A STRENGTHENING OF THE ASSMUS-MATTSON THEOREM*

A. R. Calderbank

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, NJ 07974, USA

P. Delsarte

Philips Research Laboratories
Avenue Albert Einstein 4
B-1348 Louvain-la-Neuve, Belgium

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, NJ 07974, USA

DEDICATED TO THE MEMORY OF JESSIE MACWILLIAMS (1917-1990)

ABSTRACT

Let $w_1 = d, w_2, \ldots, w_s$ be the weights of the nonzero codewords in a binary linear $[n, k, d]$ code C, and let $w'_1, w'_2, \ldots, w'_{s'}$ be the nonzero weights in the dual code $C^\perp$. Let t be an integer in the range $0 < t < d$ such that there are at most $d - t$ weights w'_i with $0 < w'_i \le n - t$. Assmus and Mattson proved that the words of any weight w_i in C form a t-design. We show that if $w_2 \ge d + 4$ then either the words of any nonzero weight w_i form a $(t+1)$-design or else the codewords of minimal weight d form a $\{1, 2, \ldots, t, t+2\}$-design. If in addition C is self-dual with all weights divisible by 4 then the codewords of any given weight w_i form either a $(t+1)$-design or a $\{1, 2, \ldots, t, t+2\}$-design. The special case of this result for codewords of minimal weight in an extremal self-dual code with all weights divisible by 4 also follows from a theorem of Venkov and Koch; however our proof avoids the use of modular forms.

---

* This paper appeared in *IEEE Trans. Inform. Theory*, **37** (1991), pp. 1261-1268.

1. A strengthened Assmus-Mattson theorem

Let C be a binary, linear $[n, k, d]$ code with nonzero weights $w_1 = d, w_2, \ldots, w_s$, and let $w'_1, \ldots, w'_{s'}$ be the nonzero weights in the dual code $C^{\perp}$. Our starting point is the following theorem.

Theorem 1 (Assmus and Mattson [2]). *Let t be the greatest integer in the range $0 < t < d$ such that there are at most $d - t$ weights w'_i with $0 < w'_i \leq n - t$. Then the codewords of any weight w_i in C form a t-design.*

Venkov [21], answering a question raised in [20], showed that this theorem has an analogue for extremal even unimodular lattices in Euclidean space of dimension $24m$. The expected analogue was that the lattice vectors of any fixed nonzero length would form a spherical 11-design. Venkov proved this and more: he showed that these vectors possess an additional symmetry, forming what he called a spherical 11½-design. His proof uses the theory of modular forms.

Venkov [21] also announced that similar results could be obtained for self-dual codes. These results are stated by Koch [15] (see also [14], [16]). In particular, Venkov and Koch show that, in any extremal binary self-dual doubly-even code C, the set P of minimal weight words has the property that a certain linear form associated with P is constant on $(t+2)$-sets. Here $t = 5$ if the length n of the code is a multiple of 24, $t = 3$ if $n \equiv 8$ (mod 24), and $t = 1$ if $n \equiv 16$ (mod 24). To prove their result they associate a unimodular lattice with C and again apply the theory of modular forms.

Our strengthened version of Theorem 1 involves the concept of a T-design, defined as follows (cf. [8]). Let Ω be the set of all d-subsets of the n-set $[1, n] = \{1, \ldots, n\}$, with $d \leq n/2$. We identify Ω with the set of all points $\xi = (\xi_1, \ldots, \xi_n)$ in R^n that satisfy $\xi_p \in \{0, 1\}$ for all p and $\Sigma_{p=1}^{n} \xi_p = d$. The vector space R^{Ω} of mappings from Ω to R is invariant under the natural action of the symmetric group S_n. The irreducible S_n-invariant subspaces of R^{Ω} are the *harmonic spaces* $\mathrm{harm}(i)$, $i = 0, 1, \ldots, d$. (These spaces are described in detail in Section 2, where in particular we give an explicit basis for $\mathrm{harm}(i)$.)

