

Handbook of Theoretical Computer Science

Volume A

ALGORITHMS AND COMPLEXITY

edited by

JAN VAN LEEUWEN,
Utrecht University, The Netherlands



1990

ELSEVIER
AMSTERDAM • NEW YORK • OXFORD • TOKYO



1990

THE MIT PRESS
CAMBRIDGE, MASSACHUSETTS

Contents

PREFACE	i
LIST OF CONTRIBUTORS TO VOLUME A	iii
CONTENTS	v
CHAPTER 1 MACHINE MODELS AND SIMULATIONS	1
<i>P. van Emde Boas</i>	
1. Introduction	3
2. Sequential machine models	16
3. The second machine class	38
4. Parallel machine models outside the second machine class	54
Acknowledgment	60
References	61
CHAPTER 2 A CATALOG OF COMPLEXITY CLASSES	67
<i>D.S. Johnson</i>	
1. Preliminaries	69
2. Presumably intractable problems	83
3. Provably intractable problems	101
4. Classes that count	106
5. Inside P	125
6. New developments: tables and figures	143
References	152
CHAPTER 3 MACHINE-INDEPENDENT COMPLEXITY THEORY	163
<i>J.I. Seiferas</i>	
1. Introduction	165
2. Simple Turing machines and space complexity	165
3. Recursion, padding and compression	167
4. Gaps and arbitrary speed-up	171
5. Effective speed-up	175
6. Fundamental Theorem for STM space	177
7. Machine independence	178
Acknowledgment	185
References	185
CHAPTER 4 KOLMOGOROV COMPLEXITY AND ITS APPLICATIONS	187
<i>M. Li and P.M.B. Vitányi</i>	
1. Introduction	189
2. Mathematical theory	196
3. Applications of compressibility	214

4. Example of an application in mathematics: weak prime number theorems	221
5. Application of incompressibility: proving lower bounds	222
6. Resource-bounded Kolmogorov complexity and its applications	236
7. Conclusion	247
Acknowledgment	247
References	248
CHAPTER 5 ALGORITHMS FOR FINDING PATTERNS IN STRINGS	255
<i>A.V. Aho</i>	
1. Introduction	257
2. Notations for patterns	258
3. Matching keywords	262
4. Matching sets of keywords	273
5. Matching regular expressions	282
6. Related problems	288
7. Concluding remarks	295
Acknowledgment	295
References	295
CHAPTER 6 DATA STRUCTURES	301
<i>K. Mehlhorn and A. Tsakalidis</i>	
1. Introduction	303
2. The dictionary problem	305
3. The weighted dictionary problem and self-organizing data structures	319
4. Persistence	323
5. The <i>Union-Split-Find</i> problem	324
6. Priority queues	326
7. Nearest common ancestors	328
8. Selection	329
9. Merging	331
10. Dynamization techniques	332
References	334
CHAPTER 7 COMPUTATIONAL GEOMETRY	343
<i>F.F. Yao</i>	
1. Introduction	345
2. Techniques and paradigms	345
3. Convex hulls	348
4. Voronoi diagrams	352
5. Proximity problems	356
6. Linear programming	360
7. Triangulation and decomposition	364
8. Planar point location	366

9. Multidimensional trees	368
10. Range search	370
11. Visibility computations	374
12. Combinatorial geometry	376
13. Other topics	378
14. Conclusion	380
References	380
CHAPTER 8 ALGORITHMIC MOTION PLANNING IN ROBOTICS	391
<i>J.T. Schwartz and M. Sharir</i>	
1. Introduction	393
2. Statement of the problem	394
3. Motion planning in static and known environments	397
4. Variants of the motion planning problem	415
5. Results in computational geometry relevant to motion planning	421
Acknowledgment	425
References	425
CHAPTER 9 AVERAGE-CASE ANALYSIS OF ALGORITHMS AND DATA STRUCTURES	431
<i>J.S. Vitter and Ph. Flajolet</i>	
0. Introduction	433
1. Combinatorial enumerations	436
2. Asymptotic methods	445
3. Sorting algorithms	458
4. Recursive decompositions and algorithms on trees	473
5. Hashing and address computation techniques	492
6. Dynamic algorithms	511
Acknowledgment	520
References	520
CHAPTER 10 GRAPH ALGORITHMS	525
<i>J. van Leeuwen</i>	
Prelude	527
1. Representation of graphs	527
2. Basic structure algorithms	551
3. Combinatorial optimization on graphs	579
References	612
CHAPTER 11 ALGEBRAIC COMPLEXITY THEORY	633
<i>V. Strassen</i>	
1. Introduction	635
2. Addition chains	637
3. Computation sequences	637
4. Substitution	638
5. Degree of transcendency	640
6. Geometric degree	641
7. Derivatives	644

8. Branching	645
9. Complexity classes	648
10. Matrix multiplication and bilinear complexity	650
11. Degeneration and asymptotic spectrum	653
12. Lower bounds for rank and border rank	656
13. Fourier transform	660
14. Complete problems	661
15. Conclusion	664
References	664
CHAPTER 12 ALGORITHMS IN NUMBER THEORY	673
<i>A.K. Lenstra and H.W. Lenstra, Jr</i>	
1. Introduction	675
2. Preliminaries	677
3. Algorithms for finite abelian groups	685
4. Factoring integers	697
5. Primality testing	706
Acknowledgment	712
References	712
CHAPTER 13 CRYPTOGRAPHY	717
<i>R.L. Rivest</i>	
1. Introduction	719
2. Basics	719
3. The goals and tools of cryptology	722
4. Mathematical preliminaries	723
5. Complexity-theoretic foundations of cryptography	725
6. Privacy	728
7. Generating random or pseudo-random sequences and functions	735
8. Digital signatures	739
9. Two-party protocols	742
10. Multi-party protocols	746
11. Cryptography and complexity theory	748
Acknowledgment	749
References	750
CHAPTER 14 THE COMPLEXITY OF FINITE FUNCTIONS	757
<i>R.B. Boppana and M. Sipser</i>	
1. Introduction	759
2. General circuits	760
3. Bounded-depth circuits	765
4. Monotone circuits	780
5. Formulas	786
6. Branching programs	796
7. Conclusion	799
Acknowledgment	800
References	800

CHAPTER 15 COMMUNICATION NETWORKS	805
<i>N. Pippenger</i>	
1. Introduction	807
2. Communication problems	809
3. The Ajtai, Komlós and Szemerédi Theorem	820
Acknowledgment	831
References	831
CHAPTER 16 VLSI THEORY	835
<i>Th. Lengauer</i>	
1. Introduction	837
2. VLSI complexity measures	839
3. The VLSI model	842
4. The basic lower bound argument	844
5. A geometric separator theorem	845
6. The communication complexity of Boolean predicates	846
7. The communication complexity of Boolean functions with many outputs	853
8. A lower bound on the switching energy of VLSI chips	857
9. Upper bounds on the AT^2 -complexity of VLSI chips	862
Acknowledgment	865
References	865
CHAPTER 17 PARALLEL ALGORITHMS FOR SHARED-MEMORY MACHINES	869
<i>R.M. Karp and V. Ramachandran</i>	
1. Introduction	871
2. Efficient PRAM algorithms	873
3. Models of parallel computation	894
4. NC-algorithms and P-complete problems	906
5. Conclusion	931
Acknowledgment	932
References	932
CHAPTER 18 GENERAL PURPOSE PARALLEL ARCHITECTURES	943
<i>L.G. Valiant</i>	
1. Introduction	945
2. Some networks	946
3. Routing	950
4. Universality	959
Acknowledgment	968
References	969
SUBJECT INDEX	973