CONTEMPORARY MATHEMATICS

633

Algorithmic Problems of Group Theory, Their Complexity, and Applications to Cryptography

AMS Special Sessions
Algorithmic Problems of Group Theory and Their Complexity
January 9–10, 2013
San Diego, California

Algorithmic Problems of Group Theory and Applications to Information Security
April 6–7, 2013
Boston College, Chestnut Hill, Massachusetts

Delaram Kahrobaei
Vladimir Shpilrain
Editors

American Mathematical Society

Algorithmic Problems of Group Theory, Their Complexity, and Applications to Cryptography

CONTEMPORARY MATHEMATICS

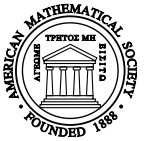
633

Algorithmic Problems of Group Theory, Their Complexity, and Applications to Cryptography

AMS Special Sessions
Algorithmic Problems of Group Theory and Their Complexity
January 9–10, 2013
San Diego, California

Algorithmic Problems of Group Theory and Applications to Information Security
April 6–7, 2013
Boston College, Chestnut Hill, Massachusetts

Delaram Kahrobaei
Vladimir Shpilrain
Editors



American Mathematical Society
Providence, Rhode Island

2010 *Mathematics Subject Classification.* Primary 20-XX, 68-XX.

Library of Congress Cataloging-in-Publication Data

Algorithmic problems of group theory, their complexity, and applications to cryptography / Delaram Kahrobaei, Vladimir Shpilrain, editors.

AMS Special Session on Algorithmic Problems of Group Theory and Their Complexity, January 9–10, 2013, San Diego, CA.

AMS Special Session on Algorithmic Problems of Group Theory and Applications to Information Security, April 6–7, 2013, Boston College, Chestnut Hill, MA.

pages cm. – (Contemporary mathematics ; volume 633)

Includes bibliographical references.

ISBN 978-0-8218-9859-8 (alk. paper)

1. Group theory–Congresses. 2. Noncummutative algebras–Congresses. 3. Algorithms–Congresses. 4. Cryptography–Congresses. 5. Data encryption (Computer science)–Congresses. 6. Algebra–Congresses. I. Kahrobaei, Delaram, 1975– editor. II. Shpilrain, Vladimir, 1960– editor.

QA176.A454 2014

652′.8015122–dc23 2014029814

Contemporary Mathematics ISSN: 0271-4132 (print); ISSN: 1098-3627 (online)

DOI: http://dx.doi.org/10.1090/conm/633

Contents

Preface

This volume consists of contributions by participants and speakers in special sessions at two AMS meetings. These special sessions concerned algorithmic problems of group theory, their complexity, and applications to cryptography. The AMS Special Session on Algorithmic Problems of Group Theory and Their Complexity was held at the San Diego Convention Center in January 2013 and the AMS Special Session on Algorithmic Problems of Group Theory and Applications to Information Security was held at Boston College in April 2013.

Over the past few years the field of group-based cryptography has attracted the attention of both group theorists and cryptographers. The new techniques inspired by algorithmic problems in non-commutative group theory and their complexity have offered promising ideas for developing new cryptographic primitives. This volume contains both survey and research papers on algorithmic group theory and applications to cryptography.

We are grateful to the American Mathematical Society for their help in the publication of this volume. In particular we thank Christine Thivierge for her patience and assistance in putting this volume together.

Delaram Kahrobaei
Vladimir Shpilrain

Selected Published Titles in This Series

633 **Delaram Kahrobaei and Vladimir Shpilrain, Editors,** Algorithmic Problems of Group Theory, Their Complexity, and Applications to Cryptography, 2015

632 **Gohar Kyureghyan, Gary L. Mullen, and Alexander Pott, Editors,** Topics in Finite Fields, 2015

631 **Siddhartha Bhattacharya, Tarun Das, Anish Ghosh, and Riddhi Shah, Editors,** Recent Trends in Ergodic Theory and Dynamical Systems, 2015

