CONTEMPORARY MATHEMATICS

677

Algebra and Computer Science

Joint AMS-EMS-SPM Meeting
Algebra and Computer Science
June 10–13, 2015: Porto, Portugal

Joint Mathematics Meetings
Groups, Algorithms, and Cryptography
January 10–13, 2015: San Antonio, TX

Joint AMS-Israel Mathematical Union Meeting
Applications of Algebra to Cryptography
June 16–19, 2014: Tel-Aviv, Israel

Delaram Kahrobaei
Bren Cavallo
David Garber
Editors

American Mathematical Society

Algebra and Computer Science

CONTEMPORARY MATHEMATICS

677

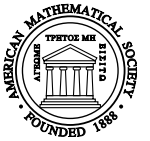
Algebra and Computer Science

Joint AMS-EMS-SPM Meeting
Algebra and Computer Science
June 10–13, 2015: Porto, Portugal

Joint Mathematics Meetings
Groups, Algorithms, and Cryptography
January 10–13, 2015: San Antonio, TX

Joint AMS-Israel Mathematical Union Meeting
Applications of Algebra to Cryptography
June 16–19, 2014: Tel-Aviv, Israel

Delaram Kahrobaei
Bren Cavallo
David Garber
Editors



American Mathematical Society
Providence, Rhode Island

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

Library of Congress Cataloging-in-Publication Data

Library of Congress Cataloging-in-Publication Data

Names: Kahrobaei, Delaram, 1975– editor. | Cavallo, Bren, 1989– editor. | Garber, David, 1973– editor.

Title: Algebra and computer science / Delaram Kahrobaei, Bren Cavallo, David Garber, editors.

Description: Providence, Rhode Island : American Mathematical Society, [2016] | Series: Contemporary mathematics ; volume 677 | Special Session at the Joint AMS-EMS-SPM Meeting, Algebra and Computer Science, June 10–13, 2015, Porto, Portugal. | Special Session at the Joint Mathematics Meetings, Groups, Algorithms, and Cryptography, January 10–13, 2015, San Antonio, TX. | Special Session at the Joint AMS-Israel Mathematical Union Meeting, Applications of Algebra to Cryptography, June 16–19, 2014, Tel-Aviv, Israel. | Includes bibliographical references.

Identifiers: LCCN 2016019097 | ISBN 9781470423032 (alk. paper)

Subjects: LCSH: Logic, Symbolic and mathematical–Congresses. | Algebra–Congresses. | Computer science–Mathematics–Congresses. | AMS: Group theory and generalizations. msc | Computer science. msc

Classification: LCC QA9.A1 A44 2016 | DDC 512.0285–dc23 LC record available at https://lccn.loc.gov/2016019097

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

DOI: http://dx.doi.org/10.1090/conm/677

Contents

Preface

This volume consists of contributions by participants and speakers in special sessions at three AMS meetings. These special sessions concerned algorithmic problems in algebra and applications to computer science and cryptography. One of the special sessions was at Tel Aviv University, Israel in June 2014, another at the University of Porto, Portugal in June 2015, and the other one at the San Antonio Convention Center, Texas in January 2015.

Over the past few years the field of interaction between computer science and algebra has attracted the attention of both algebraists and computer scientists.

This volume contains both survey and research papers on algorithmic algebra and applications in computer science, particularly cryptography and complexity theory.

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
Bren Cavallo
David Garber

Selected Published Titles in This Series

677 **Delaram Kahrobaei, Bren Cavallo, and David Garber, Editors,** Algebra and Computer Science, 2016

674 **Bogdan D. Suceavă, Alfonso Carriazo, Yun Myung Oh, and Joeri Van der Veken, Editors,** Recent Advances in the Geometry of Submanifolds, 2016

673 **Alex Martsinkovsky, Gordana Todorov, and Kiyoshi Igusa, Editors,** Recent Developments in Representation Theory, 2016

672 **Bernard Russo, Asuman Güven Aksoy, Ravshan Ashurov, and Shavkat Ayupov, Editors,** Topics in Functional Analysis and Algebra, 2016

671 **Robert S. Doran and Efton Park, Editors,** Operator Algebras and Their Applications, 2016