Let P be a subset of Ω, i.e. a constant weight code, and let $\pi(\mathsf{P}) \in \mathsf{R}^{\Omega}$ be the corresponding characteristic vector. The importance of the harmonic space $\mathrm{harm}(i)$ is that if the projection of $\pi(\mathsf{P})$ onto $\mathrm{harm}(i)$ is zero, then there is some regularity in the way the vectors of P meet an arbitrary i-subset of $[1, n]$. In particular (see [10]), P is a t-design if and only if, for all $i = 1, 2, \ldots, t$, the inner product $\langle \pi(\mathsf{P}), f \rangle = 0$ for all $f \in \mathrm{harm}(i)$. As in [8] we extend the definition of a design to subsets $T \subseteq [1, n]$ other than $[1, t]$ by saying that a collection P is a T-*design* if, for all $i \in T$, the inner product $\langle \pi(\mathsf{P}), f \rangle = 0$ for all $f \in \mathrm{harm}(i)$. (In case $0 \in T$, a T-design is defined to be a T'-design with $T' = T \setminus \{0\}$.)

When combined with the results of Section 3 of the present paper (in particular Theorem 7), the Venkov-Koch result mentioned above implies that the codewords of minimal weight in an extremal self-dual doubly-even code C form a $\{1, 2, \ldots, t, t+2\}$-design. (For in this case the linear form in Theorem 7 reduces to Venkov's form, given on page 461 of Koch [15].)

The purpose of the present paper is to give a similar generalization of the Assmus-Mattson theorem that does not assume the code is self-dual and whose proof avoids the use of modular forms. Our main theorem is the following.

Theorem 2. *Let C be a binary $[n, k, d]$ code with nonzero weights $w_1 = d$, $w_2, \ldots, w_s$, and let $w'_1, \ldots, w'_{s'}$ be the nonzero weights in the dual code $C^{\perp}$. Let t be the greatest integer in the range $0 < t < d$ such that there are at most $d - t$ weights w'_i with $0 < w'_i \le n - t$. If $w_2 \ge d + 4$ then either the codewords in C of any nonzero weight w_i form a $(t+1)$-design or else the codewords of minimal weight d form a $\{1, 2, \ldots, t, t+2\}$-design.*

The proof is given in Section 4. In one important special case we can prove slightly more.

Theorem 3. *If, in addition to the hypotheses of Theorem* 2, *C is self-dual with all weights divisible by* 4 *then the codewords of any given weight* w_i *form either a* $(t+1)$*-design or a* $\{1, 2, \ldots, t, t+2\}$*-design.*

The proof is given in Section 5.

A list of the known extremal codes is given in [6, p. 194] and [7]. We may conclude for example that the codewords of minimal weight in the [24, 12, 8] Golay code and the [48, 24, 12] extended quadratic residue code form $\{1, 2, 3, 4, 5, 7\}$-designs. The minimal weight codewords in any of the five [32, 16, 8] self-dual doubly-even codes ([5], [7]) or in the extremal self-dual codes of lengths 56, 80 and 104 form $\{1, 2, 3, 5\}$-designs, and the minimal weight words in the extremal self-dual codes of lengths 16, 40, 64, 88 and 136 form $\{1, 3\}$-designs. Other examples are given in Section 4.

The invariant linear forms associated with codes are further investigated in [3], [4]. Generalizations to nonlinear codes and other fields are considered in [3].

2. The harmonic space harm(i)

In this section we give a more precise definition of and an explicit basis for the harmonic space harm(i).

We first define the *homogeneous space* hom(i) $(0 \le i \le n)$. This is the subspace of $\mathbb{R}^{\Omega}$ represented by homogeneous polynomials $f(z) = f(z_1, \ldots, z_n)$ of total degree i and degree at most 1 in each variable z_p. Note that, since these functions are defined on Ω, z_p^2 and z_p $(1 \le p \le n)$ represent the same function, and $z_1 + z_2 + \cdots + z_p$ is the constant function d. The latter assertion implies that hom(j) is a subspace of hom(i) for $0 \le j \le i$.

