

---

## Contents

<b>1</b>	<b>Introduction</b> . . . . .	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
<b>2</b>	<b>Alphabets, Words, Languages, and Algorithmic Problems</b> .	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
<b>3</b>	<b>Finite Automata</b> . . . . .	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
<b>4</b>	<b>Turing Machines</b> . . . . .	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

<b>5</b>	<b>Computability</b> .....	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
<b>6</b>	<b>Complexity Theory</b> .....	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
<b>7</b>	<b>Algorithmics for Hard Problems</b> .....	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
<b>8</b>	<b>Randomization</b> .....	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
<b>9</b>	<b>Communication and Cryptography</b> .....	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
	<b>References</b> .....	305
	<b>Index</b> .....	309

Theoretical Computer Science

Introduction to Automata, Computability, Complexity,

Algorithmics, Randomization, Communication, and

Cryptography

Hromkovič, J.

2011, X, 313 p., Hardcover

ISBN: 978-3-540-14015-3