Finite Fields
and Applications

Springer-Verlag Berlin Heidelberg GmbH

Dieter Jungnickel
Harald Niederreiter
Editors

Finite Fields and Applications

Proceedings of The Fifth International Conference
on Finite Fields and Applications $\mathbf{F}_q5$,
held at the University of Augsburg, Germany,
August 2-6, 1999

Springer

Editors

Dieter Jungnickel
Lehrstuhl für Diskrete Mathematik,
Optimierung und Operations Research
Universität Augsburg
86135 Augsburg, Germany
e-mail: jungnickel@math.uni-augsburg.de

Harald Niederreiter
Department of Mathematics
National University of Singapore
2 Science Drive 2
Singapore 117543
Republic of Singapore
e-mail: nied@math.nus.edu.sg

Library of Congress Cataloging-in-Publication Data

International Conference on Finite Fields and Applications (5th : 1999 : University of Augsburg)
Finite fields and applications : proceedings of the Fifth International Conference on
Finite Fields and Applications Fq5, held at the University of Augsburg, Germany,
August 2-6, 1999 / Dieter Jungnickel, Harald Niederreiter, editors.
p. cm.
Includes bibliographical references.
ISBN 978-3-642-62498-8 ISBN 978-3-642-56755-1 (eBook)
DOI 10.1007/978-3-642-56755-1
1. Finite fields (Algebra)--Congresses. I. Jungnickel, D. (Dieter), 1952- II.
Niederreiter, Harald, 1944- III. Title.

QA247.3 .I57 1999
512'.3--dc21
00-054946

Mathematics Subject Classification (2000):
primary: 11Txx; secondary: 05-XX, 51Exx, 94Axx, 94Bxx

ISBN 978-3-642-62498-8

http://www.springer.de

Originally published by Springer-Verlag Berlin Heidelberg New York in 2001
Softcover reprint of the hardcover 1st edition 2001

Typeset by the authors using a Springer TEX macro package
Cover design: *design & production* GmbH, Heidelberg

SPIN: 10699437 46/3142LK - 5 4 3 2 1 0 – Printed on acid-free paper

Preface

This volume represents the refereed proceedings of the Fifth International Conference on Finite Fields and Applications ($\mathbf{F}_q5$) held at the University of Augsburg (Germany) from August 2–6, 1999, and hosted by the Department of Mathematics. The conference continued a series of biennial international conferences on finite fields, following earlier conferences at the University of Nevada at Las Vegas (USA) in August 1991 and August 1993, the University of Glasgow (Scotland) in July 1995, and the University of Waterloo (Canada) in August 1997. The Organizing Committee of $\mathbf{F}_q5$ comprised Thomas Beth (University of Karlsruhe), Stephen D. Cohen (University of Glasgow), Dieter Jungnickel (University of Augsburg, Chairman), Alfred Menezes (University of Waterloo), Gary L. Mullen (Pennsylvania State University), Ronald C. Mullin (University of Waterloo), Harald Niederreiter (Austrian Academy of Sciences), and Alexander Pott (University of Magdeburg).

The program of the conference consisted of four full days and one half day of sessions, with 11 invited plenary talks and over 80 contributed talks that required three parallel sessions. This documents the steadily increasing interest in finite fields and their applications. Finite fields have an inherently fascinating structure and they are important tools in discrete mathematics. Their applications range from combinatorial design theory, finite geometries, and algebraic geometry to coding theory, cryptology, and scientific computing. A particularly fruitful aspect is the interplay between theory and applications which has led to many new perspectives in research on finite fields. This interplay has always been a dominant theme in $\mathbf{F}_q$ conferences and was very much in evidence at $\mathbf{F}_q5$. Applied or applications-oriented topics accounted for well over half of the program.

These proceedings reflect the wide variety of topics represented at the conference. Most invited talks and a good proportion of the contributed talks are on permanent record here. All contributed talks were screened before the conference and all full papers were carefully refereed. We take this opportunity to thank the members of the Organizing Committee and all referees who helped in these tasks. These colleagues contributed enormously to the quality of the conference presentations and to guaranteeing high standards for these proceedings.

We greatly appreciate the generous financial support received for the conference. A major portion of the funds came from a grant by the German Research Council (DFG). Further sponsors were Andersen Consulting, Certicom Corp., Dresdner Bank AG, Gesellschaft der Freunde der Universität Augsburg, Hewlett Packard Laboratories, and Siemens AG. We are grateful to the University of Augsburg for providing excellent facilities for the conference and to the various officials of the City of Augsburg who helped with organizational questions. Thanks are also due to the Mayor of Augsburg who gave a reception for the participants in the splendid setting of the Great Golden Chamber of the city's renaissance town hall. Last but not least, the highly efficient and friendly manner in which the conference took place would not have been possible without the enthusiasm and hard work by the assistants, secretaries and students who saw to the many details involved in such a major event; we are grateful to all of them.

