

CONTEMPORARY MATHEMATICS

518

Finite Fields: Theory and Applications

Ninth International Conference
Finite Fields and Applications
July 13–17, 2009
Dublin, Ireland

Gary McGuire
Gary L. Mullen
Daniel Panario
Igor E. Shparlinski
Editors



American Mathematical Society

Finite Fields: Theory and Applications

CONTEMPORARY MATHEMATICS

518

Finite Fields: Theory and Applications

Ninth International Conference
Finite Fields and Applications
July 13–17, 2009
Dublin, Ireland

Gary McGuire
Gary L. Mullen
Daniel Panario
Igor E. Shparlinski
Editors



American Mathematical Society
Providence, Rhode Island

Editorial Board

Dennis DeTurck, managing editor

George Andrews Abel Klein Martin J. Strauss

2000 *Mathematics Subject Classification*. Primary 11Gxx, 11Lxx, 11Txx, 14Gxx, 51Exx, 94Axx, 94Bxx.

Library of Congress Cataloging-in-Publication Data

International Conference on Finite Fields and Applications (9th : 2009 : Ireland, Dublin)

Finite fields : theory and applications : Ninth International Conference on Finite Fields and Applications, July 13–17, 2009, Dublin, Ireland / Gary McGuire ... [et al.], editors.

p. cm. — (Contemporary Mathematics ; v. 518)

Includes bibliographical references.

ISBN 978-0-8218-4786-2 (alk. paper)

1. Finite fields (Algebra)—Congresses. 2. Arithmetical algebraic geometry—Congresses. 3. Number theory—Congresses. 4. Coding theory—Congresses. I. McGuire, Gary. II. Title.

QA247.3.I57 2009
512'.3—dc22

2010008228

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.)

© 2010 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 15 14 13 12 11 10

Contents

Preface	vii
Construction of new toric quantum codes CLARICE DIAS ALBUQUERQUE, REGINALDO PALAZZO, JR., AND EDUARDO BRANDANI SILVA	1
On the calculation of the linear complexity of periodic sequences HASSAN ALY, RADWA MARZOUK, AND WILFRIED MEIDL	11
A few more functions that are not APN infinitely often YVES AUBRY, GARY MCGUIRE, AND FRANÇOIS RODIER	23
An APN permutation in dimension six K.A. BROWNING, J.F. DILLON, M.T. MCQUISTAN, AND A.J. WOLFE	33
CCZ-equivalence of single and multi output Boolean functions LILYA BUDAGHYAN AND CLAUDE CARLET	43
Structural weaknesses of permutations with a low differential uniformity and generalized crooked functions ANNE CANTEAUT AND MARÍA NAYA-PLASENCIA	55
Solvability of systems of polynomial equations with some prescribed monomials FRANCIS N. CASTRO AND IVELISSE M. RUBIO	73
Character sums in finite fields MEI-CHU CHANG	83
Monomial functions with linear structure and permutation polynomials PASCALE CHARPIN AND GOHAR M. KYUREGHYAN	99
Primitive elements on lines in extensions of finite fields STEPHEN D. COHEN	113
Commutative semifields of order 243 and 3125 ROBERT S. COULTER AND PAMELA KOSICK	129
Normal elliptic bases and torus-based cryptography CLÉMENT DUNAND AND REYNALD LERCIER	137
Unitary superperfect binary polynomials LUIS H. GALLARDO AND OLIVIER RAHAVANDRAINNY	155

Shift-invariant polynomials and Ritts Second Theorem JOACHIM VON ZUR GATHEN	161
Waring's problem in finite fields with Dickson polynomials DOMINGO GOMEZ AND ARNE WINTERHOF	185
Jacobi sums and irreducible polynomials with prescribed trace and restricted norm S. GURAK	193
A family of binary sequences from interleaved construction and their cryptographic properties JING JANE HE, DANIEL PANARIO, AND QIANG WANG	209
Sziklai's conjecture on the number of points of a plane curve over a finite field II MASAAKI HOMMA AND SEON JEONG KIM	225
Folded algebraic-geometric codes from Galois extensions MING-DEH HUANG AND ANAND KUMAR NARAYANAN	235
A multilinear generalization of the Tate pairing MING-DEH HUANG AND WAYNE RASKIND	255
The merit factor of binary sequence families constructed from m -sequences JONATHAN JEDWAB AND KAI-UWE SCHMIDT	265
Intractable problems in cryptography NEAL KOBLITZ AND ALFRED MENEZES	279
Modular curves and coding theory: A survey WEN-CHING W. LI	301
Minimal generating sets of Weierstrass semigroups of certain m -tuples on the norm-trace function field GRETCHEN L. MATTHEWS AND JUSTIN D. PEACHEY	315
On the zeta functions of an optimal tower of function fields over \mathbb{F}_4 GARY MCGUIRE AND ALEXEY ZAYTSEV	327
The asymptotic theory of algebraic-geometry codes HARALD NIEDERREITER	339
A spectrum result on maximal partial ovoids of the generalized quadrangle $\mathcal{Q}(4, q)$, q odd VALENTINA PEPE, CORNELIA RÖSSING, AND LEO STORME	349
Cyclic codes aspects of bent functions J. WOLFMANN	363

