MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Tagungsbericht 15/1990

DESIGNS AND CODES

1.4. bis 7.4.1990

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

Die Design- und Codierungstheorie sind zwei Teilgebiete der diskreten Mathematik, welche zahlreiche inhaltliche Bezüge besitzen. Das Hauptziel dieser Tagung war es, die Interaktion dieser beiden zur Zeit sehr aktiven Theorien zu fördern, die auch zahlreiche praktische Anwendungen haben.
Dazu wurden hauptsächlich Wissenschaftler eingeladen, deren Forschung beide Gebiete betrifft. Dementsprechend standen Vorträge, die beide Theorien miteinander verbanden, im Mittelpunkt des Interesses. Diese machten einen Großteil des Programmes aus. Daneben gab es auch noch weitere Vorträge, die über neuere Entwicklungen in einem der beiden Gebiete informierten. Die vorgestellten Ergebnisse fanden großes Interesse bei den Teilnehmern, wie die allgemein regen Diskussionen zeigten.
Hervorzuheben ist, daß die Tagung einen stark internationalen Charakter hatte; es nahmen 46 Wissenschaftler aus 12 Ländern - davon 15 aus Nordamerika - teil. Von den zahlreichen auf beiden Gebieten arbeitenden Doktoranden waren einige junge Wissenschaftler eingeladen, deren sehr ansprechende Vorträge auf große Zustimmung stießen.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Vortragsauszüge:

R. AHLSWEDE:

Coding for channels with localized errors: the non-binary case

Bassalygo, Gelfand and Pinsker [1] introduced the interesting notions of localized errors and of codes correcting t of those errors. These authors also derived asymtotically exact bounds for the rates of such codes over binary alphabets. They mentioned at the Gotland meeting that, quite surprisingly, there are serious difficulties in extending their results to general alphabets. We establish here those results.
Actually, the channel model of localized errors can be viewed as a special case of the model AVC with partial side information about states. In [2] we wrote on p621 "There is a large number of coding problems for these channels, because a sender, receiver and jammer can have at every time instant t a certain side information about the past, present, and future operating of the system..."

References:
[1] L.A. Bassalygo, S.I. Gelfand and M.S. Pinsker, "Coding for channels with localized errors", Proceedings of the fourth Swedish-Soviet International Workshop on Information Theory, Gotland, Sweden, August 27 - September 1, 1989, 95-99. Also presented at the Meeting on Information Theory, Oberwolfach, May 15-20, 1989.
[2] R. Ahlswede, "Arbitrarily varying channels with states sequence known to the sender", IEEE Trans. Information Theory, vol. IT-32, no. 5, 621-629, 1986.

E.F. ASSMUS, Jr.:

Hadamard matrices, projective planes and their codes

If a symmetric design has order n, then $4n-1 \leq v \leq n^2+n+1$. Those designs meeting the lower bound are the Hadamard designs, those meeting the upper bound are the projective planes. For the Hadamard designs we have a strong "rigidity" theorem which says that for $n=2^m$ the mod 2 span of the incidence matrix of any such Hadamard design has dimension at least that of the classical design of points and hyperplanes of the projective space over GF(2) with equality iff it is the classical design. There is also a weak "rigidity" theorem which says - in the classical case with $n=p^m$, $p\neq 2$ - that if the code of an affine plane of order n satisfies $H=C(AG(2,n))\cap C(AG(2,n))^{\perp} \leq \pi \leq H^{\perp}$ then $\dim C(\pi) \geq \dim C(AG(2,n))$ with equality iff π is isomorphic to AG(2,n). The proof appears in a joint paper with J.D. Key "Affine and projective planes", Discrete Math. 83 (1990).

Th. BETH:
Some remarks on a conjecture by J.W.P. Hirschfeld

We give an algebro-geometric proof for the dimension formula of the GF(p)-code generated by the lines of PG(n,q) resp. AG(n,q). By canonically relating the projective geometry PG(n,q) to the affine geometry AG(n,q) we obtain for the respective p-dimensions p_n and a_n the recursion formula $p_n = a_n + p_{n-1}$. In determining a_n we embed the code $C = C(1,n,p)$ generated by the lines of AG(n,q) into the group ring $GF(p)[x_1,..,x_n]/_{<(x_1^p-1),..,(x_n^p-1)>}$.

