CONTEMPORARY MATHEMATICS

168

Finite Fields: Theory, Applications, and Algorithms

Second International Conference on Finite Fields:
Theory, Applications, and Algorithms
August 17–21, 1993
Las Vegas, Nevada

Gary L. Mullen
Peter Jau-Shyong Shiue
Editors

American Mathematical Society

CONTEMPORARY MATHEMATICS

168

Finite Fields: Theory, Applications, and Algorithms

Second International Conference on Finite Fields:
Theory, Applications, and Algorithms
August 17–21, 1993
Las Vegas, Nevada

Gary L. Mullen
Peter Jau-Shyong Shiue
Editors

American Mathematical Society
Providence, Rhode Island

This volume contains the refereed proceedings of the conference "Finite Fields: Theory, Applications, and Algorithms" which was held at the University of Nevada, Las Vegas, on August 17–21, 1993. This conference was supported in part by the National Security Agency, the National Science Foundation, and the University of Nevada, Las Vegas.

1991 *Mathematics Subject Classification.* Primary 11T02; Secondary 05B05, 11Y16, 94A60, 94B05.

Library of Congress Cataloging-in-Publication Data

International Conference on Finite Fields: Theory, Applications, and Algorithms (2nd: 1993: Las Vegas, Nev.)

Finite fields: theory, applications, and algorithms/Second International Conference on Finite Fields: Theory, Applications, and Algorithms, August 17–21, 1993, Las Vegas, Nevada; Gary L. Mullen, Peter Jau-Shyong Shiue, editors.

p. cm. — (Contemporary mathematics; 168)

Includes bibliographical references.

ISBN 0-8218-5183-7

1. Finite fields (Algebra)—Congresses. I. Mullen, Gary L. II. Shiue, Peter Jau-Shyong, 1941– . III. Title. IV. Series: Contemporary mathematics (American Mathematical Society); v. 168.

QA247.3.I58 1993

512′.3—dc20

94-19971

CIP

All articles in this volume were printed from copy prepared by the authors.
Some articles were typeset using AMS-TEX or AMS-LATEX,
the American Mathematical Society's TEX macro systems.

10 9 8 7 6 5 4 3 2 1 99 98 97 96 95 94

Recent Titles in This Series

168 **Gary L. Mullen and Peter Jau-Shyong Shiue, Editors,** Finite fields: Theory, applications, and algorithms, 1994

167 **Robert S. Doran, Editor,** C^*-Algebras: 1943–1993, 1994

166 **George E. Andrews, David M. Bressoud, and L. Alayne Parson, Editors,** The Rademacher legacy to mathematics, 1994

165 **Barry Mazur and Glenn Stevens, Editors,** p-adic monodromy and the Birch and Swinnerton-Dyer conjecture, 1994

164 **Cameron Gordon, Yoav Moriah, and Bronislaw Wajnryb, Editors,** Geometric topology, 1994

163 **Zhong-Ci Shi and Chung-Chun Yang, Editors,** Computational mathematics in China, 1994

162 **Ciro Ciliberto, E. Laura Livorni, and Andrew J. Sommese, Editors,** Classification of algebraic varieties, 1994

161 **Paul A. Schweitzer, S. J., Steven Hurder, Nathan Moreira dos Santos, and José Luis Arraut, Editors,** Differential topology, foliations, and group actions, 1994

160 **Niky Kamran and Peter J. Olver, Editors,** Lie algebras, cohomology, and new applications to quantum mechanics, 1994

159 **William J. Heinzer, Craig L. Huneke, and Judith D. Sally, Editors,** Commutative algebra: Syzygies, multiplicities, and birational algebra, 1994

158 **Eric M. Friedlander and Mark E. Mahowald, Editors,** Topology and representation theory, 1994

157 **Alfio Quarteroni, Jacques Periaux, Yuri A. Kuznetsov, and Olof B. Widlund, Editors,** Domain decomposition methods in science and engineering, 1994

156 **Steven R. Givant,** The structure of relation algebras generated by relativizations, 1994

