MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Tagungsbericht 17/1994

Designs and Codes

17. bis 23. April 1994

Die Tagung fand unter der Leitung von Herrn Jungnickel (Augsburg) und Herrn van Lint (Eindhoven) statt.

The 1994 meeting on Designs and Codes was the second one on this topic in Oberwolfach after the first conference in April 1990.

Design Theory and Coding Theory are two areas in Discrete Mathematics which are closely related and of course, both communities benefit from the opportunity to bring together leading researchers working in both areas, which was one of the main aims of this conference. There were 43 participants from 12 countries, among them 16 from North America.

Of the many interesting lectures, two talks provided particular highlights by solving major longstanding open problems. First, the puzzling formal duality between the Preparata and Kerdock codes has finally been explained by realizing that these non-linear binary codes are projections of linear $\mathbb{Z}_4$-codes which are in fact duals. Secondly, a major breakthrough in the asymptotic existence of designs has been achieved by proving that orthogonal arrays of arbitrary strength t (with k rows and index 1) exist for all sufficiently large orders (for fixed k, t). This is the first asymptotic result for designs with $t \geq 3$.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Vortragsauszüge

R. Ahlswede:

Number theoretic correlation inequalities for Dirichlet densities.

For sets $A, B \subset \mathbb{N}$, the set of positive integers, consider the set of least common multiples $[A, B] = \{[a, b] : a \in A, b \in B\}$, the set of largest common divisors $(A, B) = \{(a, b) : a \in A, b \in B\}$, the set of products $A \times B = \{a \cdot b : a \in A, b \in B\}$ and the set of their multiples $M(A) = A \times N$, $M(B)$, $M[A, B]$, $M(A, B)$, and $M(A \times B)$, respectively.

Our first discoveries are the inequalities

$$dM(A, B) \cdot dM[A, B] \geq dM(A) \cdot dM(B) \tag{1}$$

$$dM(A) \cdot dM(B) \geq dM(A \times B) \tag{2}$$

where d denotes the asymptotic density and A, B are finite. The first inequality is by the factor $dM(A, B)$ sharper than Behrend's well-known inequality. The second inequality does not seem to have number theoretic predecessors.

The next discovery is that (1) can easily be derived from the Ahlswede/Daykin inequality via Dirichlet series. Actually, we found this way the much more general inequality

$$\underline{D}(A, B) \cdot \underline{D}[A, B] \geq \underline{D}A \cdot \underline{D}B. \tag{3}$$

where $\underline{D}$ denotes the lower Dirichlet density and A, B are *arbitrary* subsets of $\mathbb{N}$. The applications of the AD-inequality give now correlation inequalities not only in Statistical Physics (Harris, FKG), Probability Theory (Holley), Combinatorics (Kleitman, Seymour/Webster, Marica/Schönheim), but also in Number Theory.

E.F. Assmus, Jr:

Where does the Mattson-Solomon polynomial live ?

We give an elementary proof of Berman's Theorem characterizing the Reed-Muller code $\mathcal{R}(n,m)$ as J^{m-n} where J is the Jacobson radical of the group ring $\mathbb{F}_2[G]$ where G is an elementary abelain 2-group of order 2^m. The essential new ingredient is the observation that $\mathcal{R}(n,m)$ is generated by the characteristic functions of the $(m-n)$-dimensional *subspaces* of the affine geometry of $G \approx \mathbb{F}_2^m$.

We contrast this very easy proof with the current more involved proof of Charpin's generalization to $\mathbb{F}_p$ of Berman's Theorem. We make some progress in simplifying this discussion by describing - in the most general case - an $\mathbb{F}_q$-algebra isomorphism between the $\mathbb{F}_q$-algebra

$$\mathbb{F}_q[x_1,\dots,x_m]/(x_1^q - x_1,\dots,x_m^q - x_m)$$

and the $\mathbb{F}_q$-algebra of fixed points of the Frobenius map, $\zeta \to \zeta^q$, of the algebra

$$\mathbb{F}_{q^m}[Z]/(Z^{q^m} - Z).$$

Th. Beth:

Designs, Codes and Puzzles.

Owing to the more practical problem of finding the algebraic classification of the solution for a special rather complicated toy puzzle, commercially available under the name DISCO, we consider the following

Pegging Problem: Let $N = \{w_0,\dots,w_{d-1}\}$ be a transversal for the $d =$ 14 orbits of the group $G = \mathbb{Z}_6$ acting regularly on the coordinates of $W = GF(2)^6$. By canonically embedding $W \simeq GF(2)[z]/(z^6-1)$ with the action $\mathbb{Z}_6 \ni i : w(z) \to z^i w(z) \bmod (z^6-1)$ the problem reads:

Find an arrangement $i_k \in G, j \in S_d$

$$A(z) = \left(z^{i_k} w_{jk}(z)\right)_{k=0}^{13} \bmod (z^6-1)$$

of cyclically rotated words of N in such a way that every column A_i in $A(z) = \sum_{i=0}^{5} A_i z^i$ can be partitioned into disjoint words of 3 consecutive ones, forming the *pegs*.

0	0	0
1	0	0
1	1	0
1	1	1
α	1	1
α	0	1
α	α	0
0	α	α
1	α	α
1	0	α
1	α	α
α	α	α
α	α	0
α	0	0

Several approaches to solving this problem algorithmically in spite of the huge searchspace of $(13!)\cdot 6^9\cdot 3^2\cdot 2$ are presented. By considering the patterns in W as vectors of $GF(2^6)$ with respect to a normal basis over $GF(2)$ the canonical isomorphism $\mathbb{Z}_6 \simeq \mathbb{Z}_3\times\mathbb{Z}_2$ allows a design type solution in an efficient algebraic definition of sequences in $GF(4)^3$ with $GF(4) = \{1, \alpha, \alpha + 1 = \alpha^2, 0\}$. The solution reads as in the figure.

From here it was similarly easy, to give an algebraic construction for the modified Pegging Problems

(a) with $G = \mathbb{Z}_6$ on $W - \{1\}$

(b) with $G = D_6$ on W

the latter one being the commercially available toy.

Open questions are posed as to which class of designs or codes the presented solutions belong.