We show that $C = R^{p-1}$ where R is the radical of the group ring, which has the basis $\{(x_1-1)^{i_1}\cdots(x_n-1)^{i_n} \mid 0 \leq i_k \leq p-1 \text{ for } k=1,..,n\}$. Thus R^{p-1} has the basis $\{(x_1-1)^{i_1}\cdots(x_n-1)^{i_n} \mid \Sigma i_k \geq p-1\}$. As $a_n^\perp = \dim(C^\perp) = p^n - \dim C$ we see immediatly that $\dim(C^\perp)$ is the cardinality of the "discrete" simplex. $a_n^\perp = |\{(x_1-1)^{i_1}\cdots(x_n-1)^{i_n} \mid \Sigma i_k < p-1\}| = \binom{n+p-2}{p-2}$, thus proving a conjeture by J.W.P. Hirschfeld presented earlier at this meeting.

A. BEUTELSPACHER:
Geometric authentication systems

The classical example of a "perfect" authentication system (Gilbert, MacWilliams, Sloane) is constructed from an affine plane A as follows. The messages (source states) are the parallel classes of A, the keys are the points and the authenticators (messages) are the lines of A.
The perfect authentication systems have the following disadvantages.
-They have only few messages (compared to the number of keys).
-There are only "few" examples.
-They are only secure if the key is used only once.
We discuss several examples of authentication schemes based on geometrical objects, such as spreads, conics, quadrics which solve the above mentioned problems.

I.F. BLAKE:
On the complete weight enumeration of Reed-Solomon codes

The complete weight enumerator of a code enumerates the codewords by the number of symbols of each kind contained in each codeword. As for the ordinary weight enumerators, the complete weight enumerators for linear codes satisfy a duality theorem. These weight enumerators are studied for certain realizations of Reed-Solomon codes of dimensions two, three and four over GF(2^m). Some applications of these results are considered.

A. BLOKHUIS:

Characterization of Hermitian unitals

We show that a unital in PG(2,q^2) is Hermitian if and only if it is in the code generated by the lines of PG(2,q^2). This proves a conjecture by Assmus and Key. The proof uses identities in the group algebra relating the unital with the decomposition of the Singer group in subgroups of order q^2-q+1 and q^2+q+1.

A.E. BROUWER:

Codes of classical generalized quadrangles

We study binary codes C (generated by the lines) and P (generated by the point neighbourhoods) in general and determine their dimensions for the classical quadrangles Sp(4,q) and O(5,q). As a side result we find that if a generalized quadrangle of order (s,s) contains an antiregular point, then all its points are antiregular. (Joint work with Bagchi and Wilbrink)

A.A. BRUEN:

Some remarks on geometric codes

For a binary linear code we explain the idea of a point base in terms of an intersection set for codewords, and generalize to arbitrary linear codes. Examples are discussed, including MDS codes. A new proof of Bruck-Ryser (for special cases) is sketched using point bases. Bases for certain codes in finite geometries e.g. the row space of PG(2,q) are constructed and a configuration theorem generalizing the O'Nan criterion for Hermitian unitals is presented. A connection between MDS codes and certain polynomials in GF(q)[x_1,..,x_n] with multiplicity conditions is made.

A.R. CALDERBANK:
Regularity in codes and designs

We use invariant linear forms to study regularity in designs, particularly those designs afforded by codewords of a fixed weight in some code. The most important theorem relating codes and designs is due to Assmus and Mattson, and we extend this theorem in several ways. These results specialize to give results obtained by Venkov and Koch using modular forms, but our proofs use only a little representation theory of the symmetric group. (Joint work with P. Delsarte)

G. COHEN:
Perfect multiple coverings of Hamming spaces

Let Q^n be the n-dimensional q-ary Hamming space. A perfect multiple covering PMC(q,n,M,r,μ) is a subset C (or code) of Q^n with size M such that every vector in Q^n is within distance r from exactly μ codewords of C. We give a few constructions of PMC's, focusing on the case r=1.

Theorem 1: Let q be a prime power. A linear (q,n,·,1,μ) PMC exists iff $n=(\mu q^i-1)/(q-1)$ for some $i \epsilon N_0$.

Theorem 2: Let q be a prime. A (q,n,·,1,μ) PMC exits iff $n=(\mu_0 q^i-1)/(q-1)$ for some $i \epsilon N_0$, $\mu_0 \epsilon N$, $\mu_0 | \mu$ and $\mu \leq q^i \mu_0$.

We conjecture that theorem 2 can be extended to prime powers q. (Joint work with G.J.M. van Wee and S. Litsyn)

J.A. DAVIS:
Relative difference sets in p-groups

Many of the character theory techniques that have been exploited on regular difference sets also apply to relative difference sets. These techniques can be used to provide exponent bounds, show that certain candidates for an RDS are true RDS, and use number theory to exclude extensions of Menon difference sets. I am mainly interested in determining the existence of RDS (or nonexistence), and these are powerful techniques.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

J.F. Dillon:
Some open problems on designs and codes

1. Conjecture (Dillon and Schatz). If a symmetric design with parameters (v,k,λ), $v=2^{2m}$, attains the minimum 2-rank $2m+2$ then the code of the design must contain the all-1-vector. This would imply that the designs of minimum rank are precisely those given by the words of minimum weight in the code spanned by RM(1,2m) and a difference set in F_2^{2m}.

