Combinatorial designs constructed from or with coding theory

Combinatorial designs constructed from or with coding theory

J.H. van Lint
Department of Mathematics
Eindhoven University of Technology

Most of the lecturers in this session on information theory are interested mainly in the probabilistic side of the subject. However, the participents are undoubtedly aware of the fact that much of what has been promised by probabilistic methods, e.g. by Shannon's Theorems, has not been realized constructively because constructions (of codes, etc.) have all been extremely regular. Very likely, this regularity limits the class from which one can choose so much that the results are not as good as one knows should be possible. Nevertheless, we have to manage with what we have. Thus it is not surprising that coding theorists have either rediscovered a number of concepts from the mathematical discipline known as *combinatorics* or that they have studied parts of that theory so as to apply the results to their own problems. Since the theme of this session is recent trends in information theory it seems proper to give a survey

of a development of the past few years, to wit the use of methods of coding theory to expand the mathematical theory! At present the area known as theory of designs and coding theory are influencing each other. It looks like this will become a very fruitful cooperation. It is the purpose of these lectures to explain some of the connections between these subjects to an audience familiar with algebraic coding theory. We shall assume that the reader is familiar with the standard topics from the theory as presented in E.R. Berlekamp's Algebraic Coding Theory [1] (or e.g. the author's lectures on Coding Theory [2]. A summary of what one is expected to know is given in section 2. A few years ago the author gave a similar series of lectures to an audience of experts in the theory of combinatorial designs, stressing the coding theory background. Nevertheless, much of the material for these lectures will be the same. For a complete treatment of these parts and also an extensive treatment of connections between graph theory, coding and designs we refer the reader to the published notes of these lectures [3]. Since we do not assume the reader to be more than slightly familiar with combinatorial theory we shall introduce a number of combinatorial designs in section 1. For the general theory of these topics we refer the reader to M. Hall's Combinatorial Theory [4].

The main topics, i.e. the Assmus-Mattson theorem, codes generated by designs and projective planes, and uniformly packed codes have been organized in such a way that knowledge of sections 1 and 2 is sufficient to understand the remainder of the lectures.

I. INTRODUCTION TO COMBINATORIAL DESIGNS

A) q-ary t-designs (cf. Goethals [5])

Let $R^{(n)}$ denote the set of all n-tuples from a q-symbol alphabet, e.g. $\mathbb{Z}_q$ (as usual we take this to be GF(q) if q is a prime; if q is a prime power we take GF(q) instead of $\mathbb{Z}_q$ in most applications).
For any two n-tuples $\underline{u} = (u_1,\ldots,u_n)$, $\underline{v} = (v_1,\ldots,v_n)$ of $R^{(n)}$ we say that $\underline{u}$ is *covered* by $\underline{v}$ if for all i $u_i(u_i - v_i) = 0$. Let $1 \le t \le k \le n$.

Definition 1.1. A q-ary t-design t-(n,k,λ) is a collection $\mathcal{D}$ of words of weight k from $R^{(n)}$ such that every word of weight t is covered by exactly λ words of $\mathcal{D}$. The words of $\mathcal{D}$ are usually called the *blocks* of the design.

Example 1.1. The 8 non-zero words of the ternary (4,2) Hamming code (cf. Section 2) are

0 1 1 2
0 2 2 1
1 0 1 1
1 1 2 0
1 2 0 2
2 0 2 2
2 1 0 1
2 2 1 0 .

These words all have weight 3.
The reader can easily check that each of the 24 possible words of weight 2 is covered by exactly one of the above words of weight 3. Hence we have found a ternary design 2-(4,3,1).

Example 1.2. The ternary Golay code (cf. *Example* 3.2 or Van Lint [2]) has word length 11 and minimum distance 5. The code contains 132 words of weight 5. We observe two facts:

a) two different code words of weight 5 cannot cover the same triple because if they did, then their difference would have weight at most 4. This is impossible since the code is linear;

b) each code word of weight 5 covers 10 triples.

By a) and b) the code words of weight 5 cover 1320 distinct triples. Since $1320 = \binom{11}{3} 2^3$, i.e. the total number of distinct words of weight 3, we have shown that the set of words of weight 5 in the ternary Golay code is a ternary 3-design 3-(11,5,1).

Exercise. As a preparation for a method to be used later the reader should prove that if one takes the design of the previous example, and in each block replaces all non-zero entries by ones, the result is a binary design 4-(11,5,8). In this design each block occurs 8 times. Therefore, if we take only one copy of each block we find a 4-(11,5,1).

By a straightforward counting argument one finds

Lemma 1.1. If $\mathcal{D}$ is a t-(n,k,λ) and $i \leq t$, then $\mathcal{D}$ is also an i-(n,k,λ_i), where

$$\lambda_i := \lambda \binom{n-i}{t-i} (q-1)^{t-i} / \binom{k-i}{t-i} .$$

The fact that each λ_i must be an integer provides a necessary condition for the existence of a t-design.

In the following a t-design will mean a *binary* t-design (i.e. a t-design in the usual sense). Of course a q-ary t-design $t\text{-}(n,k,\lambda)$ can be mapped in a natural way onto a t-design $t\text{-}(n,k,\mu)$ by changing all non-zero coordinates into ones. Then $\mu = \lambda(q-1)^t$. However, this has the effect that the new t-design could have several repeated blocks. This is the case in the exercise above.

Usually one requires the blocks to be distinct. With that restriction there is no non-trivial 6-design known today. Until recently very few 5-designs were known. However, many have been found in the past 10 years using coding theory.

A t-design with $\lambda = 1$ is called a *Steiner system*. A $2\text{-}(n,3,1)$ is called a *Steiner Triple System* (STS(n)).

B) Block designs (cf. Hall [4])

A $2\text{-}(v,k,\lambda)$ is usually called a (*balanced incomplete*) *block design*. For the number of blocks (i.e. λ_0) one usually uses the letter b. For the number of blocks through a point (i.e. λ_1) the letter r. By counting in two ways the sum of the numbers of points in blocks, resp. the total number of pairs of points in all the blocks one finds

$$bk = vr \ , \tag{1.1}$$

$$\lambda(v-1) = r(k-1) \ . \tag{1.2}$$

One way of describing a q-ary t-design is to list all the blocks as the rows of a matrix A. If $q = 2$ this is called the *incidence matrix* of the design. The definition implies that A, a (0,1)-matrix, is the incidence matrix of a $2\text{-}(v,k,\lambda)$ iff

$$A^T A = (r-\lambda)I + \lambda J \ , \tag{1.3}$$

where J is the matrix with all entries 1.

C) Projective planes (cf. Hall [4], Hughes and Piper [6])

A *projective plane of order* n, which we shall indicate by PG(2,n), is a system of *points* and *lines* with an incidence relation such that

i) any two points are incident with a unique line,

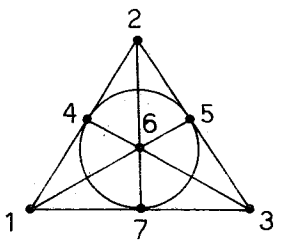
ii) any two lines are incident with a unique point,

iii) there are 4 points, no three on a line,

iv) there are n+1 points on each line, n+1 lines through each point and the total number of points (resp. lines) is n^2+n+1.