155 **William B. Jacob, Tsit-Yuen Lam, and Robert O. Robson, Editors,** Recent advances in real algebraic geometry and quadratic forms, 1994

154 **Michael Eastwood, Joseph Wolf, and Roger Zierau, Editors,** The Penrose transform and analytic cohomology in representation theory, 1993

153 **Richard S. Elman, Murray M. Schacher, and V. S. Varadarajan, Editors,** Linear algebraic groups and their representations, 1993

152 **Christopher K. McCord, Editor,** Nielsen theory and dynamical systems, 1993

151 **Matatyahu Rubin,** The reconstruction of trees from their automorphism groups, 1993

150 **Carl-Friedrich Bödigheimer and Richard M. Hain, Editors,** Mapping class groups and moduli spaces of Riemann surfaces, 1993

149 **Harry Cohn, Editor,** Doeblin and modern probability, 1993

148 **Jeffrey Fox and Peter Haskell, Editors,** Index theory and operator algebras, 1993

147 **Neil Robertson and Paul Seymour, Editors,** Graph structure theory, 1993

146 **Martin C. Tangora, Editor,** Algebraic topology, 1993

145 **Jeffrey Adams, Rebecca Herb, Stephen Kudla, Jian-Shu Li, Ron Lipsman, and Jonathan Rosenberg, Editors,** Representation theory of groups and algebras, 1993

144 **Bor-Luh Lin and William B. Johnson, Editors,** Banach spaces, 1993

143 **Marvin Knopp and Mark Sheingorn, Editors,** A tribute to Emil Grosswald: Number theory and related analysis, 1993

142 **Chung-Chun Yang and Sheng Gong, Editors,** Several complex variables in China, 1993

141 **A. Y. Cheer and C. P. van Dam, Editors,** Fluid dynamics in biology, 1993

140 **Eric L. Grinberg, Editor,** Geometric analysis, 1992

139 **Vinay Deodhar, Editor,** Kazhdan-Lusztig theory and related topics, 1992

Finite Fields: Theory, Applications, and Algorithms

Preface

This volume contains the refereed proceedings of the conference "Finite Fields: Theory, Applications, and Algorithms" held at the University of Nevada, Las Vegas, August 17-21, 1993. The Organizing Committee consisted of Ernest Peck, William Wells, Peter Shiue, Daqing Wan, Laxmi Gewali (all of the University of Nevada, Las Vegas), and Gary L. Mullen (The Pennsylvania State University).

Because of applications in so many diverse areas, finite fields continue to play increasingly important roles in modern mathematics. In particular they now play very important roles in number theory, algebra, and algebraic geometry, as well as in computer science, information theory, statistics and engineering. Areas of application include, but are certainly 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 gratefully acknowledge the very generous support of the conference by both the National Security Agency and the National Science Foundation. Without their support we would not have been able to invite so many eminent researchers in the area. Even more importantly, we would not have been able to partially support so many junior faculty members, postdocs and graduate students. We are very grateful to both of the above agencies for their generous financial support. We also thank the Institute of Combinatorics and its Applications (ICA) for partial travel support for Scott Vanstone, the ICA invited speaker.

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 rather than listing papers by areas, we have simply listed them in alphabetical order by author. These proceedings also contain a list of all conference participants and speakers and, in addition, a list of open problems and conjectures designed to stimulate further research in both theoretical and applied aspects of finite fields.

On behalf of all participants, we would like to thank the College of Science and Mathematics, the Howard R. Hughes College of Engineering, the University Office of Research, and the Department of Mathematical Sciences at the University of Nevada, Las Vegas, for their hospitality and support. Special thanks are

due Donna Fraser, Margie Wells and Debra Duddlesten for their tireless efforts in seeing to every detail, large or small.

We also express our thanks to the participants for a lively and successful conference. Many outstanding talks were presented. We would also like to thank the authors for contributing to this volume and the referees for their invaluable assistance. Thanks are also due Pat Snare and Donna Fraser for their help in preparation of parts of this volume. Last but certainly not least, we would like to express our appreciation to the American Mathematical Society for publishing this volume in their series Contemporary Mathematics, and in particular to Donna Harmon (Amer. Math. Soc.) for her patience, care, and help in the preparation of this volume.

