Finite Fields with Applications to Coding Theory, Cryptography and Related Areas

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Gary L. Mullen
Henning Stichtenoth
Horacio Tapia-Recillas
Editors

Finite Fields with Applications to Coding Theory, Cryptography and Related Areas

Proceedings of the Sixth International Conference on Finite Fields and Applications, held at Oaxaca, México, May 21–25, 2001

Springer

Editors

Gary L. Mullen
The Pennsylvania State University
Department of Mathematics
16802 University Park, PA, USA
e-mail: mullen@math.psu.edu

Henning Stichtenoth
Universität Essen
FB6 Mathematik und Informatik
45117 Essen, Deutschland
e-mail: stichtenoth@uni-essen.de

Horacio Tapia-Recillas
Universidad Autónoma Metropolitana, México
Departamento de Matemáticas
Iztapalapa 09340
Av. San Rafael Atlixco 186
09340 México, D.F., México
e-mail: htr@xanum.uam.mx

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Finite fields with applications to coding theory, cryptography and related areas: proceedings of the Sixth International Conference on Finite Fields and Applications, held at Oaxaca, México, May 21–25, 2001 / Gary L. Mullen... ed. – Berlin; Heidelberg; New York; Hong Kong; London; Milan; Paris; Singapore; Tokyo: Springer, 2002
ISBN-13:978-3-642-63976-0 e-ISBN-13:978-3-642-59435-9
DOI: 10.1007/978-3-642-59435-9

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

ISBN-13:978-3-642-63976-0

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Softcover reprint of the hardcover 1st edition 2002

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

Printed on acid-free paper SPIN 10881880 46/3142hs – 5 4 3 2 1 0

Preface

This volume represents the refereed proceedings of the "**Sixth International Conference on Finite Fields and Applications** ($Fq6$)" held in the city of Oaxaca, México, between 22–26 May 2001. The conference was hosted by the Departmento do Matemáticas of the Universidad Autónoma Metropolitana-Iztapalapa, México. This event continued a series of biennial international conferences on Finite Fields and Applications, following earlier meetings at the University of Nevada at Las Vegas (USA) in August 1991 and August 1993, the University of Glasgow (Scotland) in July 1995, the University of Waterloo (Canada) in August 1997, and at the University of Augsburg (Germany) in August 1999. The Organizing Committee of $Fq6$ consisted of Dieter Jungnickel (University of Augsburg, Germany), Neal Koblitz (University of Washington, USA), Alfred Menezes (University of Waterloo, Canada), Gary Mullen (The Pennsylvania State University, USA), Harald Niederreiter (National University of Singapore, Singapore), Vera Pless (University of Illinois, USA), Carlos Rentería (IPN, México), Henning Stichtenoth (Essen University, Germany), and Horacio Tapia-Recillas, Chair (Universidad Autónoma Metropolitan-Iztapalapa, México).

The program of the conference consisted of four full days and one half day of sessions, with 7 invited plenary talks, close to 60 contributed talks, basic courses in finite fields, cryptography and coding theory and a series of lectures at local educational institutions.

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 been a dominant theme in earlier F_q conferences and was very much in evidence at $Fq6$. Applied or applications-oriented topics accounted for a significant part 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 would like to 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 fair portion of the funds were provided by a grant from the Consejo

Nacional de Ciencia y Tecnología (CONACYT), México and from various offices of the host institution. We also thank Universidad Benito Juárez de Oaxaca, Instituto Tecnológico de Oaxaca, Dirección General de Servicios do Cómputo Académico-UNAM, Instituto Politécnico Nacional, Sociedad Matemática Mexicana, Certicom Corp., Institute of Combinatorics and Applications, and Red de Criptología (CONACYT-UAM) for diverse kinds of support.

We are grateful to various offices of the state of Oaxaca who helped with additional funds and organizational issues. Thanks are also due to the Governor of the state of Oaxaca, who gave a reception for the participants in the splendid setting of the Centro Cultural Santo Domingo in the city of Oaxaca. 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 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 edit this volume with a top publisher and in an attractive form. Working with him and all the staff at Springer-Verlag is always a pleasure.

Finally, we are pleased to confirm that the *Fq* series will continue with *Fq*7 in Toulouse, France in May 2003. We expect another lively and stimulating meeting there, which should, like the previous conferences, serve as an important meeting place for theoretical as well as applied aspects of finite fields. We hope to see you there!

May 2002

Horacio Tapia-Recillas
Gary Mullen
Henning Stichtenoth

Contents