Preface

This volume contains the refereed proceedings of the Ninth International Conference on Finite Fields and Applications, held in Dublin, Ireland, July 13–17, 2009. The purpose of this conference was to bring together finite field researchers, theoretical, as well as applied. The Organizing Committee for the conference consisted of Simeon Ball, Lynn Batten, James Hirschfeld, Dieter Jungnickel, Gary McGuire (Chair), Gary Mullen, Daniel Panario, Alexander Pott and Igor Shparlinski. There were 6 invited presentations given by Mei-Chu Chang, Steve Cohen, John Dillon, Winnie Li, Alfred Menezes and Harald Niederreiter. The program also contained 80 contributed talks. The conference honoured the 65th birthdays of Steve Cohen and Harald Niederreiter.

The present volume includes invited survey papers by all invited speakers and also some selected contributed papers. All submitted papers were very strictly refereed (including those from the invited speakers who also received independent advice from their referees) and the accepted papers are published in this volume. Limited by the page restrictions, the Editors had a hard task of making the selection of papers for this volume. Unfortunately many worthy submissions have been rejected in favour of stronger more thematically suitable ones.

Because of applications in so many diverse areas, finite fields continue to grow in mathematical importance. In particular, they now play very important roles in number theory, algebra, and algebraic geometry, as well as in computer science, statistics, and engineering. Areas of application include, but certainly are not limited to, algebraic coding theory, cryptology, and combinatorial design theory. Computational and algorithmic aspects of finite field problems also continue to grow in importance. A further sign of this vitality is the publication in late 2005 of a special issue to celebrate the first decade of the related research journal *Finite Fields and Their Applications*.

We would like to take this opportunity to sincerely thank Elva O’Sullivan, project manager of the Claude Shannon Institute, for her many tireless efforts in seeing to all of the conference details. In addition, the conference had lots of help from several local postdocs and graduate students. We believe that everyone not only enjoyed the various talks and research discussions, but attendees also spoke highly of the organizational efforts. Special thanks are also due to Elsevier, the University College Dublin seed funding scheme, and Science Foundation Ireland through the Claude Shannon Institute, for their generous financial support. Finally, sincere thanks are due Christine Thivierge for her efforts and efficiency in helping us publish the conference proceedings volume in the American Mathematical Society series *Contemporary Mathematics*.

We are very grateful to the referees that ensured the high quality of the papers in this volume:

Omran Ahmadi, Peter Beelen, Herivelto Borges, Alice Devillers, Cunsheng Ding, Nicola Durante, Washiela Fish, Arnaldo Garcia, David Glynn, Faruk Gologlu, Robert Granger, Jaime Gutierrez, Heeralal Janwa, Selcuk Kavut, Jennifer Key, Eike Kiltz, Dae San Kim, Sergei Konyagin, Gohar Kyureghyan, Honggang Hu, Michel Lauvrauw, Winnie Li, Petr Lisonek, Hiren Maharaj, Ariane Masuda, Wilfried Meidl, Alina Ostafe, Anindya Patthak, Paul Pollack, Carl Pomerance, Bernhard Schmidt, Kai-Uwe Schmidt, Jamshid Shokrollahi, Alice Silverberg, Leo Storme, Fernando Torres, Elisabeth Uhlemann, Felipe Voloch, Qiang Wang, Kenneth Williams, Colin Wilmott, Arne Winterhof, Jacques Wolfmann, Chaoping Xing, Siman Yang.

Because of the success of this conference, frequently referred to as Fq 9, and its earlier incarnations, we are absolutely delighted to be able to report that Leo Storme (ls@cage.ugent.be) of the University of Ghent, Belgium, has agreed to host Fq 10 during the period July 11-15, 2011. We look forward to what we are sure will be a very successful conference. We hope to see you there!

Gary McGuire, Gary L. Mullen, Daniel Panario, Igor E. Shparlinski
February 2010

This volume contains the proceedings of the Ninth International Conference on Finite Fields and Applications, held in Ireland, July 13–17, 2009. It includes survey papers by all invited speakers as well as selected contributed papers.

Finite fields continue to grow in mathematical importance due to applications in many diverse areas. This volume contains a variety of results advancing the theory of finite fields and connections with, as well as impact on, various directions in number theory, algebra, and algebraic geometry. Areas of application include algebraic coding theory, cryptology, and combinatorial design theory.

ISBN 978-0-8218-4786-2



CONM/518

AMS on the Web
www.ams.org