Codes and Association Schemes

DIMACS Workshop
Codes and Association Schemes
November 9–12, 1999
DIMACS Center

Alexander Barg
Simon Litsyn
Editors

American Mathematical Society
Selected Titles in This Series

56 Alexander Barg and Simon Litsyn, Editors, Codes and Association Schemes
55 Ding-Zhu Du, Panos M. Pardalos, and Jie Wang, Editors, Discrete Mathematical Problems with Medical Applications
54 Erik Winfree and David K. Gifford, Editors, DNA Based Computers V
53 Nathaniel Dean, D. Frank Hsu, and R. Ravi, Editors, Robust Communication Networks: Interconnection and Survivability
52 Sanguthevar Rajasekaran, Panos Pardalos, and D. Frank Hsu, Editors, Mobile Networks and Computing
51 Pierre Hansen, Patrick Fowler, and Maolin Zheng, Editors, Discrete Mathematical Chemistry
50 James M. Abello and Jeffrey Scott Vitter, Editors, External Memory Algorithms
49 Ronald L. Graham, Jan Kratochvíl, Jaroslav Nešetřil, and Fred S. Roberts, Editors, Contemporary Trends in Discrete Mathematics
48 Harvey Rubin and David Harlan Wood, Editors, DNA Based Computers III
47 Martin Farach-Colton, Fred S. Roberts, Martin Vingron, and Michael Waterman, Editors, Mathematical Support for Molecular Biology
46 Peng-Jun Wan, Ding-Zhu Du, and Panos M. Pardalos, Editors, Multichannel Optical Networks: Theory and Practice
45 Marios Mavronicolas, Michael Merritt, and Nir Shavit, Editors, Networks in Distributed Computing
44 Laura F. Landweber and Eric B. Baum, Editors, DNA Based Computers II
43 Panos Pardalos, Sanguthevar Rajasekaran, and José Rolim, Editors, Randomization Methods in Algorithm Design
42 Ding-Zhu Du and Frank K. Hwang, Editors, Advances in Switching Networks
41 David Aldous and James Propp, Editors, Microsurveys in Discrete Probability
40 Panos M. Pardalos and Ding-Zhu Du, Editors, Network Design: Connectivity and Facilities Location
39 Paul W. Beame and Samuel R Buss, Editors, Proof Complexity and Feasible Arithmetics
38 Rebecca N. Wright and Peter G. Neumann, Editors, Network Threats
37 Boris Mirkin, F. R. McMorris, Fred S. Roberts, and Andrey Rzhetsky, Editors, Mathematical Hierarchies and Biology
36 Joseph G. Rosenstein, Deborah S. Franzblau, and Fred S. Roberts, Editors, Discrete Mathematics in the Schools
35 Dingzhu Du, Jun Gu, and Panos M. Pardalos, Editors, Satisfiability Problem: Theory and Applications
34 Nathaniel Dean, Editor, African Americans in Mathematics
33 Ravi B. Boppana and James F. Lynch, Editors, Logic and Random Structures
32 Jean-Charles Grégoire, Gerard J. Holzmann, and Doron A. Peled, Editors, The SPIN Verification System
31 Neil Immerman and Phokion G. Kolaitis, Editors, Descriptive Complexity and Finite Models
30 Sandeep N. Bhatt, Editor, Parallel Algorithms: Third DIMACS Implementation Challenge
29 Doron A. Peled, Vaughan R. Pratt, and Gerard J. Holzmann, Editors, Partial Order Methods in Verification
28 Larry Finkelstein and William M. Kantor, Editors, Groups and Computation II
27 Richard J. Lipton and Eric B. Baum, Editors, DNA Based Computers

(Continued in the back of this publication)
Codes and Association Schemes
This page intentionally left blank
DIMACS
Series in Discrete Mathematics and Theoretical Computer Science

Volume 56

Codes and Association Schemes

DIMACS Workshop
Codes and Association Schemes
November 9–12, 1999
DIMACS Center

Alexander Barg
Simon Litsyn
Editors

NSF Science and Technology Center
in Discrete Mathematics and Theoretical Computer Science
A consortium of Rutgers University, Princeton University,
AT&T Labs–Research, Bell Labs (Lucent Technologies),
Telcordia Technologies, and NEC Research Institute

American Mathematical Society
This DIMACS volume contains papers from a DIMACS workshop on Codes and Association Schemes, held November 9–12, 1999.

