from the Past . . . 586
12.7 The Spectral Gap . . . 602
12.8 Flows of Probability: Conductance . . . 606
12.9 Expanders . . . 612
12.10 Mixing in Time and Space . . . 623
Problems . . . 626
Notes . . . 643

13 Counting, Sampling, and Statistical Physics **651**
13.1 Spanning Trees and the Determinant . . . 653
13.2 Perfect Matchings and the Permanent . . . 658
13.3 The Complexity of Counting . . . 662
13.4 From Counting to Sampling, and Back . . . 668
13.5 Random Matchings and Approximating the Permanent . . . 674
13.6 Planar Graphs and Asymptotics on Lattices . . . 683
13.7 Solving the Ising Model . . . 693
Problems . . . 703
Notes . . . 718

14 When Formulas Freeze: Phase Transitions in Computation **723**
14.1 Experiments and Conjectures . . . 724
14.2 Random Graphs, Giant Components, and Cores . . . 730
14.3 Equations of Motion: Algorithmic Lower Bounds . . . 742
14.4 Magic Moments . . . 748
14.5 The Easiest Hard Problem . . . 759
14.6 Message Passing . . . 768
14.7 Survey Propagation and the Geometry of Solutions . . . 783
14.8 Frozen Variables and Hardness . . . 793
Problems . . . 796
Notes . . . 810

15 Quantum Computation **819**
15.1 Particles, Waves, and Amplitudes . . . 820
15.2 States and Operators . . . 823
15.3 Spooky Action at a Distance . . . 833
15.4 Algorithmic Interference . . . 841
15.5 Cryptography and Shor's Algorithm . . . 848
15.6 Graph Isomorphism and the Hidden Subgroup Problem . . . 862

15.7 Quantum Haystacks: Grover's Algorithm . . . 869
15.8 Quantum Walks and Scattering . . . 876
Problems . . . 888
Notes . . . 902

A Mathematical Tools **911**
A.1 The Story of O . . . 911
A.2 Approximations and Inequalities . . . 914
A.3 Chance and Necessity . . . 917
A.4 Dice and Drunkards . . . 923
A.5 Concentration Inequalities . . . 927
A.6 Asymptotic Integrals . . . 931
A.7 Groups, Rings, and Fields . . . 933
Problems . . . 939

References **945**

Index **974**