It is easy to show that (i), (ii), (iii) imply that the number of points on a line is a constant. If we call this constant n+1, then (iv) is a consequence of (i) to (iii). If we consider the lines as (n+1)-subsets of the set of n^2+n+1 points of the plane and call the lines blocks, we see that PG(2,n) is a $2-(n^2+n+1,n+1,1)$. Here b = v.

The smallest example of a projective plane is PG(2,2) known as the Fano plane:



(This is an STS(7).)

$$\text{i.e. } A = \begin{matrix} 1&2&3&4&5&6&7 \leftarrow \text{points} \\ \end{matrix}$$

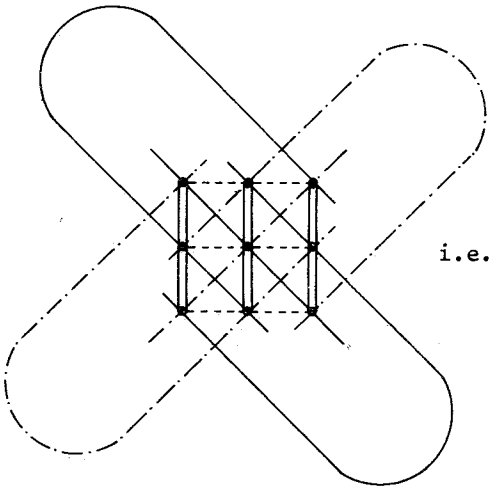
$$\begin{bmatrix} 1&1&0&1&0&0&0 \\ 0&1&1&0&1&0&0 \\ 0&0&1&1&0&1&0 \\ 0&0&0&1&1&0&1 \\ 1&0&0&0&1&1&0 \\ 0&1&0&0&0&1&1 \\ 1&0&1&0&0&0&1 \end{bmatrix} \Big\} \text{ blocks = lines} \qquad (1.4)$$

The plane PG(2,4) is a configuration of 21 points and 21 lines, with 5 points on each line and 5 lines through each point.
Observe that the 7 rows of A for PG(2,2) are exactly the 7 words of weight 3 in the (7,4) binary Hamming code.

Exercise. Consider PG(2,4). Let ℓ be a line in the plane. Let S be the set of 16 points, not on ℓ. If 3 points of S are on a line, then there is a unique fourth point on this line, not on ℓ. If 3 points of S are not on one line, then they determine 3 lines, which intersect ℓ in 3 different points. These 3 points with the original 3 points, determine a unique 7th point such that together they form the configuration of (1.4), i.e. PG(2,2). Prove this and show that we have thus constructed a 3-design on 16 points with blocks of size 4, i.e. a 3-(16,4,1).

D) Geometries (cf. Hughes and Piper [6])

The n-dimensional space $R^{(n)}$ over GF(q) can be interpreted in the usual way as an n-dimensional geometry called *affine* or *euclidean* space of dimension n, written as AG(n,q). Now we call a line through $\underline{0}$ a *projective point* and a 2-dimensional linear subspace a *projective line*, etc. We thus obtain a combinatorial configuration called (n-1)-dimensional *projective geometry* of order q, written as PG(n-1,q). The case n = 3, q a prime power gives us a system of coordinates for the projective plane PG(2,q).
Observe that AG(2,q) is a block design, namely a $2\text{-}(q^2,q,1)$. The example q = 3 yields an STS(9), namely



i.e. A =

1 1 1	0 0 0	0 0 0
0 0 0	1 1 1	0 0 0
0 0 0	0 0 0	1 1 1
1 0 0	1 0 0	1 0 0
0 1 0	0 1 0	0 1 0
0 0 1	0 0 1	0 0 1
1 0 0	0 1 0	0 0 1
0 1 0	0 0 1	1 0 0
0 0 1	1 0 0	0 1 0
1 0 0	0 0 1	0 1 0
0 1 0	1 0 0	0 0 1
0 0 1	0 1 0	1 0 0

(1.5)

In this design the fourth to twelfth block can be described by letting (i,j,k) denote the position of the one underneath the first, second and third block, respectively. Then the blocks are characterized by $i + j + k \equiv 0 \pmod 3$.

Consider the affine geometry AG(2m,2). Later on we shall be interested in the surface Q, called a *quadric*, described by the equation

$$X_1X_2 + X_3X_4 + \ldots + X_{2m-1}X_{2m} = 0 \ . \tag{1.6}$$

One easily sees that $|Q| = 2^{2m-1} + 2^{m-1}$. (The reader should check this as an exercise.)

E) Hadamard matrices and C-matrices (cf. Hall [4], Goethals and Seidel [7])

A Hadamard matrix H is a matrix with all its entries +1 or -1 such that

$$HH^T = nI \ , \tag{1.7}$$

where n is the order of H.

For the existence of H it is necessary that $n = 1$ or $n = 2$ or $n \equiv 0 \pmod 4$. It is not known whether this is sufficient.

A C-matrix is a matrix with entries 0 on the diagonal, +1 or -1 elsewhere such that

$$CC^T = (n-1)I \ , \tag{1.8}$$

where n is the order of C.

If C is a skew C-matrix, then $I + C$ is a Hadamard matrix. (The reader should also check this!) This idea was used in Paley's well-known construction of Hadamard matrices of order n, where n-1 is a prime power. E.g. a H_{12} is constructed as follows. Let $\underline{c} := (c_0, c_1, \ldots, c_{10})$, where $c_i = -1$ if i is a square mod 11 and $c_i = +1$ otherwise. Let S be a circulant matrix with $\underline{c}$ as its first row. Border S on the left by a column of -1's and border the new matrix by a row of +1's at the top. We find

$$H_{12} = \begin{bmatrix} + & + & + & + & + & + & + & + & + & + & + \\ - & + & - & + & - & - & - & + & + & + & - \\ - & + & + & - & + & - & - & - & + & + & + \\ - & - & + & + & - & + & - & - & - & + & + \\ - & + & - & + & + & - & + & - & - & - & + \\ - & + & + & - & + & + & - & + & - & - & - \\ - & + & + & + & - & + & + & - & + & - & - \\ - & - & + & + & + & - & + & + & - & + & - \\ - & - & - & + & + & + & - & + & + & - & + \\ - & + & - & - & - & + & + & + & - & + & + \\ - & - & + & - & - & - & + & + & + & - & + \end{bmatrix} \tag{1.9}$$

(cf. Hall [4], p. 209).

II. CODING THEORY PREREQUISITES (cf. Van Lint [2])

As before, $R^{(n)}$ denotes the space of all n-tuples from an alphabet of q symbols for which we take GF(q) if q is a prime power.
For $\underline{x} \in R^{(n)}$ and $\underline{y} \in R^{(n)}$ we denote by $d(\underline{x},\underline{y})$ their Hamming distance.
For $\rho > 0$ and $\underline{x} \in R^{(n)}$ we define the sphere $S_\rho(\underline{x})$ by

$$S_\rho(\underline{x}) := \{\underline{y} \in R^{(n)} \mid d(\underline{x},\underline{y}) \leq \rho\} . \tag{2.1}$$

For $S_\rho(\underline{0})$ we write S_ρ.

