MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Tagungsbericht 11/1998

Designs and Codes

15 - 21 March 1998

The meeting was organized by D. Jungnickel (Augsburg) and J. H. van Lint (Eindhoven). The central theme of the conference was the interplay between coding theory, the theory of designs and finite geometry. It brought together experts of these areas and gave the opportunity to learn and discuss the latest developments in these fields. While the mornings were filled with long talks, there was only one talk per afternoon scheduled, leaving time for private discussions and research.

Two main themes of the conference were difference sets on the one hand and $\mathbb{Z}_4$-linear codes on the other hand. The most spectacular progress reported on was probably Schmidt's work on new exponent bounds for abelian difference sets without any technical assumptions like self-conjugacy (and a variety of other structures which can be studied in terms of group rings); this result is the first major breakthrough since Turyn's classical work of 1965. The talks given on $\mathbb{Z}_4$-linear codes proved again how fruitful this point of view is in dealing with seemingly non-linear phenomena.

The conference was overshadowed by the decease of Professor Edward F. Assmus Jr., who died on March 18 during the conference. This caused the decision to continue the conference only with a final memorial session, whence only 15 talks were given.

The proceedings of the conference will now take the form of a memorial tribute to Professor Assmus; several colleagues not present at the meeting have been invited to contribute to this volume which will appear as a special volume of the journal "Designs, Codes and Crypotography".

EDWARD F. ASSMUS[1]

Variations on a theme of Delsarte: the coding theory of nets

We show how Delsarte's work on binary codes of inversive planes extends to the binary coding theory of odd-order nets. Roughly speaking, we linearize Bruck's theory of nets over the binary field. In particular, we give a necessary and sufficient condition, similar to MacLane's characterization of planar graphs, for a net to extend to an affine plane and a computable sufficient condition for a $(q+1)/2$-net of odd order q to extend to an affine plane. We indicate the generalization to affine 1-designs and give many examples. We close with several open questions.

JÜRGEN BIERBRAUER

Codes and Caps

We give a direct introduction to the theory of cyclic codes and apply it to constacyclic codes. This paves the way to a generalization of this notion, which we call *twisted codes*. The basic instrument for the determination of the basic parameters are cyclotomic cosets, the orbits under the action of the Galois group.

Twisted codes are applied (a) for the construction of good quaternary and binary codes, (b) for the construction of a 3-parameter family of 2-weight codes and strongly regular graphs, which are related to the geometrical problem of maximal arcs, and (c) for the construction of quantum codes.

We remark that the notion of twisted codes is roughly equivalent to the notion of *Reed-Solomon subspace codes*, which was developed independently by McEliece, Solomon and Hattori.

In a second part we study caps in projective and affine spaces. We review the classical recursive constructions and introduce some new constructions, which lead to good results in projective dimensions 5 and 6. Finally we give a direct construction in dimension 4 in odd characteristic, which is based on a family of ovoids on three hyperplanes in general position. The construction is couched in the language of geometric algebra. The main result are caps of size $O(5/2\,q^2)$ in $PG(4,q)$, q odd.

[1]This abstract is taken out of the "Vortragsbuch"

Aiden A. Bruen

Binary Linear Codes of Minimum Distance 4

(Joint work with David Wehlan)

We show the one-to-one correspondence between such codes C and caps S in the projective space $\Sigma = \mathrm{PG}(n,2)$, i.e. sets of points in Σ with no three collinear. It is the case that C is inextendable if and only if S is maximal.

We focus on the case when S is large (i.e. $|S| \geq 2^{n-1}+2$) and maximal. The methods of Davydov and Tomhak are described. Using a celebrated result of M. Kneser they are able to show the following result.

Theorem: If S is maximal and $|S| > 2^{n-1}$, then $|S| = 2^{n-1} + 2^i$, $i = 0, 1, \ldots, n-3, n-1$. Moreover S is obtained by successively doubling a maximal cap of size $2^{m-1}+1$ in $\mathrm{PG}(m-2)$.

