

Computation and Automata

Arto Salomaa

University of Turku
Finland



*The title of this
University of Cambridge
is given and not
all names of books
are printed by
Henry VIII in 1534.
The University has printed
and published continuously
since 1584.*

CAMBRIDGE UNIVERSITY PRESS

Cambridge

New York Port Chester

Melbourne Sydney

Contents

Editor's Statement	<i>page ix</i>
Foreword by G. Rozenberg	xi
Acknowledgments	xiii
Chapter 1 Introduction: Models of Computation	1
Chapter 2 Rudiments of Language Theory	5
2.1 Languages and Rewriting Systems	5
2.2 Grammars	14
2.3 Post Systems	24
2.4 Markov Algorithms	31
2.5 <i>L</i> Systems	35
Exercises	41
Chapter 3 Restricted Automata	44
3.1 Finite Automata	44
3.2 Kleene Characterization	48
3.3 Generalized Sequential Machines	55

3.4	Pumping Lemmas	62
3.5	Pushdown Automata	66
	Exercises	73
Chapter 4	Turing Machines and Recursive Functions	76
4.1	A General Model of Computation	76
4.2	Programming in Machine Language, Church's Thesis, and Universal Machines	83
4.3	Recursion Theorem and Basic Undecidability Results	86
4.4	Recursive and Recursively Enumerable Sets and Languages	93
4.5	Reducibilities and Creative Sets	101
4.6	Universality in Terms of Composition	111
	Exercises	114
Chapter 5	Famous Decision Problems	116
5.1	Post Correspondence Problem and Applications	116
5.2	Hilbert's Tenth Problem and Consequences: Most Questions Can Be Expressed in Terms of Polynomials	124
5.3	Word Problems and Vector Addition Systems	131
	Exercises	136
Chapter 6	Computational Complexity	139
6.1	Basic Ideas and Axiomatic Theory	139
6.2	Complexity Classes, Gap, and Compression Theorems	147
6.3	Speedup Theorem: Functions Without Best Algorithms	151
6.4	Time Bounds, the Classes \mathcal{P} and \mathcal{NP} , and \mathcal{NP} -complete Problems	160
6.5	Provably Intractable Problems	176
6.6	Space Measures and Trade-offs	180
	Exercises	184
Chapter 7	Cryptography	186
7.1	Background and Classical Cryptosystems	186
7.2	Public Key Cryptosystems	196
7.3	Knapsack Systems	206
7.4	RSA System	217
7.5	Protocols for Solving Seemingly Impossible Problems in Communication	222
	Exercises	229
Chapter 8	Trends in Automata and Language Theory	231
8.1	Petri Nets	231
8.2	Similar Grammars and Languages	240

Contents	vii
8.3 Systolic Automata	250
Exercises	262
Historical and Bibliographical Remarks	266
References	269
Index	279