ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS
Volume 25

Computation and Automata
ENCYCLOPEDIA OF MATHEMATICS
and Its Applications

GIAN-CARLO ROTA, Editor
Massachusetts Institute of Technology

Editorial Board

Janos D. Aczel, Waterloo
George E. Andrews, Penn State
Richard Askey, Madison
Michael F. Atiyah, Oxford
Donald Babbitt, U.C.L.A.
Lipman Bers, Columbia
Garrett Birkhoff, Harvard
Raoul Bott, Harvard
James K. Brooks, Gainesville
Felix E. Browder, Chicago
A. P. Calderon, Buenos Aires
Peter A. Carruthers, Los Alamos
S. Chandrasekhar, Chicago
S. S. Chern, Berkeley
Hermann Chernoff, M.I.T.

P. M. Cohn, Bedford College, London
H. S. MacDonald Coxeter, Toronto
George B. Danzig, Stanford
Nelson Dunford, Sarasota, Florida
F. J. Dyson, Inst. for Advanced Study
Harold M. Edwards, Courant
Harvey Friedman, Ohio State
Giovanni Gallavotti, Rome
Andrew M. Gleason, Harvard
James Gilpin, Courant
M. Gordon, Essex
Elias P. Glynopoulos, M.I.T.
Peter Henrici, ETH, Zurich
Nathan Jacobson, Yale
Mark Kac, U.S.C.
Shizuo Kakutani, Yale
Samuel Karlin, Stanford
J. F. C. Kingman, Oxford

Donald E. Knuth, Stanford
Joshua Lederberg, Rockefeller
André Lichnerowicz, College de France
M. J. Lighthill, London
Chia-Chiao Lin, M.I.T.
Jacques-Louis Lions, Paris
G. G. Lorentz, Austin
Roger Lyndon, Ann Arbor
Robert J. McEliece, Caltech
Henry McKean, Courant
Marvin Marcus, Santa Barbara
N. Metropolis, Los Alamos
Frederick Mosteller, Harvard
Jan Mycielski, Boulder
L. Nachbin, Rio de Janeiro and Rochester
Steven A. Orszag, M.I.T.
Alexander Ostrowski, Basel
Roger Penrose, Oxford
Carlo Pucci, Florence
Fred S. Roberts, Rutgers
Abdus Salam, Trieste
M. P. Schützenberger, Paris
Jacob T. Schwartz, Courant
Irving Segal, M.I.T.

Oved Shisha, Univ. of Rhode Island
I. M. Singer, Berkeley
Olga Taussky, Caltech
Rene Thom, Bures-sur-Yvette
John Todd, Caltech
John W. Tukey, Princeton
Veeravalli S. Varadarajan, U.C.L.A.
Antoni Zygmund, Chicago

For other books in this series see page 283
Computation and Automata

Arto Salomaa
University of Turku
Finland
Contents

Editor’s Statement  page ix

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 L 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
### Contents

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

8.3 Systolic Automata  250
Exercises  262

Historical and Bibliographical Remarks  266

References  269

Index  279
Editor’s Statement

A large body of mathematics consists of facts that can be presented and described much like any other natural phenomenon. These facts, at times explicitly brought out as theorems, at other times concealed within a proof, make up most of the applications of mathematics, and are the most likely to survive change of style and of interest.

This ENCYCLOPEDIA will attempt to present the factual body of all mathematics. Clarity of exposition, accessibility to the non-specialist, and a thorough bibliography are required of each author. Volumes will appear in no particular order, but will be organized into sections, each one comprising a recognizable branch of present-day mathematics. Numbers of volumes and sections will be reconsidered as times and needs change.

It is hoped that this enterprise will make mathematics more widely used where it is needed, and more accessible in fields in which it can be applied but where it has not yet penetrated because of insufficient information.

Gian-Carlo Rota
Foreword

The last twenty years have witnessed most vigorous growth in areas of mathematical study connected with computers and computer science. The enormous development of computers and the resulting profound changes in scientific methodology have opened new horizons for the science of mathematics at a speed without parallel during the long history of mathematics.

The following two observations should be kept in mind when reading the present monograph. First, various developments in mathematics have directly initiated the “beginning” of computers and computer science. Second, advances in computer science have induced very vigorous developments in certain branches of mathematics. More specifically, the second of these observations refers to the growing importance of discrete mathematics—and we are now witnessing only the very beginning of the influence of discrete mathematics.

Because of reasons outlined above, mathematics plays a central role in the foundations of computer science. A number of significant research areas can be listed in this connection. It is interesting to notice that these areas also reflect the historical development of computer science.

1. The classical computability theory initiated by the work of Gödel, Tarski, Church, Post, Turing, and Kleene occupies a central role. This area is rooted in mathematical logic.

2. In the classical formal language and automata theory the central notions are those of an automaton, a grammar, and a language. Apart from
developments in area (1), the work of Chomsky on the foundations of natural languages, as well as the work of Post concerning rewriting systems, should be mentioned here. It is, however, fascinating to observe that the modern theory of formal languages and rewriting systems was initiated by the work of the Norwegian mathematician Axel Thue at the beginning of this century!

3. An area initiated in the sixties is complexity theory. The performance of an algorithm is investigated. The central notions are those of a tractable and an intractable problem. This area is gaining in importance because of several reasons, one of them being the advances in area (4).

4. Quite recent developments concerning the security of computer systems have increased the importance of cryptography to a great extent. Moreover, the idea of public key cryptography is of specific theoretical interest and has drastically changed our ideas concerning what is doable in communication systems.

Areas (1) through (4) constitute the core of the present monograph. Many other important areas dealing with the mathematical foundations of computer science (e.g., semantics and the theory of correctness of programming languages, the theory of data structures, and the theory of data bases) lie beyond the scope of the present monograph and will, hopefully, be presented in other books in this series.

All the areas listed above comprise a fascinating part of contemporary mathematics that is very dynamic in character, full of challenging problems requiring most interesting and ingenious mathematical techniques.

This monograph provides a very good basis for the understanding of these developments. It presents this fascinating modern area of mathematics in a broad and clear perspective. Because everything is developed essentially from the beginning, even an uninitiated reader can use the monograph as an entry to this area. In spite of this, a glimpse of a number of very recent developments is given.

Grzegorz Rozenberg
Acknowledgments

It is difficult to list all persons who have in some way or other contributed to this book. Parts of the manuscript were used as lecture notes for courses given at the universities of Turku and Waterloo. I want to thank the participants in these courses, in particular, Juha Honkala and Sheng Yu. Tero Harju, Juha Honkala, Werner Kuich, Valtteri Niemi, and Grzegorz Rozenberg have read through at least some parts of the manuscript and given very useful comments. Moreover, I have benefited from discussions with or comments from Karel Culik II, Jozef Gruska, Helmut Jürgensen, Juhani Karhumäki, Matti Linna, Hermann Maurer, Martti Penttonen, Keijo Ruohonen, Adi Shamir, Emo Welzl, and Derick Wood. The difficult task of typing the manuscript was performed in an excellent fashion by Elisa Mikkola. I want to thank the publisher for excellent and timely editorial work with both the typescript and proofs. Last but not least, I want to acknowledge the continuing support of my wife, children, and other members of the family. In particular, discussions with Ilokivi and Turzan were always very encouraging, and the whole book would not have been possible without Ketta and Korak.

Arto Salomaa