

# 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

## EDITORIAL COMMITTEE

Dennis DeTurck, Managing Editor

Michael Loss      Kailash Misra      Martin J. Strauss

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>

---

**Copying and reprinting.** Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy select pages for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Permissions to reuse portions of AMS publication content are handled by Copyright Clearance Center's RightsLink® service. For more information, please visit: <http://www.ams.org/rightslink>.

Send requests for translation rights and licensed reprints to [reprint-permission@ams.org](mailto:reprint-permission@ams.org).

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

© 2015 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights  
except those granted to the United States Government.  
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      20 19 18 17 16 15

## Contents

Preface	vii
List of participants	ix
New recursive construction of normal polynomials over finite fields SERGEY ABRAHAMYAN and MELSIK KYUREGHYAN	1
Collineation groups strongly irreducible on an oval in a projective plane of odd order A. AGUGLIA and G. KORCHMÁROS	11
On the solvability of certain equations over finite fields IOULIA N. BAOUNINA	19
On automorphism groups of binary linear codes MARTINO BORELLO	29
Extended differential properties of cryptographic functions ANNE CANTEAUT and JOËLLE ROUÉ	43
A divisibility criterion for exceptional APN functions FLORIAN CAULLERY	71
Non weakly regular bent polynomials from vectorial quadratic functions AYÇA ÇEŞMELIOĞLU and WILFRIED MEIDL	83
Strongly regular graphs arising from Hermitian varieties A. COSSIDENTE, G. KORCHMÁROS, and G. MARINO	95
Generalized rank weights: A duality statement JÉRÔME DUCOAT	101
An upper bound for the number of Galois points for a plane curve SATORU FUKASAWA	111
A generalization of the nonlinear combination generator RAINER GÖTTFERT	121
Dedekind sums with a parameter in function fields YOSHINORI HAMAHATA	139
Numbers of points of hypersurfaces without lines over finite fields MASAAKI HOMMA	151

Optimal binary subspace codes of length 6, constant dimension 3 and minimum subspace distance 4	
THOMAS HONOLD, MICHAEL KIERMAIER, and SASCHA KURZ	157
A survey of permutation binomials and trinomials over finite fields	
XIANG-DONG HOU	177
Computing class groups of function fields using stark units	
MING-DEH HUANG and ANAND KUMAR NARAYANAN	193
Finding primitive elements in finite fields of small characteristic	
MING-DEH HUANG and ANAND KUMAR NARAYANAN	215
The coset leader and list weight enumerator	
RELINDE JURRIUS and RUUD PELLIKAAN	229
Wieferich past and future	
NICHOLAS M. KATZ	253
Field reduction and linear sets in finite geometry	
MICHEL LAVRAUW and GEERTRUI VAN DE VOORDE	271
Bent functions from spreads	
SIHEM MESNAGER	295
On the characterization of a semi-multiplicative analogue of planar functions over finite fields	
AMELIA MURATOVIĆ-RIBIĆ, ALEXANDER POTT, DAVID THOMSON, and QIANG WANG	317
A solution of an equivalence problem for semisimple cyclic codes	
MIKHAIL MUZYCHUK	327
On cross joining de Bruijn sequences	
JOHANNES MYKKELTVEIT and JANUSZ SZMIDT	335
Ambiguity and deficiency of reversed Dickson permutations	
DANIEL PANARIO, AMIN SAKZAD, and DAVID THOMSON	347
From near-bent to bent: A special case	
J. WOLFMANN	359

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

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

Zlatko Varbanov

Joachim von zur Gathen

Qi Wang

Arne Winterhof

Jacques Wolfmann

Siman Yang

Jianxing Yin

Corrado Zanella

Yue Zhou



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 on the Web  
[www.ams.org](http://www.ams.org)