Finite Fields: Theory, Applications, and Algorithms

Fourth International Conference on Finite Fields: Theory, Applications, and Algorithms
August 12-15, 1997
University of Waterloo, Waterloo, Ontario, Canada

Ronald C. Mullin
Gary L. Mullen
Editors
Selected Titles in This Series

225 Ronald C. Mullin and Gary L. Mullen, Editors, Finite fields: Theory, applications, and algorithms, 1999
224 Sang Geun Hahn, Hyo Chul Myung, and Efim Zelmanov, Editors, Recent progress in algebra, 1999
223 Bernard Chazelle, Jacob E. Goodman, and Richard Pollack, Editors, Advances in discrete and computational geometry, 1999
222 Kang-Taee Kim and Steven G. Krantz, Editors, Complex geometric analysis in Pohang, 1999
221 J. Robert Dorroh, Giséle Ruiz Goldstein, Jerome A. Goldstein, and Michael Mudi Tom, Editors, Applied analysis, 1999
220 Mark Mahowald and Stewart Priddy, Editors, Homotopy theory via algebraic geometry and group representations, 1998
219 Marc Henneaux, Joseph Krasil'shchik, and Alexandre Vinogradov, Editors, Secondary calculus and cohomological physics, 1998
218 Jan Mandel, Charbel Farhat, and Xiao-Chuan Cai, Editors, Domain decomposition methods 10, 1998
216 Akram Aldroubi and EnBing Lin, Editors, Wavelets, multiwavelets, and their applications, 1998
214 Lewis A. Coburn and Marc A. Rieffel, Editors, Perspectives on quantization, 1998
212 E. Ramirez de Arellano, N. Salinas, M. V. Shapiro, and N. L. Vasilevski, Editors, Operator theory for complex and hypercomplex analysis, 1998
211 Józef Dodziuk and Linda Keen, Editors, Lipa's legacy: Proceedings from the Bers Colloquium, 1997
210 V. Kumar Murty and Michel Waldschmidt, Editors, Number theory, 1998
209 Steven Cox and Irena Lasiecka, Editors, Optimization methods in partial differential equations, 1997
207 Yujiro Kawamata and Vyacheslav V. Shokurov, Editors, Birational algebraic geometry: A conference on algebraic geometry in memory of Wei-Liang Chow (1911–1995), 1997
206 Adam Korányi, Editor, Harmonic functions on trees and buildings, 1997
205 Paulo D. Cordaro and Howard Jacobowitz, Editors, Multidimensional complex analysis and partial differential equations: A collection of papers in honor of François Treves, 1997
204 Yair Censor and Simeon Reich, Editors, Recent developments in optimization theory and nonlinear analysis, 1997
203 Hanna Neencza and Jean-Pierre Bourguignon, Editors, Geometry and nature: In memory of W. K. Clifford, 1997
201 J. R. Quine and Peter Sarnak, Editors, Extremal Riemann surfaces, 1997

(Continued in the back of this publication)
Finite Fields:
Theory, Applications,
and Algorithms
This volume contains the refereed proceedings of the Fourth International Conference on Finite Fields: Theory, Applications and Algorithms held at the University of Waterloo, Waterloo, Ontario, Canada, August 12–15, 1997.
## Contents

Preface ix

Computing composed products of polynomials
  **Joel V. Brawley, Shuhong Gao, and Donald Mills** 1

Actions of linearized polynomials on the algebraic closure of a finite field
  **Stephen D. Cohen and Dirk Hachenberger** 17

On degree bounds for invariant rings of finite groups over finite fields
  **Peter Fleischmann and Wolfgang Lempken** 33

Irreducible polynomials of given forms
  **Shuhong Gao, Jason Howell, and Daniel Panario** 43

An application of Galois calculus to $F_q[t]$  
  **Yves Hellegouarch** 55

Composition behavior of sub-linearised polynomials over a finite field
  **Marie Henderson and Rex Matthews** 67

Kernels and defaults
  **Philippe Langevin and Patrick Solé** 77

Global function fields with many rational places and their applications
  **Harald Niederreiter and Chaoping Xing** 87

Traces of roots of unity over prime fields
  **Greg Stein** 113

The Fermat curve in characteristic $p$
  **Henning Stichtenoth** 123

Computing zeta functions over finite fields
  **Daqing Wan** 131

Cyclic alternant codes induced by an automorphism of a GRS code
  **Thierry P. Berger** 143

On Kerdock codes
  **Claude Carlet** 155

Permutation group of the $q$-ary image of some $q^m$-ary cyclic codes
  **Jérôme Lacan and Emmanuelle Delpeyroux** 165
<table>
<thead>
<tr>
<th>Title</th>
<th>Author(s)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The number of solutions to a system of equations and spectra of codes</td>
<td>Osnat Keren and Simon Litsyn</td>
<td>177</td>
</tr>
<tr>
<td>The LD probable prime test</td>
<td>Willi More</td>
<td>185</td>
</tr>
<tr>
<td>Carmichael numbers and Lucas tests</td>
<td>Siguna M. S. Müller</td>
<td>193</td>
</tr>
<tr>
<td>On the state complexity of some long codes</td>
<td>Tim Blackmore and Graham Norton</td>
<td>203</td>
</tr>
<tr>
<td>ID-based key distribution system over an elliptic curve</td>
<td>Hisao Sakazaki, Eiji Okamoto, and Masahiro Mambo</td>
<td>215</td>
</tr>
<tr>
<td>Symmetric sets of curves and combinatorial arrays</td>
<td>Ryoji Fuji-Hara and Satoshi Shinohara</td>
<td>225</td>
</tr>
<tr>
<td>Weight functions and the extension theorem for linear codes over finite rings</td>
<td>Jay A. Wood</td>
<td>231</td>
</tr>
</tbody>
</table>
Preface

This volume contains the refereed proceedings of the Fourth International Conference on Finite Fields: Theory, Applications, and Algorithms held at the University of Waterloo, August 12-15, 1997. The Organizing Committee consisted of I.F. Blake, R.C. Mullin, C.L. Stewart, S.A. Vanstone (all of the University of Waterloo), and S.D. Cohen, (University of Glasgow), G. L. Mullen, (The Pennsylvania State University), H. Niederreiter, (Austrian Academy of Sciences, Vienna).

