ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS
Volume 25

Computation and Automata

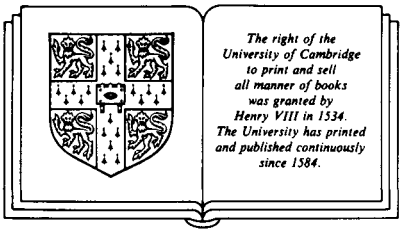
ENCYCLOPEDIA OF MATHEMATICS
and Its Applications

GIAN-CARLO ROTA, Editor
Massachusetts Institute of Technology

For other books in this series see page 283

Computation and Automata

Arto Salomaa
University of Turku
Finland



CAMBRIDGE UNIVERSITY PRESS
Cambridge
London New York New Rochelle
Melbourne Sydney

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, São Paulo, Delhi, Tokyo, Mexico City

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521177337

First published 1985
First paperback edition 2011

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data

Salomaa, Arto.

Computation and automata.

(Encyclopedia of mathematics and its applications; v. 25)

Bibliography: p.

Includes index.

1. Computable functions. 2. Computational complexity. 3. Sequential machine theory. I. Title.
II. Series.
QA9.59.S25 1985 511 84–17571

ISBN 978-0-521-30245-6 Hardback
ISBN 978-0-521-17733-7 Paperback

Contents

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