Because of the success of this conference, often referred to as Fq II, we are delighted to be able to report that the University of Glasgow, Glasgow, Scotland, has agreed to host Fq III during the second week of July, 1995. We look forward to what we are sure will be another very successful conference. We hope to see you there.

Gary L. Mullen
Peter Jau-Shyong Shiue

Contributors

The following contributors presented talks. In the case of more than one author, an asterisk (*) indicates the presenter.

MARIA T. ACOSTA-DE-OROZCO* and JAVIER GOMEZ-CALDERON, "Local Minimal Polynomials Over Finite Fields"

OSCAR MORENO, ALBERTO CÁCERES and MAYRA ALONSO*, "A Necessary and Sufficient Theorem of Chevalley-Warning Type"

YVES AUBRY, "Weil's Inequality for Singular Curves"

YVES AUBRY* and MARC PERRET, "Coverings of Singular Curves Over Finite Fields"

JEFF BONN, "On Greedy Codes"

OSCAR MORENO, FRANCIS CASTRO, and ALBERTO CÁCERES*, "Constructive Bounds on Character Sums and the Minimum Distances of Codes"

C.-Y. CHAO, "Polynomials Over Finite Fields Which Commute With a Given Polynomial"

PASCALE CHARPIN, "On Some Cosets of Some Binary Primitive Cyclic Codes"

XUEMIN CHEN*, I.S. REED, T. HELLESETH, and T.K. TRUONG, "Algebraic Decoding of Binary Cyclic Codes: A Polynomial Ideal Point of View"

ZESEN CHEN, "Constructing Error Correcting Codes Using Drinfeld Modules"

ZHIBO CHEN, "Permutation-Type Formulas of the Frobenius Map and Their Applications"

WUN-SENG CHOU, "On Inversive Maximal Period Polynomials Over Finite Fields"

JAMES R. CLAY, "The Sum of the Angles of a Triangle is 180°"

STEPHEN D. COHEN, "Polynomial Factorization, Graphs and Designs"

ED DAWSON* and DIANE DONOVAN, "A Discussion of an Authentication Scheme Based on Latin Squares"

ANGELA ISABEL BARBERO DIEZ, "An Algorithm for Characterizing Linear Product Codes"

JOHN F. DILLON, "Designs From Finite Fields"

STEPHEN A. DIPIPPO, "Spaces of Rational Functions on Curves Over Finite Fields"

GOVE EFFINGER, "Some Numerical Implications of Additive Number Theory of Polynomials Over a Finite Field"

RON EVANS, "Orthogonal Character Sums Diagonalizing Adjacency Operators of Cayley Graphs"

HENRI FAURE, "The Problem of Lower Bounds for the Discrepancy of Special Sequences"

MIKE FRIED, "Carlitz's Conjecture and General Exceptional Covers"

RYOH FUJI-HARA, "An Implementation of Finite Fields to a Symbolic Computational Language"

SHU TEZUKA and MASANORI FUSHIMI*, "A Method of Designing Cellular Automata as Pseudorandom Number Generators for Built-in Self-test for VLSI"

SHUHONG GAO, "Specific Irreducible Polynomials with Linearly Independent Roots Over Finite Fields"

JOACHIM VON ZUR GATHEN, "Factoring Polynomials Over Finite Fields"

HEMAR GODINHO, "Additive Forms of degree 2^l"

SEUNG-CHEOL GOH* and DAI-KI LEE, "A New Pseudo Random Permutation Generator"

RAINER GÖTTFERT* and HARALD NIEDERREITER, "Hasse-Teichmüller Derivatives and Products of Linear Recurring Sequences"

STAN GURAK, "Factors of Period Polynomials for Finite Fields, II"

DAVID R. HAYES, "Additive Number Theory in $F_q[T]$"

NOBORU HAMADA and TOR HELLESETH*, "A Characterization of Some Ternary Codes Meeting the Griesmer Bound"