A k-dimensional linear subspace C of $R^{(n)}$ is called a *linear code* or (n,k)-code. The code is described by a *generator matrix* G which has as its rows a basis of C.

The dual code $C^\perp$ is defined by

$$C^\perp := \{\underline{x} \in R^{(n)} \mid \forall_{\underline{y}\in C} [(\underline{x},\underline{y}) = 0]\} , \tag{2.2}$$

where $(\underline{x},\underline{y})$ denotes the usual inner product. A matrix H with a basis of $C^\perp$ as its rows is called a *parity check* matrix of C. Clearly

$$C = \{\underline{x} \in R^{(n)} \mid \underline{x}H^T = \underline{0}\} . \tag{2.3}$$

As usual $\bar{C}$ denotes the code C, extended by an extra parity check bit, such that for every word in the extended code the sum of the coordinates is 0. An e-error-correcting code is a code C with $d(\underline{x},\underline{y}) \geq 2e+1$ for all distinct pairs $(\underline{x},\underline{y})$ in C.

A cyclic code C is a code with

$$\forall_{(c_0,c_1,\ldots,c_{n-1})\in C}[(c_{n-1},c_0,c_1,\ldots,c_{n-2}) \in C] . \tag{2.4}$$

By the identification $(c_0,c_1,\ldots,c_{n-1}) \leftrightarrow c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$ the code is mapped into a subset of GF(q)[x] mod$(x^n - 1)$. It is easy to show that a code is cyclic iff the image is an ideal in this polynomial ring. Hence every cyclic code is described by a generator polynomial g(x), where $g(x) \mid (x^n - 1)$. One often characterizes g(x) by giving sufficiently many zeros of g(x) in some extension field of GF(q).

We shall use the following codes in our examples:

(i) If α is a primitive element of $GF(2^m)$, $n = 2^m - 1$, and $m_1(x)$ is the minimal polynomial for α, then the cyclic code generated by $m_1(x)$ is the $(n,n-m)$-*Hamming code*.

(ii) If α is a primitive n-th root of unity in an extension field of GF(q) and the polynomial g(x) is the polynomial of lowest degree for which $g(\alpha) = g(\alpha^2) = \ldots = g(\alpha^{d-1}) = 0$, then the corresponding cyclic code is the *BCH-code* of designed distance d. Its minimum distance is at least d.

(iii) If q is a prime, $q^{\frac{n-1}{2}} \equiv 1 \pmod{n}$ and g(x) is the polynomial for which α^r is a zero iff r is a quadratic residue (mod n), (α is a primitive n-th root of unity in $GF(q^m)$), then the corresponding code is called a *quadratic residue code* (QR-code). Its minimum distance d satisfies $d(d-1) \geq n-1$. (This is known as the square root bound.)

(iv) Consider AG(m,2). Let $n = 2^m$. For $k = 0,1,\ldots,r$ we consider the (0,1)-vector of length n which is the characteristic function of a subspace $\{\underline{x} \in AG(m,2) \mid x_{i_1} = 0 \wedge \ldots \wedge x_{i_k} = 0\}$. These vectors

generate a binary code known as the r-*th order Reed-Muller code* of length 2^m.

(v) The reader is also assumed to be familiar with the *Preparata codes* (cf. e.g. Cameron and Van Lint [3]). These are nonlinear codes C_m with $|C_m| = 2^{2n-2m}$ where $n = 2^m-1$, m odd. They have minimum distance 5 and word length 2n+1.

In the following we shall frequently use the *MacWilliams relations* for the *weight-enumerator* of a code and its dual. They are the basis for most of the results treated in these lectures.

If C is a code in $R^{(n)}$, then the polynomial

$$A(\xi,\eta) := \sum_{i=0}^{n} A_i \xi^i \eta^{n-i} , \tag{2.5}$$

where A_i is the number of code words of weight i, is called the weight-enumerator of the code.

The reader is assumed to be familiar with the following theorem (but we give the proof anyway).

Theorem 2.1. Let $A(\xi,\eta)$ be the weight enumerator of an (n,k)-code over GF(q) and let $A^{\perp}(\xi,\eta)$ be the weight enumerator of the dual code. Then

$$A^{\perp}(\xi,\eta) = q^{-k}A(\eta - \xi, \quad \eta + (q-1)\xi) .$$

The proof of this theorem depends on the following lemma. (We write R instead of $R^{(n)}$.)

Lemma 2.1. Let χ be a non-trivial character on the group $(GF(q), +)$ and for any $\underline{v} \in R$ define $\chi_{\underline{v}} : R \to \mathbb{C}$ by

$$\forall_{\underline{u}\in R}\,[\chi_{\underline{v}}(u) := \chi((\underline{u},\underline{v}))] .$$

If A is a vector space over $\mathbb{C}$, $f : R \to A$, and if $g : R \to A$ is defined by

$$\forall_{\underline{u}\in R}\,[g(\underline{u}) := \sum_{\underline{v}\in R} f(\underline{v})\chi_{\underline{v}}(\underline{u})] ,$$

then for any linear subspace $V \subset R$ and the dual subspace $V^{\perp}$ we have

$$\sum_{\underline{u}\in V} g(\underline{u}) = |V| \sum_{\underline{v}\in V^{\perp}} f(\underline{v}) .$$

Proof. $\sum_{\underline{u}\in V} g(\underline{u}) = \sum_{\underline{u}\in V} \sum_{\underline{v}\in R} f(\underline{v})\chi_{\underline{v}}(\underline{u}) = \sum_{\underline{v}\in R} f(\underline{v}) \sum_{\underline{u}\in V} \chi((\underline{u},\underline{v})) =$

$$= |V| \sum_{\underline{v}\in V^{\perp}} f(\underline{v}) + \sum_{\underline{v}\notin V^{\perp}} f(\underline{v}) \sum_{\underline{u}\in V} \chi((\underline{u},\underline{v})) .$$

In the inner sum of the second term $(\underline{u},\underline{v})$ takes on every value in GF(q) the same number of times and since $\sum_{\alpha\in GF(q)} \chi(\alpha) = 0$ for every non-trivial character, this proves the lemma. □

Proof of Theorem 2.1. In Lemma 2.1 let A be the space of all polynomials in 2 variables ξ, η with coefficients in $\mathbb{C}$ and let $f(\underline{v}) := \xi^{w(\underline{v})}\eta^{n-w(\underline{v})}$. If $a \in GF(q)$ write $w(a) := 1$ if $a \neq 0$, $w(0) := 0$.

Then we have

$$g(\underline{u}) = \sum_{v_1 \in GF(q)} \cdots \sum_{v_n \in GF(q)}$$

$$\xi^{w(v_1)+\ldots+w(v_n)} \eta^{(1-w(v_1))+\ldots+(1-w(v_n))} \chi(u_1v_1+\ldots+u_nv_n) =$$

$$= \prod_{i=1}^{n} \{ \sum_{v \in GF(q)} \xi^{w(v)} \eta^{1-w(v)} \chi(u_i v) \} .$$

Since the inner sum is $\eta + (q-1)\xi$ if $u_i = 0$ and $\eta + \xi(\sum_{\alpha \in GF(q)\setminus\{0\}} \chi(\alpha)) = \eta - \xi$ if $u_i \neq 0$, we find

$$g(\underline{u}) = (\eta + (q-1)\xi)^{n-w(\underline{u})} (\eta - \xi)^{w(\underline{u})} .$$

Now by the result of Lemma 2.1 we have (taking V = C) :

$$\sum_{\underline{v} \in C^{\perp}} f(\underline{v}) = A^{\perp}(\xi,\eta) = q^{-k} \sum_{\underline{u} \in C} g(\underline{u}) = q^{-k} A(\eta - \xi, \eta + (q-1)\xi) . \quad \square$$

Later we shall show how this equation played a role in recent investigations on the existence of a projective plane of order 10.