I. F. Blake:
Decoding Reed-Solomon codes.

The Welsh-Berlekamp algorithm is an efficient means of decoding Reed-Solomon codes that does not involve the computation of syndromes. A brief description of this algorithm is given, showing in particular how the set of equations requiring simultaneous solution, is carried out. It is also shown the problem can be translated to an algorithm for the solution of polynomial congruences. A new module theoretic approach to the solution of such congruences is proposed. From this approach new and efficient parallel algorithms to solve the WB equations are derived.

A. Brouwer:
Correspondence between symmetric bilinear forms and alternating forms.

In a dual polar space (in the classical situations where maximal totally isotropic or totally singular subspaces have half the dimension of the surrounding space) the collection of t.i. (t.s.) subspaces disjoint from a given one can be naturally identified with a space of forms or matrices: one gets

(i) all alternating matrices (from D_n)
(ii) all symmmetric matrices (from C_n)
(iii) all Hermitian matrices.

Noting that a nondegenerate hyperplane in a D_n geometry carries a B_{n-1} geometry, and that in even characteristic $B_{n-1} \cong C_{n-1}$, we find in even characteristic a one-to-one correspondence

$$P \longrightarrow \begin{pmatrix} 0 & \sqrt{d}^T \\ \sqrt{d} & P + \sqrt{d}\sqrt{d}^T \end{pmatrix}$$

between symmetric matrices of order m and alternating matrices of order order $m+1$. One of the consequences is a geometric explanation of a property noted by Calderbank.

A. A. Bruen:

(a) 10_3 configurations in Desarguesian planes.

(Joint work with J.C.Fisher)

(b) Independent sets of points in projective and affine spaces.

(Joint work with D.Wehlau and L.Haddad)

(a) We briefly discuss a beautiful observation by G. Pickert, pursuant to a paper by Bruen and Fisher, on the embeddability of a certain 10_3 configuration in a projective plane which is Desarguesian but not Pappian.

(b) In PG(n,q) let S be line-free. Then $\overline{S}$, the complement of S, intersects all lines. If $\overline{S}$ does not contain a hyperplane we say that S is *projective*; otherwise, S is affine. If S is projective, each hyperplane contains at least one point of S. We elaborate on the following observation:

If $|S|$ is large, S must be affine. In particular, in PG$(n,2)$, if $|S| > 5{\cdot}2^{n-3}$ then S must be affine.

We also desribe other intersection properties in PG$(n,2)$. Results similar to some of these have been obtained by E. Clark and by A.A. Davydov and L.M. Tombak.

The geometries AG$(n,3)$ and PG$(n,2)$ are Steiner triple systems and colourings of their points, such that no line is monochromatic, are of interest. These colourings give line-free sets. In AG$(4,3)$ we show that a line-free set has at most 20 points and we describe geometrically the unique line-free set on 20 points. (Part of this result, at least, is due originally to R. Hill.) We also skirmish with line-free sets in AG$(5,3)$.

A.R. Calderbank:

Codes, Geometries and Extremal Sets of Euclidean Lines with Prescribed Angles.

We describe how Kerdock codes over the binary field $\mathbb{Z}_2$ and over the ring $\mathbb{Z}_4$ of integers modulo 4 determine extremal sets of lines in real and complex Euclidean space with only two angles. Extraspecial 2-groups serve as the bridge between discrete and Euclidean geometries. Classical geometric/group theoretic connections between binary symplectic and orthogonal geometries are expressed as a correspondence between binary symmetric $m \times m$ matrices and binary skew-symmetric $(m+1) \times (m+1)$ matrices.

G. Cohen:

Generalized Weights (upper bounds).

The *generalized i-distance* d_i of an $[n, k]$ binary linear code C is the minimum size of the union of the supports of i independent codewords of C. We derive new upper bounds on d_i (Hamming, Plotkin, Elias). For the last one, which is the strongest asymptotically, we need a nonlinear extension of the concept of i-distance:

Definition: Let C be any binary code (subset of $\mathbb{F}_2^n$). Then set

$$d_i(C) := min|supp(c_1 + t) \cup supp(c_2 + t) \cup \ldots \cup supp(c_i + t)|,$$

where the minimum is taken over all $(i+1)$-tuples $(t, c_1, c_2, \ldots, c_i)$ such that $c_1 + t$. $c_2 + t$, …, $c_i + t$ are linearly independent.

Theorem: Fix i. Let $R(\delta_i)$ be the largest possible asymptotic rate (k/n) of a code with normalized i-distance $d_i/n = \delta_i$. Then

$$R(\delta_i) \leq 1 - H(\lambda),$$

where $H(\cdot)$ is the binary entropy function and λ is the smallest root of

$$\delta_i = 1 - x^{i+1} - (1-x)^{i+1}.$$

M. Daberkow:

Computing invariants of algebraic number fields.

We gave a list of major problems in the field of constructive algebraic number theory, which is due to H. Zassenhaus:

For a given number field F we are interested in the computation of the following invariants of F:

- the ring of integers o_F
- the unit group U_F
- the class group Cl_F and the class number h_F
- the Galois group.

Starting with the Round-2 algorithm by H. Zassenhaus, we presented some algorithms for the construction of integral basis and introduced the idea of p-maximal overorders. Based on the Round-2 we showed some improvements using p-adic numbers. If the field $F = \mathbb{Q}(\alpha)$ is generated by a root of the polynomial $f(t) \in \mathbb{Z}[t]$, one can use a factorization of f modulo p and Hensel's Lifting to get polynomials $f_1, \dots, f_k$, such that the p-maximal order of $\mathbb{Z}[\alpha]$ can be derived from the p-maximal orders of $G_i := \mathbb{Q}[t]/(f_i(t))$ $(1 \leq i \leq k)$.

The final part of the talk dealed with the problem of relative integral bases in extensions E/F with $\mathbb{Q} \subsetneq F \subsetneq E$. In the case $[E : F] = 2$, a solution of this problem has been given.