2. Conjecture (Dillon). If a group of order 2^{2m} contains a normal subgroup $E \cong Z_2^m$, then G contains a nontrivial difference set. This result would follow if for every subgroup L of order 2^{2m} in GL(m,2) the matrix $M=[l(x)]$ whose rows and columns are indexed by L and F_2^m, resp., has a transversal.

3. Problem. Determine the groups of order 64 which have a (nontrivial) difference set. In particular, settle the case of the modular group $G=<a,b \mid a^2=b^{32}=1, aba^{-1}=b^{17}>$.

G. GODSIL:
Edge recontructions of graphs and minimum distance

A graph F is a edge-reconstruction of a graph G if there is a bijection ß from the edges of G to the edges of F such that $G\backslash e \cong F\backslash ß(e)$, for all edges e of G. If any edge-reconstruction of G is isomorphic to G, then we say G is edge-reconstructible. Müller proved that a graph on n vertices with m edges is edge-reconstructible if $m-1>\log_2(n!)$. I outline a new proof of this, which reduces to a determination of the minimum distance of the Reed-Muller code R(k-1,m). The argument also yields several generalisations of Müller's result. (Joint work with Krasikov and Roddity)

H.D. Gronau:
On a conjecture of Demetrovics, Füredi and Katona concerning partitions

Demetrovics, Füredi and Katona considered in 1980 the following problem which originally arose from the theory of data bases.

Problem: Given an n-element set X, say $X=\{1,2,..,n\}$, $n\geq 2$. Do there exist n partitions $P_1,P_2,..,P_n$ of X such that their pairwise intersections are just the atoms of the partition lattice of X?

Gefördert durch DFG Deutsche Forschungsgemeinschaft

It is simple to check the answer for small values of n:

n	2	3	4	5	6	7
answer	yes	no	yes	no	no	yes

They constructed solutions of the problem for all $n\equiv 1$ or 4 mod 12, and gave the

<u>Conjecture</u>: The problem has solutions for all $n\geq 7$.

Ganter and Gronau (see "Kombinatorik", Feb. 26, - March 4, 1989, Oberwolfach) proved that the conjecture fails for $n=8$, is true for all $n\equiv 1$ mod 3 (actually they proved a stronger result) and is true for all sufficiently large n.

In this talk, which is based on joint work with R.C. Mullin (Waterloo), we present and sketch the proof of the final

<u>Theorem</u>: The conjecture is true for all $n\neq 3,5,6,8$.

D. HACHENBERGER:

Translation nets

A translation net of order s and degree $r\geq 3$ with translation group G is a pair (N,G), where N is an (s,r) Bruck net (i.e. an affine $S_r(1,s,s^2)$) which admits G as an automorphism group acting regularly on the set of points of N and fixing each parallel class.
An (s,r)-translation net exists iff there is a set $H=\{H_1,..,H_r\}$ of subgroups of G satisfying $|H_i|=s$ for $i=1,..,r$ and $H_iH_j=G$ for $i,j=1,..,r$ and $i\neq j$. H is called an (s,r)-partial congruence partition (PCP for short).
We summarize the main group theoretic techniques which lead to existence results on translation nets. Let $T(G)=\max\{r\,|\,\text{there is an }(s,r)\text{-PCP in }G\}$. If G is a p-group of order p^{2n} and not elementary abelian, where p is odd and $n\geq 4$ we prove $T(G)<p^{n-1}$. This generalizes a result of D. Frohardt who dealt with 2-groups. Furthermore we prove that $T(G)\leq p^2+1$ holds if G is not elementary abelian of order p^6 (p odd). We characterize all groups of order p^4 (p prime) which admit a $(p^2,3)$-PCP and determine T(G) in all these cases.

J. HAYDEN:

(P,L)-transitivity in finite planes and generalized Hadamard matrices

Let π be a finite plane of order n. If P is a point incident with a line L of π, the plane is said to have a (P,L)-transitivity if there exist n elations with axis L and center P. These n elations form a group G called a cartesian group. The structure of the group G is, in general, not known. If π admits further elations with axis L, a theorem of Baer implies G is an elementary abelian p-group for some prime p. A theorem of Hayden implies G must be elementary abelian if certain additional homologies with axis L exist. We study the case when no extra collineations are assumed. The main result is:

Theorem: Assume π is a projective plane of order n and π admits a group G of n elations with axis L and center $P \epsilon L$. If G is abelian, then G is an elementary abelian p-group for some prime p. In particular, n is a prime power.

