Contents

Preface ix

0 Prologue 1
0.1 Books and algorithms 1
0.2 Enter Fibonacci 2
0.3 Big-O notation 6
Exercises 8

1 Algorithms with numbers 11
1.1 Basic arithmetic 11
1.2 Modular arithmetic 16
1.3 Primality testing 23
1.4 Cryptography 30
1.5 Universal hashing 35
Exercises 38

Randomized algorithms: a virtual chapter 29

2 Divide-and-conquer algorithms 45
2.1 Multiplication 45
2.2 Recurrence relations 49
2.3 Mergesort 50
2.4 Medians 53
2.5 Matrix multiplication 56
2.6 The fast Fourier transform 58
Exercises 70

3 Decompositions of graphs 80
3.1 Why graphs? 80
3.2 Depth-first search in undirected graphs 83
3.3 Depth-first search in directed graphs 87
3.4 Strongly connected components 91
Exercises 95

4 Paths in graphs 104
4.1 Distances 104
4.2 Breadth-first search 105

4.3 Lengths on edges 107
4.4 Dijkstra's algorithm 108
4.5 Priority queue implementations 113
4.6 Shortest paths in the presence of negative edges 115
4.7 Shortest paths in dags 119
Exercises 120

5 Greedy algorithms **127**
5.1 Minimum spanning trees 127
5.2 Huffman encoding 138
5.3 Horn formulas 144
5.4 Set cover 145
Exercises 148

6 Dynamic programming **156**
6.1 Shortest paths in dags, revisited 156
6.2 Longest increasing subsequences 157
6.3 Edit distance 159
6.4 Knapsack 164
6.5 Chain matrix multiplication 168
6.6 Shortest paths 171
6.7 Independent sets in trees 175
Exercises 177

7 Linear programming and reductions **188**
7.1 An introduction to linear programming 188
7.2 Flows in networks 198
7.3 Bipartite matching 205
7.4 Duality 206
7.5 Zero-sum games 209
7.6 The simplex algorithm 213
7.7 Postscript: circuit evaluation 221
Exercises 222

8 NP-complete problems **232**
8.1 Search problems 232
8.2 NP-complete problems 243
8.3 The reductions 247
Exercises 264

9 Coping with NP-completeness **271**
9.1 Intelligent exhaustive search 272
9.2 Approximation algorithms 276
9.3 Local search heuristics 285
Exercises 293

10 Quantum algorithms 297
10.1 Qubits, superposition, and measurement 297
10.2 The plan 301
10.3 The quantum Fourier transform 303
10.4 Periodicity 305
10.5 Quantum circuits 307
10.6 Factoring as periodicity 310
10.7 The quantum algorithm for factoring 311
Exercises 314

Historical notes and further reading 317

Index 319