F. De Clerck:
On Generalized Quadrangles minus a Hyperplane.

P.J. Cameron raised the question of finding a characterization of partial quadrangles which have linear representations. An almost complete answer was given by R. Calderbank et al., the proof was a number-theoretic one. Here we discussed a more general class of geometries, S_p, those coming from generalized quadrangles S by deleting the set $p^\perp$, for a point p of S. S_p has the property that it is a $(0,1)$-geometry, but the graph is only strongly regular (hence S_p is a partial quadrangle) if $t = s^2$. S_p has the property $(*)$:

If L and M are two disjoint lines of S_p, then there are either 0, $s-1$ or s lines of S_p concurrent to both L and M.

Our result (joint work with Hendrik Van Maldeghem) is:

If $T_n^*(K)$ $(n \geq 3)$ is a linear representation of a $(0,1)$-geometry satisfying $(*)$, and if $s > 2$, then $T_n^*(K)$ is the partial quadrangle $T_3^*(O)$, O an ovoid.

J. Doyen:
Lotto Numbers and Steiner Systems.

The Lotto number $L(n,k,l,t)$ is defined as the smallest number of k-subsets (= Lotto tickets) of the set $N = \{1, 2, \dots, n\}$ such that any l-subset of N meets at least one of them in at least t elements (this l-subset is interpreted as the set of winning numbers). We gave lower and upper bounds for the numbers $L(42,6,6,t)$ and $L(49,6,6,t)$ corresponding to the Lotto as played in Belgium and Germany. The upper bounds often use Steiner systems. For example, using Denniston's $S(4,6,27)$, we get $1014 \leq L(49,6,6,4) \leq 13120$ (after the talk, this upper bound was lowered to 3784 by Andries Brouwer).

D. A. Drake:
A Theorem on Squeezes in the Game of Bridge.

Let p be the number of cards remaining per hand, and let r be the number of tricks which can run by North/South in a no-trump contract. Then North/South can only "squeeze" East/West out of another trick if $r = 1$ and $p = 3$ or if $p \leq 2r$. There are no squeezes with $p < 3$, and the inequality is best possible for every p with $3 \leq p \leq 12$. It is also true that the only no-trump squeezes with $p = 2r$ are triple squeezes.

T. Etzion:
Generalized designs and constant weight codes over finite alphabets.

We consider optimal constant weight codes over finite alphabets. These codes can be considered as generalization of Steiner systems. Other codes are reductions of orthogonal arrays into constant weight codes. Finally, in some of these codes two types of Steiner systems exist, generalized and non-generalized.

M. van Eupen:
An optimal ternary [69,5,45] code and related codes.

A ternary [69,5,45] code is constructed, thus solving the problem of finding the minimum length of a ternary code of dimension 5 and minimum distance 45. Furthermore, this code is shown to be a unique two-weight code with weight enumerator $1 + 210z^{45} + 32z^{54}$. It is also shown that a ternary [70,6,45] code, which would have been a projective two-weight code giving rise to a new strongly regular graph, does not exist. In order to prove the main results, the uniqueness of some other optimal ternary codes with specified weight enumerators is also established.

D. Hachenberger:
On Finite Elation Generalized Quadrangles with Symmetries.

We consider the structure of finite groups which act as elation groups with symmetries on finite generalized quadrangles. Such a group is related to the translation group of a translation transversal design with parameters depending on that of the quadrangle. Using results on the structure of p-groups which act as translation groups on a transversal design, and results on the index of the Hughes subgroup of a finite p-group, we can show how restricted the structure of an elation group with symmetries of some finite generalized quadrangle is. One of our main results is the following:

If G is a finite group of even order s^2t which admits a 4-gonal family $(\mathcal{F}, \mathcal{F}^*)$ of type (s, t), and if one member of $\mathcal{F}$ is a normal subgroup of G, then, necessarily, G is an elementary abelian 2-groups

W. Haemers:
Spreads in Strongly Regular Graphs.

Let G be a strongly regular graph with eigenvalues k, r and s $(k > r > s)$. Delsarte proved that a clique has at most $1 - k/s$ vertices. Cliques with this size are called lines. A spread of G is a partition of the vertex set into lines. Such a spread gives rise to a 3-class association scheme. A necessary condition for the complement of G to have a spread is $kr \geq s^2$. Examples come from spreads and fans in (partial) geometries. An interesting example was found by Tonchev, who found spreads in the McLaughlin graph.

R. Hill:
"Mastermind" for four-year-olds.

We consider some variants of the game of "Mastermind" including the following version, which is suitable for play with 4-year-olds.

A coder chooses a codeword which is a permutation (i.e. no repetitions) of k colours from n. A guesser must determine the codeword by making guesses, each guess being a permutation. After each guess the coder says which colours are correct. Let $f(n, k)$ be the smallest number of guesses needed to determine any codeword. Clearly $f(n, k) \leq n$ and we conjecture that $f(n, k) = n$ for all n and k $(k \leq n)$. The conjecture is easily proved for $k \leq 4$ (all n) and for $n = k$.

J.W.P. Hirschfeld:
Projective Geometry Codes.

Let M be a $b \times v$ incidence matrix of $v = |PG^{(0)}(n, q)|$ points and $b = |PG^{(r)}(n, q)|$ subspaces of dimension r for a finite projective space $PG(n, q)$. Let $C(r, n, q)$ be the code generated over $\mathbb{F}_p$, p prime where $q = p^h$, by the rows of M and let $C^*(r, n, q)$ be the dual code, which therefore represents sets of weighted points meeting each r-space in a multiple of p points. Hamada's formula says that

Gefördert durch DFG Deutsche Forschungsgemeinschaft

$$\dim C^{*}(r,n,q) = \frac{q^{n+1}-1}{q-1} - \sum_{(s_0,\ldots,s_h)} \prod_{j=0}^{h-1} \sum_{i=0}^{L(s_{j+1},s_j)} (-1)^i \binom{n+1}{i} \binom{n+s_{j+1}p-s_j-ip}{n},$$

where the first sum is over all ordered sets $(s_0,\ldots,s_h)$ of $h+1$ integers s_j such that

$$s_h = s_0,\ 0 \leq s_j \leq n-r,\ 0 \leq s_{j+1}p - s_j \leq (n+1)(p-1),$$

and

$$L(s_{j+1},s_j) = \lfloor (s_{j+1}p - s_j)/p \rfloor.$$

It is shown that, when $h = 1$, this formula can be replaced by a single summation:

$$\dim C^{*}(r,n,p) = \sum_{j=0}^{r-1} (-1)^j \binom{(r-j)(p-1)-1}{j} \binom{n+(r-j)p-r}{n-j}.$$

C.Y. Ho:

Regular collineation groups of a finite projective plane.

