CONTENTS

Preface to the First Edition x
To the student x
To the educator xi
The first edition xii
Feedback to the author xii
Acknowledgments xiii

Preface to the Second Edition (International) xv

0 Introduction 1
0.1 Automata, Computability, and Complexity 1
Complexity theory 2
Computability theory 2
Automata theory 3
0.2 Mathematical Notions and Terminology 3
Sets 3
Sequences and tuples 6
Functions and relations 7
Graphs 10
Strings and languages 13
Boolean logic 14
Summary of mathematical terms 16
0.3 Definitions, Theorems, and Proofs 17
Finding proofs 17

0.4 Types of Proof 21
Proof by construction 21
Proof by contradiction 21
Proof by induction 22
Exercises, Problems, and Solutions 25

Part One: Automata and Languages 29

1 Regular Languages **31**
1.1 Finite Automata 31
Formal definition of a finite automaton 35
Examples of finite automata 37
Formal definition of computation 40
Designing finite automata 41
The regular operations 44
1.2 Nondeterminism 47
Formal definition of a nondeterministic finite automaton 53
Equivalence of NFAs and DFAs 54
Closure under the regular operations 58
1.3 Regular Expressions 63
Formal definition of a regular expression 64
Equivalence with finite automata 66
1.4 Nonregular Languages 77
The pumping lemma for regular languages 77
Exercises, Problems, and Solutions 82

2 Context-Free Languages **101**
2.1 Context-free Grammars 102
Formal definition of a context-free grammar 104
Examples of context-free grammars 105
Designing context-free grammars 106
Ambiguity 107
Chomsky normal form 108
2.2 Pushdown Automata 111
Formal definition of a pushdown automaton 113
Examples of pushdown automata 114
Equivalence with context-free grammars 117
2.3 Non-context-free Languages 125
The pumping lemma for context-free languages 125
Exercises, Problems, and Solutions 130

Part Two: Computability Theory

3 The Church–Turing Thesis 139
3.1 Turing Machines 139
Formal definition of a Turing machine 141
Examples of Turing machines 144
3.2 Variants of Turing Machines 150
Multitape Turing machines 150
Nondeterministic Turing machines 152
Enumerators 154
Equivalence with other models 155
3.3 The Definition of Algorithm 156
Hilbert's problems 156
Terminology for describing Turing machines 158
Exercises, Problems, and Solutions 161

4 Decidability 167
4.1 Decidable Languages 168
Decidable problems concerning regular languages 168
Decidable problems concerning context-free languages 172
4.2 The Halting Problem 175
The diagonalization method 176
The halting problem is undecidable 181
A Turing-unrecognizable language 183
Exercises, Problems, and Solutions 184

5 Reducibility 191
5.1 Undecidable Problems from Language Theory 192
Reductions via computation histories 196
5.2 A Simple Undecidable Problem 203
5.3 Mapping Reducibility 210
Computable functions 210
Formal definition of mapping reducibility 211
Exercises, Problems, and Solutions 215

6 Advanced Topics in Computability Theory 221
6.1 The Recursion Theorem 221
Self-reference 222
Terminology for the recursion theorem 225
Applications 226

6.2 Decidability of logical theories 228
A decidable theory 231
An undecidable theory 233
6.3 Turing Reducibility 236
6.4 A Definition of Information 237
Minimal length descriptions 238
Optimality of the definition 242
Incompressible strings and randomness 243
Exercises, Problems, and Solutions 246

Part Three: Complexity Theory 249

7 Time Complexity 251
7.1 Measuring Complexity 251
Big-O and small-o notation 252
Analyzing algorithms 255
Complexity relationships among models 258
7.2 The Class P 260
Polynomial time 260
Examples of problems in P 262
7.3 The Class NP 268
Examples of problems in NP 271
The P versus NP question 273
7.4 NP-completeness 275
Polynomial time reducibility 276
Definition of NP-completeness 280
The Cook–Levin Theorem 280
7.5 Additional NP-complete Problems 287
The vertex cover problem 288
The Hamiltonian path problem 290
The subset sum problem 295
Exercises, Problems, and Solutions 298

8 Space Complexity 307
8.1 Savitch's Theorem 309
8.2 The Class PSPACE 312
8.3 PSPACE-completeness 313
The TQBF problem 314
Winning strategies for games 317
Generalized geography 319

8.4 The Classes L and NL . . . 324
8.5 NL-completeness . . . 327
Searching in graphs . . . 329
8.6 NL equals coNL . . . 330
Exercises, Problems, and Solutions . . . 332

9 Intractability **339**
9.1 Hierarchy Theorems . . . 340
Exponential space completeness . . . 347
9.2 Relativization . . . 352
Limits of the diagonalization method . . . 353
9.3 Circuit Complexity . . . 355
Exercises, Problems, and Solutions . . . 364

10 Advanced topics in complexity theory **371**
10.1 Approximation Algorithms . . . 371
10.2 Probabilistic Algorithms . . . 374
The class BPP . . . 374
Primality . . . 377
Read-once branching programs . . . 382
10.3 Alternation . . . 386
Alternating time and space . . . 387
The Polynomial time hierarchy . . . 392
10.4 Interactive Proof Systems . . . 393
Graph nonisomorphism . . . 393
Definition of the model . . . 394
IP = PSPACE . . . 396
10.5 Parallel Computation . . . 405
Uniform Boolean circuits . . . 406
The class NC . . . 408
P-completeness . . . 410
10.6 Cryptography . . . 411
Secret keys . . . 411
Public-key cryptosystems . . . 413
One-way functions . . . 413
Trapdoor functions . . . 415
Exercises, Problems, and Solutions . . . 417

Selected Bibliography **421**

Index **427**