2000 Mathematics Subject Classification. Primary 94Bxx, 05E30, 05E35.

Library of Congress Cataloging-in-Publication Data
DIMACS Workshop Codes and Association Schemes (1999 : DIMACS Center)
Codes and association schemes : DIMACS Workshop Codes and Association Schemes, November 9–12, 1999, DIMACS Center / Alexander Barg, Simon Litsyn, editors.
p. cm. — (DIMACS series in discrete mathematics and theoretical computer science ; v. 56) Includes bibliographical references.
ISBN 0-8218-2074-5 (alk. paper)
QA268.D55 1999
003'.54—dc21 00-053129

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 Assistant to the Publisher, American Mathematical Society, P. O. Box 6248, Providence, Rhode Island 02940-6248. 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.)

© 2001 by the American Mathematical Society. All rights reserved.
The American Mathematical Society retains all rights except those granted to the United States Government.
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 URL: http://www.ams.org/

10 9 8 7 6 5 4 3 2 1 06 05 04 03 02 01
## Contents

Preface ix  
Foreword xi  
Harmonic weight enumerators of nonbinary codes and MacWilliams identities  
**Christine Bachoc** 1  
Numerical results on the asymptotic rate of binary codes  
**Alexander Barg and David B. Jaffe** 25  
Weakly biased arrays, almost independent arrays and error-correcting codes  
**Jürgen Bierbrauer and Holger Schellwat** 33  
Indexes of spherical codes  
**Peter Boyvalenkov, Danyo Danev, and Peter Kazakov** 47  
Codes over $\mathbb{Z}_p^n$ and association schemes  
**Paul Camion** 59  
Bent, resilient functions and the Numerical Normal Form  
**Claude Carlet and Philippe Guillot** 87  
On identifying codes  
**Gérard D. Cohen, Iiro Honkala, Antoine Lobstein, and Gilles Zémor** 97  
Ternary Hamming and binary perfect covering codes  
**Italo J. Dejter and Kevin T. Phelps** 111  
A Riemann hypothesis analogue for self-dual codes  
**Iwan Duursma** 115  
On perfect codes in the Johnson scheme  
**Tuvi Etzion** 125  
On perfect constant weight codes  
**Tuvi Etzion and Jack van Lint** 131  
On additive $GF(4)$ codes  
**Philippe Gaborit, W. Cary Huffman, Jon-Lark Kim, and Vera Pless** 135
Integral zeroes of Krawtchouk polynomials
   LAURENT HABSIEGER 151

Some algebra related to $P$- and $Q$-polynomial association schemes
   TATSURO ITO, KENICHIRO TANABE, AND PAUL TERWILLIGER 167

Bounds for the Christoffel-Darboux kernel of the binary Krawtchouk
   polynomials
   ILIA KRASIKOV 193

Survey of binary Krawtchouk polynomials
   ILIA KRASIKOV AND SIMON LITSYN 199

On an algebraic method for bounding the covering radius
   TERO LAIHONEN 213

Design systems: Combinatorial characterizations of Delsarte $T$-designs via
   partially ordered sets
   WILLIAM J. MARTIN 223

The isomorphism problem for circulant graphs via Schur ring theory
   MIKHAIL MUZYCHUK, MIKHAIL KLIN, AND REINHARD PÖSCHEL 241

New 1-generator quasi-twisted codes over $GF(5)$
   IRFAN SIAP, NUH AYDIN, AND DIJEN RAY-CHAUDHURI 265

Communication complexity and orthogonal polynomials
   ULRICH TAMM 277

Estimates of the distance distribution of nonbinary codes, with applications
   ALEXEI ASHIKHMIN, ALEXANDER BARG, AND SIMON LITSYN 287
Preface

Though theory of association schemes first appeared in statistical applications, its development is mostly associated with a general view of error-correcting codes suggested by Delsarte in 1973. Since then it has grown into an independent branch of combinatorics, while maintaining a sustained connection with coding theory.

This volume collects papers presented at or closely related to the workshop “Codes and Association Schemes” held at DIMACS, Rutgers University, Piscataway, NJ in November 1999. The goal of the workshop was to demonstrate new applications of the theory of association schemes to coding and to give coding theorists an opportunity to familiarize themselves with new properties of association schemes, both polynomial and general.

