

CONTEMPORARY MATHEMATICS

579

Theory and Applications of Finite Fields

The 10th International Conference
on Finite Fields and Their Applications
July 11–15, 2011
Ghent, Belgium

Michel Lavrauw
Gary L. Mullen
Svetla Nikova
Daniel Panario
Leo Storme
Editors



American Mathematical Society

Theory and Applications of Finite Fields

CONTEMPORARY MATHEMATICS

579

Theory and Applications of Finite Fields

The 10th International Conference
on Finite Fields and Their Applications
July 11–15, 2011
Ghent, Belgium

Michel Lavrauw
Gary L. Mullen
Svetla Nikova
Daniel Panario
Leo Storme
Editors



American Mathematical Society
Providence, Rhode Island

EDITORIAL COMMITTEE

Dennis DeTurck, Managing Editor

Michael Loss Kailash Misra Martin J. Strauss

2010 *Mathematics Subject Classification*. Primary 05Bxx, 11Gxx, 11Lxx, 11Txx, 14Gxx, 51Exx, 94A60, 94Bxx.

Library of Congress Cataloging-in-Publication Data

International Conference on Finite Fields and Applications (10th : Ghent, Belgium : 2011).

Theory and applications of finite fields : 10th International Conference on Finite Fields and Their Applications, July 11–15, 2011, Ghent, Belgium / Michel Lavrauw, Gary L. Mullen, Svetla Nikova, Daniel Panario, Leo Storme, editors.

p. cm. — (Contemporary mathematics ; v. 579)

Includes bibliographical references.

ISBN 978-0-8218-5298-9 (alk. paper)

1. Finite fields (Algebra)—Congresses. 2. Arithmetical algebraic geometry—Congresses. 3. Number theory—Congresses. 4. Coding theory—Congresses. I. Lavrauw, Michel, 1974—editor of compilation. II. Title.

QA247.3.I57 2011
512'.3—dc23

2012023438

Copying and reprinting. Material in this book may be reproduced by any means for educational and scientific purposes without fee or permission with the exception of reproduction by services that collect fees for delivery of documents and provided that the customary acknowledgment of the source is given. This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to reprint-permission@ams.org.

Excluded from these provisions is material in articles for which the author holds copyright. In such cases, requests for permission to use or reprint should be addressed directly to the author(s). (Copyright ownership is indicated in the notice in the lower right-hand corner of the first page of each article.)

© 2012 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights
except those granted to the United States Government.

Copyright of individual articles may revert to the public domain 28 years
after publication. Contact the AMS for copyright status of individual articles.

Printed in the United States of America.

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.

Visit the AMS home page at <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 17 16 15 14 13 12

Contents

Preface	vii
Low dimensional models of the finite split Cayley hexagon JOHN BAMBERG and NICOLA DURANTE	1
Davenport's constant for groups with large exponent GAUTAMI BHOWMIK and JAN-CHRISTOPH SCHLAGE-PUCHTA	21
Permanent has less zeros than determinant over finite fields MIKHAIL V. BUDREVICH and ALEXANDER E. GUTERMAN	33
On a series of modules for the symplectic group in characteristic 2 ILARIA CARDINALI and ANTONIO PASINI	43
Exact divisibility of exponential sums and some consequences FRANCIS N. CASTRO, RAÚL FIGUEROA, and LUIS A. MEDINA	55
Additive character sums of polynomial quotients ZHIXIONG CHEN and ARNE WINTERHOF	67
5-Designs related to binary extremal self-dual codes of length $24m$ JAVIER DE LA CRUZ and WOLFGANG WILLEMS	75
Sequences of Dedekind sums in function fields YOSHINORI HAMAHATA	81
Niho bent functions and Subiaco hyperovals TOR HELLESETH, ALEXANDER KHOLOSHA, and SIHEM MESNAGER	91
A bound on the number of points of a curve in a projective space over a finite field MASAAKI HOMMA	103
Designs in projective Hjelmslev spaces MICHAEL KIERMAIER and IVAN LANDJEV	111
On the nuclei of a finite semifield GIUSEPPE MARINO and OLGA POLVERINO	123
Small-bias sets from extended norm-trace codes GRETCHEN L. MATTHEWS and JUSTIN D. PEACHEY	143
On the Waring problem with multivariate Dickson polynomials ALINA OSTAFE, DAVID THOMSON, and ARNE WINTERHOF	153