In order to obtain the structure of S we need the structure of a maximal cap T with $|T| = 2^{n-1}+1$ in $\mathrm{PG}(n,2)$. Examples of such T are described using the tangent hyperplane construction and the "quasidoubling" construction. We also discuss quasimaximal caps and give structure theorems in various cases. A connection with the colouring of graphs and Tutte's 2-blocks is also described.

Robert Calderbank

Orthogonal Geometry and Quantum Error Correction

(Joint work with Eric Rains, Peter Shor, and Neil Sloane)

Quantum effects are seldom evident in today's electronic devices since the quantum states of many millions of atoms are averaged together blurring their discreteness. But in quantum computing the foundations of quantum mechanics are finding direct and visible application in information processing. The unreasonable effectiveness of quantum computing is founded on coherent quantum superposition or entanglement which allows a large number of calculations to be performed simultaneously. This coherence is lost as a quantum system interacts with its environment and an important challenge today is to devise means of preserving it.

A quantum error correcting code is a way of encoding quantum states into qubits so that error or decoherence in a small number of individual qubits has little or no effect on the encoded data. This talk will describe a beautiful group theoretic framework that simplifies the presentation of known quantum error correcting codes and greatly facilitates the construction of new examples.

IWAN DUURSMA

Split weight enumerators for Preparata codes with applications to designs

(Joint work with Chunming Rong and Kyeongcheol Yang)

Quaternary Preparata codes have a 2-transitive affine automorphism group. Their combinatorial structure is richer than indicated by the automorphism group. Helleseth, Rong and Yang found various 3-designs by taking the supports of codewords as blocks. In a joint work with these authors we obtain the stronger property that the split complete weight enumerator of a Preparata code at three given positions does not depend on the three positions.

SHUHONG GAO

Absolute irreducibility of polynomials via Newton polytopes

Absolute irreducibility of polynomials is crucial in many applications, including finite geometry and algebraic geometric codes. In this talk, we develop a new method for proving absolute irreducibility of multivariable polynomials over any field. We associate a polynomial with a polytope, called the Newton polytope of the polynomial. A polynomial is absolutely irreducible if its Newton polytope is indecomposable. This can be viewed as a generalization of Eisenstein's criterion. We construct several classes of indecomposable polytopes and thus give many infinite families of absolutely irreducible polynomials over an arbitrary field. We apply this technique to polynomials related to codes over finite fields.

Tor Helleseth

3-Designs from Preparata codes, Kerdock codes and related codes over $\mathbb{Z}_4$

The Preparata code $\mathcal{P}_m$ of length 2^m over $\mathbb{Z}_4$ has parity-check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \beta & \beta^2 & \cdots & \beta^{2^m-2} \end{bmatrix}.$$

where β is an element of order $2^m - 1$ in the Galois ring $GR(4, m)$.

A vector is denoted to be of the type $1^{n_1}\,2^{n_2}\,3^{n_3}\,0^{n_0}$ if i occurs n_i times, $i = 0, 1, 2, 3$, as a component. The nonzero positions (or supports) of a fixed type of low Hamming weight in the Preparata code over $\mathbb{Z}_4$ are shown to form 3-designs.The codewords of minimum Lee weight in the Preparata code $\mathcal{P}_m$ forany odd integer m are of the type $1^3\,2^1\,3^1\,0^{n-5}$ or $1^1\,2^1\,3^3\,0^{n-5}$. Changing the sign of a codeword leads to a codeword with the same support. Hence, to construct simple designs (designs without repeated blocks), we only consider the former type. Note that the codewords of minimal Lee weight have Hamming weight 5.

Theorem: The supports of the codewords of type $1^3\,2^1\,3^1\,0^{n-5}$ (or $1^1\,2^1\,3^3\,0^{n-5}$) in the Preparata code $\mathcal{P}_m$ over $\mathbb{Z}_4$ form a 3-$(2^m, 5, 10)$ design for any odd integer $m \geq 3$.