For the sake of completeness we mention that generalisations of Theorem 2.1 to nonlinear codes are known.

III. THE ASSMUS-MATTSON THEOREM

Many of the most interesting t-designs with $t > 2$ which are known today were either found by applying a theorem due to E.F. Assmus, Jr. and H.F.Mattson, Jr. [8] or they could have been found in this way. This theo-

rem is one of the really important links between combinatorial theory and coding theory.

We first prove a lemma on t-designs.

Lemma 3.1. Let $\mathcal{D}$ be a t-design on the points of S. Then the complements of the blocks of $\mathcal{D}$ also form a t-design.

Proof. Let T be a t-subset of S. Denote by α_k the number of blocks D of $\mathcal{D}$ with $|D \cap T| = k$. Then by Lemma 1.1 we have

$$\sum_{k=0}^{t} \binom{k}{j}\alpha_k = \binom{t}{j}\lambda_j \qquad (j = 0,1,\ldots,t) .$$

By solving these equations we find that α_k does not depend on the choice of the set T. The statement for k = 0 implies that the complements of the blocks of $\mathcal{D}$ also form a t-design. □

In the following, if A is a linear code with minimum weight d, we shall consider words of weight v determined except for a scalar factor by their supports. We claim this is true if $v - \lceil \frac{v}{q-1} \rceil < d$. Indeed, if two words of weight v have the same support we consider the quotients of entries in corresponding places. These take q-1 nonzero values. So at least one of them occurs $\lceil \frac{v}{q-1} \rceil$ times. Hence there is a linear combination of the two words with weight $\leq v - \lceil \frac{v}{q-1} \rceil$. Since this weight is less than d, the linear combination is 0.

Theorem 3.1. Let A be an (n,k)-code over GF(q) and let $A^{\perp}$ be the (n,n-k) dual code. Let the minimum weights of these codes be d and e. Let t be an

integer less than d. Let v_0 be the largest integer satisfying $v_0 - \lceil \frac{v_0}{q-1} \rceil < d$ and w_0 the largest integer satisfying $w_0 - \lceil \frac{w_0}{q-1} \rceil < e$, where if $q = 2$, we take $v_0 = w_0 = n$. Suppose the number of non-0 weights of $A^\perp$ which are less than or equal to $n-t$ is itself less than or equal to $d-t$. Then, for each weight v with $d \le v \le v_0$, the subsets of $S := \{1,2,\ldots,n\}$ which support code words of weight d in A form a t-design. Furthermore, for each weight w with $e \le w \le \min\{n-t, w_0\}$, the subsets of S which support code words of weight w in $A^\perp$ form a t-design.

Proof. In the proof we shall use the following notation. For $A^\perp$ we write B. If t is a fixed t-subset of S and C is any code then we denote by C' the code obtained by deleting the coordinates in T from the code words of C which have zeros at all the positions of T.

(i) Consider any d-1 columns of the generator matrix of A and delete these. From the definition of d it follows that the resulting matrix still has rank k.

(ii) Consider any t-subset T of S. By (i) A' is an (n-t,k)-code. Clearly $(B_0)' \subset (A')^\perp$. The dimension of B_0' is at least n-k-t. Hence $B_0' = (A')^\perp$. Let $0 < v_1 < v_2 < \ldots < v_r \le n-t$ (where $r \le d-t$) be the possible nonzero weights less than or equal to n-t in the code B. Then these are also the only possible nonzero weights for B_0'. Since the minimum weight of A' is at least d-t we know d-t coefficients of the weight enumerator of A'. This is $\ge$ the number of coefficients of the weight enumerator of B_0' which we do not know yet. The MacWilliams relations, i.e. Theorem 2.1, yield a system of linearly independent equations which we can solve in principle. The important observation, however, is that the

solution, i.e. the weight enumerator of B_0', does not depend on the choice of T. Since $A' = (B_0')^{\perp}$ the same holds for A', again by Theorem 2.1.

(iii) We first prove the second assertion of the theorem. Let $w \le \min\{n-t, w_0\}$. Let $\mathcal{E}$ be the collection of w-subsets of S which support words of weight w in B. Consider the set $\mathcal{E}'$ of complements of sets in $\mathcal{E}$. For any t-subset T of s, $w \le w_0$ implies that the number of sets of $\mathcal{E}'$ containing T is $\frac{1}{q-1}$ times the number of words of weight w in B_0'. By (ii) this number does not depend on T. Hence $\mathcal{E}'$ is a t-design. By Lemma 3.1 $\mathcal{E}$ is also a t-design.

(iv) To prove the first assertion of the theorem we start with $v = d$. Let $\mathcal{D}$ be the collection of v-subsets of S which support words of weight v in A. In the same way as in (iii) we see that the number of sets in $\mathcal{D}$ containing a given t-subset T of S is $\frac{1}{q-1}$ times the number of words of weight d-t in A'. By (ii) this number does not depend on T. We now proceed by induction. Let $d \le v \le v_0$ and assume that the assertion of the theorem is true for all v' with $d \le v' < v$. Let $\mathcal{D}$ be as before. The number of subsets of $\mathcal{D}$ containing a given t-subset T of S is $\frac{1}{q-1}$ times the number of words of weight v-t in A' corresponding to words of weight v in A. By (ii) the total number of words of weight v-t in A' does not depend on T. By the induction hypothesis and Lemma 3.1 the number of words of weight v-t in A' corresponding to words of weight < v in A is also independent of T. Hence $\mathcal{D}$ is a t-design. □

We consider several examples.

Example 3.1. Take n = 8, k = 4, q = 2 and let $A = A^{\perp}$ be the extended (8,4)-Hamming code. Then d = e = 4. Take t = 3. The condition of Theorem 3.1 is satisfied. Taking v = 4, we find a 3-design with 14 blocks of size 4. This design is also known as a Hadamard-design. Consider a H_8 with a first row of +'s only. For the remaining 7 rows replace + by 1 and - by 0. Then take the complements of these rows. We find the same design as above.

Example 3.2. Take n = 12, k = 6, q = 3 and let $A = A^{\perp}$ be the extended ternary Golay code *). Then d = e = 6. The condition of Theorem 3.1 is satisfied for t = 5. We now find a 5-design!

Example 3.3. Let A be a $(12\ell,6\ell)$-self-dual code over GF(3). Suppose $d > 3\ell$. Take t = 5. Since all weights in A are divisible by 3 the condition of the theorem is satisfied. Taking v = d we find that the supports of the minimum weight words of A form a 5-design.