We mention the following results:

(1) A characterization of an abelian planar Singer group.

(2) The multiplier group of a planar Singer group always fixes a line.

(3) Let H be an abelian group of multipliers of a planar Singer group of planar order n. If $|H| = n+1$, then n^2+n+1 is a prime. If $|H|$ is odd, then $|H|$ is at most $n+1$.

(4) For any complex number x, let $v(x) = x^2+x+1$. If p is any prime different from 3 and m is any positive integer, then $v(m^p) = \prod_{\sigma \in <\theta>} v(m\sigma)$, where θ is a complex p-th root of unity. Also the greatest common divisor of $v(m)$ and $v(m^p)/v(m)$ divides p.

(5) Suppose an abelian Singer group is not normal in the collineation group. If the planar order n is not a square or $n = m^2$ with $m \equiv 2,3$ (mod 4), then the plane is Desarguesian.

J.D. Key:

Extending Steiner triple systems using codes.

We use the linear code associated with a design by forming the space spanned by the incidence vectors of the blocks over a finite field $\mathbb{F}_p$, where p is a prime, to give some partial answers to the following question: Can every Steiner triple system be extended?

Let $\mathcal{D}$ be a $2-(v,3,1)$ design and let $C_p(\mathcal{D})$ denote its code over $\mathbb{F}_p$. Then if $p = 2$ and $2^d - 1 \leq v < 2^{d+1} - 1$, $C_2(\mathcal{D}) \geq \mathcal{H}_d$, a Hamming code: if $p = 3$ and $3^d - 1 \leq v < 3^{d+1}$, $C_3(\mathcal{D}) \geq \mathcal{R}_{\mathbb{F}_3}(2(d-1),d)$, a generalized Reed-Muller code. From this we have:

(i) If $v = 2^d - 1$ and $\dim(C_2(\mathcal{D})) = 2^d - d$, then $\mathcal{D}$ can be extended and in such a way that the binary code of the extension is the extended code:

(ii) if $v = 3^d$ and $\dim(C_3(\mathcal{D})) = 3^d - d$, then $\mathcal{D}$ can be extended.

I. Landgev:

Nonexistence of some Quaternary Codes.

We demonstrate the nonexistence of quaternary codes with parameters [56,4,41], [104,4,77].

This result violates also codes with parameters [57,4,42], [105,4,78], [106,4,79], [107,4,80].

Thus the only value of d, for which $n_4(4,d)$ remains unknown is $d = 37$.

S.L. Ma:

Regular Automorphism groups on partial geometries.

Suppose a partial geometry $pg(s+1,t+1,\alpha)$ admits an automorphism group G acting regularly on the points so that the points of the geometry can be identified with the elements of G. Let $L_0, L_1, \ldots, L_t$ be the lines passing through e. I find that G is a direct product of two groups of relatively prime orders and if $L_i = L_i^{(-1)}$ for all i, then the geometry is a translation net. Applying the result to the case when $s = t$ and G is abelian, I find that either the geometry is a translation net or all the lines of the geometry are of the form gL_0, $g \in G$. Also, for the latter case, all known examples have parameters $\alpha = s$ or $s+1$ except for the $pg(6,6,2)$ obtained by van Lint and Schrijver which has $(s,\alpha) = (5,2)$. I have checked that this is the only example if $s \leq 500$.

S. S. Magliveras:

Block Transitive Resolutions of t-designs and Room Rectangles.

(Joint work with R.A. Liebler and S.V. Tsaranov)

We call a partition of the trivial design $\binom{X}{k}$ of all k-subsets of a v-set X into $t-(v', k, \lambda)$ designs, $v' \leq v$, a *resolution* of t-designs. A resolution of t-designs with $v = v'$ is also called a *large set* of t-designs. A *Room rectangle* R, based on $\binom{X}{k}$ is a rectangular array whose nonempty entries are k-sets. This array has the furhter property that taken together the rows (columns) form a resolution of t_1-(t_2)-designs. One of these structures admits G as a block transitive automorphism group if G is a permutation group on the set X leaving invariant the structure and the k-sets of X fall in a single G-orbit. Some examples of block transitive resolutions of nontrivial t-designs $t \geq 2$ are:

(1) an M_{11}-invariant set of $3-(10,4,1)$ designs,
(2) an M_{12}-invariant set of $4-(11,5,1)$ designs,
(3) an M_{24}-invariant set of $2-(21,5,1)$ designs,
(4) a $P\Gamma L_2(2^s)$-invariant set of $3-(2^s,4,1)$ designs ($s = 3$ or 5),
(5) a $P\Gamma L_2(32)$-invariant set of $2-(16,4,1)$ designs, and
(6) a variety of $PSL_2(q)$-invariant sets of 2-designs with $k = 3$.

We show that this is a complete list. In particular there are no block transitive large sets of t-designs. Moreover, if $1 \neq a < b < c$ are odd integers such that $gcd(a.b) = 1$ and $ab|c$, then we construct a block transitive Room rectangle based on the 3-subsets of a $7^c + 1$-set whose rows (columns) are Steiner triple systems on 7^a (7^b) point.

K. Metsch:

Characterization of certain distance regular graphs.

We present some recent results that characterize the following distance regular graphs in terms of their parameters.

(1) The folded Johnson graphs $\bar{J}(2m, m)$, $m \geq 6$.
(2) The folded halved cubes of diameter $d \geq 8$.
(3) The Grassmann graphs $\Gamma(e, q, n)$ for $q \geq 4$, $2 < e < \frac{n-1}{2}$.

G. E. Moorhouse:

New distance regular graphs related to Preparata codes.

(Joint work with D. de Caen and R. Mathon.)