Corollary: Let $X = (x_{i,j})$ be a matrix of order n whose entries $x_{i,j}$ are from an abelian group G of order n. If $\{(x_{m,i})^{-1} x_{k,i} \mid i = 1,..,n\} = G$ whenever $m \neq k$, then G must be an elementary abelian p-group.

The matrix X is called a generalized Hadamard matrix of order n and the corollary follows from the fact that such a matrix is equivalent to a plane of order n with a (P,L)-transitivity.

R. HILL:
Optimal linear codes

Let $n_q(k,d)$ denote the smallest value of n for which there exists a linear code of lenght n, dimension k and minimum distance d over a field of q elements. The problem of finding $n_q(k,d)$ for binary codes (i.e. $q=2$) has received much attention and has been completely solved for $k \leq 7$, for all d. We briefly mention some new results concerning $n_2(k,d)$ for $k \geq 8$. We then consider the problem for ternary codes ($q=3$) and show that $n_3(k,d)$ is known for $k \leq 4$ for all d. We discuss also some of the thirty cases for which $n_3(5,d)$ remains unknown; they raise intriguing open questions concerning the existence or otherwise of certain two-weight or tree-weight codes.

J.W.P. HIRSCHFELD:
Projective geometry codes

The projective geometry code $C^*(r,n,q)$ is dual to that generated by the incidence matrix of points and r-spaces in a finite projective space PG(n,q). Some properties of the geometry of such codes were given. A formula for the dimension of C^* is due to Hamada; for q a prime p this reduces to

Gefördert durch DFG Deutsche Forschungsgemeinschaft

$$\sum_{s=0}^{n-r} \sum_{i=0}^{\lfloor s(p-1)/p \rfloor} (-1)^{i} \binom{n+1}{i} \binom{n+s(p-1)-ip}{n}$$

It was suggested that, for r = 1, this equals $\binom{n+p-1}{n}$. During the conference, this was proved by J.H. van Lint and an outline of the geometric reason for the latter number was given by Th. Beth.

C. Y. HO:

Planar difference sets

The study of finite cyclic planar difference sets is equivalent to the study of finite cyclic planes. A recent result of Kantor followed by work of Feit rekindled interest in finite cyclic planes. Pott and I proved recently that if the order of a group of multipliers is divisible by the odd part of the order of the automorphism group of a Singer group, then the order of the plane is 2,3,4 or 8. This yields another proof of Feit's result mentioned above. Also we prove that n + 1 is an upper bound for the odd part of the order of a group of multipliers. This bound is best in the sense that n + 1 is attainable. Note that n + 1 is the factor appearing in the critical case in Kantor's result. Some other recent results of the speaker will be discussed.

D.R. HUGHES:

Extended partial geometries

The problem of finding geometries for $\circ\overset{c}{—}\circ\underset{d}{—}\circ$ is considered. These EpG's fall into certain types, and we discuss the problem and give some examples and characterization theorems for the case of dual linear spaces and of generalised quadrangles in particular. All known extended dual projective geometries, affine geometries are listed. All known extended generalised quadrangles are (1) extensions of grids (a large and difficult class), (2) extensions of grids (unique), (3) have order (2,t) (ten examples exactly), (4) have order (3,9), (4,2), (9,3) or (3,3) or (5) have order (q-1,q+1), with q a prime-power q≥5. These results are due to many authors.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

J.D. KEY:

Steiner systems and Hadamard matrices

A construction of Shrikande and Singhi (1963), and Goethals and Seidel (1970) produces Hadamard matrices of size $4k^2 x 4k^2$ from Steiner designs with parameters 2-$(2k^2$-k,k,1). If the Steiner design is resolvable then the Hadamard matrix can be taken to be of constant row sum. If D is a Steiner 2-$(2k^2$-k,k,1) design, T a Hadamard 3-$(4k^2,2k^2,k^2$-1) design and S a symmetric $(4k^2,2k^2 \pm k,k^2 \pm k)$ design, where T and S are derived from D in this way, then, if p | k and is a prime, $\dim C_p(T) = \dim C_p(D) - \dim(C_p(D) \cap C_p(D)^{\perp}) + 1$ (where $C_p(D)$ denotes the row space over GF(p) of an incidence matix for D) and for p=2, $\dim C_2(S) = \dim_2 C(T) + 1$. An infinite class of designs D that have these parameters are given by the oval designs of Bose and Shrikande (1960). All known cases have $k = 2^n$ for some n. For m=2, $C_2(T)$ = RM(1,4), the finite order Reed-Muller code, but for m=3, $C_2(T)$ has dimension 13, and is thus not RM(1,6). For a regular oval in a desarguesian plane of order 2^m we conjecture that $\dim C_2(T) = 2^{m-1}m + 1$.