Further all codewords of a fixed type of support size 6 form a design. As an example we have:

Theorem: The supports of the codewords of type $1^5\,2^0\,3^1\,0^{n-6}$ in the Preparata code $\mathcal{P}_m$ over $\mathbb{Z}_4$ form a 3-$(2^m,\ 6,\ 2^m - 8)$ design for any odd integer $m \geq 5$.

The dual code of the Preparata code over $\mathbb{Z}_4$ is the Kerdock code over $\mathbb{Z}_4$.The codewords of each type in the Kerdock code over $\mathbb{Z}_4$ give a design. As an example we have:

Theorem: The supports of the codewords of the type $1^{n_1}\,2^{n_2}\,3^{n_3}\,0^{n-n_1-n_2-n_3}$ in the Kerdock code $\mathcal{K}_m$ of length $n = 2^m$ over $\mathbb{Z}_4$ form a 3-$(2^m, k, \lambda)$ design for any odd integer $m \geq 3$, where $k = 2^{m-1} + 2^{m-2} - 2^{\frac{m-3}{2}}$, $\lambda = k(k-1)(k-2)/(2^m - 2)$ and $n_1 = 2^{m-2} + 2^{\frac{m-3}{2}}$, $n_2 = n_3 = 2^{m-2} - 2^{\frac{m-3}{2}}$.

Further results also reveal similar examples of 3-designs in the Goethals code over $\mathbb{Z}_4$.

Yury J. Ionin

A technique for constructing symmetric designs

We introduce a uniform technique for constructing a family of symmetric designs with parameters $(v(q^{m+1}-1)/(q-1), kq^m, \lambda q^m)$, where m is any positive integer, (v, k, λ) are the parameters of a smaller symmetric design, and $q = k^2/(k-\lambda)$ is a prime power. In this technique, the incidence matrix of the initial symmetric (v, k, λ)-design is to be contained in a set $\mathcal{M}$ of matrices of order v satisfying conditions (i) each matrix $X \in \mathcal{M}$ has a constant row sum $r(X)$ and (ii) there exists a bijection $\sigma : \mathcal{M} \to \mathcal{M}$ such that σ^{q-1} is the identity, $(\sigma X)(\sigma Y)^T = XY^T$ for any $X, Y \in \mathcal{M}$, $r(\sigma X) = r(X)$ and $\sum_{i=1}^{q-1} \sigma^i X = ((q-1)r(X)/v)J$ for any $X \in \mathcal{M}$.

We utilize the Davis and Jedwab approach to constructing difference sets to show that our construction works whenever (v, k, λ) are the parameters of a McFarland difference set or its complement, a Spence difference set or its complement, a Davis-Jedwab difference set or its complement, or a Hadamard difference set of order $9 \cdot 4^d$, thus obtaining seven infinite families of symmetric designs.

Jonathan Jedwab

Golay complementary sequences and Reed-Muller codes

(Joint work with James Davis)

In order to solve an applied problem in digital communication engineering we examined the structure of binary "Golay sequences" of length 2^m, namely sequences A belonging to a Golay complementary pair $\{A, B\}$. This unusual formulation led us to discover an unexpected connection with Reed-Muller codes. Specifically, we can represent $2^{m+1}m!/2$ binary Golay sequences as $m!/2$ cosets of $\mathrm{RM}(1, m)$ within $\mathrm{RM}(2, m)$. For each such sequence A we can exhibit four sequences B forming a Golay complementary pair with A. This result generalises naturally from the binary alphabet to the 2^h-ary alphabet, connecting 2^h-ary Golay sequences of length 2^m to a new generalisation of the Reed-Muller code over the ring $\mathbb{Z}_{2^h}$. We give an efficient recursive decoding algorithm for the new Reed-Muller code involving a modification of the fast Hadamard transform.