The papers in the volume can be divided into the following categories: applications of association schemes to codes with a special subsection on the applications of the polynomial method, structural results for codes, structural results for schemes, and properties of orthogonal polynomials and their applications in combinatorics. In the first area the paper by C. Bachoc discusses a refined version of weight enumerators of nonbinary linear codes, called harmonic weight enumerators. As usual, they satisfy MacWilliams-type identities and provide a tool for computing the intersection numbers and coset weight distribution of self-dual codes. P. Camion in his paper characterizes Gray-map-like isometries between integer residue rings and their residue fields. T. Etzion rules out new sets of parameters of perfect codes in the Johnson space, making an advance in the difficult problem raised by Delsarte over 25 years ago. Applications of the polynomial method are discussed in the paper by T. Laihonen where he establishes a new upper bound on the covering radius of a linear code via its dual distance. Along the same lines, P. Boyvalenkov, D. Danev and P. Kazakov prove new results on indexes of spherical designs, A. Ashikhmin, A. Barg, and S. Litsyn give new bounds on the distance distribution of nonbinary codes and discuss their applications, and A. Barg and D. B. Jaffe collect some experimental results on the asymptotic rate of binary codes implied by the polynomial method and speculate on its potential limits.

The most prominent families of orthogonal polynomials appearing in coding theory are Krawtchouk polynomials, orthogonal on \{0,1,\ldots,n-1\} with weight \(q^{-n}\binom{n}{r}(q-1)^r\) and a particular family of discrete Hahn polynomials. A collection of properties of binary Krawtchouk polynomials appears in the paper by I. Krasikov and S. Litsyn, written with coding theory applications in mind. L. Habsieger makes advances in a difficult problem of bounding the number of integer zeros
of Krawtchouk polynomials. I. Krasikov presents refined bounds for the Christoffel-Darboux kernel of binary Krawtchouk polynomials. U. Tamm suggests new applications of the Krawtchouk and Hahn polynomials in the rank method of bounding the communication complexity of functions related to the Hamming distance.

Structural properties of association schemes are studied in the paper by T. Ito, K. Tanabe, and P. Terwilliger which fits in the general program of classifying metric/cometric association schemes. The main results of the paper are related to classification of some irreducible modules in the subconstituent algebra of the scheme. W. J. Martin extends the notion of T-design to families of association schemes represented by maximal elements of partially ordered sets. The paper by M. Muzychuk, M. Klin and R. Pöschel surveys properties of Schur rings and applies them to obtain new necessary conditions for the isomorphism problem of circulant graphs.

Finally, papers in a large group devoted to properties of error-correcting codes, though they sometimes do not mention explicitly the context of association schemes, deal with problems motivated by the combinatorial view of codes. In this vein, T. Etzion and J. van Lint present a family of perfect single error correcting constant weight codes over the alphabets of size $2^k + 1$, and J. Bierbrauer and H. Schellwat investigate combinatorial applications of codes with a known dual distance. More diverse results in the remaining papers still follow the same general view of codes and fit well in the cultural paradigm of combinatorial coding theory. G. D. Cohen, I. Honkala, A. Lobstein and G. Zémor discuss parameters of codes in which every point is identified uniquely by the set of its closest neighbors. I. J. Dejter and K. T. Phelps give a simple characterization of a perfect dominating set in the 13-dimensional cube. C. Carlet and P. Guillot contribute to the program of classifying maximally nonlinear (bent) functions and P. Gaborit, W. C. Huffman, J.-L. Kim, and V. Pless classify short additive quaternary codes. New codes over $GF(5)$ are constructed in the paper by I. Siap, N. Aydin, and D. Ray-Chaudhuri. I. Duursma suggests an unexpected analogy between algebraic curves and linear codes based on a new form of the weight enumerator of the code and formulates a "Riemann hypothesis" for the zeros of the new enumerator.

We would like to use this opportunity to thank DIMACS Center for financial and organizational support of the workshop. The help provided by the Center turned the meeting into an enjoyable event for the organizers and hopefully for the other participants.