We present a new family of antipodal distance regular graphs $\Gamma(q, \sigma)$ of diameter three, related to the classical Preparata codes. Here $q = 2^{2t-1}$ and

Gefördert durch DFG Deutsche Forschungsgemeinschaft

$\langle\sigma\rangle = \mathrm{Aut}(GF(q))$. The graph $\Gamma(q,\sigma)$ is a q-fold cover of K_{2q}. For $q \geq 2^5$, we have $|\mathrm{Aut}\Gamma(q,\sigma)| = 2q(q-1)(2t-1)$, and $\Gamma(q,\sigma') \cong \Gamma(q,\sigma)$ iff $\sigma' = \sigma^{\pm 1}$. These results are analogous to those of Kantor (1983) for extended Preparata codes. Moreover, the Preparata codes may be synthetically produced from our graphs. The three-class association scheme for $\Gamma(q,\sigma)$ is formally dual to the scheme for the known systems of linked symmetric designs arising from Kerdock sets. This formal duality appears to be related to the formal duality between Preparata and Kerdock codes. It is hoped that the algebraic duality between $\mathbb{Z}_4$-linear Preparata and Kerdock codes (recently discovered by Sloane, Calderbank et al.) may help to explain this.

R. Mullin:
The Structure of Normal Bases over Finite Fields and some Specific Completely Normal Polynomials.

A normal basis of a finite field GF(q^n) over GF(q) can be defined to be a set S of zeroes of an irreducible polynomial of degree n over GF(q) which has the additional property that S is linearly independent. Such bases have applications in certain aspects of Communications Engeneering. In this talk, an example of such an application will be used to motivate the investigation of normal bases. A structural characterization of such bases will be given, and this will be used to construct infinite families of completely normal polynomials, that is, polynomials whose zeroes contain normal bases for all subfields between GF(q) and GF(q^n).

S. E. Payne:
New Hyperovals in PG$(2,q)$.

Let $q = 2^e$, $F =$GF(q). A q-clan is a set

$$C = \{A_t = \begin{pmatrix} x_t & y_t \\ 0 & z_t \end{pmatrix} : t \in F\}$$

of q 2×2 matrices over F for which $A_s - A_t$ is anisotropic for all $s,t \in F$, $s \neq t$. Since $q = 2^e$, a q-clan gives a generalized quadrangle of order (q^2, q) with subquadrangles of order q associated with ovals in PG$(2,q)$. As for all prime powers q there is also a flock of a quadratic cone, a line spread of PG$(3,q)$ and a translation plane. For each $q = 2^e$ there is a new so-called Subiaco q-clan. When $e \not\equiv 2 \pmod 4$, i.e., 5 does not divide $q+1$, there is, up to projective equivalence, just one oval with a stabilizer of order $2e$. When $e \equiv 2 \pmod 4$, there are two Subiaco ovals, one with stabilizer isomorphic to $C_5 \rtimes C_{2e}$, the other with stabilizer isomorphic to $C_5 \rtimes C_{e/2}$. We give here the one with the larger group, since it is the only case where the description is rather easy to give. Here GF(4) $\leq F$, so let $w \in F$ satisfy $w^2 + w + 1 = 0$. Then the oval has the form $\mathcal{O} = \{(1, t, f(t)) : t \in F\} \cup \{(0, 1, 0)\}$, with nucleus $(0, 0, 1)$, where $f(t) = \frac{w^2(t^4+t)}{(t^2+wt+1)^2} + t^{\frac{1}{2}}$.

K. Phelps:

Perfect Codes and Quadruple Systems.

We consider the question of whether every Steiner triple system of order 15 occurs as the words of weight 3 of some nonlinear perfect binary code of length 15. We review related results and describe an approach to answering this question. We also present some new discoveries.

V. Pless:

Generators for quadratic residue codes over various fields.

A class of cyclic codes called quadratic residue (Q.R.) codes over GF(q) exist at all prime length p where q is a square (mod p) and $\gcd(p, q) = 1$. For such a pair of p and q we define $Q(x) = \sum x^i$ where i ranges over the quadratic residues in GF(p) and $N(x) = \sum x^i$ for i a non-residue. The idempotent generator of any Q.R. code is of the form $a_0 + a_1 Q + a_2 N$. We give explicit values of a_0, a_1, a_2 for Q.R. codes over fields of characteristic 2 and 3 and also for GF(q) where q is odd, the length of p is $\equiv 3 \pmod 4$, and q divides $p + 1$.

A. Pott:

A new class of symmetric designs.

(Joint work with D. Jungnickel.)

We describe a construction of symmetric (v, k, λ)-designs with parameters

$$v = p^s \frac{q^{2m}-1}{q-1},\ k = p^{s-1} q^{2m-1} \text{ and } \lambda = p^{s-1} q^{2m-2} \frac{p^{s-1}-1}{p-1}$$

of order $p^{2s-2} q^{2m-2}$ provided that p is a prime and q is a prime power with $q = \frac{p^s-1}{p-1}$.

M. J. de Resmini:

Hyperovals in Figueroa Planes.

(Joint work with Nicholas Hamilton, U.W.A. Perth.)

We construct Hyperovals in the Figueroa planes of order q^3, q a power of 2, which are inherited from regular hyperovals in the Desarguesian plane

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

$PG(2, q^3)$ which are stabilized by the automorphism α of order 3. $\langle\alpha\rangle = \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^3})$ which provides the construction of the Figueroa plane.

M.A. Shokrollahi:
Stickelberger Codes.

Let p be an odd prime. The Stickelberger ideal $\mathcal{S}_p$ is an ideal in the integral group ring $\mathbb{Z}[G]$, G being the Galois group of the cyclotomic field $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. $\mathcal{S}_p$ annihilates the class group of $\mathbb{Q}(\zeta_p)$. Let q be another prime which is not a divisor of $p-1$ ($q = p$ possible !). We study the cyclic code ($\mathcal{S}_p$ mod q) $\trianglelefteq \mathbb{F}_q[G]$ of length $(p-1)$ and show that its dimension is closely related to the relative class number of $\mathbb{Q}(\zeta_p)$.

G. Simonyi:
Entropy and Uniform Hypergraphs.

Hypergraph entropy is an information theoretical functional on a hypergraph with a probability distribution on its vertex set. It is sub-additive with respect to the union of hypergraphs. In case of simple graphs, exact additivity for the entropy of a graph and its complement with respect to every probability distribution on the vertex set gives a characterization of perfect graphes.

