CONTEMPORARY MATHEMATICS

349

Computational and Experimental Group Theory

AMS-ASL Joint Special Session
Interactions Between Logic, Group Theory and Computer Science

January 15–16, 2003
Baltimore, Maryland

Alexandre V. Borovik
Alexei G. Myasnikov
Editors

American Mathematical Society

http://dx.doi.org/10.1090/conm/349

Computational and Experimental Group Theory

CONTEMPORARY MATHEMATICS

349

Computational and Experimental Group Theory

AMS-ASL Joint Special Session
Interactions Between Logic, Group Theory and Computer Science

January 15–16, 2003
Baltimore, Maryland

Alexandre V. Borovik
Alexei G. Myasnikov
Editors

American Mathematical Society
Providence, Rhode Island

This volume contains papers based on the major themes of the AMS-ASL Joint Special Session "Interactions Between Logic, Group Theory and Computer Science", held in Baltimore, MD, January 15–16, 2003.

2000 *Mathematics Subject Classification.* Primary 20B40, 20E05, 20F28, 81P68; Secondary 68Q05, 68Q17, 68Q42, 68Q45, 68T05.

Library of Congress Cataloging-in-Publication Data

Computational and experimental group theory : AMS-ASL joint special session, interactions between logic, group theory, and computer science, January 15–16, 2003, Baltimore, Maryland / Alexandre V. Borovik, Alexei G. Myasnikov, editors.

p. cm. (Contemporary mathematics, ISSN 0271-4132 ; 349)

Includes bibliographical references.

ISBN 0-8218-3483-5 (acid-free paper)

1. Permutation groups—Congresses. 2. Non-Abelian groups—Congresses. 3. Quantum theory—Mathematics—Congresses. I. Borovik, Alexandre. II. Myasnikov, Alexei G., 1955- III. Title. IV. Contemporary mathematics (American Mathematical Society) ; v. 349.

QA175.C69 2004

512′.21—dc22 2004046351

Contents

Preface

The papers in this volume are loosely based around the major themes of the AMS/ASL Joint Special Session "Interactions Between Logic, Group Theory and Computer Science" held in Baltimore, MD, in January 2003. The preliminary versions of most of them were reported at the session. We wish to express our thanks to the American Mathematical Society and the Association for Symbolic Logic for their invitation to organize the session and their support, which allowed this unusual interdisciplinary meeting to take place.

Since the pioneering works of Novikov and Maltsev, group theory has been a testing ground for mathematical logic in its many manifestations, from the theory of algorithms to model theory. This interaction between logic and group theory led to many prominent results which enriched both disciplines. In this volume we collect under one cover several papers that discuss the first attempts to develop a similar interaction between group theory and computer science.

The papers reflect the paradigm change in algorithmic group theory. Since its origin in works by Dehn in the early 20th century, combinatorial group theory has been primarily concerned with algorithms for solving particular problems on groups given by generators and relations: word problems, conjugacy problems, isomorphism problems, etc. Recent years have seen the focus of algorithmic group theory shift from the decidabiliy/undecidability type of results to complexity of algorithms. Also, a non-deterministic approach to computation on groups started to play a prominent role, especially in the theory of black box groups. The works presented in this volume are concerned with even less traditional approaches to computation on groups: quantum computing, pattern recognition, genetic algorithms. New approaches mean, of course, new models of computation and new concepts of complexity.

The first paper in the volume, by Michael Batty, Samuel Braunstein, Andrew Duncan and Sarah Rees, is a detailed survey of the state of the art in the design of quantum algorithms on groups. Although quantum computers still do not exist in real life, they provide an exciting new model of computation, with the main impact on complexity theory. Indeed, it can be seen that a quantum computer can be simulated on a classical computer (albeit very slowly), so quantum computing does not change the classical decidable/undecidable boundary. Instead, the main issue is, how wide is the class of classical algorithms and problems amenable to the exponential speed up promised by quantum computing? Starting from Shor's seminal work on prime factorization, group theory is playing an increasingly important part in providing such algorithms.

Two further papers, by Richard Booth, Dmitry Bormotov and Alexandre Borovik, and by Alex Miasnikov and Alexei Myasnikov, discuss group-theoretic

applications of genetic (evolutionary) algorithms. In brief, a genetic algorithm is a search strategy for finding an optimal value in the space of all possible values. Being inspired by natural evolution, it treats the set of approximate solutions as a population that evolves from generation to generation by mutation and breeding (crossover) and, crucially, under the action of selection operators. The latter are biased towards individuals with better values of the *fitness function*, which, ideally, should ensure that evolution eventually—and the sooner the better—produces an individual with the optimal value of the fitness function.

Booth, Bormotov and Borovik use genetic algorithms for solving equations in free groups and free semigroups. Besides solving equations which previously were not susceptible to known methods, genetic algorithms for solving equations in free groups exhibit a remarkable property: it is possible to trace how a co-evolution of the population of fitness function converges to a deterministic solution. A short paper by Gilman and Myasnikov exploits the theory of context-free languages to describe the structure of solution sets of equations in one variable over free groups. In particular, their paper provides insight into the reasons for efficiency of genetic algorithms for this particular problem.

Miasnikov and Myasnikov developed a genetic version of the classical Whitehead's algorithm for the automorphic conjugacy problem on free groups. (See Section 2 of their paper for a concise introduction to Whitehead's problem.) The experimental data show that genetic algorithms are much more efficient than the classical deterministic Whitehead's algorithm (which has exponential time complexity). The main conclusion of the paper is that this surprisingly good performance strongly suggests that, although the worst-case complexity of Whitehead's problem might be exponential, it is likely to have low "average" complexity or low "generic" complexity. It also gives strong evidence to the existence of a very efficient deterministic algorithm. This experimental study has already outspun theoretical research (to be published elsewhere) aimed at the explanation of observed phenomena.

The prominent role of certain graphs associated with the automorphic orbits of elements in the free group is already apparent in the paper by Miasnikov and Myasnikov. The next paper, by Bilal Khan, is devoted to a detailed study of these *Whitehead graphs* in the free group of rank 2 which leads to a quadratic bound for complexity of Whitehead's algorithm. Although theoretical by its nature, Khan's work would never have advanced that far without the use of sophisticated software tools for visualization and statistical analysis of graphs.

The last two papers, by Haralick, Miasnikov and Myasnikov, and by Bormotov, show how the industrial machinery of pattern recognition can be applied to the classical and rather subtle problem of automorphic conjugacy in the free group F_2. Some standard methods of pattern recognition have turned out to be very efficient in recognizing primitive and Whitehead minimal elements in F_2. Here, a Whitehead minimal element is an element of minimal length with respect to its orbit under the action of $\mathrm{Aut}(F_2)$.

Alexandre Borovik and Alexei Myasnikov
December 2003

Since its origin in the early 20th century, combinatorial group theory has been primarily concerned with algorithms for solving particular problems on groups given by generators and relations: word problems, conjugacy problems, isomorphism problems, etc. Recent years have seen the focus of algorithmic group theory shift from the decidability/undecidability type of result to the complexity of algorithms. Papers in this volume reflect that paradigm shift.

Articles are based on the AMS/ASL Joint Special Session, Interactions Between Logic, Group Theory and Computer Science.

The volume is suitable for graduate students and research mathematicians interested in computational problems of group theory.

ISBN 0-8218-3483-5

9 780821 834831

CONM/349