MARIE HENDERSON* and REX MATTHEWS, "Permutation Behaviour of Chebyshev Polynomials of the Second Kind Over a Finite Field"

J.W.P. HIRSCHFELD, "Projective Geometry Codes"

KLAUS HUBER, "Codes Over Eisenstein-Jacobi Integers"

JUN IMAI, "Coding Theory and Galois Representations"

JØRN M. JENSEN, "Q-ary Image of a Class of Constacyclic Codes"

GREGORY KABATIANSKII, "On Applications of the Bose-Chowla Theorem to Coding Theory and Cryptography"

JIDING KANG, "A Relation Between M_3 and Linear Congruences"

WEN-FONG KE and HUBERT KIECHLE*, "On the Solutions of the Equation $x^m + y^m - z^m = 1$ in a Finite Field"

NEAL KOBLITZ, "Varieties Over Finite Fields and Combinatorially Based Cryptography"

JOHN J. KOMO* and SHYH-CHANG LIU, "Crosscorrelation of Frequency Hopping M-Sequences"

ARNOLD KNOPFMACHER, "Ordered and Unordered Factorizations of Polynomials Over Finite Fields"

JINGHUA KUANG, "Unitary Representations and Weil Representation of $Sp(n)$ Over Finite Fields"

PHILIPPE LANGEVIN, "Some Sequences"

DAVID LEEP, "Pairs of Quadratic Forms Over Finite Fields"

JOSEPH J. LIANG* and JUNG-FANG SUN, "On the Polynomial $x^{q^4+q^3+\cdots+1} - ax^{q^3+q^2+q+1} - bx^{q^2+q+1} - cx^{q+1} - dx - e$ Over a Finite Field"

CANTIAN LIN* and PETER JAU-SHYONG SHIUE, "Some New Classes of Periodic Complementary Binary Sequences"

HONGWEN LU, "The Pellian Equation Conjecture and Absolutely Nonsingular Projective Varieties Over Finite Fields"

RUDOLF LIDL and REX MATTHEWS*, "Strong Pseudoprimes and Generalised Carmichael Numbers"

ROBERT M. MCCONNEL, "Permutation Polynomials on a Finite Field"

HEERALAL JANWA, GARY M. MCGUIRE*, and RICHARD M. WILSON, "On the Absolute Irreducibility of Polynomials Over Finite Fields"

ATSUKO MIYAJI, "Isogenous Elliptic Curve Cryptosystems"

LAURA MONROE, "Greedy Codes Over Fields of Order 2**(2**a)"

OSCAR MORENO, "Technology Transfer from Communication Science to Mathematics"

ILENE H. MORGAN, "A New Definition of Orthogonality for Frequency Hypercubes and Its Connection to Finite Fields and Hadamard Matrices"

PETER MÜLLER, "Exceptional Indecomposable Polynomials with Non-Affine Monodromy Groups"

JOHANNES BUCHMANN and VOLKER MÜLLER*, "Parallel Algorithms for Matrices - Practical Experiences"

KENJI NAGASAKA*, MITSUO FUSE, and WUN-SENG CHOU, "The Computational Complexity of Exact Computation by a Matrix Method"

HIROSHI NAGASE*, HIROSHI SUZUKI, MASAYOSHI KAJI, and MASARU KAKUMA, "Toward a Finite Field Computer - Theory and Its Applications"

HARALD NIEDERREITER, "Deterministic Factorization Algorithms for Polynomials Over Finite Fields"

ANDREW ODLYZKO, "Discrete Logarithms and Smooth Polynomials"

HONG G. PARK, "P-Groups in the Betti-Mathieu Group"

VERA PLESS, "Parents, Children, Neighbors and the Shadow"

A. POLI* and E. WEN, "Construction of Self Complementary Normal Bases"

BART PRENEEL, "A Spectral Characterization of Propagation Criteria"

PABLO M. SALZBERG* and PETER JAU-SHYONG SHIUE, "A Family of Cryptosystems Based on Combinatorial Properties of Finite Geometries"

