CONTEMPORARY MATHEMATICS

381

Coding Theory and Quantum Computing

An International Conference
on Coding Theory and Quantum Computing
May 20–24, 2003
University of Virginia

David Evans
Jeffrey J. Holt
Chris Jones
Karen Klintworth
Brian Parshall
Olivier Pfister
Harold N. Ward
Editors

American Mathematical Society

http://dx.doi.org/10.1090/conm/381

CONTEMPORARY MATHEMATICS

381

Coding Theory and Quantum Computing

An International Conference
on Coding Theory and Quantum Computing
May 20–24, 2003
University of Virginia

David Evans
Jeffrey J. Holt
Chris Jones
Karen Klintworth
Brian Parshall
Olivier Pfister
Harold N. Ward
Editors

American Mathematical Society
Providence, Rhode Island

Coding Theory and Quantum Computing

This volume contains the proceedings of an international conference, "Coding Theory and Quantum Computing", held at the University of Virginia on May 20–24, 2003.

2000 *Mathematics Subject Classification.* Primary 81P68, 68Q05, 94B05, 05E20.

Library of Congress Cataloging-in-Publication Data

International Conference on Coding Theory and Quantum Computing (2003 : University of Virginia)

Coding theory and quantum computing : an International Conference on Coding Theory and Quantum Computing, May 20–24, 2003, University of Virginia / David Evans ... [et al.], editors.

p. cm. — (Contemporary mathematics, ISSN 0271-4132 ; 381)

Includes bibliographical references.

ISBN 0-8218-3600-5 (softcover : alk. paper)

1. Quantum theory–Mathematics–Congresses. 2. Coding theory–Mathematics–Congresses. 3. Quantum computers–Mathematics–Congresses. 4. Cryptography–Mathematics–Congresses. I. Evans, David, 1971–. II. Title. III. Contemporary mathematics (American Mathematical Society) ; v. 381.

QC173.96.I53 2003
530.12—dc22 2005041088

♾ 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 10 09 08 07 06 05

Contents

Coding Theory

Quantum Computing

Preface

This volume contains the proceedings of an international conference on "Coding Theory and Quantum Computing", held at the University of Virginia on May 20–24, 2003. The goal of the conference was to provide an opportunity for computer scientists, mathematicians, and physicists to interact about subjects of common interest. In all, 97 scientists attended the conference, including 35 graduate students and 6 undergraduate students. There were representatives from colleges, universities, government, and industry.

The conference opened with an instructional workshop that consisted of three mini-courses given by Robert Calderbank (AT&T Labs), Samuel Lomonaco (University of Maryland, Baltimore County), and David Meyer (University of California, San Diego).

The mini-courses (which are not included in this volume) were designed to provide nonexperts with an introduction to various aspects of quantum computing and coding theory. As the participants represented a wide array of disciplines, the mini-courses played a key role, allowing attendees to fill in gaps in their knowledge.

The workshop was followed by thirteen talks, including hour-long presentations by:

- Steven van Enk, Bell Labs
- Shuhong Gao, Department of Mathematical Sciences, Clemson University
- Mark Hillery, Department of Physics, Hunter College of CUNY
- Gretchen Matthews, Department of Mathematical Sciences, Clemson University
- Barbara Terhal, IBM Watson Research Center
- Lorenza Viola, Los Alamos National Laboratory
- Caspar van der Wal, Department of Physics, Harvard University, Harvard-Smithsonian Center for Astrophysics
- Qing Xiang, Department of Mathematical Sciences, University of Delaware

This volume is divided into two parts: Coding Theory and Quantum Computing. In the first section, the paper by Harold Ward is the record of an introduction to coding theory given as a set of lectures prior to the conference. Among the topics the lectures include are bounds, MacWilliams identities, cyclic codes, and generalized Reed-Muller codes. Although the emphasis is on linear codes, there is a description of Kerdock and Preparata codes and some of the related geometry.

The three contributed papers on coding theory are surveys of recent important work. In *Gröbner bases, Padé approximation, and decoding of linear codes,* Farr and Gao discuss a coding-theory application of Gröbner bases. Thinking of codes presented as the evaluation vectors (on a specified set of points) of a family of polynomials for which a Gröbner basis has been set up, Farr and Gao outline a decoding scheme that directly involves the Gröbner basis. They describe how their methods cover a number of standard codes. Moreover, they include a useful summary of the underlying algebraic ingredients in their presentation.

In her paper *Some computational tools for estimating the parameters of algebraic geometry codes,* Matthews describes computational methods for estimating the parameters of codes defined by algebraic curves. The main ingredient is the Weierstrass gap set of a collection of points on a curve. The computational "toolkit" Matthews outlines can be implemented easily with standard computer algebra packages. She includes examples of codes shown to be optimal by the methods presented.