Alexander Barg  
Math. Research  
Bell Labs, Lucent Technologies  
600 Mountain Ave., Rm. 2C-375  
Murray Hill, NJ 07974, USA  
abarg@research.bell-labs.com

Simon Litsyn  
Dept. of EE-Systems  
Tel-Aviv University  
Ramat Aviv 69978, Israel  
litsyn@eng.tau.ac.il
Foreword

The Workshop on Codes and Association Schemes was held November 9–12, 1999 at the DIMACS Center at Rutgers University in Piscataway, NJ. We would like to express our appreciation to Alexander Barg and Simon Litsyn for their efforts to organize and plan this successful conference. This volume consists of papers either presented at the workshop or closely related to it.

The theory of association schemes has taken its position as a branch of combinatorics, with close ties to coding theory. This volume collects papers on applications of association schemes to codes, structural results for codes, structural results for schemes, and properties of orthogonal polynomials (with applications in combinatorics).

DIMACS gratefully acknowledges the generous support that makes both its workshop and its publication programs possible. Special thanks go to the National Science Foundation, through its Science and Technology Centers program, the New Jersey Commission on Science and Technology, and DIMACS’s partners at Rutgers, Princeton, AT&T Labs-Research, Bell Labs, NEC Research Institute, and Telcordia Technologies.

Fred S. Roberts
Director

Robert Sedgewick
Co-Director for Princeton
This page intentionally left blank
This page intentionally left blank
Selected Titles in This Series

(Continued from the front of this publication)

26 David S. Johnson and Michael A. Trick, Editors, Cliqu es, Coloring, and Satisfiability: Second DIMACS Implementation Challenge
25 Gilbert Baum slag, David Epstein, Robert Gilman, Hamish Short, and Charles Sims, Editors, Geometric and Computational Perspectives on Infinite Groups
23 Panos M. Pardalos, David I. Shalloway, and Guoliang Xue, Editors, Global Minimization of Nonconvex Energy Functions: Molecular Conformation and Protein Folding
22 Panos M. Pardalos, Mauricio G. C. Resende, and K. G. Ramakrishnan, Editors, Parallel Processing of Discrete Optimization Problems
21 D. Frank Hsu, Arnold L. Rosenberg, and Dominique Sotteau, Editors, Interconnection Networks and Mapping and Scheduling Parallel Computations
20 William Cook, László Lov ász, and Paul Seymour, Editors, Combinatorial Optimization
19 Ingemar J. Cox, Pierre Hansen, and Bela Julesz, Editors, Partitioning Data Sets
18 Guy E. Blelloch, K. Mani Chandy, and Su resh Jagannathan, Editors, Specification of Parallel Algorithms
17 Eric Sven Ristad, Editor, Language Computations
16 Panos M. Pardalos and Henry Wolkowicz, Editors, Quadratic Assignment and Related Problems
15 Nathaniel Dean and Gregory E. Shannon, Editors, Computational Support for Discrete Mathematics
14 Robert Calderbank, G. David Forney, Jr., and Nader Moayeri, Editors, Coding and Quantization: DIMACS/IEEE Workshop
13 Jin-Yi Cai, Editor, Advances in Computational Complexity Theory
12 David S. Johnson and Catherine C. McGeoch, Editors, Network Flows and Matching: First DIMACS Implementation Challenge
11 Larry Finkelstein and William M. Kantor, Editors, Groups and Computation
10 Joel Friedman, Editor, Expanding Graphs
9 William T. Trotter, Editor, Planar Graphs
8 Simon Gindikin, Editor, Mathematical Methods of Analysis of Biopolymer Sequences
7 Lyle A. McGeoch and Daniel D. Sleator, Editors, On-Line Algorithms
6 Jacob E. Goodman, Richard Pollack, and William Steiger, Editors, Discrete and Computational Geometry: Papers from the DIMACS Special Year
5 Frank Hwang, Fred Roberts, and Clyde Monma, Editors, Reliability of Computer and Communication Networks
4 Peter Gritzmann and Bernd Sturmfels, Editors, Applied Geometry and Discrete Mathematics, The Victor Klee Festschrift
3 E. M. Clarke and R. P. Kurshan, Editors, Computer-Aided Verification '90
2 Joan Feigenbaum and Michael Merritt, Editors, Distributed Computing and Cryptography
1 William Cook and Paul D. Seymour, Editors, Polyhedral Combinatorics