---

*) Besides trivial examples there are only 2 *perfect codes* with e > 1. (A perfect e-error-correcting code is a code for which the set $\bigcup_{x \in C} S_e(x)$ is the whole space $R^{(n)}$.) These codes are the so called *Golay codes*. Both are examples of Q.R. codes. E.g. the binary Golay code has n = 23 and hence by the square root bound it has $d \geq 6$. Since d must be odd $d \geq 7$. It follows by a counting argument that the code is perfect. From the definition of perfect codes it is immediately clear that the words of weight 7 in the code form a 4-(23,7,1). This is a design which can then be *extended* to the design of Example 3.4 (cf. Cameron and Van Lint [3]),

Example 3.4. Take n = 24, k = 12, q = 2 and let $A = A^{\perp}$ be the extended binary Golay code $\bar{C}$ (see * on p.18). Then d = e = 8. Since C is perfect the weight enumerator is determined. It is easy to check that 0, 8, 12, 16 and 24 are the only weights which occur. Therefore we can again apply the theorem with t = 5. The supports of the code words of weight 8 in A form the well-known 5-(24,8,1) Steiner system.

We consider another interesting application.

Definition 3.1. Let $q \equiv -1 \pmod 6$. We define a *symmetry code* of dimension q + 1 as a (2q+2,q+1)-code Sym_{2q+2} over GF(3) with generator

$$G_{2q+2} := (I_{q+1} C_{q+1})$$

where C_{q+1} is a C-matrix of order q+1. If q is a power of an odd prime we take C_{q+1} to be defined by the Paley construction (cf. Hall [4]).

The symmetry codes (defined by V. Pless [9]) have the following properties (for proofs cf. Cameron and Van Lint [3]).

(i) A Sym_{2q+2} is self-dual (and therefore all weights are $\equiv 0 \pmod 3$),

(ii) for q a power of an odd prime we have a C-matrix with $C_{q+1}^{T} = (-1)^{\frac{q-1}{2}} C_{q+1}$. Then

$$G^{*}_{2q+2} := \left((-1)^{\frac{q+1}{2}} C_{q+1} I_{q+1}\right)$$

is also a generator for Sym_{2q+2},

(iii) if $w_\ell(\underline{x})$ and $w_r(\underline{x})$ respectively denote the weight of the first half of $\underline{x}$, resp. the second half then

(a) $w_\ell(\underline{x}) = 1 \Rightarrow w_r(\underline{x}) = q$,

(b) $w_\ell(\underline{x}) = 2 \Rightarrow w_r(\underline{x}) = (q+3)/2$,

(c) $w_\ell(\underline{x}) = 3 \Rightarrow w_r(\underline{x}) \geq \lceil 3(q-3)/4 \rceil$,

(d) if there is a code word $\underline{x}$ with $w_\ell(\underline{x}) = w_1$, $w_r(\underline{x}) = w_2$, then there is a code word $\underline{y}$ with $w_\ell(\underline{y}) = w_2$, $w_r(\underline{y}) = w_1$,

(e) all code words $\underline{x}$ have $w_r(\underline{x}) > 0$.

Example 3.5. Consider the example $q = 17$. It is now easy to show that Sym_{36} has minimum weight 12. From the properties stated above we see that only the possibility $w_\ell = 4$, $w_r = 5$ must be ruled out. Using the circulant structure of C_{18} one can limit the amount of computation enough to make the problem feasible for hand computation. For a computer it is a trivial problem. Applying Theorem 3.1 we therefore find 5-designs on 36 points with blocks of size 12, 15, 18 or 21. These designs were discovered in this way.

We mention one more example of an application of Theorem 3.1. This example will turn up later in a different way.

Example 3.6. Consider a $(2^{2\ell-1} - 1,\ 2^{2\ell-1} - 1 - 2\ell)$-2-error-correcting primitive binary BCH-code C. Using Theorem 2.1 one can show that in $C^\perp$ the only weights which occur are $2^{2\ell-2}$, $2^{2\ell-2} \pm 2^{\ell-1}$. Now take $n = 2^{2\ell-1}$,

$k = 2^{2\ell-1} - 1 - 2\ell$, $q = 2$ and let A be $\bar{C}$. In $A^{\perp}$ only 3 weights occur. Hence if we take $t = 3$ the condition of Theorem 3.1 is satisfied. It follows that for each v the subsets which support code words of weight v form a 3-design.

IV. LINEAR CODES SUPPORTED BY STEINER TRIPLE SYSTEMS

A number of known codes, e.g. examples 3.1, 3.2, 3.4 have the property that the words of minimum weight form a t-design with $\lambda = 1$, i.e. a Steiner system.

In 1971 Assmus and Mattson [10] proposed a search for single-error-correcting linear codes for which the supports of the words of weight 3 are a STS. If the word length of C is n, then $n \equiv 1$ or 3 (mod 6) and the STS is a 2-(n,3,1). If we look at the 0's of any word in $C^{\perp}$ it is clear that the STS must have a subsystem on these positions. Hence, if we assume that the STS has *no* non-trivial subsystem, then the minimum weight in $C^{\perp}$ must be $\geq n-3$. Also the weight n-2 cannot occur. By Theorem 3.1 we see that this indeed yields a STS.

A few months ago L.M.H.E. Driessen, G.H.M. Frederix and the author found an infinite class of codes supported by AG(2,3) (cf. (1.5)). Let

$$H := \begin{pmatrix} 0 & 0 & 0 & -1 & -\alpha & -\alpha^2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & -1 & -\alpha & -\alpha^2 \\ -1 & -\alpha & -\alpha^2 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

where α is a primitive 3^{rd} root of 1 in GF(q), $q \equiv 1 \pmod 3$. Then H is the parity check matrix of the required code C. Clearly $(1,\alpha,\alpha^2,0,0,0,0,0,0)$ and cyclic shifts over 3 or 6 places are code words of C yielding the first 3 blocks of (1.5). To find other code words we must find a linear combination of

$$\begin{pmatrix} 0 \\ 1 \\ -\alpha^i \end{pmatrix}, \quad \begin{pmatrix} -\alpha^j \\ 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -\alpha^\ell \\ 0 \end{pmatrix}$$

which is $\underline{0}$. The reader should have no difficulty checking that this implies $i+j+k \equiv 0 \pmod 3$ as in (1.5).

One can show that a STS on 13 points cannot support a code. PG(2,2), as we know, supports the (7,4) Hamming code. In fact it supports a linear code over GF(q) iff $q = 2^\alpha$. This research is being continued.

V. PROJECTIVE PLANES AND CODES

We now consider another way to relate designs and codes. Consider the incidence matrix A of a projective plane PG(2,n). We consider the subspace C of $R^{(n^2+n+1)}$ over GF(2) which is generated by the rows of A. If n is odd it is easy to see what the code C is. If we take the sum of the rows of A which have a 1 in a fixed position the result is a row with a 0 in that position and 1's elsewhere. These vectors generate the subspace of $R^{(n^2+n+1)}$ consisting of all words of even weight and this is C (because C obviously has no words of odd weight). The case of even n is

more difficult.

Theorem 5.1. If $n \equiv 2 \pmod 4$ then the rows of the incidence matrix A of PG(2,n) generate a code C with dimension $\frac{1}{2}(n^2+n+2)$.

Proof. (i) Since n is even the code $\bar{C}$ is self-orthogonal, i.e. $\bar{C} \subset (\bar{C})^{\perp}$. Therefore $\dim C \leq \frac{1}{2}(n^2+n+2)$.