670 **Krishnendu Gongopadhyay and Rama Mishra, Editors,** Knot Theory and Its Applications, 2016

669 **Sergiĭ Kolyada, Martin Möller, Pieter Moree, and Thomas Ward, Editors,** Dynamics and Numbers, 2016

668 **Gregory Budzban, Harry Randolph Hughes, and Henri Schurz, Editors,** Probability on Algebraic and Geometric Structures, 2016

667 **Mark L. Agranovsky, Matania Ben-Artzi, Greg Galloway, Lavi Karp, Dmitry Khavinson, Simeon Reich, Gilbert Weinstein, and Lawrence Zalcman, Editors,** Complex Analysis and Dynamical Systems VI: Part 2: Complex Analysis, Quasiconformal Mappings, Complex Dynamics, 2016

666 **Vicenţiu D. Rădulescu, Adélia Sequeira, and Vsevolod A. Solonnikov, Editors,** Recent Advances in Partial Differential Equations and Applications, 2016

665 **Helge Glöckner, Alain Escassut, and Khodr Shamseddine, Editors,** Advances in Non-Archimedean Analysis, 2016

664 **Dihua Jiang, Freydoon Shahidi, and David Soudry, Editors,** Advances in the Theory of Automorphic Forms and Their L-functions, 2016

663 **David Kohel and Igor Shparlinski, Editors,** Frobenius Distributions: Lang-Trotter and Sato-Tate Conjectures, 2016

662 **Zair Ibragimov, Norman Levenberg, Sergey Pinchuk, and Azimbay Sadullaev, Editors,** Topics in Several Complex Variables, 2016

661 **Douglas P. Hardin, Doron S. Lubinsky, and Brian Z. Simanek, Editors,** Modern Trends in Constructive Function Theory, 2016

660 **Habib Ammari, Yves Capdeboscq, Hyeonbae Kang, and Imbo Sim, Editors,** Imaging, Multi-scale and High Contrast Partial Differential Equations, 2016

659 **Boris S. Mordukhovich, Simeon Reich, and Alexander J. Zaslavski, Editors,** Nonlinear Analysis and Optimization, 2016

658 **Carlos M. da Fonseca, Dinh Van Huynh, Steve Kirkland, and Vu Kim Tuan, Editors,** A Panorama of Mathematics: Pure and Applied, 2016

657 **Noé Bárcenas, Fernando Galaz-García, and Mónica Moreno Rocha, Editors,** Mexican Mathematicians Abroad, 2016

656 **José A. de la Peña, J. Alfredo López-Mimbela, Miguel Nakamura, and Jimmy Petean, Editors,** Mathematical Congress of the Americas, 2016

655 **A. C. Cojocaru, C. David, and F. Pappalardi, Editors,** SCHOLAR—a Scientific Celebration Highlighting Open Lines of Arithmetic Research, 2015

654 **Carlo Gasbarri, Steven Lu, Mike Roth, and Yuri Tschinkel, Editors,** Rational Points, Rational Curves, and Entire Holomorphic Curves on Projective Varieties, 2015

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

CONM 677

Algebra and Computer Science • Kahrobaei et al., Editors

This volume contains the proceedings of three special sessions: Algebra and Computer Science, held during the Joint AMS-EMS-SPM meeting in Porto, Portugal, June 10–13, 2015; Groups, Algorithms, and Cryptography, held during the Joint Mathematics Meetings in San Antonio, TX, January 10–13, 2015; and Applications of Algebra to Cryptography, held during the Joint AMS-Israel Mathematical Union meeting in Tel-Aviv, Israel, June 16–19, 2014.

Papers contained in this volume address a wide range of topics, from theoretical aspects of algebra, namely group theory, universal algebra and related areas, to applications in several different areas of computer science. From the computational side, the book aims to reflect the rapidly emerging area of algorithmic problems in algebra, their computational complexity and applications, including information security, constraint satisfaction problems, and decision theory.

The book gives special attention to recent advances in quantum computing that highlight the need for a variety of new intractability assumptions and have resulted in a new area called group-based cryptography.

ISBN 978-1-4704-2303-2
9 781470 423032
CONM/677

AMS