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

http://dx.doi.org/10.1090/conm/518

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

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

Contents

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

9 780821 847862

CONM/518