## CONTENTS

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

Preface to the Second Edition xvii

Preface to the Third Edition xx

0 Introduction 1
  0.1 Automata, Computability, and Complexity .......... 1
    Complexity theory .................................... 2
    Computability theory .................................. 3
    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

1 Regular Languages
   1.1 Finite Automata
      Formal definition of a finite automaton
      Examples of finite automata
      Formal definition of computation
      Designing finite automata
      The regular operations
   1.2 Nondeterminism
      Formal definition of a nondeterministic finite automaton
      Equivalence of NFAs and DFAs
      Closure under the regular operations
   1.3 Regular Expressions
      Formal definition of a regular expression
      Equivalence with finite automata
   1.4 Nonregular Languages
      The pumping lemma for regular languages

Exercises, Problems, and Solutions

2 Context-Free Languages
   2.1 Context-Free Grammars
      Formal definition of a context-free grammar
      Examples of context-free grammars
      Designing context-free grammars
      Ambiguity
      Chomsky normal form
   2.2 Pushdown Automata
      Formal definition of a pushdown automaton
      Examples of pushdown automata
      Equivalence with context-free grammars
   2.3 Non-Context-Free Languages
      The pumping lemma for context-free languages
   2.4 Deterministic Context-Free Languages
      Properties of DCFLs
      Deterministic context-free grammars
      Relationship of DPDAs and DCFGs
      Parsing and LR(k) Grammars

Exercises, Problems, and Solutions

Part Two: Computability Theory

3 The Church-Turing Thesis
   3.1 Turing Machines
      Formal definition of a Turing machine
# CONTENTS

Examples of Turing machines ........................................ 170

3.2 Variants of Turing Machines ..................................... 176
   Multitape Turing machines ...................................... 176
   Nondeterministic Turing machines .............................. 178
   Enumerators .................................................... 180
   Equivalence with other models ................................. 181

3.3 The Definition of Algorithm ...................................... 182
   Hilbert's problems ............................................. 182
   Terminology for describing Turing machines ................. 184

Exercises, Problems, and Solutions ............................... 187

4 Decidability .......................................................... 193
4.1 Decidable Languages ............................................... 194
   Decidable problems concerning regular languages ........ 194
   Decidable problems concerning context-free languages ... 198

4.2 Undecidability ..................................................... 201
   The diagonalization method .................................. 202
   An undecidable language ...................................... 207
   A Turing-unrecognizable language ............................ 209

Exercises, Problems, and Solutions ............................... 210

5 Reducibility .......................................................... 215
5.1 Undecidable Problems from Language Theory ............... 216
   Reductions via computation histories ......................... 220
5.2 A Simple Undecidable Problem .................................. 227
5.3 Mapping Reducibility ............................................. 234
   Computable functions ......................................... 234
   Formal definition of mapping reducibility ................... 235

Exercises, Problems, and Solutions ............................... 239

6 Advanced Topics in Computability Theory ....................... 245
6.1 The Recursion Theorem ........................................... 245
   Self-reference .................................................. 246
   Terminology for the recursion theorem ...................... 249
   Applications .................................................. 250
6.2 Decidability of logical theories ................................. 252
   A decidable theory ............................................ 255
   An undecidable theory ........................................ 257
6.3 Turing Reducibility ............................................... 260
6.4 A Definition of Information ..................................... 261
   Minimal length descriptions .................................. 262
   Optimality of the definition .................................. 266
   Incompressible strings and randomness ....................... 267

Exercises, Problems, and Solutions ............................... 270
Part Three: Complexity Theory

7 Time Complexity

7.1 Measuring Complexity
- Big-O and small-o notation
- Analyzing algorithms
- Complexity relationships among models

7.2 The Class P
- Polynomial time
- Examples of problems in P

7.3 The Class NP
- Examples of problems in NP
- The P versus NP question

7.4 NP-completeness
- Polynomial time reducibility
- Definition of NP-completeness
- The Cook–Levin Theorem

7.5 Additional NP-complete Problems
- The vertex cover problem
- The Hamiltonian path problem
- The subset sum problem

Exercises, Problems, and Solutions

8 Space Complexity

8.1 Savitch’s Theorem
8.2 The Class PSPACE
8.3 PSPACE-completeness
- The TQBF problem
- Winning strategies for games
- Generalized geography

8.4 The Classes L and NL
8.5 NL-completeness
- Searching in graphs

8.6 NL equals coNL
Exercises, Problems, and Solutions

9 Intractability

9.1 Hierarchy Theorems
- Exponential space completeness

9.2 Relativization
- Limits of the diagonalization method

9.3 Circuit Complexity
Exercises, Problems, and Solutions

10 Advanced Topics in Complexity Theory

10.1 Approximation Algorithms
10.2 Probabilistic Algorithms ........................................... 396
    The class BPP ................................................. 396
    Primality ....................................................... 399
    Read-once branching programs ............................... 404
10.3 Alternation ...................................................... 408
    Alternating time and space .................................. 410
    The Polynomial time hierarchy ............................... 414
10.4 Interactive Proof Systems ...................................... 415
    Graph nonisomorphism ....................................... 415
    Definition of the model ..................................... 416
    IP = PSPACE .................................................. 418
10.5 Parallel Computation ............................................ 427
    Uniform Boolean circuits .................................... 428
    The class NC .................................................. 430
    P-completeness ............................................... 432
10.6 Cryptography ................................................... 433
    Secret keys .................................................... 433
    Public-key cryptosystems .................................... 435
    One-way functions .......................................... 435
    Trapdoor functions .......................................... 437
Exercises, Problems, and Solutions ......................... 439

Selected Bibliography ............................................ 443

Index ............................................................. 448