Here we investigate uniform hypergraphs with an analogous behaviour of their entropy. The main result is the characterization of 3-uniform hypergraphs having this entropy splitting property. Partitioning the edge set of the complete uniform hypergraph into more than two parts with similar criteria is also discussed. For k larger than 3 it turns out that no non-trivial k-uniform hypergraph splits entropy in the above manner.

E. Spence:
Hadamard Matrices of order 28.

We report on an independent verification of a recent result of Kimura that there are precisely 487 pairwise non-isomorphic Hadamard matrices of order 28. We consider also the classification of skew Hadamard matrices of order 28 (in total there are 54) and mention an application of these to the possible construction of a symmetric (81, 16, 3) design, using an idea of Tonchev.

T. Szönyi:
Cyclic caps.

Consider a cyclic Singer group S of a Desarguesian projective space $PG(n, q)$,

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

and let H be a subgroup of S. We concentrate on the following question:

When are the point-orbits of H caps (complete caps)?

Using elementary properties of fields we give a short proof of some theorems by Ebert. Keeping $|H|$ fixed, these orbits are always caps if the characteristic of GF(q) is large enough compared to $|H|$.

J.A. Thas:

Symplectic spreads in PG($3,q$), inversive planes and projective planes.

A (line) spread in PG($3,q$) is any set of q^2+1 disjoint lines in PG($3,q$). The spread S is called symplectic if all lines in S are totally isotropic for some symplectic polarity ζ of PG($3,q$). An ovoid of PG($3,q$), $q>2$, is a set of q^2+1 points, no three of which are collinear; an ovoid of PG($3,2$) is the same as an elliptic quadric. An ovoid of the nonsingular quadric $Q(4,q)$ of PG($4,q$) is any set O of points of $Q(4,q)$ which has exactly one point in common with each line of $Q(4,q)$. Symplectic spreads of PG($3,q$) and ovoids of $Q(4,q)$ are equivalent objects, and, for q even, also ovoids of $Q(4,q)$ and ovoids of PG($3,q$) are equivalent objects.

With each symplectic spread of PG($3,q$) there corresponds a plane of order q^2. A $3-(q^2+1,q+1,1)$ design is called an inversive plane of order q. With each ovoid of PG($3,q$) there corresponds an inversive plane of order q.

Here we survey some important characterizations of inversive planes, the inversive planes of small order, the planes of small order arising from symplectic spreads of PG($3,q$), and all known classes of ovoids of PG($3,q$) resp. $Q(4,q)$.

V.D. Tonchev:

(a) Preparata Codes and a Class of 4-Designs.

(b) The Existence of extremal self-dual [50,25,10] codes and quasi-symmetric $2-(49,9,6)$ designs.

(a) An extension theorem for t-designs is proved. As an application, a class of $4-(4^m+1,5,2)$ designs is constructed by extending designs related to 3-designs formed by the minimum weight vectors in the Preparata code of length $n=4^m$, $m\geq 2$. The derived designs are doubles of AG($2m,2$). Although these 4-designs contain repeated blocks, they provide an infinite class of 4-designs with the smallest known fixed λ.

(b) All extremal binary self-dual [50,25,10] codes with an automorphism of order 7 fixing one coordinate are enumerated. The minimum weight codewords yield (previously unknown) quasi-symmetric $2-(49, 9, 6)$ designs.

S.A. Vanstone:
Graphs, Codes and Difference Sets.

Let G be a finite graph having p vertices, q edges and girth g. It is well known that the cycle space of G gives rise to a binary $[q, q-p+1, g]$-code C. In this talk we discuss various properties of these codes. For example, when p is even and $p \geq 2g$ (p odd and $p \geq 2g+1$) then one can always embed C in a binary $[q, q-p+2, g]$-code. This is accomplished by showing that every connected graph with an even number of vertices contains an odd spanning subgraph. We also determine when the code C coming from the complete graph is contained in a Hamming code. This result relies on the existence of certain difference sets in the elementary abelian 2-group. We conclude the talk with the discussion of constructing ternary codes from directed graphs and various open problems.

W. Willems:
Radical Codes.

By results of Berman and Charpin, Reed-Muller Codes over the prime field $\mathbb{F}_p$ may be considered as powers of the Jacobson radical of an elementary abelian p-group C_p^m. From this point of view, one easily sees that the affine general linear group AGL(m, p) acts on the radical powers $J^r(\mathbb{F}_p C_p^m)$. Moreover, via this action $\mathbb{F}_p C_p^m$ becomes a uniserial $\mathbb{F}_p$AGL(m, p)-module. As a consequence we have the Theorem (Knörr, Wi.):

Let C be a linear code over $\mathbb{F}_p$ of length p^m. Then AGL$(m, p) \leq Aut(C)$, if and only if C is a Reed-Muller Code.

This explains why the Reed-Muller Codes $J^{k(p-1)}(\mathbb{F}_p C_p^m)$ $(1 \leq k \leq m)$ are exactly the duals of the affine geometry codes. Now, from the point of view of group theory, there is no reason to restrict ourself to elementary abelian p-groups and the prime field. So let K be any finite field of characteristic p and let G be a finite p-group. Let U be a subgroup of G with $|G:U| = p^m$ and consider the radical powers $1_U^G J^r(KG)$ of the permutation module 1_U^G endowed with the natural basis $\{Ug | g \in G\}$. With this notation, a student of mine, A. Faldum, proved:

Theorem: (a) If dim $1_U^G J^r(KG) \overset{>}{\geq}$ dim $J^s(KC_p^m) \geq 1$, then for the minimum distances we have $d(1_U^G J^r(KG)) \overset{<}{\leq} d(J^s(KC_p^m))$.

(b) Suppose equality holds everywhere and dim$J^s(KC_p^m) \notin \{0, 1, p^m -$

$1, p^m\}$. Then either (1) $U \trianglelefteq G$ and $G/U \cong C_p^m$ or (2) $p = 2$, $r = 2s - 1$ and some conditions on the group G.

Remark: The Code $1_U^G J^r(KG)$ in the latter case is equivalent to $J^s(KC_p^m)$ for $r = 2s - 1$.