In his paper *Recent results on p-ranks and Smith normal forms of some $w-\langle v,k,2\rangle$ designs*, Xiang puts forth the Smith normal form (SNF) of the incidence matrix of a design as an important invariant of the design. He gives examples of the computation of the SNF for several general classes of designs, such as unitals and designs based on the subspaces of a projective space. The computations require subtle combinatorial and number-theoretic arguments. As an illustration of the power of the SNF invariant, Xiang shows how the SNF was used to distinguish two families of difference sets defined by Lin and by Helleseth, Kumar, and Martinsen.

The quantum computing part of the conference was intentionally made very broad to reflect the openness and interdisciplinarity of the field. Beyond the two mini-courses given on the basics of quantum computing, quantum algorithms, and quantum games by Samuel Lomonaco and David Meyer, and in addition to Robert Calderbank's remarks on Calderbank-Shor-Steane quantum error correction, the invited papers covered a wide variety of directions in quantum information, with an emphasis on the understanding of entanglement, which still appears to be the core cause of the spectacular performance of quantum computing.

In an introductory paper, *Entangled states of light*, van Enk explores the description of entanglement and its meaning in the particular case of light. There have, indeed, been common misrepresentations in terms of "entangled photons", where photons are given more particular individuality than they should have. Viola generalizes this line of research in *Entanglement beyond subsystems* and presents a powerful mathematical treatment of entanglement using Lie algebras, with the goal of understanding the nature of entanglement generated by the symmetrization postulate in systems of indistinguishable quantum particles. In *Quantum walks on graphs and quantum scattering theory*, Feldman and Hillery explore how entanglement can evolve in quantum random walks. This work has interest in investigating speedups relative to classical random walk algorithms. It also presents a fascinating connection with optical interferometry. Finally, two articles explore potentially new paradigms in quantum computing. First, Lomonaco and Kauffman propose a continuous-variable implementation of Shor's algorithm in their paper *A continuous variable Shor algorithm.* It is still an open question to know whether this approach would be efficiently simulatable classically, as continuous-variable algorithms have recently been proven to be for quantum systems with a positive Wigner function. Finally, in *Generalized GHZ states and distributed quantum computing*, Yimsiriwattana and Lomonaco investigate the implementation of distributed quantum computing for the quantum Fourier transform, an important theoretical step to help overcome decoherence, the biggest challenge to the experimental realization of the quantum computer.

In addition to the talks listed above, one afternoon of the conference was set aside for a general discussion of the direction of the fields of coding theory and quantum computing. In particular, this discussion led to a number of suggested problems and questions for further research. Below we list some of the topics/questions brought up, organized by general categories:

Quantum Computing:

- Is the Church-Turing thesis dependent upon the physical laws involved in computation? Quantum computing seems to be challenging the Church-Turing thesis.
- Similarly, is the P – NP question dependent on physical laws? Quantum computing changes the way people think about NP problems, since with a quantum computer with enough qubits, it may be possible to execute a nondeterministic algorithm as quickly as a deterministic one.
- Is there a quantum analog of von Neumann architecture for computers? This relates to incorporating unitary operations into a quantum computer.
- Could quantum computing help solve big problems like the Riemann Hypothesis and the halting problem?
- Is the essence of exponentially faster quantum algorithms completely described by the Hidden Subgroup Problem (HSP)? Is there an HSP that describes nonexponential algorithms, that is, algorithms of the Grover type? How do we find more or even all quantum algorithms?
- HSP for nonabelian groups. This area has connections to lattice reduction (finding short vectors) and the graph isomorphism problem. The latter is currently being investigated as a major challenge for quantum computing.
- Is distributed quantum computing possible? This would in particular provide an avenue for addressing the issue of decoherence in quantum computing. The topic of quantum communication complexity is the subject of intensive research.

Quantum Communication:

- Quantum communication itself is essential to the last subtopic, of course. Another link between quantum communication and quantum computing is that, in addition to quantum repeaters, quantum teleportation has been found to be relevant to the realization of quantum logic gates.
- Continuous variables: quantum teleportation and cryptography have now been implemented using continuous quantum variables. Quantum error-correction protocols and quantum algorithms have also been proposed. What is the potential of continuous variables in quantum information, as compared to discrete variables?

Classical and Quantum Coding Theories:

- What about degenerate quantum error-correcting codes? These interesting codes are not as amenable to proof techniques that carry over from classical codes as are nondegenerate codes.
- The MacWilliams identities of classical coding theory are connected to the Fourier transform. Can quantum superposition in quantum computing provide advantages in dealing with the identities and with other classical coding operations?