P. LANDROCK:

Codes and group algebras

A number of classical linear codes turn out to admit a very natural algebraic structure on the vector space in such a way that they become (right) ideals. These algebras are all group algebras. This is a classical result for the Reed-Muller codes, but we have shown how this can be used to obtain a new decoding algorithm.

Likewise the Golay codes G_{12} and G_{24} are (right) ideals in the ternary twisted group algebra over A_4 and the binary group algebra over Σ_4.

Finally we mention a result that states that the Slepian problem of group codes for the Gaussian channel is equivalent to finding certain primitive idempotents in the group algebra. (Joint work with O. Manz)

M. LECLERC:

Network security: An implementation of the McEliece cryptosystem

McEliece proposed an asymmetric cryptosystem based on Goppa codes. An efficient software implementation is described. It was found that this system's performance is far better than the one of others like RSA or Discrete Exponentiation.

H. LENZ:

In memoriam RICHARD RADO (April 28, 1906 - December 23, 1989)

The main dates of his life and some of his mathematical achievements were sketched.
Life: Youth in Berlin. Studies of Mathematics in Göttingen and Berlin. Dissertation "Studien zur Kombinatorik" (adviser I. Schur) 1931. Habilation became impossible after Hitler came to power. Emigration to England 1933. Marriage in the same year. 1935 British PhD (adviser G.H. Hardy) in Cambridge. From 1934-1983 joint work with Paul Erdös. 1936 Assistant lecturer at the University of Sheffield. 1947 King's College London. 1954 Full Professor at the University of Reading. 1971 retired. 1972 Senior Berwick Prize. 1978 Fellow of the Royal Society. Honorary doctor Berlin 1981, Waterloo 1986. 1983 serious car accident. 1984 Book on Combinatorial set theory together with Erdös, Hajnal and Mate. 1986 last of about 115 mathematical papers.
Some of his best known results were sketched (Dissertation, Contributions to Ramsey theory, Rado's selection theorem, contributions to matroid theory).

V.I. LEVENSHTEIN:

Perfect deletion correcting codes and ordered Steiner systems

We consider a new kind of combinatorial designs, which are connected with the perfect codes capable of correcting a deletion of letters. Let a k-set be a set of k elements of a fixed alphabet $A(v)=\{0,..,v-1\}$, $v\geq 2$, and a k-multiset be a collection of k-elements of $A(v)$, which can be identical. We denote the set of all k-sets (k-multisets) by $P_k(v)$ ($P_k^*(v)$ resp.). A subset S of $P_k(v)$ (S of $P_k^*(v)$) is called a Steiner system and denoted by $S(t,k,v)$ ($S^*(t,k,v)$ resp.), if every t-set (t-multiset) belongs to exactly one element of S. Let $A_k^*(v)$ be the set of all words of length k over the alphabet $A(v)$ and $A_k(v)$ be the subset of $A_k^*(v)$ which contains all words with different letters. The subset T of $A_k(v)$ (T of $A_k^*(v)$) is called an ordered Steiner system and denoted by $T(t,k,v)$ ($T^*(t,k,v)$ resp.), if every word of $A_t(v)$ ($A_t^*(v)$ resp.) is a subsequence of exactly one word of T. In particular, it was proved that there is a partition of $P_t^*(v)$ into v Steiner systems $S^*(k-1,k,v)$, there is a partition of $A_k^*(2)$ into k+1 ordered Steiner systems $T^*(k-1,k,2)$, there is a partition of $A_k(k)$ into k systems $T(k-1,k,k)$, and for even v there are systems $T(3,4,v)$ and $T(3,4,v)$.

S.L. MA:

Reversible difference sets and relative difference sets

A subset D of a group G is called reversible if $D^{(-1)}=\{d^{-1} \mid d \in D\}=D$, i.e. -1 is a multiplier fixing D. I shall talk about the case when D is a difference set or relative difference set. Examples and necessary conditions will be given.

R.C. MULLIN:

Calculation in finite fields

Calculation with normal bases for $GF(2^n)$ over GF(2) has the advantage that in the coordinate representation of the field relative to such a basis, squaring is represented by a cyclic shift. In addition, there is some advantage to be gained from the fact that the n bilinear forms giving the coefficients of $a \cdot b$ in terms of the coordinate vectors for a and b in normal basis representation are related by cyclic shifts, too. The straight-forward implementation of circuitry to evaluate such a quadratic form lacks a feature known as regularity in VLSI implementation. An alternate method of performing the calculations, which leads to a regular implementation will be dicussed.

A. NEUMAIER:

Completely regular codes

A new approach to completely regular codes giving a very elementary proof of Lloyd's theorem and a proof of the nonexistence of perfect binary codes of minimum distance >3 without using Krawtchouk polynomials.