Summarizing the above results we see that in the large class of radicals of permutation modules over p-groups, the radical powers of a group-algebra over an elementary abelian p-group (which are the Reed-Muller Codes for $K = \mathbb{F}_p$) are optimal.

R.M. Wilson:

Two-error-correcting codes and absolutely irreducible polynomials over GF(2).

Let $n = 2^r + 1$, let ω be a primitive element in $\mathrm{GF}(2^r)$, and let C_t denote the set of binary polynomials $f(x)$ of degree $\leq n$ so that $f(\omega) = f(\omega^t) = 0$. That is, C_t is the binary cyclic code of length n generated by $m_1(x)m_t(x)$.

Words of weight ≤ 4 in C_t correspond to zeros of the projective plane curve

$$g_t(x,y,z) = \frac{x^t + y^t + z^t + (x+y+z)^t}{(x+y)(x+z)(y+z)}$$

with distinct coordinates over $\mathrm{GF}(2^r)$. Factorizations of $g_t(x,y,z)$ for $t = 2^i + 1$ and $t = 2^{2i} - 2^i + 1$ can be used to prove that such words do not exist, i.e. that C_t is two-error-correcting, when t has either of these forms with $(i, r) = 1$.

We conjecture that $g_t(x,y,z)$ is absolutely irreducible if t does not have one of these two forms. If $g_t(x,y,z)$ is absolutely irreducible, then the codes C_t are two-error-correcting for at most finitely many values of $n = 2^r - 1$. We prove the absolute irreducibility of $g_t(x,y,z)$ for $t \equiv 3 (\mathrm{mod}\ 4)$, $t > 3$. This is joint work with H. Janwa and G. McGuire.

R.M. Wilson:

Blanchard's theorem on asymptotic existence of transversal designs of strength $t \geq 3$.

This talk describes a recent result of John Blanchard. A *transversal design* TD(t, k, n) consists of a set X of kn points partitioned into k groups $G_1, G_2, \ldots, G_k$ of size n and a family $\mathcal{A}$ of transverse k-subsets so that every transverse t-subset of X is contained in exactly one member of $\mathcal{A}$. Here, a transverse subset of X is one that meets each group G_i in at most one point.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

Transversal designs TD$(2, k, n)$ are equivalent to $k-2$ pairwise orthogonal Latin squares of order n and the Chowla-Erdös-Straus theorem asserts that these exist for all n sufficiently large with respect to k. Blanchard's theorem is that for any strength t and block size k, $t \leq k$, transversal designs TD(t, k, n) exist for all $n > n(k)$.

The proof combines recursive constructions and direct constructions involving finite fields. We specifically discuss a technique that may be called 'spreading blocks' where a family of subsets $\mathcal{A}$ of a set U that covers some t-subsets q times and others not at all may be 'lifted' to a family of transverse subsets of $U \times V$ that covers *uniquely* those and only those transverse t-subsets that project onto covered subsets of U, when q is a prime power and where V is a vector space over GF(q) of dimension $d \geq \binom{|U|}{t}$.

V.A. Zinoviev:

On Preparata-like Codes and 2-Resolvable Steiner Quadruple Systems.

(Joint work with A.R. Calderbank.)

A binary code with length $n = 4^m$, $m = 2, 3, \dots$, minimal distance $d = 6$ and cardinality $N = 2^{4^m - 4m}$ we call (extended) Prepatrata-like code and denote it by P. A binary code with parameters $n = 2^n$, $d = 4$, $N = 2^{n-1-u}$ we call (extended) Hamming-like code and denote it by H. We have several new statements.

Theorem 1: Let P be any Preparata-like code of length $n = 4^m$. Then the Hamming-like code H which contains P (for any P there is always a H such that $P \subset H$) is partitioned into P and its translates. This partition is completely regular in this Hamming code H.

Theorem 2: Let P be any Preparata-like code of length n. Then this code implies the existence of a 2-resolvable Steiner system $S(3, 4, n)$.

Theorem 3: Let P and P' be any two known nonisomorphic Preparata-like codes of length n, $n = 4^m$, $m = 3, 4, \dots$. Then these codes induce nonisomorphic 2-resolutions of the same Steiner system $S(3, 4, n)$ (which are planes of the affine geometry AG$(2m, 2)$).

Berichterstatter: D. Hachenberger

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Tagungsteilnehmer

Prof.Dr. Rudolf Ahlswede
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131

D-33501 Bielefeld

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

Bethlehem , PA 18015-1237
USA

Prof.Dr. Thomas Beth
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe

D-76128 Karlsruhe

Prof.Dr. Ian F. Blake
Dept. of Electrical Engineering
University of Waterloo

Waterloo, Ontario N2L 3G1
CANADA

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

NL-5600 MB Eindhoven

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

London, Ontario N6A 5B7
CANADA

Prof.Dr. A.Robert Calderbank
AT and T Bell Laboratories
Room 2C-363
600 Mountain Avenue

Murray Hill, NJ 07974
USA

Dr. Frank de Clerck
Department of Pure Mathematics and
Computer Algebra
University of Gent
Galglaan 2

B-9000 Gent

Prof.Dr. Gerard Cohen
ENST
46, rue Barrault

F-75013 Paris

Mario Daberkow
Karl-Pokern-Str. 14

D-12587 Berlin

Prof.Dr.Jean Doyen
Dept. de Mathematiques
Universite Libre de Bruxelles
CP 214 Campus Plaine
Bd. du Triomphe

B-1050 Bruxelles

Prof.Dr. David A. Drake
Math. Department
University of Flórida

Gainesville, Florida 32611
USA

Prof.Dr. Tuvi Etzion
Computer Science Department
TECHNION
Israel Institute of Technology

Haifa 32000
ISRAEL

Marijn van Eupen
c/o Prof. Dr. Jacobus H. van Lint
Department of Mathematics,HG 9.87
Technische Universiteit Eindhoven
Postbus 513

NL-5600 MB Eindhoven

Dr. Dirk Hachenberger
Institut für Mathematik
Universität Augsburg

D-86135 Augsburg

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

NL-5000 LE Tilburg

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. Chat Yin Ho
Dept. of Mathematics
University of Florida
201, Walker Hall

