

CONTEMPORARY MATHEMATICS

523

Error-Correcting Codes, Finite Geometries and Cryptography

Conference on
Error-Control Codes, Information Theory
and Applied Cryptography
December 5–6, 2007
Fields Institute, Toronto, Ontario, Canada

Canadian Mathematical Society Special Session
Error Control Codes, Information Theory
and Applied Cryptography
CMS Winter Meeting
December 8–10, 2007
London, Ontario, Canada

Aiden A. Bruen, David L. Wehlau
Editors



Error-Correcting Codes, Finite Geometries and Cryptography

CONTEMPORARY MATHEMATICS

523

Error-Correcting Codes, Finite Geometries and Cryptography

Conference on
Error-Control Codes, Information Theory
and Applied Cryptography
December 5–6, 2007
Fields Institute, Toronto, Ontario, Canada

Canadian Mathematical Society Special Session
Error Control Codes, Information Theory
and Applied Cryptography
CMS Winter Meeting
December 8–10, 2007
London, Ontario, Canada

Aiden A. Bruen, David L. Wehlau
Editors



American Mathematical Society
Providence, Rhode Island

Editorial Board

Dennis DeTurck, managing editor

George Andrews Abel Klein Martin J. Strauss

This volume contains the proceedings of two conferences on Error-control Codes, Information Theory and Applied Cryptography. The first was held at the Fields Institute, Toronto, ON, Canada, from December 5–6, 2007, and the second was a Canadian Mathematical Society Special Session at the CMS Winter Meeting, London, ON, Canada, from December 8–10, 2007.

2000 *Mathematics Subject Classification*. Primary 05B25, 94B05, 94A60, 94B25, 05B15, 51E14, 81P94, 68W35, 94B35, 94A05.

Library of Congress Cataloging-in-Publication Data

Conference on Error-control Codes, Information Theory, and Applied Cryptography (2007 : Toronto, Ont.)

Error-correcting codes, finite geometries, and cryptography : Conference on Error-control Codes, Information Theory, and Applied Cryptography, December 5–6, 2007, Fields Institute, Toronto, Ontario, Canada : Canadian Mathematical Society Special Session on Error Control Codes, Information Theory, and Applied Cryptography, Dec. 8–10, 2007, CMS Winter Meeting, London, Ontario, Canada / Aiden A. Bruen, David L. Wehlau, editors.

p. cm. — (Contemporary mathematics ; v. 523)

Includes bibliographical references.

ISBN 978-0-8218-4956-9 (alk. paper)

1. Computer security—Congresses. 2. Cryptography—Congresses. I. Bruen, Aiden A., 1941– II. Wehlau, David L., 1960– III. Canadian Mathematical Society. Special Session on Error Control Codes, Information Theory, and Applied Cryptography (2007 : London, Ont.) IV. Title.

QA76.9.A25C6675 2007
005.8—dc22

2010013261

Copying and reprinting. Material in this book may be reproduced by any means for educational and scientific purposes without fee or permission with the exception of reproduction by services that collect fees for delivery of documents and provided that the customary acknowledgment of the source is given. This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to reprint-permission@ams.org.

Excluded from these provisions is material in articles for which the author holds copyright. In such cases, requests for permission to use or reprint should be addressed directly to the author(s). (Copyright ownership is indicated in the notice in the lower right-hand corner of the first page of each article.)

© 2010 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights
except those granted to the United States Government.

Copyright of individual articles may revert to the public domain 28 years
after publication. Contact the AMS for copyright status of individual articles.

Printed in the United States of America.

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.

Visit the AMS home page at <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 15 14 13 12 11 10

Contents

Cryptography

Heterogeneous Hash Families and Covering Arrays CHARLES J. COLBOURN and JOSE TORRES-JIMENEZ	3
Resilient Functions: Just How Resilient Are They? WILLIAM J. MARTIN and BERK SUNAR	17
Quantum Coins MICHELE MOSCA and DOUGLAS STEBILA	35
Optimal Block Lengths for Secret Key Distillation JOSEPH R. OLDFORD and DAVID L. WEHLAU	49

