
Contents

1	Introduction	1
1.1	What Is Computer Science?	1
1.2	A Fascinating Theory	5
1.3	To the Student	8
1.4	Structure of the Book	11
2	Alphabets, Words, Languages, and Algorithmic Problems .	15
2.1	Objectives	15
2.2	Alphabets, Words, and Languages	16
2.3	Algorithmic Problems	27
2.4	Kolmogorov Complexity	37
2.5	Summary and Outlook	51
3	Finite Automata	55
3.1	Objectives	55
3.2	Different Representations of Finite Automata	55
3.3	Simulations	67
3.4	Proofs of Nonexistence	69
3.5	Nondeterminism	78
3.6	Summary	90
4	Turing Machines	93
4.1	Objectives	93
4.2	The Turing Machine Model	94
4.3	Multitape Turing Machines and the Church–Turing Thesis	104
4.4	Nondeterministic Turing Machines	115
4.5	Coding of Turing Machines	120
4.6	Summary	123

5	Computability	127
5.1	Objectives	127
5.2	The Diagonalization Method	128
5.3	The Reduction Method	138
5.4	Rice's Theorem	150
5.5	Post Correspondence Problem	154
5.6	The Kolmogorov-Complexity Method	163
5.7	Summary	166
6	Complexity Theory	169
6.1	Objectives	169
6.2	Complexity Measures	171
6.3	Complexity Classes and the Class P	178
6.4	Nondeterministic Complexity Measures	187
6.5	The Class NP and Proof Verification	194
6.6	NP-Completeness	199
6.7	Summary	221
7	Algorithmics for Hard Problems	223
7.1	Objectives	223
7.2	Pseudopolynomial Algorithms	225
7.3	Approximation Algorithms	231
7.4	Local Search	238
7.5	Simulated Annealing	245
7.6	Summary	249
8	Randomization	251
8.1	Objectives	251
8.2	Elementary Probability Theory	253
8.3	A Randomized Communication Protocol	256
8.4	Abundance of Witnesses and Randomized Primality Testing ..	261
8.5	Fingerprinting and Equivalence of Two Polynomials	267
8.6	Summary	272
9	Communication and Cryptography	275
9.1	Objectives	275
9.2	Classical Cryptosystems	276
9.3	Public-Key Cryptosystems and RSA	278
9.4	Digital Signatures	284
9.5	Interactive Proof Systems and Zero-Knowledge Proofs	287
9.6	Design of an Interconnection Network	292
9.7	Summary	302
	References	305
	Index	309