Research in computational group theory, an active subfield of computational algebra, has emphasized four areas: finite permutation groups, finite solvable groups, matrix representations of finite groups, and finitely presented groups. This book deals with the last of these areas. It is the first text to present the fundamental algorithmic ideas which have been developed to compute with finitely presented groups that are infinite, or at least not obviously finite. The book describes methods for working with elements, subgroups, and quotient groups of a finitely presented group. The author emphasizes the connection with fundamental algorithms from theoretical computer science, particularly the theory of automata and formal languages, from computational number theory, and from computational commutative algebra. The LLL lattice reduction algorithm and various algorithms for Hermite and Smith normal forms are used to study the abelian quotients of a finitely presented group. The work of Baumslag, Cannonito, and Miller on computing nonabelian polycyclic quotients is described as a generalization of Buchberger's Gröbner basis methods to right ideals in the integral group ring of a polycyclic group. Researchers in computational group theory, mathematicians interested in finitely presented groups, and theoretical computer scientists will find this book useful.

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

EDITED BY G.-C. ROTA

Volume 48

Computation with finitely presented groups

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

4 Willard Miller, Jr. *Symmetry and Separation of Variables*
5 David Ruelle *Thermodynamic Formalism: The Mathematical Structures of Classical Equilibrium Statistical Mechanics*
6 Henryk Minc *Permanents*
7 Fred S. Roberts *Measurement Theory with Applications to Decisionmaking, Utility, and the Social Sciences*
11 William B. Jones and W. J. Thron *Continued Fractions: Analytic Theory and Applications*
12 Nathaniel F. G. Martin and James W. England *Mathematical Theory of Entropy*
15 E. C. Beltrametti and G. Cassinelli *The Logic of Quantum Mechanics*
17 M. Lothaire *Combinatorics on Words*
18 H. O. Fattorini *The Cauchy Problem*
19 G. G. Lorentz, K. Getter, and S. D. Riemenschneider *Birkhoff Interpolation*
21 W. T. Tutte *Graph Theory*
22 Julio R. Bastida *Field Extensions and Galois Theory*
23 John Rozier Cannon *The One-Dimensional Heat Equation*
24 Stan Wagon *The Banach–Tarski Paradox*
25 Arto Salomaa *Computation and Automata*
26 Neil White (ed.) *Theory of Matroids*
27 N. H. Bingham, C. M. Goldie, and J. L. Teugels *Regular Variation*
28 P. P. Petrushev and V. A. Popov *Rational Approximation of Real Functions*
29 N. White (ed.) *Combinatorial Geometries*
30 M. Pohst and H. Zassenhaus *Algorithmic Algebraic Number Theory*
31 J. Aczel and J. Dhombres *Functional Equations in Several Variables*
32 M. Kuczma, B. Choczewski, and R. Ger *Iterative Functional Equations*
33 R. Ambatzumain *Factorization Calculus and Geometric Probability*
34 G. Gripenberg, S.-O. Londen, and O. Staffans *Volterra Integral and Functional Equations*
35 George Gasper and Mizan Rahman *Basic Hypergeometric Series*
36 Erik Torgersen *Comparison of Statistical Experiments*
37 A. Neumaier *Interval Methods for Systems Equations*
38 N. Korneichuk and K. Ivanov *Exact Constants in Approximation Theory*
39 R. A. Brualdi and H. J. Ryser *Combinational Matrix Theory*
40 N. White (ed.) *Matroid Applications*
41 S. Sakai *Operator Algebras in Dynamical Systems*
42 W. Hodges *Model Theory*
43 H. Stahl and V. Totik *General Orthogonal Polynomials*
44 R. Schneider *Convex Bodies*
45 G. Da Prato and J. Zabcyck *Stochastic Equations in Infinite Dimensions*
46 A. Bjorner et al. *Oriented Mappings*
47 G. A. Edgar and Louis Sucheston *Stopping Times and Directed Processes*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Computation with finitely presented groups

CHARLES C. SIMS

Rutgers University

CAMBRIDGE
UNIVERSITY PRESS

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
40 West 20th Street, New York, NY 10011-4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1994

Printed in the United States of America

Library of Congress Cataloging-in-Publication Data

Sims, Charles C.
Computation with finitely presented groups / Charles C. Sims
p. cm. – (Encyclopedia of mathematics and its applications ; v. 48)
Includes bibliographical references and index.
ISBN 0-521-43213-8
1. Group theory – Data processing. 2. Finite groups – Data processing. 3. Combinatorial group theory – Data processing. I. Title. II. Series.
QA171.S6173 1993
512′.2 – dc20 92-32383
CIP

A catalog record for this book is available from the British Library

ISBN 0-521-43213-8 hardback

To Annette

Contents

Preface

In 1970, John Cannon, Joachim Neubüser, and I considered the possibility of jointly producing a single book which would cover all of computational group theory. A draft table of contents was even produced, but the project was not completed. It is a measure of how far the subject has progressed in the past 20 years that it would now take at least four substantial books to cover the field, not including the necessary background material on group theory and the design and analysis of algorithms. In addition to a book like this one on computing with finitely presented groups, there would be books on computing with permutation groups, on computing with finite solvable groups, and on computing characters and modular representations of finite groups.