Finite Geometries

Hyperconics and Multiple Weight Codes for OCDMA T. L. ALDERSON	67
Blocking Sets and Large Transversal-Free Systems of Mutually Orthogonal Latin Squares AIDEN A. BRUEN	77
Incidence Matrices with Forbidden Configurations AIDEN A. BRUEN, TREVOR C. BRUEN, and ROBERT SILVERMAN	83
A New Method to Construct Maximal Partial Spreads of Smallest Size in $PG(3, q)$ MAURIZIO IURLO and SANDRO RAJOLA	89
A Representation of the Projective Space $P(r, k)$ on the Affine Plane $A(2, k)$ and the Geometric Equivalence between the Veblen Configuration in $P(3, k)$ and the Desargues Configuration in $A(2, k)$ MARIA SCAFATI TALLINI	109
André Embeddings of Affine Planes J. A THAS and H. VAN MALDEGHEM	123

Codes

Near MDS Poset Codes and Distributions ALEXANDER BARG and PUNARBASU PURKAYASTHA	135
--	-----

Geometric Constructions of Quantum Codes JÜRGEN BIERBRAUER, D. BARTOLI, S. MARCUGINI, and F. PAMBIANCO	149
An Exact Analytical-Expression for the Read Sensor Signal in Magnetic Data Storage Channels A. BOGATYREV, M. HASSNER, and D. YARMOLICH	155
Blocking Sets and Low-Weight Codewords in the Generalized Reed-Muller Codes AIDEN A. BRUEN	161
Low-Power LDPC Decoding by Exploiting the Fault-Tolerance of the Sum-Product Algorithm VINCENT C. GAUDET	165
On Perfect Codes over Non Prime Power Alphabets OLOF HEDEN	173
Linear Codes from Projective Spaces MICHEL LAVRAUW, LEO STORME, and GEERTRUI VAN DE VOORDE	185
The Dimension of the Code of a Strongly Resolvable Design T. P. MCDONOUGH and V. C. MAVRON	203
Codes of Nets and Projective Planes G. ERIC MOORHOUSE	207
Minimum Output Symbol Error Variance of Forward Error Control Codes CHRISTIAN SCHLEGEL	217
Multi-Stream Information Transmission in Random Power Attenuation Environments DMITRI TRUHACHEV and MANDANA RAHBARI	227

Preface

In December 2007 two back-to-back interdisciplinary conferences on Error Correcting Codes, Information Theory and Applied Cryptography took place. The first one was held at the Fields Institute in Toronto. The follow-up was in the format of a “Special Session” at the Winter Meeting of the Canadian Mathematical Society in London, Ontario. The organizers, in each case, were the Editors of this Volume. The Editors were very pleased by the large number of distinguished participants from several countries who journeyed to Ontario for these conferences. We were also gratified by the high quality of the results that were presented. This Volume is an outgrowth of the two meetings. It features contributions both from participants and from authors who, for one reason or another, had not been able to attend. The interdisciplinary nature can best be understood from a perusal of the table of contents. The papers are split within the areas of Cryptography, Finite Geometries and Error-Control Codes. Several of the papers could easily fit in two, or even all three, of these categories. It becomes ever more difficult to affect a separation of the areas. In fact we are convinced that the future of the three areas lies in an interdisciplinary approach and in a common treatment wherever possible.

The Cryptography section features papers in “classical” topics such as hash functions, privacy amplification and key distribution as well as the latest on “Quantum Coins”. In Finite Geometries there are contributions about nets, partial spreads, geometric incidence matrices, Andre embeddings along with geometric configurations, planar representations, partial spreads and families of mutually orthogonal latin squares.

The largest section deals with codes in one form or another. The hardy perennials of MDS codes, such as Reed-Solomon and LDPC codes are well represented as well as perfect codes, orthogonal codes and quantum codes. There is a paper on classical linear codes and their duals. The p -ranks for designs are studied. In communication theory we have papers on iterative and concatenated codes and on communications over a random-access channel. Another paper deals with recent work on very applied topics relating to magnetic data-storage systems

We would be remiss were we not to acknowledge the gracious hospitality of the Fields Institute and Massey College in the University of Toronto. We also thank Professor Carl Riehm of the Fields Institute together with Gertrud Jeewanjee and the staff at the Canadian Mathematical Society.