ALFRED SCHEERHORN, "Iterated Construction of Normal Bases Over Finite Fields"

LAWRENCE SOMER, "Periodicity Properties of kth Order Linear Recurrences Whose Characteristic Polynomial Splits Completely Over a Finite Field, I"

HONG Y. SONG* and SOLOMON W. GOLOMB, "Generalized Welch-Costas Sequences"

MARK STAMP* and CLYDE F. MARTIN, "A New Derivation of the Chan-Games Algorithm"

STEPHAN J. SUCHOWER, "Nonisomorphic Complete Sets of F-rectangles with Prime Power Dimensions"

JOHAN VAN TILBURG, "On the Non-Existence of Digital Signature Schemes Based on Maximum Likelihood Decoding"

VLADIMIR TONCHEV, "Quasi-symmetric Designs, Codes, Quadrics, and Hyperplane Sections"

CYNTHIA E. TRIMBLE, "Finite Field Sums from p-adic K-Bessel Functions"

GERHARD TURNWALD, "A New Criterion for Permutation Polynomials"

SCOTT VANSTONE, "The Knapsack Problem in Cryptography"

ANTONIO VANTAGGIATO, "A Model For Finite Fields: Computational Issues and Applications"

DAQING WAN, "L-functions of p-adic Representations"

JACQUES WOLFMANN, "New Results on Diagonal Equations Over Finite Fields from Cyclic Codes"

E.A. YFANTIS*, F.S. MAKRI, and P.J.-S. SHIUE, "An Algorithm for Generating Uniform Random Numbers With Large Periodicities"

PAUL THOMAS YOUNG, "On the Gross-Koblitz Formula"

JIE-TAI YU, "An Iterative Algorithm of SLSR For Mutiple Sequences With Different Lengths"

JING YU, "On Class Groups of Function Fields"

OSCAR MORENO and VICTOR A. ZINOVIEV*, "Transformations of 4-regular Graphs and Equations of Chevalley-Warning Type"

Conference Participants

The following is a list of all participants registered for the conference.

Justo Abia
Paseo Del Cauce Sin
47011 Valladolid
Valladolid, SPAIN

Maria T. Acosta-De-Orozco
Department of Mathematics
Southwest Texas State University
601 University Drive
San Marcos, TX 78666-4616
e-mail: ma05@swtexas.bitnet

Mayra Alonso
Department of Natural Science
Sacred Heart University
P.O. Box 12383 Loiza Station
Santurce, PUERTO RICO 00914

Malwane M.A. Ananda
Department of Mathematical Sciences
University of Nevada, Las Vega
Las Vegas, NV 89154
e-mail: ananda@nevada.edu

Jeff Angel
Department of Mathematics, 0112
University of California at San Diego
La Jolla, CA 92093
e-mail: jangle@euclid.ucsd.edu

Guillermo E. Atkin
Illinois Institute of Technology
ECE Dept.
3301 S. Dearborn
Chicago, IL 60616

Yves Aubry
Laboratoire de Mathématiques
Discrétes du C.N.R.S.
Luminy Case 930-13288
Marseille Cedex 9
FRANCE
e-mail: aubry@lmd.univ-mrs.fr

Jacob Beard
Mathematics Department
Tennessee Technological University
Box 5132
Cookeville, TN 38505

Clark Benson
8404 Timberland Circle
Ellicott City, MD 21043

Gene Berg
National Security Agency
D5, Building OP5-2A
Fort Meade, MD 20755-6000

Lanner Bernhard
Neubruweg 1
9061 Wofnitz, AUSTRIA

Barbara Blythin
Department of Mathematical Sciences
University of Nevada, Las Vegas
Las Vegas, NV 89154

Michael Boehm
Bunderamt fuer Sicherheit in der
Informationstechnik
Godesberger Allec 183
Postfach 200363
W 5300 Bonn, GERMANY

Jeff Bonn
Department of Mathematics
Southern Illinois University
Carbondale, IL 62901
e-mail: bonnj@siucvmb.siu.edu