630 **Pierre Albin, Dmitry Jakobson, and Frédéric Rochon, Editors,** Geometric and Spectral Analysis, 2014

629 **Milagros Izquierdo, S. Allen Broughton, Antonio F. Costa, and Rubí E. Rodríguez, Editors,** Riemann and Klein Surfaces, Automorphisms, Symmetries and Moduli Spaces, 2014

628 **Anita T. Layton and Sarah D. Olson, Editors,** Biological Fluid Dynamics: Modeling, Computations, and Applications, 2014

627 **Krishnaswami Alladi, Frank Garvan, and Ae Ja Yee, Editors,** Ramanujan 125, 2014

626 **Veronika Furst, Keri A. Kornelson, and Eric S. Weber, Editors,** Operator Methods in Wavelets, Tilings, and Frames, 2014

625 **Alexander Barg and Oleg R. Musin, Editors,** Discrete Geometry and Algebraic Combinatorics, 2014

624 **Karl-Dieter Crisman and Michael A. Jones, Editors,** The Mathematics of Decisions, Elections, and Games, 2014

623 **Pramod N. Achar, Dijana Jakelić, Kailash C. Misra, and Milen Yakimov, Editors,** Recent Advances in Representation Theory, Quantum Groups, Algebraic Geometry, and Related Topics, 2014

622 **S. Ejaz Ahmed, Editor,** Perspectives on Big Data Analysis, 2014

621 **Ludmil Katzarkov, Ernesto Lupercio, and Francisco J. Turrubiates, Editors,** The Influence of Solomon Lefschetz in Geometry and Topology, 2014

620 **Ulrike Tillmann, Søren Galatius, and Dev Sinha, Editors,** Algebraic Topology: Applications and New Directions, 2014

619 **Gershon Wolansky and Alexander J. Zaslavski, Editors,** Variational and Optimal Control Problems on Unbounded Domains, 2014

618 **Abba B. Gumel, Editor,** Mathematics of Continuous and Discrete Dynamical Systems, 2014

617 **Christian Ausoni, Kathryn Hess, Brenda Johnson, Wolfgang Lück, and Jérôme Scherer, Editors,** An Alpine Expedition through Algebraic Topology, 2014

616 **G. L. Litvinov and S. N. Sergeev, Editors,** Tropical and Idempotent Mathematics and Applications, 2014

615 **Plamen Stefanov, András Vasy, and Maciej Zworski, Editors,** Inverse Problems and Applications, 2014

614 **James W. Cogdell, Freydoon Shahidi, and David Soudry, Editors,** Automorphic Forms and Related Geometry, 2014

613 **Stephan Stolz, Editor,** Topology and Field Theories, 2014

612 **Patricio Cifuentes, José García-Cuerva, Gustavo Garrigós, Eugenio Hernández, José María Martell, Javier Parcet, Keith M. Rogers, Alberto Ruiz, Fernando Soria, and Ana Vargas, Editors,** Harmonic Analysis and Partial Differential Equations, 2014

611 **Robert Fitzgerald Morse, Daniela Nikolova-Popova, and Sarah Witherspoon, Editors,** Group Theory, Combinatorics, and Computing, 2014

For a complete list of titles in this series, visit the
AMS Bookstore at **www.ams.org/bookstore/conmseries/**.

CONM 633

Group Theory, Complexity, Cryptography • Kahrobaei et al., Editors

This volume contains the proceedings of the AMS Special Session on Algorithmic Problems of Group Theory and Their Complexity, held January 9–10, 2013 in San Diego, CA and the AMS Special Session on Algorithmic Problems of Group Theory and Applications to Information Security, held April 6–7, 2013 at Boston College, Chestnut Hill, MA.

Over the past few years the field of group-based cryptography has attracted attention from both group theorists and cryptographers. The new techniques inspired by algorithmic problems in non-commutative group theory and their complexity have offered promising ideas for developing new cryptographic protocols. The papers in this volume cover algorithmic group theory and applications to cryptography.

ISBN 978-0-8218-9859-8

9 780821 898598

CONM/633

AMS