VLADIMIR I. LEVENSHTEIN

Relationships between bounds for codes and designs in the Hamming and Johnson spaces

For a P- and Q-polynomial association scheme (graph) X, the problems of finding the maximum size $A(X,d)$ of a code $C \subseteq X$ with the minimum distance d and the minimum size $B(X,d)$ of a code $C \subseteq X$ with the minimum dual distance d (or, equivalently, $(d-1)$-design $C \subseteq X$) are considered. In particular, for the Hamming space $X = H_v^n$, $B(X, t+1)$ is the minimum size lv^t of an orthogonal array $OA_l(t,n,v)$ of strength t and, for the Johnson space $X = J_w^n$, $B(X, t+1)$ is the minimum size $l\binom{n}{t}/\binom{w}{t}$ of a block t-design $S_l(t,w,n)$. For optimal codes there is the Bassalygo-Elias inequality $\binom{n}{w}A(H_2^n, 2d) \leq 2^n A(J_w^n, d)$, where the Johnson distance equals half of the Hamming distance between binary vectors. This inequality was used to obtain the best asymptotic bound on $A(H_2^n, 2d)$ using bounds on $A(J_w^n, d)$. The problem is to find an analogue of this inequality for optimal designs and improve bound for $B(H_2^n, 2d)$ using the known bounds on $B(J_w^n, d)$. A solution of this problem will be given, but only in terms of the linear programming bounds.

Delsarte considered two (*code* and *design*) linear programming problems for both the systems P and Q of orthogonal polynomials and proved that

$$A(X,d) \leq \min(A_Q(X,d), |X'|/B_P(X,d)),$$
$$B(X,d) \geq \max(B_Q(X,d), |X|/A_P(X,d)),$$

where $A_Q(X,d)$ and $A_P(X,d)$ are the solutions of the code problem for systems Q and P, respectively, and $B_Q(X,d)$ and $B_P(X,d)$ are those for the design problem. Rodemich found the following analogue of the Bassalygo-Elias inequality in terms of the linear programming bounds: $\binom{n}{w}A_Q(H_2^n, 2d) \leq 2^n A_Q(J_w^n, d)$. Recently the author proved that

$$A_Q(X,d)B_P(X,d) = A_P(X,d)B_Q(X,d) = |X|.$$

This inequality, applied to $X = H_2^n$ and $X = J_w^n$, the coincidence Q with P for the Hamming space, and the Rodemich result imply that $B_Q(H_2^n, 2d) = B_P(H_2^n, 2d) \geq B_P(J_w^n, d) = \binom{n}{w}/A_Q(J_w^n, d)$. In particular, this approach allows one to improve upon the Rao and Ray-Chaudhuri-Wilson bounds on the size of orthogonal arrays and block designs when their strength t is sufficiently large as compared to n with the help of the author's upper bound of 1978 on the size of codes in the Hamming and Johnson spaces.

BERNHARD SCHMIDT

Towards Ryser's conjecture and more

In this talk, a new approach to the study of cyclotomic integers of prescribed absolute value is presented which has strong implications on several combinatorial structures including (relative) difference sets, quasiregular projective planes, planar functions, and group invariant weighing matrices. One of the main consequences is that the exponent of an abelian group G containing a (v,k,λ,n)-difference set cannot exceed $\left(\frac{2^{s-1}F(v,n)}{n}\right)^{\frac{1}{2}} v$, where s is the number of odd prime divisors of v and $F(v,n)$ is a number theoretic parameter whose order of magnitude usually is the square free part of v. This implies, for instance, that for any finite set P of primes there is a constant C such that $\exp(G) \leq C|G|^{1/2}$ for any abelian group G containing a Hadamard difference set whose order is a product of powers of primes in P. Furthermore, we are able to verify Ryser's conjecture for most parameter series of known difference sets. This includes a striking progress towards the circulant Hadamard matrix conjecture. A computer search showed that there is no Barker sequence of length l with $13 < l \leq 4 \cdot 10^{12}$. Finally, we present new necessary conditions for the existence of quasiregular projective planes and group invariant weighing matrices including asymptotic exponent bounds for cases which previously had been completely intractable.