Polynomials modulo p and the theory of Galois sets	163
MICHAEL ROSEN	
Additive decompositions induced by multiplicative characters over finite fields	179
DAVIDE SCHIPANI and MICHELE ELIA	
Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic two	187
SIMONE UGOLINI	

Preface

This volume of Contemporary Mathematics of the American Mathematical Society contains the proceedings of the 10th International Conference on Finite Fields and Their Applications (Fq 10), held in Ghent, Belgium, July 11–15, 2011. This conference continued the already two-decades long tradition of bringing together researchers working on various topics on finite fields, to present their results, and to discuss problems on finite fields.

The local organizing committee consisted of Jan De Beule, Frank De Clerck (Chair), Yves Edel, Michel Lavrauw, Svetla Nikova, Bart Preneel and Leo Storme. The scientific committee consisted of Simeon Ball, Michel Lavrauw, Gary McGuire, Gary L. Mullen, Harald Niederreiter, Svetla Nikova, Daniel Panario, Bart Preneel, Igor Shparlinski and Leo Storme (Chair).

At the conference, there were 149 participants, five invited presentations given by Joachim von zur Gathen, Tor Helleseeth, Tanja Lange, Olga Polverino and Michael Rosen, together with 97 contributed talks. The conference honored the 64th birthday of Gary L. Mullen, who initiated this series of international conferences on finite fields and the international journal *Finite Fields and Their Applications*, and the 200th birthday of Évariste Galois, the founder of finite fields theory.

The present volume contains three invited papers by world experts on diverse topics in finite fields, and 14 contributed papers. All submitted papers, including the invited papers, were strictly refereed according to the high standards required for publication in the Contemporary Mathematics Book Series of the American Mathematical Society. The topics include finite geometry, finite semifields, bent functions, polynomial theory, designs, and function fields.

We wish to thank the financial support of

- (1) BCRYPT: Belgian Fundamental Research on Cryptology and Information Security,
- (2) Elsevier,
- (3) FWO: Research Foundation - Flanders,
- (4) Research Fund of the Faculty of Sciences of Ghent University,
- (5) Research Group ESAT/COSIC, Department of Electrical Engineering, KU Leuven,
- (6) Research Group Incidence Geometry, Department of Mathematics, Ghent University.

We also wish to thank Samuel Perez and Sonia Surmont, the administrative staff of the Department of Mathematics of Ghent University, and the staff of the conference centre “Het Pand” of Ghent University for their help in organizing Fq 10. A special thank you also goes out to Christine Thivierge (AMS) for her advise and

help in publishing these conference proceedings in the Contemporary Mathematics Book Series of the American Mathematical Society.

The refereeing process of the submitted articles cannot take place without the help of many referees. We thank the referees for their work in helping us to ensure the high quality of the proceedings of this conference.

Scientific research on finite fields and their applications still flourishes. Many problems still need to be solved and many paths still are unexplored. It is our pleasure to report that Prof. Dr. Alexander Pott (Otto-von-Guericke Universität, Magdeburg, Germany) will organize Fq 11 from July 22–26, 2013, in Magdeburg, Germany. In this way, the city of Magdeburg will add its name to the list of Las Vegas (Fq 1 and Fq 2), Glasgow (Fq 3), Waterloo (Fq 4), Augsburg (Fq 5), Oaxaca (Fq 6), Toulouse (Fq 7), Melbourne (Fq 8), Dublin (Fq 9), and Ghent (Fq 10) as venues for an Fq conference. The success of all ten previous Fq conferences already convinces us to be certain that Fq 11 will also be a great success. We are looking forward to this next edition within the Fq conferences series, and, together with Prof. Dr. Alexander Pott and his organizing team, invite you to attend the Fq 11 conference, and hope to see you there!