- Data mining - what will quantum computation lead to, beyond Grover's algorithm?
- Intermediate quantum coding: qubit encoding, gate fidelity.
- What are the implications of the no-cloning theorem for data compression and decompression?
- How does one optimize quantum error-correction "overhead"? There are many practical questions for implementation; quantum computing is much more "expensive" per operation, even though overhead stays polynomial and most speedups are exponential.

General Problems in Quantum Information:

- Quantum state discrimination – for a particle in one of two nonorthogonal states, how does one determine which? Discrimination of mixed states is particularly difficult.
- Entanglement in general, especially in second-quantized systems, and in relativistic systems. It appears that entanglement is profoundly modified in these contexts. A more general theory of entanglement, possibly independent of subsystems, is needed.
- How does quantum computation interact with foundational questions of quantum mechanics? Entanglement is at the heart of many debates on completeness (the Einstein-Podolsky-Rosen paradox, the Bell theorems) and on the interpretation of quantum mechanics. In particular, one may want to test the validity of quantum mechanics in regimes such as meso/macroscopic entanglement ("Schrödinger's kitten/cat") which have not been explored yet.

We thank all of the conference speakers and participants, and the authors whose papers appear in this volume. We also appreciate the contributions of the referees who reviewed the papers appearing here. We gratefully acknowledge financial support for the conference provided by the National Science Foundation (DMS-0308708), as well as the following sponsors from the University of Virginia: the Dean of the College of Arts and Sciences, the Department of Mathematics, the Institute of Mathematical Sciences, and the NanoQuEST Institute. Finally, we thank Christine Thivierge of the AMS for her guidance in preparing this proceedings.

The Editors

List of Participants

Mehrdad Adibzadeh
University of Virginia

Christopher Altman
University of Amsterdam

Michael A. Balazs
Johns Hopkins University

Richard Barnes
University of Virginia

Darren N. Bly
Shenandoah University

Arthur S. Brill
University of Virginia

Vikram Buddhi
Purdue University

Robert Calderbank
AT&T Labs Research

Isaac Carey
University of Virginia

Brent Cody
University of Virginia

Wesley Cramer
University of Virginia

James A. Davis
University of Richmond

Robert L. Dawes
Hampton University

Benjamin Deissler
University of Virginia

Donald C. Dimitroff
Univ. of Maryland, Baltimore County

Katie Durham
Clemson University

Nicholas Dzhelepov
Univ. of Illinois at Urbana-Champaign

David Evans
University of Virginia

Jeff Farr
Clemson University

Robert B. Feinberg
Defense Department

Andrew Fenley
Virginia Tech

Frank Fiedler
University of Delaware

Joe Fields
So. Connecticut State University

Eric Finster
University of Virginia

Joe Fox
Western Michigan University

Shuhong Gao
Clemson University

Manish Gupta
Arizona State University

Esfan Haghverdi
Indiana University

Aloysius (Loek) Helminck
North Carolina State University

Mark Heiligman
National Security Agency

Mark Hillery
Hunter College of CUNY

Ben Hocking
University of Virginia

Terrell Hodge
Western Michigan University

Mike Hogye
Metron, Inc.

Jeff Holt
University of Virginia

Jim Howland
University of Virginia

K. Jeramy Hughes
University of Virginia

Ashraf Ibrahim
Southern Illinois Univ/Carbondale

Jonathan Jedwab
University of Richmond

Greg Jennings
University of Virginia

Chris Jones
Washington and Lee University

P. K. Kabir
University of Virginia

Adrian C. Keister
Virginia Tech

Patrick Keith-Hynes
University of Virginia

Christine Kelley
University of Notre Dame

Jon-Lark Kim
University of Nebraska-Lincoln

Karen Klintworth
University of Virginia

Matthew Koetz
University of Nebraska-Lincoln

Robert Konik
University of Virginia

Sergei Krutelevich
Yale University

Yoonjin Lee
Smith College

Prasit Limbupasiriporn
Clemson University

Shih Chin Lin
Syracuse University

Edward Loeb
University of Nebraska-Lincoln

Samuel Lomonaco, Jr.
Univ. of Maryland, Baltimore County

Tom Marley
University of Nebraska-Lincoln

Gretchen Matthews
Clemson University

Justin Mauger
Whittier College

Kevin McCrimmon
University of Virginia

David Meyer
UC San Diego

Bryan Osborn
Metron, Inc.