U. OTT:

Rank of {0,1}-matrices

In the study of graphs, codes and finite geometries {0,1}-matrices play an important role. Using the terminology of finite geometry we may regard a {0,1}-matrix as the incidence matrix of a finite geometry consisting of v points, b lines and m flags: $G=(\Gamma_1,\Gamma_2,I)$. The only known result about the class of projective planes is

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Theorem (Bruen, Ott): Let M be the incidence matrix of a projective plane of order n. Then we have $\mathrm{rank}_k(M) \geq n\sqrt{n}+1$.

The central point in the course of the argument is the following. Sufficient information concerning the dimension of a certain module - the so-called Steinberg module of the geometry - is enough to produce a good estimate for the rank. More recently the following results have been established.

Theorem (Hillebrandt): Let M be the incidence matrix of a (connected) semilinear space. Then $\mathrm{rank}(M) \geq (m-v-b+1)^{1/2}$.

Theorem (Hillebrandt): Let M be the incidence matrix of a linear space. For any line a let T(a) denote the set of lines x with $a \cap x = \phi$. Then $(\mathrm{rank}(M))^2 \geq (v-|a|)(|a|-1) + \sum_{x \in T(a)} (|x|-1)$.

O. PFAFF:
On the classification of the 2-transitive affine 2-designs

A 2-transitive permutation group has a unique minimal normal subgroup which is either elementary abelian or simple by Burnside (1911). We are able to prove that the unique Hadamard 3-design on 12 points and $AG_2(3,2)$ are the affine 2-designs with a 2-transitive automorphism group which has a simple normal subgroup. Thus we have to consider the case of an elementary abelian normal subgroup for the classification of the 2-transitive affine 2-designs. This case is not completely solved yet, but we can describe the remaining affine 2-designs which might have a 2-transitive automorphism group precisely by means of spreads. Nevertheless we are able to prove that a 3-transitive affine 3-design is either an affine space AG(2,q) or the Hadamard 3-design on 12 points. This shows the correctness of Norman's conjecture (1968).

V. PLESS:
Orphans of the first order Reed-Muller codes

If C is a code, an orphan is a coset which is not a descendant. Orphans arise naturally in the investigation of the covering radius. We characterize cosets which are orphans, and then prove the existence of a family of orphans of the first order Reed-Muller codes R(1,m). For m less than or equal to 5 all orphans of R(1,m) are identified.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

We investigate a new method of combining two codes which we call the outer product. First order Reed-Muller codes are outer products of a number of copies of the full binary space of length 2. We apply our results to obtain cosets of the Reed-Muller codes which are orphans. This work is based on the following two papers. "Orphans of the First Order Reed-Muller Codes" by R.A. Brualdi and V. Pless, to appear in Trans. of the IEEE on Information Theory and "Structure of Orphans of the First Order Reed-Muller Codes" by R.A. Brualdi, N. Cai and V. Pless, preprint.

A. POTT:

On quasiregular collineation groups of finite planes

Case (d) in the classification of Dembowski and Piper on quasiregular collineation groups of finite planes corresponds to an affine difference set of order n. If the underlying group Γ is abelian, we prove that the Sylow 2-subgroup of Γ is cyclic, lending support to the conjecture: All abelian affine difference sets live in cyclic groups. We further show that the multiplier group of the associated affine difference set of order n has a unique involution, namely n. Some improvements of a result of Hoffman on the fixed structure of the given plane by a multiplier are also obtained.

R.L. ROTH:

Mappings of sets of pairwise orthogonal orthomorphisms

When σ and μ are permutations of the finite group $(G,+)$, σ and μ are said to be orthogonal if the function $x \rightarrow x^{\sigma}-x^{\mu}$ is also a permutation of G. The Latin square associated with σ is given by $L_{\sigma}(x,y)=x^{\sigma}-y$ and $\sigma \perp \mu$ iff $L_{\sigma} \perp L_{\mu}$. We denote by N'(G) the maximum size of a set of pairwise orthogonal permutations of G which can be assumed to contain id_G and other permutations, all fixing 0_G. Such a permutation, fixing 0_G and orthogonal to id_G, is called an orthomorphism of G. Orthomorphisms of $C_6 \oplus C_2$, C_{15}, and $C_6 \oplus C_2^2$ have been used to set the current "world records" for N(12), N(15), and N(24) (namely 5, 4, and 4 resp.) where N(n) denotes the maximum size of a set of pairwise orthogonal Latin squares of order n. The "record" for n=15 was set by considering only inverse preserving orthomorphisms which comprise less than the 1200th part of the total number, 2.424.195, of orthomorphisms of C_{15}. In joint work with R.M. Wilson, the entire set of orthomorphisms was exhaustively examined and (unfortunatly) the value $N'(C_{15})=4$ was determined. However, techniques were developed which will be useful in the study of N'(G) for $|G| \in \{20,21,24\}$. These techniques include the construction of mappings which partition the collection of m-sets of pairwise

Gefördert durch DFG Deutsche Forschungsgemeinschaft

orthogonal orthomorphisms into relatively few equivalence classes; and only one member from each class need be tested for extendability to a set of $m+1$ pairwise orthogonal orthomorphisms.