Antoon Bosselaers
ESAT/Katholifke Universiteit Leuven
K. Mercierlaan 94
B-3001 Heverlee
BELGIUM

Harold Bowman
Department of Mathematical Science
University of Nevada, Las Vegas
Las Vegas, NV 89154

Joel Brawley
Department of Mathematical Sciences
Clemson University
Clemson, SC 29631
e-mail: jvbrw@clemson.bitnet

Priscilla Bremser
Dept. of Mathematics
& Computer Science
Middlebury College
Middlebury, VT 05753

Tom Brown
Department of Mathematics/Statistics
Simon Fraser University
Burnaby, CANADA V5 A1 S6
e-mail: tbrown@sfu.ca

Alberto Cáceres
University of Puerto Rico-Humacao
Math. Dept., CUH Station
Humacao, PUERTO RICO 00791
e-mail: a-caceres@cuhac.upr.clu.edu

C.Y. Chao
Department of Mathematics
and Statistics
University of Pittsburgh
Pittsburgh, PA 15260

Pascale Charpin
INRIA, Domaine de Voluceau
Rocquencourt, BP 105, 78153
Le Chesnay Cedex
FRANCE
email: charpin@hecate.inria.fr

Ching-Shyang Chen
Department of Mathematical Sciences
University of Nevada, Las Vegas
Las Vegas, NV 89154

Xuemin Chen
Department of Electrical Engineering
University of Southern California
Los Angeles, CA 90089-2565
e-mail: xchen@zsazsa.ucs.edu

Zesen Chen
Department of Mathematics
University of Massachusetts
at Amherst
Amherst, MA 01003
e-mail: chen@math.umass.edu

Zhibo Chen
Department of Mathematics
Pennsylvania State University
McKeesport, PA 15132
e-mail: zxc4@psuvm.psu.edu

Wun-Seng Chou
Institute of Mathematics
Academia Sinica
Nankang
Taipei 11529, Taiwan
REPUBLIC OF CHINA
e-mail: macws@twnas886.bitnet

James Clay
Department of Mathematics
University of Arizona
Tucson, AZ 85721

Stephen Cohen
Department of Mathematics
University of Glasgow
Glasgow G12 8QW
SCOTLAND
e-mail: gamx02@cms.gla.ac.uk

Maria Contessa
Mathematics Department
Brandeis University
Waltham, MA 02254-9110

Scott Contini
Mathematics Department
University of Wisconsin, Milwaukee
Milwaukee, WI 53201

David Costa
Department of Mathematical Sciences
University of Nevada, Las Vegas
Las Vegas, NV 89154
e-mail: costa@nevada.edu

Rohan Dalpatadu
Department of Mathematical Sciences
University of Nevada, Las Vegas
Las Vegas, NV 89154

Ed Dawson
Info. Security Research Centre
Queensland University of Technology
GPO Box 2434
Brisbane Queensland 4001
AUSTRALIA

Angela Isabel Barbero Díez
Departmento de Matematica
Aplicada a la Ingenieria
E.T.S. de Ingenieros Industriales
Universidad de Valladolid
Paseo del Cance s/n
E-47011 Valladolid, SPAIN
e-mail: abarbero@cpd.uva.es

Whitfield Diffie
Sun Microsystems, MTV14-203
2550 Garcia Ave.
Mountain View, CA 94043
e-mail: diffie@eng.sun.com

John Dillon
National Security Agency
Fort George G. Meade, MD 20755-6000

Stephen A. DiPippo
2 Holyoke Street #41
Cambridge, MA 02138

Derrick DuBose
Department of Mathematical Sciences
University of Nevada, Las Vegas
Las Vegas, NV 89154
e-mail: dubose@nevada.edu

Gove Effinger
Department of Mathematics
Skidmore College
Saratoga Springs, NY 12866

Ronald Evans
Math. Department C-010
University of California, San Diego
LaJolla, CA 92093
e-mail: revans@euclid.ucsd.edu

