CONTEMPORARY MATHEMATICS

632

Topics in Finite Fields

11th International Conference
Finite Fields and their Applications
July 22–26, 2013
Magdeburg, Germany

Gohar Kyureghyan
Gary L. Mullen
Alexander Pott
Editors

American Mathematical Society

Topics in Finite Fields

CONTEMPORARY MATHEMATICS

632

Topics in Finite Fields

11th International Conference
Finite Fields and their Applications
July 22–26, 2013
Magdeburg, Germany

Gohar Kyureghyan
Gary L. Mullen
Alexander Pott
Editors

American Mathematical Society
Providence, Rhode Island

2010 *Mathematics Subject Classification.* Primary 05Bxx, 11Txx, 11Gxx, 12Exx, 12Fxx, 12Yxx, 20Cxx, 51Exx, 94Axx, 94Bxx.

Library of Congress Cataloging-in-Publication Data

International Conference on Finite Fields and Their Applications (11th : 2013 : Magdeburg, Germany) Topics in finite fields : 11th International Conference on Finite Fields and Their Applications, July 22–26, 2013, Magdeburg, Germany / Gohar Kyureghyan, Gary L. Mullen, Alexander Pott, editors.

pages cm. – (Contemporary mathematics ; volume 632)

Includes bibliographical references.

ISBN 978-0-8218-9860-4 (alk. paper)

1. Finite fields (Algebra)–Congresses. 2. Commutative rings–Congresses. 3. Combinatorial analysis–Congresses. 4. Arithmetical algebraic geometry–Congresses. 5. Group theory–Congresses. I. Kyureghyan, Gohar, 1974– editor. II. Mullen, Gary L., editor. III. Pott, Alexander, 1961– editor. IV. Title.

QA247.3.I57 2013
512′.3–dc23 2014022869

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

DOI: http://dx.doi.org/10.1090/conm/632

Contents

Preface

This volume of Contemporary Mathematics published by the American Mathematical Society contains the proceedings of the 11th International Conference on Finite Fields and Their Applications (Fq11), held in Magdeburg, Germany, July 22–26, 2013. Magdeburg, the city of the first Holy Roman Emperor Otto I, provided an excellent and exciting setting for the conference. The conference Fq11 brought together researchers from all over the world, researchers working in various areas related to the theory and application of finite fields.

The present volume contains five invited papers and 21 contributed papers. All submitted papers, including the invited papers, were strictly refereed. The accepted papers consider theoretical and algorithmic aspects of finite fields as well as applications in coding theory, combinatorics and cryptography.

We would like to take this opportunity to thank various institutions for their financial support. These include support by the German Research Foundation, Elsevier, and Otto-von-Guericke University of Magdeburg. Our special thanks are due Christine M. Thivierge for her help publishing this conference proceedings volume. We are very grateful to the referees who ensured the high quality of the papers included in this volume.

We are happy to be able to announce that Gove Effinger will host the 12th International Conference on Finite Fields and Their Applications at Skidmore College in upstate New York during the period July 13–17, 2015. We look forward to what we are sure will be another very successful conference. We hope to see you at Fq12!

Gohar Kyureghyan, Gary L. Mullen, Alexander Pott
April 2014

List of participants

Kanat Abdukhalikov
Sergey Abrahamyan
Angela Aguglia
Nurdagül Anbar
Daniel Augot
Ioulia Baoulina
Linda Beukemann
Martino Borello
Herivelto Borges
Anne Canteaut
Philippe Cara
Cícero Carvalho
Chris Castillo
Florian Caullery
Ayça Çeşmelioğlu
Pascale Charpin
Eun Ju Cheon
Ricardo Conceição
Gary R. Cook
Robert Coulter
James A. Davis
Jan De Beule
Beiliang Du
Jérôme Ducoat
Yves Edel
Gove Effinger
Yury Ermishkin
Sergei Evdokimov
Tao Feng
Ryoh Fuji-Hara
Satoru Fukasawa
Stephen M. Gagola III
Sugata Gangopadhyay
Theo Garefalakis
Alexander Gavrilyuk
Gennian Ge
Sergey Goryainov
Rainer Göttfert
Maciej Grześkowiak
Cem Güneri
Yoshinori Hamahata
Yutaka Hiramine
Masaaki Homma
Thomas Honold
Xiang-dong Hou
Ming-Deh Huang
Sophie Huczynska
Hye-Jeong Hwang
Ferdinand Ihringer
Leyla Isik
Lijun Ji
Dieter Jungnickel

Relinde Jurrius
Giorgos Kapetanakis
Daniel J. Katz
Nicholas Katz
Michael Kiermaier
Seon Jeong Kim
Gábor Korchmáros
Gohar M. Kyureghyan
Ivan Landjev
Alain Lasjaunias
Michel Lavrauw
Ka Hin Leung
Chunlei Li
Jiyou Li
Nian Li
Xiao-Nan Lu
Anton Malevich
Gary McGuire
Wilfried Meidl
Sihem Mesnager
Ying Miao
Vladimir Mironkin
Ivan Yu Mogilnykh
Gary L. Mullen
Amela Muratović-Ribić
Misha Muzychuk
Nobuo Nakagawa
Anand Kumar Narayanan
Harald Niederreiter
Alina Ostafe
Ferruh Özbudak
Buket Özkaya
Daniel Panario
Enes Pasalic
Alexander Pott
Sara Rottey
Elif Sacikara
Simona Samardjiska
Tilla Schade
Uwe Schauz
Kai-Uwe Schmidt
Igor Shparlinski
John Sheekey
Alessandro Siciliano
Faina Solov'eva
Karanikolopoulos Sotirios
Henning Stichtenoth
Leo Storme
Wei Su
Valentin Suder
Chihiro Suetake
Janusz Szmidt
Ming Ming Tan
Hiroaki Taniguchi
Horacio Tapia-Recillas
Dirk Oliver Theis
Anitha Thillaisundaram
David Thomson
Alev Topuzoğlu
Simone Ugolini
Christopher Umans
Geertrui Van de Voorde
Peter Vandendriessche
Jordy Vanpoucke

Zlatko Varbanov

Joachim von zur Gathen

Qi Wang

Arne Winterhof

Jacques Wolfmann

Siman Yang

Jianxing Yin

Corrado Zanella

Yue Zhou

CONM 632

Topics in Finite Fields • Kyureghyan et al., Editors

This volume contains the proceedings of the 11th International Conference on Finite Fields and their Applications (Fq11), held July 22–26, 2013, in Magdeburg, Germany.

Finite Fields are fundamental structures in mathematics. They lead to interesting deep problems in number theory, play a major role in combinatorics and finite geometry, and have a vast amount of applications in computer science.

Papers in this volume cover these aspects of finite fields as well as applications in coding theory and cryptography.

ISBN 978-0-8218-9860-4

9 780821 898604

CONM/632

AMS