MOHAN S. SHRIKHANDE

On classification of two class partially balanced designs

Let $\Gamma = (V, E)$ be a strongly regular graph and $\mathcal{B}$ a family of k-subsets (blocks) of V. The pair $D = (V, \mathcal{B})$ is a partially balanced (v,k,λ,μ)-design on Γ if for any distinct vertices x and y, the number of blocks containing $\{x,y\}$ is λ if $\{x,y\}$ is an edge and is μ otherwise. In such a design, the replication number r satisfies $r \geq 2\lambda - \mu$.

We obtain a complete classification of designs with $r = 2\lambda - \mu$ in case Γ has an eigenvalue -2. We show there are three infinite families (and their complements) and several sporadic designs. The sporadic designs correspond to the Petersen, Clebsch, and Shrikhande graphs and the triangular graph $T(4)$.

VLADIMIR D. TONCHEV

Linear Perfect Codes and a Characterization of the Classical Designs

A new definition for the dimension of a combinatorial t-(v, k, λ) design over a finite field is proposed. The complementary designs of the hyperplanes in a finite projective or affine geometry, and the finite Desarguesian planes in particular, are characterized as the unique (up to isomorphism) designs with the given parameters and minimum dimension. This generalizes a well-known characterization of the binary hyperplane designs in terms of their minimum 2-rank. The proof utilizes the q-ary analogue of the Hamming code, and a group-theoretic characterization of the classical designs.

HAROLD N. WARD

Divisible Codes

Let C be a linear code over GF(q). An integer D is a divisor of C if D divides the weight of every member of C. C is called divisible if it has a divisor bigger than 1. When D and q are relatively prime, C is equivalent to a D-fold replicated code, perhaps with extra zero coordinates.

If q is a power of the prime p, and p^e divides C but p^{e+1} does not, e is called the exponent of C. If G is a subgroup of the group of C, one seeks to relate e to properties of C as a G-module. The present paper illustrates these connections for the case $q = 2$. They are established by using a polarization process applied to the weight function w on C and to $w/2^e$ read modulo 2. The results presented are in part a summary of material from the author's chapter in the forthcoming "Handbook of Coding Theory." The talk mentions recent applications to codes meeting the Griesmer bound.

Qing Xiang

Hyperovals, cyclic difference sets and codes

(Joint work with Ron Evans and Christian Krattenthaler)

Recently, Maschietti constructed three families of $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$ cyclic difference sets by using monomial hyperovals in $PG(2, 2^d)$. In this talk, we first give a new proof for Maschietti's construction by using Jacobi sums. Then using Stickelberger's theorem on the prime ideal factorization of Gauss sums, we compute the 2-ranks for the difference sets from the Segre hyperovals. For the difference sets from the Glynn hyperovals, we conjecture that their 2-ranks satisfy certain 5-term recurrence relations.

Victor Zinoviev

On $\mathbb{Z}_4$-linear Goethals codes and Kloosterman sums

(Joint Work with Tor Helleseth)

Studying the coset weight distributions of the well known binary $\mathbb{Z}_4$-linear Goethals codes, we connect these codes with the Kloosterman sums. From one side, we obtain for some cases, of the cosets of weight four, the exact expressions for the number of code words of weight four in terms of the Kloosterman sums. From the other side, we obtain some limitations for the possible values of the Kloosterman sums, which improve the well known results due to Lachaud and Wolfmann.