Aiden A Bruen, University of Calgary

David L. Wehlau, Royal Military College of Canada
February 2010

Titles in This Series

- 528 **Alberto Farina and Enrico Valdinoci, Editors**, Symmetry for elliptic PDEs, 2010
- 527 **Ricardo Castaño-Bernard, Yan Soibelman, and Ilia Zharkov, Editors**, Mirror symmetry and tropical geometry, 2010
- 526 **Helge Holden and Kenneth H. Karlsen, Editors**, Nonlinear partial differential equations and hyperbolic wave phenomena, 2010
- 525 **Manuel D. Contreras and Santiago Díaz-Madrigal, Editors**, Five lectures in complex analysis, 2010
- 524 **Mark L. Lewis, Gabriel Navarro, Donald S. Passman, and Thomas R. Wolf, Editors**, Character theory of finite groups, 2010
- 523 **Aiden A. Bruen and David L. Wehlau, Editors**, Error-correcting codes, finite geometries and cryptography, 2010
- 522 **Oscar García-Prada, Peter E. Newstead, Luis Álvarez-Cónsul, Indranil Biswas, Steven B. Bradlow, and Tomás L. Gómez, Editors**, Vector bundles and complex geometry, 2010
- 521 **David Kohel and Robert Rolland, Editors**, Arithmetic, geometry, cryptography and coding theory 2009, 2010
- 520 **Manuel E. Lladser, Robert S. Maier, Marni Mishna, and Andrew Rechnitzer, Editors**, Algorithmic probability and combinatorics, 2010
- 519 **Yves Félix, Gregory Lupton, and Samuel B. Smith, Editors**, Homotopy theory of function spaces and related topics, 2010
- 518 **Gary McGuire, Gary L. Mullen, Daniel Panario, and Igor E. Shparlinski, Editors**, Finite fields: Theory and applications, 2010
- 517 **Tewodros Amdeberhan, Luis A. Medina, and Victor H. Moll, Editors**, Gems in experimental mathematics, 2010
- 516 **Marlos A.G. Viana and Henry P. Wynn, Editors**, Algebraic methods in statistics and probability II, 2010
- 515 **Santiago Carrillo Menéndez and José Luis Fernández Pérez, Editors**, Mathematics in finance, 2010
- 514 **Arie Leizarowitz, Boris S. Mordukhovich, Itai Shafrir, and Alexander J. Zaslavski, Editors**, Nonlinear analysis and optimization II, 2010
- 513 **Arie Leizarowitz, Boris S. Mordukhovich, Itai Shafrir, and Alexander J. Zaslavski, Editors**, Nonlinear analysis and optimization I, 2010
- 512 **Albert Fathi, Yong-Geun Oh, and Claude Viterbo, Editors**, Symplectic topology and measure preserving dynamical systems, 2010
- 511 **Luise-Charlotte Kappe, Arturo Magidin, and Robert Fitzgerald Morse, Editors**, Computational group theory and the theory of groups, II, 2010
- 510 **Mario Bonk, Jane Gilman, Howard Masur, Yair Minsky, and Michael Wolf, Editors**, In the Tradition of Ahlfors-Bers, V, 2010
- 509 **Primitivo B. Acosta-Humánez and Francisco Marcellán, Editors**, Differential algebra, complex analysis and orthogonal polynomials, 2010
- 508 **Martin Berz and Khodr Shamseddine, Editors**, Advances in p -Adic and non-archimedean analysis, 2010
- 507 **Jorge Arvesú, Francisco Marcellán, and Andrei Martínez-Finkelshtein, Editors**, Recent trends in orthogonal polynomials and approximation theory, 2010
- 506 **Yun Gao, Naihuan Jing, Michael Lau, and Kailash C. Misra, Editors**, Quantum affine algebras, extended affine Lie algebras, and their applications, 2010
- 505 **Patricio Cifuentes, José García-Cuerva, Gustavo Garrigós, Eugenio Hernández, José María Martell, Javier Parcet, Alberto Ruiz, Fernando Soria, José Luis Torrea, and Ana Vargas, Editors**, Harmonic analysis and partial differential equations, 2010
- 504 **Christian Ausoni, Kathryn Hess, and Jérôme Scherer, Editors**, Alpine perspectives on algebraic topology, 2009

