

Contents

PART I: ALGORITHMS	1
1 Problems and Algorithms	3
1.1 Graph reachability	3
1.2 Maximum flow and matching	8
1.3 The traveling salesman problem	13
1.4 Notes, references, and problems	14
2 Turing machines	19
2.1 Turing machine basics	19
2.2 Turing machines as algorithms	24
2.3 Turing machines with multiple strings	26
2.4 Linear speedup	32
2.5 Space bounds	34
2.6 Random access machines	36
2.7 Nondeterministic machines	45
2.8 Notes, references, and problems	51
3 Computability	57
3.1 Universal Turing machines	57
3.2 The halting problem	58
3.3 More undecidability	60
3.4 Notes, references, and problems	66

PART II: LOGIC	71
4 Boolean logic	73
4.1 Boolean Expressions	
4.2 Satisfiability and validity	76
4.3 Boolean functions and circuits	79
4.4 Notes, references, and problems	84
5 First-order logic	87
5.1 The syntax of first-order logic	87
5.2 Models	90
5.3 Valid expressions	95
5.4 Axioms and proofs	100
5.5 The completeness theorem	105
5.6 Consequences of the completeness theorem	110
5.7 Second-order logic	113
5.8 Notes, references, and problems	118
6 Undecidability in logic	123
6.1 Axioms for number theory	123
6.2 Complexity as a number-theoretic concept	127
6.3 Undecidability and incompleteness	131
6.4 Notes, references, and problems	135
PART III: P AND NP	137
7 Relations between complexity classes	139
7.1 Complexity classes	139
7.2 The hierarchy theorem	143
7.3 The reachability method	146
7.4 Notes, references, and problems	154
8 Reductions and completeness	159
8.1 Reductions	159
8.2 Completeness	165

8.3	Logical characterizations	172	
8.4	Notes, references, and problems	177	
9	NP-complete problems		181
9.1	Problems in NP	181	
9.2	Variants of satisfiability	183	
9.3	Graph-theoretic problems	188	
9.4	Sets and numbers	199	
9.5	Notes, references, and problems	207	
10	coNP and function problems		219
10.1	NP and coNP	219	
10.2	Primality	222	
10.3	Function problems	227	
10.4	Notes, references, and problems	235	
11	Randomized computation		241
11.1	Randomized algorithms	241	
11.2	Randomized complexity classes	253	
11.3	Random sources	259	
11.4	Circuit complexity	267	
11.5	Notes, references, and problems	272	
12	Cryptography		279
12.1	One-way functions	279	
12.2	Protocols	287	
12.3	Notes, references, and problems	294	
13	Approximability		299
13.1	Approximation algorithms	299	
13.2	Approximation and complexity	309	
13.3	Nonapproximability	319	
13.4	Notes, references, and problems	323	

14	On P vs. NP	329
14.1	The map of NP	329
14.2	Isomorphism and density	332
14.3	Oracles	339
14.4	Monotone circuits	343
14.5	Notes, references, and problems	350
PART IV: INSIDE P		357
15	Parallel computation	359
15.1	Parallel algorithms	359
15.2	Parallel models of computation	369
15.3	The class NC	375
15.4	RNC algorithms	381
15.5	Notes, references, and problems	385
16	Logarithmic space	395
16.1	The $L \stackrel{?}{=} NL$ problem	395
16.2	Alternation	399
16.3	Undirected reachability	401
16.4	Notes, references, and problems	405
PART V: BEYOND NP		409
17	The polynomial hierarchy	411
17.1	Optimization problems	411
17.2	The hierarchy	424
17.3	Notes, references, and problems	433
18	Computation that counts	439
18.1	The permanent	439
18.2	The class $\oplus P$	447
18.3	Notes, references, and problems	452

19	Polynomial space	455
19.1	Alternation and games	455
19.2	Games against nature and interactive protocols	469
19.3	More PSPACE -complete problems	480
19.4	Notes, references, and problems	487
20	A glimpse beyond	491
20.1	Exponential time	491
20.2	Notes, references, and problems	499
	Index	509
	Author index	519