Because of applications in so many diverse areas, finite fields continue to grow in importance in modern mathematics. 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.

We greatly acknowledge the very generous support of the conference by our sponsors, namely The University of Waterloo, The National Security Agency, The National Science Foundation, CERTICOM Corp., and the Institute for Combinatorics and its Applications. Without their support, we would not have been able to invite so many eminent researchers, or to partially support junior faculty members, postdocs and graduate students.

The purpose of the conference was to bring together workers in theoretical, applied, and algorithmic finite field theory. All papers in this volume have been refereed, and have been very loosely classified as theoretical and applied, and are listed alphabetically by contact author under these very general headings.

On behalf of all of the participants, we would like to thank the Faculty of Mathematics and the Department of Combinatorics and Optimization at the University of Waterloo for their hospitality and support. Special thanks are due to Kim Gingerich and Marg Feeney for their tireless efforts in attending to every detail of the conference.

We also express our thanks to the participants for a lively and successful conference. We would also like to thank the authors for contributing to this volume and the referees for their invaluable assistance. Thanks are also due to Barbara Baum and Frances Hannigan for their help in preparation of parts of this volume. We also express our appreciation to the American Mathematical Society for publishing this volume in their series Contemporary Mathematics, and in particular to Christine Thivierge (Amer. Math. Soc.) for her patience, care, and great assistance in the preparation of this volume.

Because of the success of this conference, frequently referred to as Fq4, and its earlier incarnations, we are delighted to report that Prof. D. Jungnickel of Augsburg
University, Augsberg, Germany, has agreed to host Fq5 on August 2–6, 1999. We look forward to what we are sure will be another very successful conference. We hope to see you there.

Gary L. Mullen
Ronald C. Mullin
Selected Titles in This Series

(Continued from the front of this publication)

198 Donald G. Saari and Zhigong Xia, Editors, Hamiltonian dynamics and celestial mechanics, 1996
197 J. E. Bonin, J. G. Oxley, and B. Servatius, Editors, Matroid theory, 1996
196 David Bao, Shing-shen Chern, and Zhongmin Shen, Editors, Finsler geometry, 1996
195 Warren Dicks and Enric Ventura, The group fixed by a family of injective endomorphisms of a free group, 1996
194 Seok-Jin Kang, Myung-Hwan Kim, and Insook Lee, Editors, Lie algebras and their representations, 1996
193 Chongying Dong and Geoffrey Mason, Editors, Moonshine, the Monster, and related topics, 1996
192 Tomek Bartoszyński and Marion Scheepers, Editors, Set theory, 1995
191 Tuong Ton-That, Kenneth I. Gross, Donald St. P. Richards, and Paul J. Sally, Jr., Editors, Representation theory and harmonic analysis, 1995
190 Mourad E. H. Ismail, M. Zuhair Nashed, Ahmed I. Zayed, and Ahmed F. Ghaleb, Editors, Mathematical analysis, wavelets, and signal processing, 1995
188 Alejandro Adem, R. James Milgram, and Douglas C. Ravenel, Editors, Homotopy theory and its applications, 1995
187 G. W. Brumfiel and H. M. Hilden, SL(2) representations of finitely presented groups, 1995
186 Shreeram S. Abhyankar, Walter Feit, Michael D. Fried, Yasutaka Ihara, and Helmut Voelklein, Editors, Recent developments in the inverse Galois problem, 1995
185 Raúl E. Curto, Ronald G. Douglas, Joel D. Pincus, and Norberto Salinas, Editors, Multivariable operator theory, 1995
183 William C. Connett, Marc-Olivier Gebuhrer, and Alan L. Schwartz, Editors, Applications of hypergroups and related measure algebras, 1995
182 Selman Akbulut, Editor, Real algebraic geometry and topology, 1995
181 Mila Cenkl and Haynes Miller, Editors, The Čech Centennial, 1995
180 David E. Keyes and Jinchao Xu, Editors, Domain decomposition methods in scientific and engineering computing, 1994
179 Yoshiaki Maeda, Hideki Omoro, and Alan Weinstein, Editors, Symplectic geometry and quantization, 1994
178 Hélène Barcelo and Gil Kalai, Editors, Jerusalem Combinatorics '93, 1994
177 Simon Gindikin, Roe Goodman, Frederick P. Greenleaf, and Paul J. Sally, Jr., Editors, Representation theory and analysis on homogeneous spaces, 1994
176 David Ballard, Foundational aspects of “non”standard mathematics, 1994
175 Paul J. Sally, Jr., Moshe Flato, James Lepowsky, Nicolai Reshetikhin, and Gregg J. Zuckerman, Editors, Mathematical aspects of conformal and topological field theories and quantum groups, 1994
174 Nancy Childress and John W. Jones, Editors, Arithmetic geometry, 1994
173 Robert Brooks, Carolyn Gordon, and Peter Perry, Editors, Geometry of the spectrum, 1994

(See the AMS catalog for earlier titles)