A. D. Parks
Naval Surface Warfare Center

Brian Parshall
University of Virginia

Karen Parshall
University of Virginia

Nathanael Paul
University of Virginia

Walter Pechenuk
Kent State University

Olivier Pfister
University of Virginia

Raphael Pooser
University of Virginia

Narasimhan Ramakrishnan
University of Southern Mississippi

Jennifer Roche
University of Virginia

Yongwu Rong
NSF and George Washington University

Gary Salazar
Trinity University

Leonard Scott
University of Virginia

Mitra Shabestari
University of Virginia

Swapneel Sheth
University of Alabama in Huntsville

Deirdre Smeltzer
Eastern Mennonite University

Robert Snelsire
Clemson University

Scott Spence
Department of the Navy

Charles Swannack
Clemson University

Tatsu Takeuchi
Virginia Tech

Barbara Terhal
IBM Watson Research Center

James Troupe
Naval Surface Warfare Center

Caspar van der Wal
Harvard University

Steven van Enk
Bell Labs

Thomas Vandervelde
University of Virginia

Lorenza Viola
Los Alamos National Laboratory

Petr Vojtechovsky
University of Denver

Jin Wang
Univ. of Illinois at Urbana-Champaign

Harold N. (Thann) Ward
University of Virginia

Tzu-Chieh Wei
Univ. of Illinois at Urbana-Champaign

Stephen G. Wilson
University of Virginia

Qing Xiang
University of Delaware

Maosheng Xiong
Univ. of Illinois at Urbana-Champaign

Bo Xu
University of Virginia

Anocha Yimsiriwattana
Univ. of Maryland, Baltimore County

Hussain Zaidi
University of Virginia

Yong Zhang
University of South Carolina

Titles in This Series

381 **David Evans, Jeffrey J. Holt, Chris Jones, Karen Klintworth, Brian Parshall, Olivier Pfister, and Harold N. Ward, Editors,** Coding theory and quantum computing, 2005

380 **Andreas Blass and Yi Zhang, Editors,** Logic and its applications, 2005

379 **Dominic P. Clemence and Guoqing Tang, Editors,** Mathematical studies in nonlinear wave propagation, 2005

378 **Alexandre V. Borovik, Editor,** Groups, languages, algorithms, 2005

377 **G. L. Litvinov and V. P. Maslov, Editors,** Idempotent mathematics and mathematical physics, 2005

376 **José A. de la Peña, Ernesto Vallejo, and Natig Atakishiyev, Editors,** Algebraic structures and their representations, 2005

375 **Joseph Lipman, Suresh Nayak, and Pramathanath Sastry,** Variance and duality for cousin complexes on formal schemes, 2005

374 **Alexander Barvinok, Matthias Beck, Christian Haase, Bruce Reznick, and Volkmar Welker, Editors,** Integer points in polyhedra—geometry, number theory, algebra, optimization, 2005

373 **O. Costin, M. D. Kruskal, and A. Macintyre, Editors,** Analyzable functions and applications, 2005

372 **José Burillo, Sean Cleary, Murray Elder, Jennifer Taback, and Enric Ventura, Editors,** Geometric methods in group theory, 2005

371 **Gui-Qiang Chen, George Gasper, and Joseph Jerome, Editors,** Nonlinear partial differential equations and related analysis, 2005

370 **Pietro Poggi-Corradini, Editor,** The p-harmonic equation and recent advances in analysis, 2005

369 **Jaime Gutierrez, Vladimir Shpilrain, and Jie-Tai Yu, Editors,** Affine algebraic geometry, 2005

368 **Sagun Chanillo, Paulo D. Cordaro, Nicholas Hanges, Jorge Hounie, and Abdelhamid Meziani, Editors,** Geometric analysis of PDE and several complex variables, 2005

367 **Shu-Cheng Chang, Bennett Chow, Sun-Chin Chu, and Chang-Shou Lin, Editors,** Geometric evolution equations, 2005

366 **Bernhelm Booß-Bavnbek, Gerd Grubb, and Krzysztof P. Wojciechowski, Editors,** Spectral geometry of manifolds with boundary and decompositon of manifolds, 2005

365 **Robert S. Doran and Richard V. Kadison, Editors,** Operator algebras, quantization, and non-commutative geometry, 2004

364 **Mark Agranovsky, Lavi Karp, David Shoikhet, and Lawrence Zalcman, Editors,** Complex analysis and dynamical systems, 2004

363 **Anthony To-Ming Lau and Volker Runde, Editors,** Banach algebras and their applications, 2004

362 **Carlos Concha, Raul Manasevich, Gunther Uhlmann, and Michael S. Vogelius, Editors,** Partial differential equations and inverse problems, 2004