Regarding the present proceedings, we thank Dr. Martin Peters of Springer Verlag who gave us the opportunity to place this volume with a top publisher and in a form which we find both attractive and practical (no rapidly deteriorating soft covers for once!). The cooperation with him and all the staff at Springer Verlag was always a pleasure.

Finally, we are pleased to confirm that the series of $\mathbf{F}_q$ conferences will continue with $\mathbf{F}_q6$ in Mexico in May 2001. We expect another lively and stimulating conference there, which should, like the previous conferences, serve as an important marketplace of ideas for the finite fields community.

October 2000

Dieter Jungnickel
Harald Niederreiter

Contents

Projective Generalized Reed-Muller Codes over p-adic Numbers and Finite Rings 1
Kanat Abdukhalikov

Towards a Basis for the Space of Regular Functions in a Tower of Function Fields Meeting the Drinfeld-Vladut Bound 14
Ilia Aleshnikov, Vinay Deolalikar, P. Vijay Kumar, Henning Stichtenoth

Self–Dual Normal Bases and Related Topics 25
*Eva Bayer–Fluckiger**

Permutations amongst the Dembowski-Ostrom Polynomials 37
Aart Blokhuis, Robert S. Coulter, Marie Henderson, Christine M. O'Keefe

Associative Rational Functions in Two Variables 43
Joel V. Brawley, Shuhong Gao and Donald Mills*

A Note on the Minimal Polynomial of the Product of Linear Recurring Sequences 57
Emrah Çakçak

Gelfond-Gramain's Theorem for Function Fields 70
Mireille Car

On Generalized Bent and q-ary Perfect Nonlinear Functions 81
Claude Carlet, Sylvie Dubuc

Divisible Designs Admitting, as an Automorphism Group, an Orthogonal Group or a Unitary Group 95
Cinzia Cerroni, Ralph–Hardo Schulz

A Permutation of a Small Infinite Field 109
Stephen D. Cohen

Almost Perfect Nonlinear Power Functions on GF(2^n): A New Case for n Divisible by 5 113
Hans Dobbertin

On Non-Abelian Semi-Regular Relative Difference Sets 122
Dominic Elvira, Yutaka Hiramine

Applications of Arithmetical Geometry to Cryptographic Constructions 128
*Gerhard Frey**

Gauß Periods in Finite Fields 162
*Joachim von zur Gathen**, *Igor Shparlinski*

Constructions of Orthomorphisms of $\mathbb{Z}_2^n$ 178
Solomon W. Golomb, Guang Gong, Lothrop Mittenthal

Period Polynomials for F_{p^2} of Fixed Small Degree 196
Stanley Gurak

Universal Generators for Primary Closures of Galois Fields 208
*Dirk Hachenberger**

Irreducible Polynomials Generated by Decimations 224
Fritz von Haeseler and Wibke Jürgensen

Decoding Reed-Muller Codes beyond Half the Minimum Distance 232
Agnes E. Heydtmann, Thomas Jakobsen

On Binary Cyclic Codes With Few Weights 251
*Henk D. L. Hollmann, Qing Xiang**

MacWilliams Identities for Linear Codes over Finite Frobenius Rings .. 276
Thomas Honold, Ivan Landjev

Cyclotomic Function Fields with Many Rational Places 293
Alice Keller

On the Siamese Twin Designs 303
H. Kharaghani

On the Brauer Monoid for Finite Fields 313
Vladimir V. Kirichenko, Boris V. Novikov

Algorithms for Factoring Polynomials over Finite Fields 319
Tanja Lange, Arne Winterhof

Gauss Sums over Quasi-Frobenius Rings 329
Philippe Langevin, Patrick Solé

On the Early History of Galois Fields 341
*Heinz Lüneburg**

Linear Blocking Sets: a Survey 356
Guglielmo Lunardon, Olga Polverino

Comparison of Techniques on Divisibility Properties of Exponential Sums and Applications ... 363
*Oscar Moreno**, *Francis N. Castro*

On the Rank of Appearance and the Number of Zeros of the Lucas Sequences over $\mathbb{F}_q$ ... 390
Siguna Müller

A Permutation Problem for Finite Fields ... 409
Alan R. Prince

The L-Function of Gold Exponential Sum ... 418
Kenneth Shum, P. Vijay Kumar, Tor Helleseth

On Permutation Polynomials and Derivable Translation Planes ... 428
Rita Vincenti

Pure L-Functions from Algebraic Geometry over Finite Fields ... 437
*Daqing Wan**

Incomplete Additive Character Sums and Applications ... 462
Arne Winterhof

Applications of Algebraic Curves to Constructions of Codes and Almost Perfect Sequences ... 475
*Chaoping Xing**, *Harald Niederreiter*

Author Index ... 490

* invited speaker