(ii) Let $\dim C = r$ and let $k := n^2+n+1-r = \dim C^{\perp}$. Let H be a parity check matrix of rank k for C and assume the coordinate places have been permuted in such a way that H has the form $(I_k \quad P)$.

Define $N := \begin{pmatrix} I_k & P \\ 0 & I_r \end{pmatrix}$. Interpret A and N as rational matrices. Then $\det AN^T = \det A = (n+1)n^{\frac{1}{2}(n^2+n)}$. Since all entries in the first k columns of AN^T are even we find that $2^k | \det A$. It then follows that $r \geq \frac{1}{2}(n^2+n+2)$. Form (i) and (ii) the theorem follows. □

From Theorem 5.1 we immediately have:

Theorem 5.2. If $n \equiv 2 \pmod 4$ then the rows of the incidence matrix A of PG(2,n) generate a code C, for which $\bar{C}$ is self-dual.

We continue with a few other properties of the plane PG(2,n), where $n \equiv 2 \pmod 4$, interpreted in coding terms.

Theorem 5.3. The code C of Theorem 5.1 has minimum weight n+1 and every vector of minimum weight is a line in PG(2,n).

Proof. Let $\underline{v} \neq 0$ be a code word with $w(\underline{v}) = d$. Since every line has a 1 as overall parity check we see that:

(i) if d is odd then $\underline{v}$ meets every line at least once and

(ii) if d is even then every line through a fixed point of $\underline{v}$ meets $\underline{v}$ in a second point.

In case (ii) we immediately have $d > n+1$. In case (i) we find $(n+1)d \geq n^2+n+1$, i.e. $d \geq n+1$. If $w(\underline{v}) = n+1$ then there is a line ℓ of PG(2,n) which meets $\underline{v}$ in at least 3 points. If there is a point of ℓ not on $\underline{v}$, then every line $\neq \ell$ through this point meets $\underline{v}$ by (i). This would yield $d \geq n+3$. □

Definition 5.1. An s-arc in PG(2,n) is a set of s points no three of which are collinear.

Theorem 5.4. The vectors of weight n+2 in C are precisely the (n+2)-arcs of PG(2,n).

Proof. (i) Let $\underline{v} \in C$ and $w(\underline{v}) = n+2$. Every line meets $\underline{v}$ in an even number of points. Let ℓ be a line and suppose $\underline{v}$ and ℓ have 2a points in common. Each of the n lines $\neq \ell$ through one of these 2a points meets $\underline{v}$ at least once more. Therefore $2a+n \leq n+2$, i.e. $a = 0$ or $a = 1$.

(ii) Let $\underline{v}$ be an (n+2)-arc. Let S be the set of $\frac{1}{2}(n+1)(n+2)$ distinct lines of PG(2,n) through the pairs of points of $\underline{v}$. Each line of S contains n-1 points not in $\underline{v}$. In this way we count $\frac{1}{2}(n+2)(n^2-1)$ points. There are n^2-1 points not in $\underline{v}$ and each of these is on at least $\frac{1}{2}(n+2)$ lines of S. Therefore each of these is on exactly $\frac{1}{2}(n+2)$ lines of S.

Each point of $\underline{v}$ is on n+1 lines of S. Therefore $\underline{v}$ is the sum of the lines of S, i.e. $\underline{v} \in C$. (Also see Assmus and Mattson [10].) □

Remark. We leave it as an interesting exercise for the reader to check that Theorem 5.4 also holds for the code generated by PG(2,4).

In fact this code is even more interesting from a geometrical point of view. It is easy to check that the code has

(i) 21 words of weight 5, the lines of PG(2,4) ,

(ii) 210 " " " 8, pairs of lines of PG(2,4) ,

(iii) 280 " " " 9, triples of nonconcurrent lines in PG(2,4) ,

(iv) 360 " " " 7, all the subplanes PG(2,2) contained in PG(2,4) ,

(v) 168 " " " 6, the 6-arcs of the plane ,

(vi) 1008 " " " 10, each a subplane + a line meeting it in one point ,

(vii) the complements of these .

Using a little group theory (cf. Lüneburg [11]) one can show that the 6-arcs and subplanes can be split into 3 equivalence classes in such a way that the following construction works: Take 3 new points p, q, r. Make new blocks as follows :

(a) to a line add p,q,r

(b) to a pair of lines add nothing

(c) to a 6-arc in "class r" add p,q (cyclic)

(d) to a subplane in class r add r ,

(cf. Cameron and Van Lint [3]).

The result is a set of 759 blocks of size 8 which is now a 5-design, namely the Steiner system 5-(24,8,1). Since one can show that this design and the Golay code are both unique it follows that these 8-tuples are exactly the words of weight 8 in the extended binary Golay code! (cf. Example 3.4).

For a self-dual (n,k) code C over GF(q) we find from Theorem 2.1 the following relation for the weight enumerator $A(\xi,\eta)$:

$$A(\xi,\eta) = q^{-k}A(\eta - \xi,\ \eta + (q-1)\xi)\ , \tag{5.1}$$

where $k = \frac{1}{2}n$. This means that the polynomial is invariant under the linear transformation with matrix $q^{-\frac{1}{2}}\begin{pmatrix} -1 & q-1 \\ 1 & 1 \end{pmatrix}$. If q = 2, all code words of C have even weight, i.e. $A(\xi,\eta)$ is invariant under the transformation $\xi \to -\xi$. The 2 transformations generate the dihedral group $\mathcal{D}_8$. It was shown by A.M. Gleason [12] that the ring of polynomials in ξ and η which are invariant under this group is the free ring generated by $\xi^2+\eta^2$ and $\xi^2\eta^2(\xi^2-\eta^2)^2$.

Let us now consider a possible plane of order 10. From Definition 5.1 and Theorems 5.1 and 5.2 we know that the incidence matrix of this plane generates a code C for which $\bar{C}$ is a (112,56)-self-dual code and that the weight enumerator $A(\xi,\eta)$ of C has coefficients $A_0 = 1$, $A_1 = A_2 = \ldots = A_{10} = 0$, $A_{11} = 111$.

Since all the generators of $\bar{C}$ have weight 12 and any two words of $\bar{C}$ have an even number of 1's in common we see that all weights in $\bar{C}$ are divisible by 4. Therefore $A_{13} = A_{14} = 0$. By substituting this in (5.1) or by using Gleason's result one sees that $A(\xi,\eta)$ is uniquely determined if we know A_{12}, A_{15} and A_{16}. Recently F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson [13] investigated the code words of weight 15 in C. It was assumed that the incidence matrix of the plane led to a code for which $A_{15} \neq 0$. Arguments of the same type as the ones we used in proving Theorems 5.3 and 5.4 severely restricted the possibilities. In fact it was found that the plane had to contain a particular configuration of 15 lines. A computer search showed that starting from such a configuration the plane could not be completed. Therefore we now know that if a plane of order 10 exists, then

$$A_{15} = 0 .$$

Another way in which coding theory could help in finding PG(2,10) is to use Theorem 5.2 and 5.3 as follows. Construct a (112,56) self-dual code and then find the words of minimum weight. A very promising approach is to use ideas similar to symmetry codes. We give one example. There is a block design 2-(56,11,2) for which the incidence matrix A is a symmetric matrix of size 56×56. Clearly $(I_{56} \quad A)$ is the generator matrix of a (112,56) self-dual code $\bar{C}$. In the same way as we did in Example 3.5 it is easy to show that $\bar{C}$ has minimum weight 12. That is where our luck ends! The code C has only 48 words of weight 11. It is still possible that another choice for A would yield the required result!

