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
Algebra and Computer Science
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
Contents

Preface vii

Generic properties of subgroups of free groups and finite presentations
Frédérique Bassino, Cyril Nicaud, and Pascal Weil 1

A new multi-server scheme for private information retrieval
Chi Sing Chum and Xiaowen Zhang 45

On secret sharing protocols
Chi Sing Chum, Benjamin Fine, Anja I. S. Moldenhauer, Gerhard Rosenberger, and Xiaowen Zhang 51

A verifiable secret sharing scheme using non-abelian groups
Maggie E. Habeeb 79

Non-associative public-key cryptography
Arkadius Kalka 85

Non-associative key establishment protocols and their implementation
Arkadius Kalka and Mina Teicher 113

Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups
Daniel König, Markus Lohrey, and Georg Zetzsche 129

On the Tits alternative for a class of finitely presented groups with a special focus on symbolic computations
Anja I. S. Moldenhauer, Gerhard Rosenberger, and Kristina Rosenthal 145

Geometry of the conjugacy problem in lamplighter groups
Andrew Sale 171

A logspace solution to the word and conjugacy problem of generalized Baumslag-Solitar groups
Armin Weiss 185

Cryptographic hash functions from sequences of lifted Paley graphs
Serena Yuan 213
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


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


669 Sergii 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


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


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


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