Berichterstatter: Jörg Eisfeld (Gießen)

Programme of the conference

Monday, 16 March 1998

09:15–09:30	JACOBUS H. VAN LINT: Welcome
	Chair: Jacobus H. van Lint
09:30–10:30	AIDEN BRUEN: Binary linear codes of minimum distance 4
10:30–11:30	YURY J. IONIN: A technique for constructing symmetric designs
11:30–12:30	ROBERT A. CALDERBANK: Orthogonal geometry and quantum error correction
	Chair: Jacob J. Seidel
16:00–17:00	HAROLD N. WARD: Divisible Codes

Tuesday, 17 March 1998

	Chair: James W. P. Hirschfeld
09:15–10:15	VLADIMIR I. LEVENSHTEIN: Relationships between bounds for codes and designs in the Hamming and Johnson spaces
10:20–11:20	QING XIANG: Hyperovals, Cyclic difference sets and codes
11:25–12:25	E. F. ASSMUS: Variations on a theme of Delsarte: the coding theory of nets
	Chair: Richard M. Wilson
16:00–17:00	JÜRGEN BIERBRAUER: Codes and caps

Wednesday, 18 March 1998

	Chair: Joseph A. Thas
09:15–10:15	VICTOR A. ZINOVIEV: On $\mathbb{Z}_4$-linear Goethals codes and Kloosterman sums
10:20–11:20	MOHAN SHRIKHANDE: On classification of two class partially balanced designs
11:25–12:25	SHUHONG GAO: Absolute irreducibility of polynomials via Newton polytopes

Thursday, 19 March 1998

	Chair: Marialuisa de Resmini
09:15–10:15	BERNHARD SCHMIDT: Towards Ryser's conjecture and more

* * *

Memorial session for E. F. Assmus

	Chair: Dieter Jungnickel
14:00–14:25	TOR HELLESETH: 3-Designs from Preparata codes, Kerdock codes and related codes over $\mathbb{Z}_4$
14:25–14:50	IWAN DUURSMA: Split weight enumerators for Preparata codes with applications to designs
14:50–15:45	JONATHAN JEDWAB: Golay complementary sequences and Reed-Muller codes
16:30–17:25	VLADIMIR D. TONCHEV: Linear perfect codes and a characterization of the classical designs
17:30–17:45	ROBERT A. CALDERBANK: E. F. Assmus

Gefördert durch DFG Deutsche Forschungsgemeinschaft

List of email-addresses

Simeon Ball	simeon@win.tue.nl
Jürgen Bierbrauer	jbierbra@mtu.edu
Aart Blokhuis	aartb@win.tue.nl
Andries E. Brouwer	aeb@win.tue.nl
Aiden A. Bruen	bruen@uwovax.uwo.ca
Robert A. Calderbank	rc@research.att.com
Yuqing Chen	yuqchen@math.ohio-state.edu
Gerard D. Cohen	cohen@inf.enst.fr
James Davis	jdavis@richmond.edu
Michel M. Deza	deza@dmi.ens.fr
John F. Dillon	jfdillon@afterlife.ncsc.mil
Hans Dobbertin	dobbertin@skom.rhein.de
Iwan Duursma	duursma@resaerch.att.com
Jörg Eisfeld	joerg.eisfeld@math.uni-giessen.de
Shuhong Gao	sgao@math.clemson.edu
Chris Godsil	chris@bilby.uwaterloo.ca
Willem H. Haemers	haemers@kub.nl
Tor Helleseth	tor.helleseth@ii.uib.no
Raymond Hill	r.hill@cms.salford.ac.uk
James W. P. Hirschfeld	jwph@sussex.ac.uk
Henk D. L. Hollmann	hollmann@natlab.research.philips.com
Daniel R. Hughes	d.r.hughes@qmw.ac.uk
Yury J. Ionin	yury.ionin@cmich.edu
Jonathan Jedwab	jij@hplb.hpl.hp.com
Dieter Jungnickel	jungnickel@math.uni-augsburg.de
Jennifer D. Key	keyj@math.clemson.edu
Vladimir I. Levenshtein	leven@spp.keldysh.ru
Jacobus H. van Lint	wsdwjhvl@urc.tue.nl
Klaus Metsch	klaus.metsch@math.uni-giessen.de
Christine O'Keefe	cokeefe@maths.adelaide.edu.au
Alexander Pott	pott@math.uni-augsburg.de
Marialuisa de Resmini	resmini@mercurio.mat.uniroma1.it