Projective planes are also connected to so called *equidistant codes*.

Definition 5.2. An equidistant (m,k)-code is an m-subset S of $R^{(n)}$ such that

$$\forall_{\underline{x}\in S}\ \forall_{\underline{y}\in S}\ [\underline{x} \neq \underline{y} \Rightarrow d(\underline{x},\underline{y}) = k] .$$

If H is a Hadamard matrix of order n then the n rows of $\frac{1}{2}(H+J)$ form an equidistant binary $(n,\frac{1}{2}n)$-code. From now on we take q = 2. With an equidistant (m,2k)-code S we associate the matrix C which has as its rows all the words of S. Each column C of S, interpreted as a binary vector, has a weight. If all these weights are 0, 1, m-1 or m, we call S a trivial equidistant code. E.g. if $C = (I_m I_m \ldots I_m)$, k copies of I_m, then S is trivial with distance 2k.

Let B be the incidence matrix of PG(2,k) and let J be the k^2+k+1 by k-1 matrix of 1's. Then

$$C = \begin{pmatrix} 0 & 0 \ldots 0 & 0 \ldots 0 \\ & & \vdots \\ & B & J \end{pmatrix}$$

represents an equidistant $(k^2+k+2,2k)$-code which is nontrivial. It was shown by M. Deza [14] that a nontrivial equidistant (m,2k)-code has $m \leq k^2+k+2$. The case of equality is interesting.

Theorem 5.5. If a nontrivial equidistant $(k^2+k+2,2k)$-code exists, then the projective plane PG(2,k) exists.

For a proof we refer to Van Lint [15].

For the case k = 6, where the projective plane does not exist, the theorem states that the maximum number m of words in an equidistant code with d = 12, is ≤ 43. Using PG(2,5) one easily constructs an example with 32 words. Recently A.J.E.M. Jansen, A.W.J. Kolen and the author have shown that in fact m ≤ 33. The final step was made in the week before this course when J.I. Hall and the author showed that m ≤ 32. Clearly, solving the problem for k = 10 is only possible if one can decide first whether PG(2,10) exists or not.

VI. UNIFORMLY PACKED CODES

We shall now consider a class of codes which generalize the idea of perfect codes. These codes are being studied extensively because they lead to t-designs. As an introduction we consider a special case first (cf. Van Lint [16]). Let C be a binary code of length n and minimum distance d = 2e+1. We define

$$C_e := \{\underline{x} \in R^{(n)} \mid \rho(\underline{x},C) \geq e\} , \tag{6.1}$$

where $\rho(\underline{x},C)$ is the distance from $\underline{x}$ to the nearest code word. For all $\underline{z} \in C_e$ we define

$$r(\underline{z}) := |C \cap S_{e+1}(\underline{z})| , \tag{6.2}$$

i.e. the number of code words with distance e or e+1 from $\underline{z}$.

By the triangle inequality

$$r(\underline{z}) \leq \left\lfloor \frac{n+1}{e+1} \right\rfloor . \tag{6.3}$$

Since

$$\sum_{\underline{z}\in C_e} r(\underline{z}) = |C| \{\binom{n}{e} + \binom{n}{e+1}\}$$

and

$$C_e = 2^n - |C| \sum_{i=0}^{e-1} \binom{n}{i} ,$$

we find that the *average value* r of $r(\underline{z})$ satisfies

$$|C| \left\{\sum_{i=0}^{e-1} \binom{n}{i} + \frac{1}{r}(\binom{n}{e} + \binom{n}{e+1})\right\} = 2^n . \tag{6.4}$$

Observe that $r = \frac{n+1}{e+1}$ in (6.1) would imply that C is perfect.

Definition 6.1. A binary *uniformly packed* code C is a code for which $r(\underline{z}) = r$ for all $\underline{z} \in C_e$.

Example 6.1. Consider the matrix H_{12} of (1.9). We form

$$A := \begin{pmatrix} \frac{1}{2}(H_{12} + J) \\ \frac{1}{2}(-H_{12} + J) \end{pmatrix}$$

and then remove the first column. The result is a list of 24 words in $R^{(11)}$ with all distances ≥ 5. Let this be the code C. Suppose there is a $z \in C_2$ with $r(\underline{z}) = 4$. By suitable multiplications of certain positions by -1 and by permuting symbols this would mean w.l.o.g. that $\underline{z}$ and the four code words $\underline{x}_1,\ldots,\underline{x}_4$ at distance 2 or 3 are

$$\underline{z} = - - \quad + + + \quad + + + \quad + + +$$

$$\underline{x}_1 = + + \quad + + + \quad + + + \quad + + +$$

$$\underline{x}_2 = - - \quad - - - \quad + + + \quad + + +$$

$$\underline{x}_3 = - - \quad + + + \quad - - - \quad + + +$$

$$\underline{x}_4 = - - \quad + + + \quad + + + \quad - - -$$

W.l.o.g. the removed first coordinate of $\underline{z}_1$ to $\underline{x}_4$ is respectively +,−, −, −. Then $\underline{x}_1 - \underline{x}_2 - \underline{x}_3 - \underline{x}_4 = 4(1,1,1,0,0,\ldots,0)$ and no row of $\pm$ 1's can be orthogonal to this. It follows that for all $\underline{z} \in C_2$ we have $r(\underline{z}) \geq 3$. For r we find form (6.4) the value 3. Hence $r(\underline{z}) = 3$ for all $\underline{z} \in C_e$. Hence C is a uniformly packed 2-error-correcting code. Observe that again the words of minimum weight in the code C form a design, namely a Hadamard 3-design. We shall see later that this is not a coincidence.

Example 6.2. Let C be the Preparata code of length 2n+1, where $n = 2^m - 1$, m odd. Again e = 2. By (6.3) we have $r(\underline{z}) \leq \lfloor \frac{1}{3} 2^{m+1} \rfloor = \frac{2^{m+1} - 1}{3}$. Substituting the known values of $|C|$, e and n in (6.4) we find

$$2^{2n-2m} \left\{ 1 + (2^{m+1} - 1) + \frac{1}{r} \frac{2^{m+1}(2^{m+1} - 1)(2^{m+1} - 2)}{6} \right\} = 2^{2n+1} ,$$

i.e. $r = \frac{2^{m+1} - 1}{3}$. Therefore all $r(\underline{z})$ must be equal to the maximum value! Therefore this is a uniformly packed code with equality in (6.3). Such a code is called *nearly perfect* (cf. Goethals and Snover [17]).

We now look at the more general case (alphabet GF(q)) (cf. Goethals and Van Tilborg [18]).

Definition 6.2. The *covering radius* $\rho(C)$ of a code $C \subset R^{(n)}$ is the smallest number ρ such that $R^{(n)} \subset \bigcup_{\underline{x} \in C} S_\rho(\underline{x})$.