Computational group theory was originated by individuals trained as group theorists. However, there has been a steadily increasing participation in the subject by computer scientists. There are two reasons for this phenomenon. First, group-theoretic algorithms, particularly ones related to permutation groups, were found to be useful in attacking the graph isomorphism problem, a central problem in theoretical computer science. Once computer scientists began looking at group-theoretic algorithms, it was natural for them to attempt to determine the complexity of these algorithms. Second, the techniques and data structures of computer science have proved valuable in improving existing group-theoretic algorithms and in developing new ones.

This book is intended to be a graduate-level text. I have made a deliberate attempt to make the material accessible to students of both mathematics and computer science. The first chapter contains a quick review of elementary group theory, which would not be necessary if the target audience consisted only of graduate students in mathematics. It also contains a discussion of backtrack searches, which should be familiar to any undergraduate computer science major but which are probably not frequently encountered by mathematics majors. I suspect that initially the computer scientists may have an easier time than the mathematicians, since the first

half of the book includes a substantial discussion of the theory of automata and rational languages, topics more familiar to computer scientists than to mathematicians. Moreover, the first half requires only relatively elementary results about groups. However, in the second half, deeper results from group theory are required, and here the computer scientists may find the going somewhat more difficult.

Ideally this book should be accompanied by computer software that would permit the reader to experiment with implementations of the procedure discussed. Unfortunately, an appropriate package does not currently exist, although several of the available systems would be useful in connection with certain topics. Writing my own software would have delayed the publication of the book by several years, at least. The lack of computer support has meant that substantial examples and exercises have been largely omitted, since it is only with the help of the proper software that the reader would be able to explore such material successfully.

I have tried to include as many exercises as I could, but some of the later sections are not as well covered as I would have preferred. The exercises are of two types. Some require only a routine application of a technique discussed in that section. Others are intended to provide new insight. It is not always immediately obvious into which category a particular exercise falls, so the reader is encouraged to look carefully at all of the exercises. The more challenging ones are marked with an asterisk. In a few cases, I don't know the answer to the problems.

A substantial effort was made to include as complete a set of references as possible. To assist instructors in providing reading lists, the Bibliography has been divided into two sections, the first containing books on topics related to the material discussed here, and the second listing articles in journals and conference proceedings. References to books are enclosed in brackets, whereas references to articles are enclosed in parentheses. Michael Vaughan-Lee has written a book on the restricted Burnside problem and an article on the efficient computation of products in large p-groups. Both works appeared in 1990. Information about the book [Vaughan-Lee 1990] is in the book section of the Bibliography, but to find publication data for (Vaughan-Lee 1990) one must look in the articles section.

It is not usual for an author of a mathematics text to make evaluative judgments concerning the works in the Bibliography, and I have agonized over my decision to break with this practice. However, I feel an obligation to the reader to state my opinion that the quality of the papers dealing with the computation of Hermite and Smith normal forms is on average noticeably below the level in the other works cited. In a significant number of these papers there are deficiencies in the exposition and even in the validity of the arguments. I shall mention only one example of the problems I found. Given a set of homogeneous linear equations with integer coefficients, there are efforts to describe a basis of integer solutions. The authors frequently fail to make clear whether they are referring to a vector

space basis for the set of all rational solutions of the system such that each basis vector has integer components, or to a $\mathbb{Z}$-basis for the subgroup of all integer vectors which are solutions of the system. Having reached my conclusion, I was faced with several options. I could remain silent, I could provide critiques of individual papers, or I could omit the papers I found questionable from the Bibliography. None of these possibilities seemed appropriate. The problems are significant enough that I could not remain silent. There are simply too many papers to permit me to make detailed comments concerning each one. I do not have the time, and the book is already long. I have read through, at least quickly, all of these papers, so I feel obligated to include them in the Bibliography. Moreover, each of them has some merit. I realize that by making these comments and not identifying the papers I find deficient, I am raising doubts about the quality of all of them, including papers with substantial contributions. To the authors of these papers I apologize.

It is traditional for the preface to explain the numbering system used for sections, propositions, examples, exercises, figures, and tables. Section 3.4 is the fourth section of Chapter 3. Sections and chapters carrying an asterisk may be skipped without affecting the continuity of the material. The second proposition in Section 3.4 is referred to as Proposition 4.2 or as Proposition 4.2 of Chapter 3. The end of a proof is signaled by the symbol "□". Within a given section, the propositions, theorems, lemmas, and corollaries are numbers in a single series. Examples and exercises are numbered separately. The numbering for figures and tables always includes the number of the chapter. Thus, Table 1.8.1 is the first table in Section 8 of Chapter 1.

A great many people have assisted in the preparation of this book. John Cannon, George Havas, Joachim Neubüser, and Michael Newman all made suggestions which improved the exposition. Special thanks go to Steve Schibell, who read the entire manuscript and provided detailed comments which were extremely useful. Gretchen Ostheimer and Eddie Lo helped with the proofreading. The staff of Cambridge University Press have been very supportive. David Tranah has quietly but persistently been after me to write a book for Cambridge for roughly a decade. Lauren Cowles has greatly facilitated my dealings with the New York office. Finally, Edith Feinstein and Jim Mobley have shown remarkable tolerance for my somewhat idiosyncratic style.

Considerable effort has been expended in trying to get the algorithm descriptions in this book right. However, errors almost certainly remain, and I would welcome information about any problems which are discovered. Other comments are also encouraged. My current address for electronic mail is sims@math.rutgers.edu.

Charles Sims