Bernhard Schmidt	schmidt@cco.caltech.edu
Mohan Shrikhande	3iamxmz@cmuvm.csv.cmich.edu
Gabor Simonyi	simonyi@circle.math-inst.hu
Tamas Szőnyi	szonyi@cs.elte.hu
Joseph A. Thas	jat@cage.rug.ac.be
Aimo Tietäväinen	tietavai@cs.utu.fi
Henk C. A. van Tilborg	henkvt@win.tue.nl
Vladimir D. Tonchev	tonchev@mtu.edu
Scott A. Vanstone	savanstone@crypto3.uwaterloo.ca
Harold N. Ward	hnw@server1.mail.virginia.edu
Richard M. Wilson	rmw@cco.caltech.edu
Qing Xiang	xiang@ceres.math.udel.edu
Victor A. Zinoviev	zinov@ippi.ras.ru

Tagungsteilnehmer

Prof.Dr. Edward F. Assmus
Department of Mathematics
Lehigh University
14 E. Packer Avenue

Bethlehem , PA 18015-1237
USA

Prof.Dr. Aiden A. Bruen
Dept. of Mathematics
University of Western Ontario

London, Ontario N6A 5B7
CANADA

Dr. Simeon Ball
Department of Mathematics
Technische Universiteit Eindhoven
Postbus 513

NL-5600 MB Eindhoven

Prof.Dr. A. Robert Calderbank
AT&T Labs-Research
PO Box 971
180 Park Avenue

Florham Park , NJ 07932-0971
USA

Dr. Jürgen Bierbrauer
Dept. of Mathematical Sciences
Michigan Technological University
1400 Townsend Drive

Houghton , MI 49931-1295
USA

Yuqing Chen
Department of Mathematics
Ohio State University
231 West 18th Avenue

Columbus , OH 43210-1174
USA

Prof.Dr. Aart Blokhuis
Department of Mathematics
Technische Universiteit Eindhoven
Postbus 513

NL-5600 MB Eindhoven

Prof.Dr. Gerard D. Cohen
ENST
Dept. d'Informatique
46, rue Barrault

F-75013 Paris

Prof.Dr. Andries E. Brouwer
Department of Mathematics
Technische Universiteit Eindhoven
Postbus 513

NL-5600 MB Eindhoven

Dr. James Davis
Dept. of Math. and Computer Science
University of Richmond

Richmond , VA 23173
USA

Prof.Dr. Michel M. Deza
CNRS
17, passage de l'Industrie

F-75010 Paris

Dr. John F. Dillon
National Security Agency
Dept. of Defense
Office of Mathematical Research

Fort George G. Meade MD 20755
USA

Prof.Dr. Hans Dobbertin
Masurenweg 5

53119 Bonn

Dr. Iwan Duursma
AT&T Labs-Research
PO Box 971
180 Park Avenue

Florham Park , NJ 07932-0971
USA

Dr. Joerg Eisfeld
Mathematisches Institut
Universität Gießen
Arndtstr. 2

35392 Gießen

Prof.Dr. Shuhong Gao
Dept. of Mathematical Sciences
Clemson University
Martin Hall

Clemson , SC 29634-1907
USA

Prof.Dr. Chris Godsil
Department of Combinatorics and
Optimization
University of Waterloo

Waterloo , Ont. N2L 3G1
CANADA

Dr. W. Willem H. Haemers
Department of Econometrics
Tilburg University
P. O. Box 90153

NL-5000 LE Tilburg

Prof.Dr. Tor Helleseth
Department of Informatics
University of Bergen
Hoyteknologisenteret

N-5020 Bergen

Prof.Dr. Raymond Hill
Dept. of Mathematics
University of Salford

GB-Salford M5 4WT

Prof.Dr. James W.P. Hirschfeld
School of Mathematical and
Physical Sciences
University of Sussex