Let C be a code with covering radius $\rho(C) = e + 1$ and minimum distance $d \geq 2e + 1$. We again consider the set C_e of words of $R^{(n)}$ with distance e or e + 1 to the code.

Definition 6.3. The code C is called *uniformly packed* with parameters λ and μ if

(i) every $\underline{z} \in C_e$ with $\rho(\underline{z},C) = e$ is at distance e + 1 form exactly λ code words,

and

(ii) every $\underline{z} \in C_e$ with $\rho(\underline{z},C) = e+1$ is at distance e + 1 from exactly μ code words.

Remarks. a) in Definition 6.1 we had $q = 2$ and $\lambda + 1 = \mu = r$,

b) $\lambda = 0 \Leftrightarrow d = 2e + 2$ or $2e + 3$,

c) if $\lambda = 0$ and $\mu = 1$ then $d = 2e + 3$ and C is a *perfect* (e+1)-error-correcting code!

From the point of view of design theory the interesting thing about these codes is that the words of fixed weight form a design. We shall only prove part of this.

Theorem 6.1. Let C be a q-ary code with $\rho(C) = e + 1$, $d = 2e + 1$ and let C be uniformly packed with parameters λ and μ. Assume $\underline{0} \in C$. Then the words of weight $2e + 1$ in C form a q-ary $e\text{-}(n, 2e+1, \lambda)$.

Proof. Let $\underline{u}$ be any word of weight e in $R^{(n)}$. Since $d(\underline{u}, \underline{0}) = e$ and C has minimum distance $2e + 1$, we have $d(\underline{u}, \underline{c}) \geq e + 1$ for all nonzero $\underline{c} \in C$. By Definition 6.3 (i) there are exactly λ code words $\underline{c}_1, \ldots, \underline{c}_\lambda$ such that $d(\underline{u}, \underline{c}_i) = e + 1$. For such a code word

$$w(\underline{c}_i) \leq w(\underline{u}) + d(\underline{u}, \underline{c}_i) = 2e + 1 ,$$

with equality only if $\underline{u}$ is covered by $\underline{c}_i$. However, equality must occur because C has minimum distance $2e + 1$ and $\underline{0} \in C$. Therefore $\underline{u}$ is covered by the λ code words $\underline{c}_i$ of weight $2e + 1$. On the other hand, if $\underline{u}$ is covered by a code word $\underline{c}$ of weight $2e + 1$, then $d(\underline{u}, \underline{c}) = e + 1$, i.e. $\underline{c}$ is one of the $\underline{c}_i$. □

The methods which are used to treat uniformly packed codes involve quite a lot of abstract algebra. The results are deep and provide us among others with a very strong necessary condition for existence. Very recently H.C.A. van Tilborg [19] used this condition to show that (except for known perfect codes) there is *no* code satisfying Definition 6.1 with $e > 2$.

We mention one interesting result obtained by using the algebraic methods and by applying Theorem 2.1.

Theorem 6.2. A *linear* single-error-correcting code C is uniformly packed (with certain parameters) iff $C^\perp$ is a two-weight code.

Example 6.3. Consider the quadric Q in AG(2m,2) described in (1.6). Let the $n := 2^{2m-1} + 2^{m-1} - 1$ non-zero points of Q be coordinate places for a code space $R^{(n)}$. As in the description of RM codes consider the 2^m characteristic functions $\underline{a}_i$ of the hyperplanes $\{\underline{x} \in AG(2m,2) \mid x_i = 1\}$, but only on the points of Q, i.e. we intersect the hyperplanes with Q. A relatively simple counting argument shows that any hyperplane $\{\underline{x} \in AG(2m,2) \mid \sum_{i=1}^{2m} \alpha_i x_i = 1\}$ intersects $Q\backslash\{\underline{0}\}$ in w_1 or w_2 points. In other words: the 2m vectors $\underline{a}_i$ are the basis vectors of a linear code $C^{\perp}$ with word length $2^{2m-1} + 2^{m-1} - 1$ which has w_1 and w_2 as its only weights. By Theorem 6.2 this implies that the dual code C is uniformly packed. Therefore by Theorem 6.1 the words of weight 3 in C form a 1-design. This is not too interesting but a simple extension of Theorem 6.1 shows that the words of weight 4 in $\bar{C}$ form a 2-design. The reader should check that this also follows from Theorem 3.1.

As an exercise we invite the reader to show that the codes of Example 3.7 are uniformly packed, thus providing a second explanation for the occurrence of 3-designs in their extended codes.

REFERENCES

1. Berlekamp, E.R., *Algebraic Coding Theory*, McGraw Hill, New York, 1968.
2. Lint, J.H. van, *Coding Theory*, Lecture Notes in Math. 201, Springer Verlag, Berlin, 1971.

3. Cameron, P.J. and Lint, J.H. van, *Graph Theory, Coding and Block Designs*, London Math. Soc. Lecture Notes Series 19, Cambridge Univ. Press, 1975.

4. Hall, M., *Combinatorial Theory*, Blaisdell, Waltham, Mass. 1967.

5. Goethals, J.M., Generalized t-designs and majority decoding of linear codes, Report R282, M.B.L.E. Research Lab., Brussels 1975.

6. Hughes, D.R. and Piper, F.C., *Projective Planes*, Springer Verlag, New York, 1973.

7. Goethals, J.M. and Seidel, J.J., Orthogonal matrices with zero diagonal, *Canad. J. Math.* 19, 1001, 1967.

8. Assmus, E.F. and Mattson, H.F., New 5-designs, *J. Comb. Theory* 6, 122, 1969.

9. Pless, V., Symmetry codes over GF(3) and new 5-designs, *J. Comb. Theory* 12, 119, 1972.

10. Assmus, E.F. and Mattson, H.F., Algebraic Theory of Codes, Report AFCRL-0013, Appl. Research Lab. of Sylvania Electronic Systems, Bedford, Mass. 1971.

11. Lüneburg, H., Über die Gruppen von Mathieu, *Journal of Algebra* 10, 194, 1968.

12. Gleason, A.M., Weight polynomials of self-dual codes and the MacWilliams identities, in *Actes Congrès Intern. Math.* 1970, vol. 3, 211.

13. Mac Williams, F.J., Sloane, N.J.A., and Thompson, J.G., On the existence of a projective plane of order 10, *J. Comb. Theory*, 14, 66, 1973.

14. Deza, M., Une propriété extremal des plans projectifs finis dans une classe de codes equidistants, *Discrete Math.* 6, 343, 1973.

15. Lint, J.H. van, A theorem on equidistant codes, *Discrete Math.* 6, 353, 1973.

16. Lint, J.H. van, Recent results on perfect codes and related topics, in *Combinatorics* I (Hall, M. and Lint, J.H. van, Eds.) Mathematical Centre Tracts 55, 158, 1974.

17. Goethals, J.M. and Snover, S.L. Nearly perfect binary codes, *Discrete Math.* 2, 65, 1972.

18. Goethals, J.M. and Tilborg, H.C.A. van, Uniformly packed codes, Philips Res. Repts. 30, 9, 1975.

19. Tilborg, H.C.A. van, All binary (n,e,r) uniformly packed codes are known, Memorandum 1975-08, T.H. Eindhoven.