TITLES IN THIS SERIES

- 503 **Marcel de Jeu, Sergei Silvestrov, Christian Skau, and Jun Tomiyama, Editors**, Operator structures and dynamical systems, 2009
- 502 **Viviana Ene and Ezra Miller, Editors**, Combinatorial Aspects of Commutative Algebra, 2009
- 501 **Karel Dekimpe, Paul Igodt, and Alain Valette, Editors**, Discrete groups and geometric structures, 2009
- 500 **Philippe Briet, François Germinet, and Georgi Raikov, Editors**, Spectral and scattering theory for quantum magnetic systems, 2009
- 499 **Antonio Giambruno, César Polcino Milies, and Sudarshan K. Sehgal, Editors**, Groups, rings and group rings, 2009
- 498 **Nicolau C. Saldanha, Lawrence Conlon, Rémi Langevin, Takashi Tsuboi, and Pawel Walczak, Editors**, Foliations, geometry and topology, 2009
- 497 **Maarten Bergvelt, Gaywalee Yamskulna, and Wenhua Zhao, Editors**, Vertex operator algebras and related areas, 2009
- 496 **Daniel J. Bates, GianMario Besana, Sandra Di Rocco, and Charles W. Wampler, Editors**, Interactions of classical and numerical algebraic geometry, 2009
- 495 **G. L. Litvinov and S. N. Sergeev, Editors**, Tropical and idempotent mathematics, 2009
- 494 **Habib Ammari and Hyeonbae Kang, Editors**, Imaging microstructures: Mathematical and computational challenges, 2009
- 493 **Ricardo Baeza, Wai Kiu Chan, Detlev W. Hoffmann, and Rainer Schulze-Pillot, Editors**, Quadratic Forms—Algebra, Arithmetic, and Geometry, 2009
- 492 **Fernando Giráldez and Miguel A. Herrero, Editors**, Mathematics, Developmental Biology and Tumour Growth, 2009
- 491 **Carolyn S. Gordon, Juan Tirao, Jorge A. Vargas, and Joseph A. Wolf, Editors**, New developments in Lie theory and geometry, 2009
- 490 **Donald Babbitt, Vyjayanthi Chari, and Rita Fiorese, Editors**, Symmetry in mathematics and physics, 2009
- 489 **David Ginzburg, Erez Lapid, and David Soudry, Editors**, Automorphic Forms and L -functions II. Local aspects, 2009
- 488 **David Ginzburg, Erez Lapid, and David Soudry, Editors**, Automorphic forms and L -functions I. Global aspects, 2009
- 487 **Gilles Lachaud, Christophe Ritzenthaler, and Michael A. Tsfasman, Editors**, Arithmetic, geometry, cryptography and coding theory, 2009
- 486 **Frédéric Mynard and Elliott Pearl, Editors**, Beyond topology, 2009
- 485 **Idris Assani, Editor**, Ergodic theory, 2009
- 484 **Motoko Kotani, Hisashi Naito, and Tatsuya Tate, Editors**, Spectral analysis in geometry and number theory, 2009
- 483 **Vyacheslav Futorny, Victor Kac, Iryna Kashuba, and Efim Zelmanov, Editors**, Algebras, representations and applications, 2009
- 482 **Kazem Mahdavi and Deborah Koslover, Editors**, Advances in quantum computation, 2009
- 481 **Aydın Aytuna, Reinhold Meise, Tosun Terzioğlu, and Dietmar Vogt, Editors**, Functional analysis and complex analysis, 2009
- 480 **Nguyen Viet Dung, Franco Guerriero, Lakhdar Hammoudi, and Pramod Kanwar, Editors**, Rings, modules and representations, 2008
- 479 **Timothy Y. Chow and Daniel C. Isaksen, Editors**, Communicating mathematics, 2008
- 478 **Zongzhu Lin and Jianpan Wang, Editors**, Representation theory, 2008

For a complete list of titles in this series, visit the
AMS Bookstore at www.ams.org/bookstore/.

This interdisciplinary volume contains papers from both a conference and special session on Error-Control Codes, Information Theory and Applied Cryptography. The conference was held at the Fields Institute in Toronto, ON, Canada from December 5–6, 2007, and the special session was held at the Canadian Mathematical Society’s winter meeting in London, ON, Canada from December 8–10, 2007.

The volume features cutting-edge theoretical results on the Reed–Muller and Reed–Solomon codes, classical linear codes, codes from nets and block designs, LDPC codes, perfect quantum and orthogonal codes, iterative decoding, magnetic storage and digital memory devices, and MIMO channels. There are new contributions on privacy reconciliation, resilient functions, cryptographic hash functions, and new work on quantum coins. Related original work in finite geometries concerns two-weight codes coming from partial spreads, $(0,1)$ matrices with forbidden configurations, André embeddings, and representations of projective spaces in affine planes.

Great care has been taken to ensure that high expository standards are met by the papers in this volume. Accordingly, the papers are written in a user-friendly format. The hope is that this volume will be of interest and of benefit both to the experienced and to newcomers alike.

ISBN 978-0-8218-4956-9



CONM/523

AMS on the Web
www.ams.org