GB-Brighton BN1 9QH

Prof.Dr. Dieter Jungnickel
Institut für Mathematik
Universität Augsburg

86135 Augsburg

Prof.Dr. Henk D.L. Hollmann
Philips Research Laboratories
Room WY 8.56

NL-5656 AA Eindhoven

Prof.Dr. Jennifer D. Key
Dept. of Mathematical Sciences
Clemson University
Martin Hall

Clemson , SC 29634-1907
USA

Prof.Dr. Daniel R. Hughes
School of Mathematical Sciences
Queen Mary and Westfield College
University of London
Mile End Road

GB-London , E1 4NS

Prof.Dr. Vladimir I. Levenshtein
M.V. Keldysh Institute of Applied
Mathematics
Russian Academy of Sciences
Miusskaya pl. 4

125047 Moscow
RUSSIA

Prof.Dr. Yury J. Ionin
Dept. of Mathematics
Central Michigan University

Mt Pleasant , MI 48859
USA

Prof.Dr. Jacobus H. van Lint
Dept. of Mathematics and
Computing Science
Eindhoven University of Technology
Postbus 513

NL-5600 MB Eindhoven

Dr. Jonathan Jedwab
Hewlett-Packard Labs.
Filton Road, Stoke Gifford

GB-Bristol , BS 12 6QZ

Dr. Klaus Metsch
Mathematisches Institut
Universität Gießen
Arndtstr. 2

35392 Gießen

Prof.Dr. Christine O'Keefe
Department of Pure Mathematics
University of Adelaide

Adelaide S.A. 5005
AUSTRALIA

Prof.Dr. Mohan Shrikhande
Dept. of Mathematics
Central Michigan University

Mt Pleasant , MI 48859
USA

Prof.Dr. Alexander Pott
Institut für Mathematik
Universität Augsburg

86135 Augsburg

Prof.Dr. Gabor Simonyi
Mathematical Institute of th
Hungarian Academy of Scienc
P.O. Box 127
Realtanoda u. 13-15

H-1364 Budapest

Prof.Dr. Marialuisa de Resmini
Dipartimento di Matematica
Universita degli Studi di Roma I
"La Sapienza"
Piazzale Aldo Moro, 2

I-00185 Roma

Prof.Dr. Tamas Szőnyi
Department of Computer Science
Eötvös University
ELTE TTK
Muzeum krt. 6 - 8

H-1088 Budapest VIII

Dr. Bernhard Schmidt
Institut für
Angewandte Mathematik II
Universität Augsburg

86135 Augsburg

Prof.Dr. Joseph A. Thas
Seminar of Geometry & Combinatorics
Universiteit Gent
Krijgslaan 281

B-9000 Gent

Prof.Dr. Jacob J. Seidel
Vesaliuslaan 26

NL-5644 HK Eindhoven

Prof.Dr. Aimo Tietäväinen
Institute of Mathematical Sciences
University of Turku

SF-20014 Turku

Prof.Dr. Henk C.A. van Tilborg
Department of Mathematics
Technische Universiteit Eindhoven
Postbus 513

NL-5600 MB Eindhoven

Dr. Qing Xiang
Department of Mathematical Sciences
University of Delaware
501 Ewing Hall

Newark , DE 19716-2553
USA

Prof.Dr. Vladimir D. Tonchev
Dept. of Math. Sciences
Michigan Technological University
1400 Townsend Drive

Houghton , MI 49931
USA

Prof.Dr. Victor A. Zinoviev
Inst. for Information and
Transmission Problems
Russian Academy of Sciences
Bol'shoi Karetnyi 19

101447 Moscow GSP-4
RUSSIA

Prof.Dr. Scott A. Vanstone
Department of Combinatorics and
Optimization
University of Waterloo

Waterloo , Ont. N2L 3G1
CANADA

Prof.Dr. Harold N. Ward
Dept. of Mathematics
University of Virginia
Kerchof Hall
Cabell Drive

Charlottesville , VA 22903-3199
USA

Prof.Dr. Richard M. Wilson
Dept. of Mathematics
California Institute of Technology

Pasadena , CA 91125
USA