

Contents

Introduction	1
Some notation and definitions	2
1 Models of Computation	5
1.1 Finite automata	7
1.2 The Turing machine	10
1.3 The Random Access Machine	21
1.4 Boolean functions and Boolean circuits	27
2 Algorithmic decidability	37
2.1 Recursive and recursively enumerable languages	38
2.2 Other undecidable problems	43
2.3 Computability in logic	49
2.3.1 Gödel's incompleteness theorem	49
2.3.2 First-order logic	52
3 Computation with resource bounds	59
3.1 Polynomial time	62
3.2 Other complexity classes	74
3.3 General theorems on space and time complexity	77
4 Non-deterministic algorithms	87
4.1 Non-deterministic Turing machines	88
4.2 Witnesses and the complexity of non-deterministic algorithms	90
4.3 Examples of languages in NP	95
4.4 NP-completeness	103
4.5 Further NP-complete problems	109
5 Randomized algorithms	119
5.1 Verifying a polynomial identity	119
5.2 Primality testing	123

5.3	Randomized complexity classes	128
6	Information complexity	133
6.1	Information complexity	134
6.2	Self-delimiting information complexity	139
6.3	The notion of a random sequence	143
6.4	Kolmogorov complexity, entropy and coding	145
7	Pseudorandom numbers	153
7.1	Classical methods	154
7.2	The notion of a pseudorandom number generator	156
7.3	One-way functions	160
7.4	Candidates for one-way functions	164
7.4.1	Discrete square roots	164
8	Decision trees	167
8.1	Algorithms using decision trees	168
8.2	Non-deterministic decision trees	173
8.3	Lower bounds on the depth of decision trees	176
9	Algebraic computations	183
9.1	Models of algebraic computation	183
9.2	Multiplication	185
9.2.1	Arithmetic operations on large numbers	185
9.2.2	Matrix multiplication	187
9.2.3	Inverting matrices	189
9.2.4	Multiplication of polynomials	190
9.2.5	Discrete Fourier transform	192
9.3	Algebraic complexity theory	194
9.3.1	The complexity of computing square-sums	194
9.3.2	Evaluation of polynomials	195
9.3.3	Formula complexity and circuit complexity	198
10	Parallel algorithms	201
10.1	Parallel random access machines	201
10.2	The class NC	206
11	Communication complexity	211
11.1	Communication matrix and protocol-tree	212
11.2	Examples	217
11.3	Non-deterministic communication complexity	219
11.4	Randomized protocols	223

12 An application of complexity: cryptography	225
12.1 A classical problem	225
12.2 A simple complexity-theoretic model	226
12.3 Public-key cryptography	227
12.4 The Rivest–Shamir–Adleman code (RSA code)	229
13 Circuit complexity	233
13.1 Lower bound for the Majority Function	234
13.2 Monotone circuits	237
14 Interactive proofs	239
14.1 How to save the last move in chess?	239
14.2 How to check a password – without knowing it?	241
14.3 How to use your password – without telling it?	241
14.4 How to prove non-existence?	243
14.5 How to verify proofs that keep the main result secret?	246
14.6 How to referee exponentially long papers?	246
14.7 Approximability	248