The editors

Michel Lavrauw, Gary L. Mullen, Svetla Nikova, Daniel Panario, Leo Storme
May 2012

Selected Published Titles in This Series

- 579 **Michel Lavrauw, Gary L. Mullen, Svetla Nikova, Daniel Panario, and Leo Storme, Editors**, *Theory and Applications of Finite Fields*, 2012
- 575 **Yunping Jiang and Sudeb Mitra, Editors**, *Quasiconformal Mappings, Riemann Surfaces, and Teichmüller Spaces*, 2012
- 573 **Francis Bonahon, Robert L. Devaney, Frederick P. Gardiner, and Dragomir Šarić, Editors**, *Conformal Dynamics and Hyperbolic Geometry*, 2012
- 572 **Mika Seppälä and Emil Volcheck, Editors**, *Computational Algebraic and Analytic Geometry*, 2012
- 571 **José Ignacio Burgos Gil, Rob de Jeu, James D. Lewis, Juan Carlos Naranjo, Wayne Raskind, and Xavier Xarles, Editors**, *Regulators*, 2012
- 570 **Joaquín Pérez and José A. Gálvez, Editors**, *Geometric Analysis*, 2012
- 569 **Victor Goryunov, Kevin Houston, and Roberta Wik-Atique, Editors**, *Real and Complex Singularities*, 2012
- 568 **Simeon Reich and Alexander J. Zaslavski, Editors**, *Optimization Theory and Related Topics*, 2012
- 567 **Lewis Bowen, Rostislav Grigorchuk, and Yaroslav Vorobets, Editors**, *Dynamical Systems and Group Actions*, 2012
- 566 **Antonio Campillo, Gabriel Cardona, Alejandro Melle-Hernández, Wim Veys, and Wilson A. Zúñiga-Galindo, Editors**, *Zeta Functions in Algebra and Geometry*, 2012
- 565 **Susumu Ariki, Hiraku Nakajima, Yoshihisa Saito, Ken-ichi Shinoda, Toshiaki Shoji, and Toshiyuki Tanisaki, Editors**, *Algebraic Groups and Quantum Groups*, 2012
- 564 **Valery Alexeev, Angela Gibney, Elham Izadi, János Kollár, and Eduard Looijenga, Editors**, *Compact Moduli Spaces and Vector Bundles*, 2012
- 563 **Primitivo B. Acosta-Humánez, Federico Finkel, Niky Kamran, and Peter J. Olver, Editors**, *Algebraic Aspects of Darboux Transformations, Quantum Integrable Systems and Supersymmetric Quantum Mechanics*, 2012
- 562 **P. Ara, K. A. Brown, T. H. Lenagan, E. S. Letzter, J. T. Stafford, and J. J. Zhang, Editors**, *New Trends in Noncommutative Algebra*, 2012
- 561 **Óscar Blasco, José A. Bonet, José M. Calabuig, and David Jornet, Editors**, *Topics in Complex Analysis and Operator Theory*, 2012
- 560 **Weiping Li, Loretta Bartolini, Jesse Johnson, Feng Luo, Robert Myers, and J. Hyam Rubinstein, Editors**, *Topology and Geometry in Dimension Three*, 2011
- 559 **Guillaume Bal, David Finch, Peter Kuchment, John Schotland, Plamen Stefanov, and Gunther Uhlmann, Editors**, *Tomography and Inverse Transport Theory*, 2011
- 558 **Martin Grohe and Johann A. Makowsky, Editors**, *Model Theoretic Methods in Finite Combinatorics*, 2011
- 557 **Jeffrey Adams, Bong Lian, and Siddhartha Sahi, Editors**, *Representation Theory and Mathematical Physics*, 2011
- 556 **Leonid Gurvits, Philippe Pébay, J. Maurice Rojas, and David Thompson, Editors**, *Randomization, Relaxation, and Complexity in Polynomial Equation Solving*, 2011
- 555 **Alberto Corso and Claudia Polini, Editors**, *Commutative Algebra and Its Connections to Geometry*, 2011
- 554 **Mark Agranovsky, Matania Ben-Artzi, Greg Galloway, Lavi Karp, Simeon Reich, David Shoikhet, Gilbert Weinstein, and Lawrence Zalcman, Editors**, *Complex Analysis and Dynamical Systems IV: Part 2. General Relativity, Geometry, and PDE*, 2011

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 the 10th International Conference on Finite Fields and their Applications (Fq 10), held July 11–15, 2011, in Ghent, Belgium.

Research on finite fields and their practical applications continues to flourish. This volume's topics, which include finite geometry, finite semifields, bent functions, polynomial theory, designs, and function fields, show the variety of research in this area and prove the tremendous importance of finite field theory.

ISBN 978-0-8218-5298-9



9 780821 852989

CONM/579

AMS on the Web
www.ams.org