J.J. SEIDEL:
Designs in euclidean space

Analogs to ordinary designs t-(v,k,λ) are the spherical t-designs on the unit sphere S in euclidean R^d. Recently this last notion was generalized to a measure of strength t in R^d. On the other hand, optimal designs have been developed since the late fifties by Kiefer and others, both experimentally (finite) and abstract (as a measure). We develop the theory of these notions in the setting of polynomials of degree $\leq \frac{1}{2}t$ in R^d and their inner products. (Joint work with A. Neumaier)

M.A. SHOKROLLAHI:
Minimum distance of elliptic codes

Following Goppa's construction of linear codes on algebraic curves we take elliptic curves over finite fields and construct geometric Goppa codes. These codes are "almost-MDS", that is if n,k,d denote the block length, the dimension and the minimal distance of these codes, then $d=n-k$ or $d=n-k+1$. Three types of elliptic codes are considered and it is shown that in the majority of cases these codes are not MDS, hence $d=n-k$. It is shown that the MDS-codes derived from these constructions are of Reed-Solomon type.

J. SIMONIS:
A short proof of the Delsarte-MacWilliams inequalities

(Based on an idea of C. de Vroedt) The Delsarte-MacWilliams inequalities $\sum_{i=0}^{n} K_k(i)A_i(c)\geq 0$ for $k=0,..,n$ are derived by first proving the $k=1$ case by means of a "Plotkin-type" argument, and then applying this inequality to the code C_k of length $\binom{n}{k}$ obtained by taking all sums of k columns of a codeword list of the original code C.

E. SPENCE:
Some new regular two-graphs

In [1] the authors give all known regular two-graphs on n≤50 vertices and conjecture that in the case n=36 the list containing 91 is complete. This turns out not to be the case as a further 136 have been found using an incomplete back-tracking search. A characterization of a large number of these regular two-graphs is given in terms of one of them.

[1] F.C. Bussemaker, R.A. Mathon, J.J. Seidel, Tables of two-graphs, Report Techn. Univ., Eindhoven 79-Wsk-05, (1979), 99.

A. TIETÄVÄINEN:
Covering radius

Recently a number of bounds have been obtained for the covering radius of a code with given length and cardinality. In this talk we show that - perhaps surprisingly - the covering radius of a code depends heavily on its dual distance. We consider an arbitrary finite Abelian group alphabet though in the applications the alphabet is very often GF(2).

V.D. TONCHEV:
Quasi symmetric designs and codes

The four 2-(64,28,12) designs with the symmetric difference property are characterized as the only designs with the given parameters and minimal rank over GF(2). These designs give non-isomorphic quasi-symmetric 2-(36,16,12) and 2-(28,12,11) designs as residual and derived designs. The binary codes of the quasi- symmetric 2-(28,12,11) designs provide four inequivalent self-orthogonal doubly-even (28,7,12) codes. This gives a negative answer to the question for the uniqueness of the code of the Hermitian unital of order 3. (Joint work with D. Jungnickel)

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

S.A. VANSTONE:
Codes from Graphs

In this lecture we make several observations about the code obtained from the cycle space of a graph. Most notably we give an algorithm based on combinatorial optimization for decoding such codes. We examine the code arising from the complete graph and its relationship to the Hamming codes. Finally, some remarks about codes derivable from K_6 are given.

Berichterstatter: O. Pfaff

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Tagungsteilnehmer

Prof.Dr. Rudolf Ahlswede
Fakultät für Mathematik
der Universität Bielefeld
Postfach 8640

4800 Bielefeld 1

Prof.Dr. Krishnasamy Arasu
Department of Mathematics
Wright State University

Dayton , OH 45435
USA

Prof.Dr. Edward F. Assmus, Jr.
Dept. of Mathematics
Lehigh University

Bethlehem , PA 18015
USA

Prof.Dr. Thomas Beth
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Am Fasanengarten 5, Geb. 5034

7500 Karlsruhe 1

Prof.Dr. Albrecht Beutelspacher
Mathematisches Institut
der Universität Giessen
Arndtstr. 2

6300 Gießen

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

Waterloo, Ontario N2L 3G1
CANADA

Dr. Aart Blokhuis
Dept. of Mathematics and
Computer Science
Technical University Eindhoven
Postbus 513

NL-5600 MB Eindhoven

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

NL-5600 MB Eindhoven

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

London, Ontario N6A 5B7
CANADA

Prof.Dr. Robert Calderbank
AT & T
Bell Laboratories
600 Mountain Avenue

Murray Hill , NJ 07974-2070
USA

Prof.Dr. Gerard Cohen
ENST
46, rue Barrault

F-75013 Paris

Dr. James Davis
Dept. of Mathematics
University of Richmond

Richmond VA 23173
USA

Dr. John F. Dillon
7505 Powhatan St.