361 **Ali Enayat and Roman Kossak, Editors,** Nonstandard models of arithmetic and set theory, 2004

360 **Alexei G. Myasnikov and Vladimir Shpilrain, Editors,** Group theory, statistics, and cryptography, 2004

359 **S. Dostoglou and P. Ehrlich, Editors,** Advances in differential geometry and general relativity, 2004

358 **David Burns, Christian Popescu, Jonathan Sands, and David Solomon, Editors,** Stark's Conjectures: Recent work and new directions, 2004

TITLES IN THIS SERIES

357 **John Neuberger, Editor,** Variational methods: open problems, recent progress, and numerical algorithms, 2004

356 **Idris Assani, Editor,** Chapel Hill ergodic theory workshops, 2004

355 **William Abikoff and Andrew Haas, Editors,** In the tradition of Ahlfors and Bers, III, 2004

354 **Terence Gaffney and Maria Aparecida Soares Ruas, Editors,** Real and complex singularities, 2004

353 **M. C. Carvalho and J. F. Rodrigues, Editors,** Recent advances in the theory and applications of mass transport, 2004

352 **Marek Kubale, Editor,** Graph colorings, 2004

351 **George Yin and Qing Zhang, Editors,** Mathematics of finance, 2004

350 **Abbas Bahri, Sergiu Klainerman, and Michael Vogelius, Editors,** Noncompact problems at the intersection of geometry, analysis, and topology, 2004

349 **Alexandre V. Borovik and Alexei G. Myasnikov, Editors,** Computational and experimental group theory, 2004

348 **Hiroshi Isozaki, Editor,** Inverse problems and spectral theory, 2004

347 **Motoko Kotani, Tomoyuki Shirai, and Toshikazu Sunada, Editors,** Discrete geometric analysis, 2004

346 **Paul Goerss and Stewart Priddy, Editors,** Homotopy theory: Relations with algebraic geometry, group cohomology, and algebraic K-theory, 2004

345 **Christopher Heil, Palle E. T. Jorgensen, and David R. Larson, Editors,** Wavelets, frames and operator theory, 2004

344 **Ricardo Baeza, John S. Hsia, Bill Jacob, and Alexander Prestel, Editors,** Algebraic and arithmetic theory of quadratic forms, 2004

343 **N. Sthanumoorthy and Kailash C. Misra, Editors,** Kac-Moody Lie algebras and related topics, 2004

342 **János Pach, Editor,** Towards a theory of geometric graphs, 2004

341 **Hugo Arizmendi, Carlos Bosch, and Lourdes Palacios, Editors,** Topological algebras and their applications, 2004

340 **Rafael del Río and Carlos Villegas-Blas, Editors,** Spectral theory of Schrödinger operators, 2004

339 **Peter Kuchment, Editor,** Waves in periodic and random media, 2003

338 **Pascal Auscher, Thierry Coulhon, and Alexander Grigor'yan, Editors,** Heat kernels and analysis on manifolds, graphs, and metric spaces, 2003

337 **Krishan L. Duggal and Ramesh Sharma, Editors,** Recent advances in Riemannian and Lorentzian geometries, 2003

336 **José González-Barrios, Jorge A. León, and Ana Meda, Editors,** Stochastic models, 2003

335 **Geoffrey L. Price, B. Mitchell Baker, Palle E.T. Jorgensen, and Paul S. Muhly, Editors,** Advances in quantum dynamics, 2003

334 **Ron Goldman and Rimvydas Krasauskas, Editors,** Topics in algebraic geometry and geometric modeling, 2003

333 **Giovanni Alessandrini and Gunther Uhlmann, Editors,** Inverse problems: Theory and applications, 2003

332 **John Bland, Kang-Tae Kim, and Steven G. Krantz, Editors,** Explorations in complex and Riemannian geometry, 2003

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

A conference, Coding Theory and Quantum Computing, was held in Charlottesville, VA, to provide an opportunity for computer scientists, mathematicians, and physicists to interact about subjects of common interest. This proceedings volume grew out of that meeting.

It is divided into two parts: "Coding Theory" and "Quantum Computing". In the first part, Harold Ward gives an introduction to coding theory. Other papers survey recent important work, such as coding theory applications of Gröbner bases, methods of computing parameters of codes corresponding to algebraic curves, and problems in the theory of designs. The second part of the book covers a wide variety of directions in quantum information with an emphasis on understanding entanglement.

The material presented is suitable for graduate students and researchers interested in coding theory and in quantum computing.

ISBN 0-8218-3600-5

9 780821 836002

CONM/381

AMS *on the* Web
www.ams.org