Henri Faure
Universite of Marseille
1331 Marseille Cedex 3
FRANCE
e-mail: faure@gyptis.univ-mrs.fr

Birger Faxen
Foersvarets Radioanstalt
Foer Utbetalningar
S-16126 Bromma, SWEDEN

Claes Fernstrom
Foersvarets Radioanstalt
Foer Utbetalningar
S-16126 Bromma, SWEDEN

John Flynn
Department of Mathematics
University of California, Berkeley
Berkeley, CA 94720
e-mail: flynn@math.berkeley.edu

Michael Fried
Department of Mathematics
University of California at Irvine
Irvine, CA 92717
e-mail: mfried@math.uci.edu

Ryoh Fuji-Hara
Institute of Socio-Economic Planning
University of Tsukuba
Tsukuba, Ibaraki
JAPAN
e-mail: fujihara@shako.sk

Masanori Fushimi
Dept. of Math. Eng. & Inf. Physics
Faculty of Engineering
University of Tokyo
7-3-1 Hongo, Bunkyo-ku
Tokyo 113, JAPAN
e-mail: fushimi@misojiro.u-tokyo.ac.jp

Shuhong Gao
Department of Combinatorics
& Optimization
University of Waterloo
Waterloo, Ontario
CANADA N2L 3G1
e-mail: sgao@violet.uwaterloo.ca

Eric Garrido
Thomson Company
66 Rue du Fosse Blanc
Gennevilliers, 92231
FRANCE

Joachim von zur Gathen
Department of Computer Science
University of Toronto
Toronto, Ontario M5S 1A4
CANADA
e-mail: gathen@cs.toronto.edu

Laxmi Gewali
Department of Computer Science
University of Nevada, Las Vegas
Las Vegas, NV 89154

Hemar Godinho
Departmento de Matematica
Universidade de Brasilia
Brasilia, DF, BRAZIL 70-910
e-mail: hemar@brunb.bitnet
@vtvm2.cc.vt.edu

Seung-Cheol Goh
Electronics and Telecommunications
Research Institute
P.O. Box 8, DaeDuk Science Town
Daejeon, 305-606
SOUTH KOREA
e-mail: codel@etrivax.etri.re.kr

Javier Gomez-Calderon
Pennsylvania State University
3550 Seventh Street Road
New Kensington, PA 15068-1798

Rainer Göttfert
Austrian Academy of Sciences
Institute for Information Processing
Sonnenfelsgasse 19
A-1010 Vienna, AUSTRIA

John Greene
Department of Math. & Stat.
University of Minnesota, Duluth
Duluth, MN 55812
e-mail: jgreen@ucd.um.edu

Stan Gurak
Dept. of Mathematics & Comp. Sci.
University of San Diego
5998 Alcalá Park
San Diego, CA 92110-2492
e-mail: gurak@uscdcsv.cusd.edu

Kaj Schmidt Hansen
Danish Defense Staff
Kastellet 30
DK-2100 Kobenhavno
DENMARK
e-mail: imai@cslab.kecl.ntt.jp

David Hayes
Dept. of Mathematics & Statistics
University of Massachusetts
Amherst, MA 01003

Tor Helleseth
Department of Informatics
University of Bergen
Hoyteknologisenteret
N-5020 Bergen, NORWAY

Rose-Marie Henderson
Department of Computer Science
University of Queensland
Brisbane 4072
AUSTRALIA

J.W.P. Hirschfeld
School of Mathematical & Physical
Sciences
University of Sussex
Palmer, Brighton BN1 9QH
United Kingdom
e-mail: mmfd4@central.sussex.ac.uk

Klaus Huber
Deutsche Bundespost Telekom
Research Institute
P.O. Box 100003
Darmstadt 64276
GERMANY
e-mail: fi17d@vm.xa.fz.telekom.de

Jun Imai
NTT Communication
Science Laboratories
2-2, Mikaridai, Seika-cho, Soraku-gun
Kyoto G19-02
JAPAN

Jorn M. Jensen
Mathematical Institute, Blg. 303
The Technical University of Denmark
DK-2800 Lyngby
DENMARK