New Carrollton , MD 20784
USA

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

Waterloo, Ontario N2L 3G1
CANADA

Prof.Dr. Hans-Dietrich Gronau
Sektion Mathematik
Ernst-Moritz-Arndt-Universität
F.-L.-Jahn-Str. 15a

DDR-2200 Greifswald

Dirk Hachenberger
Mathematisches Institut
der Universität Giessen
Arndtstr. 2

6300 Gießen

Prof.Dr. John L. Hayden
Dept. of Mathematics
Bowling Green State University

Bowling Green , OH 43403
USA

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

GB- Salford M5 4WT

Prof.Dr. James Hirschfeld
Mathematics Division
University of Sussex
Falmer

GB- Brighton , BN1 9QH

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

Gainesville , FL 32611
USA

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

GB- London , E1 4NS

Prof.Dr. Dieter Jungnickel
Mathematisches Institut
der Universität Giessen
Arndtstr. 2

6300 Gießen

Prof.Dr. Jennifer Key
Dept. of Mathematics and Statistics
The University of Birmingham
P. O. Box 363

GB- Birmingham , B15 2TT

Prof.Dr. Peter Landrock
Matematisk Institut
Aarhus Universitet
Ny Munkegade
Universitetsparken

DK-8000 Aarhus C

Dr. Matthias Leclerc
ZFE IS KOM 42
SIEMENS AG
Otto-Hahn-Ring 6

8000 München 83

Prof.Dr. Hanfried Lenz
Institut für Mathematik II
der Freien Universität Berlin
Arnimallee 3

1000 Berlin 33

Prof.Dr. Vladimir Levenstein
Keldysh Institute of Applied
Mathematics
Academy of Science of the USSR
Miusskaya sq. 4

125047 Moscow
USSR

Prof.Dr. Jacobus H. van Lint
Department of Mathematics
Technische Universiteit Eindhoven
Postbus 513

NL-5600 MB Eindhoven

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

Singapore 0511
SINGAPORE

Prof.Dr. Robert L. McFarland
Dept. of Mathematics and Statistics
Univ. of Minnesota

Duluth MN 55812
USA

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

Waterloo, Ontario N2L 3G1
CANADA

Prof.Dr. Arnold Neumaier
Institut für Angewandte Mathematik
der Universität Freiburg
Hermann-Herder-Str. 10

7800 Freiburg

Prof.Dr. Udo Ott
Institut für Geometrie
der TU Braunschweig
Pockelsstr. 14

3300 Braunschweig

Oliver Pfaff
Mathematisches Institut
der Universität Giessen
Arndtstr. 2

6300 Gießen

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

Chicago , IL 60680
USA

Dr. Alexander Pott
Mathematisches Institut
der Universität Giessen
Arndtstr. 2

6300 Gießen

Prof.Dr. Robert L. Roth
Dept. of Mathematics and
Computer Science
Emory University

Atlanta , GA 30322
USA

Tilla Schade
Mathematisches Institut
der Universität Giessen
Arndtstr. 2

6300 Gießen

Prof.Dr. Jacob J. Seidel
Department of Mathematics
Technische Universiteit Eindhoven
Postbus 513

NL-5600 MB Eindhoven

Mohammed Amin Shokrollahi
Institut für Informatik V
Universität Bonn
Römerstr. 164

5300 Bonn 1

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Prof.Dr. Juriaan Simonis
Dept. of Mathematics and
Computer Science
Delft University of Technology
P. O. Box 356

NL-2600 AJ Delft

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

GB- Glasgow , G12 8QW

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

SF-20500 Turku

Prof.Dr. Vladimir Tonchev
Mathematisches Institut
der Universität Giessen
Arndtstr. 2

6300 Gießen

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

Waterloo, Ontario N2L 3G1
CANADA

Prof.Dr. Jacques Wolfmann
GECT
Universite de Toulon et du Var
Chateau St. Michel

F-83130 La Garde

Gefördert durch
DFG Deutsche
Forschungsgemeinschaft

Gefördert durch
DFG Deutsche
Forschungsgemeinschaft