Gainesville . FL 32611-2082
USA

Prof.Dr. Daniel R. Hughes
Dept. of Mathematics
Royal Holloway College
Egham, Surrey

GB-Surrey TW20 0EX

Prof.Dr. Dieter Jungnickel
Institut für Mathematik
Universität Augsburg

D-86135 Augsburg

Prof.Dr. Jennifer D. Key
Department of Mathematical Sciences
Clemson University

Clemson , SC 29634
USA

Prof.Dr. Ivan Landgev
c/o Prof. Dr. R. Hill
Dept. of Mathematics & Comp. Sc.
University of Salford

GB-Salford M5 4WT

Prof.Dr. Jacobus H. van Lint
Rector Magnificus
Technische Universiteit Eindhoven
Postbus 513

NL-5600 MB Eindhoven

Prof.Dr. Siu-Lun Ma
Department of Mathematics
National University of Singapore
10 Kent Ridge Cresent

Singapore 0511
SINGAPORE

Prof.Dr. Spyros S. Magliveras
Department of Computer Science
University of Nebraska, Lincoln
Ferguson Hall

Lincoln , NE 68588-0115
USA

Dr. Klaus Metsch
Mathematisches Institut
Universität Giessen
Arndtstr. 2

D-35392 Gießen

Prof.Dr. Eric Moorhouse
Dept. of Mathematics
Inst. of Scientific Computation
University of Wyoming
Box 3036 University Station

Laramie , WY 82071
USA

Prof.Dr. Ronald C. Mullin
Department of Combinatorics and
Optimization
University of Waterloo

Waterloo , Ont. N2L 3G1
CANADA

Prof.Dr. Stanley Payne
Dept. of Mathematics
University of Colorado at Denver
Campus Box 170

Denver, CO 80204
USA

Prof.Dr. Kevin Phelps
Department of Discrete Mathematics
and Statistics
Auburn University
120 Math Annex

Auburn , AL 36840-5307
USA

Prof.Dr. Vera Pless
Dept. of Mathematics
University of Illinois at Chicago
Box 4348

Chicago , IL 60680
USA

Dr. Alexander Pott
Institut für
Angewandte Mathematik II
Universität Augsburg

D-86135 Augsburg

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

I-00185 Roma

Dr. Mohammad Amin Shokrollahi
Institut für Informatik V
Universität Bonn
Römerstr. 164

D-53117 Bonn

Dr. Gabor Simonyi
Mathematical Institute of the
Hungarian Academy of Sciences
P.O. Box 127
Realtanoda u. 13-15

H-1364 Budapest

Prof.Dr. Edward Spence
Department of Mathematics
University of Glasgow
University Gardens

GB-Glasgow , G12 8QW

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

H-1088 Budapest VIII

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

B-9000 Gent

Prof.Dr. Vladimir D. Tonchev
Mathematics Department
Michigan Technical University
1400 Townsend Drive

Houghton , MI 49931
USA

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

Waterloo , Ont. N2L 3G1
CANADA

Prof.Dr. Wolfgang Willems
Fachbereich Mathematik
Universität Mainz

D-55099 Mainz

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

Pasadena , CA 91125
USA

Prof.Dr. Viktor A. Zinoviev
INRIA, Codes
Domaine de Voluceau-Rocquencourt
B.P. 105

F-78153 Le Chesnay-Cedex

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

E-mail Adressen

E.F. Assmus, Jr.	efa0@lehigh.edu
Th. Beth	eiss_office@ira.uka.de Fax: +49-721-696893
I.F. Blake	ifblake@claude.uwaterloo.ca
A. Brouwer	aeb@cwi.nl
A.A. Bruen	Bruen@uwovax.uwo.ca
A.R. Calderbank	rc@research.att.com
G. Cohen	COHEN@INF.ENST.FR
M. Daberkow	daberkow@math.tu-berlin.de
F. De Clerck	fdc@cage.rug.ac.be
D.A. Drake	dad@math.ufl.edu
T. Etzion	ETZION@TECHSEL.BITNET
M. van Eupen	eupen@win.tue.nl
D. Hachenberger	Hachenberger@uni-augsburg.de
W. Haemers	haemers@kub.nl
R. Hill	R.Hill@MCS.Salford.ac.uk
J.W.P. Hirschfeld	jwph@sussex.ac.uk
C.Y. Ho	cyh@math.ufl.edu
D.R. Hughes	d.r.hughes@gmw.ac.uk
D. Jungnickel	Jungnickel@uni-augsburg.de
J.D. Key	keyj@math.clemson.edu
J.H. van Lint	WSDWJHVL@URC.TUE.NL
I. Landgev	I.Landgev@mes.salford.ac.uk (until 10.8.94) sectmoi@bgearn.bitnet (after 10.8.94)
S.L. Ma	matmasl@nusvm.bitnet
S.S. Magliveras	spyros@helios.unl.edu
K. Metsch	KLAUS.METSCH@MATH.UNI-GIESSEN.DE
G.E. Moorhouse	eric@silver.uwyo.edu
R. Mullin	RCMULLIN@MATH.UWATERLOO.CA
S.L. Payne	SPAYNE@CUDNVR.DENVER.COLORADO.EDU
K. Phelps	PhelpKT@Mail.Auburn.Edu
V. Pless	U09012@UICVM.BITNET
A. Pott	Pott@uni-augsburg.de
M.J. de Resmini	MARILUIS@ITCASPUR.BITNET
M.A. Shokrollahi	AMIN@LEON.CS.UNI-BONN.DE
G. Simonyi	simonyi@konig.elte.hu
E. Spence	ted@maths.gla.ac.uk
T. Szönyi	SZTOMI@LUDENS.ELTE.HU
J.A. Thas	JAT@CAGE.RUG.AC.BE
V.D. Tonchev	tonchev@math.mtu.edu
S.A. Vanstone	savanstone@crypto3.uwaterloo.ca
W. Willems	Willems@mat.mathematik.uni-mainz.de
R.M. Wilson	rmw@math.caltech.edu
V. Zinoviev	ZINOV@loki.inria.fr

Gefördert durch
DFG Deutsche Forschungsgemeinschaft