The monomials $z_{p_1} z_{p_2} \cdots z_{p_i}$ are linearly independent and span $\mathrm{hom}(i)$. Thus the dimension of $\mathrm{hom}(i)$ is $\binom{n}{i}$ (cf. [10]).

The Laplacian Δ is the differential operator given by

$$\Delta f(z) \;=\; \sum_{p=1}^{n} \frac{\partial f(z)}{\partial z_p} \;.$$

This maps $\mathrm{hom}(i)$ onto $\mathrm{hom}(i-1)$, and the kernel is the *harmonic space* $\mathrm{harm}(i)$. In [10] it is shown that there is an orthogonal decomposition

$$\mathrm{hom}(i) \;=\; \mathrm{harm}(i) \,\oplus\, \mathrm{hom}(i-1) \;, \qquad (1 \le i \le n) \;,$$

with respect to the inner product $\langle f, g \rangle = \sum_{\xi \in \Omega} f(\xi) g(\xi)$, from which it follows that the dimension of $\mathrm{harm}(i)$ is $\binom{n}{i} - \binom{n}{i-1}$ $\mathrm{Hom}(0) = \mathrm{harm}(0)$ is the 1-dimensional space of constant functions.

Theorem 4. *For any i-subset* $\{q_1, \ldots, q_i\}$ *of* $[1,n]$ *we define an element* ϕ *of* R^{Ω} *by*

$$\phi(z_1, \ldots, z_n) \;=\; \sum_{j=0}^{i} (-1)^j \binom{i}{j}^{-1} \binom{d-j}{i-j} \binom{n-i+1}{j} \sigma_j (z_{q_1}, \ldots, z_{q_i}) \;, \tag{1}$$

where $\sigma_j (z_{q_1}, \ldots, z_{q_i})$ *is the sum of the characteristic functions* $z_{p_1} z_{p_2} \cdots z_{p_j}$ *of all j-subsets* $\{p_1, \ldots, p_j\}$ *of* $\{q_1, \ldots, q_i\}$. *Then the set of all* $\binom{n}{i}$ *such* ϕ*'s spans* $\mathrm{harm}(i)$.

Proof. Consider a monomial $m(z)$ in $\mathrm{hom}(i)$. Without loss of generality we may take

$$m(z) \;=\; z_1 z_2 \cdots z_i \;.$$

For an integer $u \in [0, i]$ we define $\phi_u(z) \in \mathrm{hom}(i)$ to be the sum of all monomials of degree i having exactly u variables z_p in common with $m(z)$. We first show that

$$\Delta \phi_u(z) \;=\; (i-u+1) g_{u-1}(z) \;+\; (n-2i+u+1) g_u(z) \;, \tag{2}$$

where $g_j(z) \in \mathrm{hom}(i-1)$ is the sum of all monomials of degree $i-1$ having exactly j variables in common with $m(z)$. We write $z = (x, y)$, where $x = (z_1, \ldots, z_i)$ and $y = (z_{i+1}, \ldots, z_n)$. Then by definition,

$$\phi_u(z) = \sigma_u(x)\sigma_{i-u}(y) , \qquad g_j(z) = \sigma_j(x)\sigma_{i-j-1}(y) , \tag{3}$$

where $\sigma_j(w) = \sigma_j(w_1, \ldots, w_r) = \Sigma\, w_{p_1} w_{p_2} \cdots w_{p_j}$ denotes the elementary symmetric function of degree j in the variables $w_1, \ldots, w_r$. Note that $\sigma_j(x)$ is the sum of all monomials of degree j dividing $m(z)$. Equation (2) follows from the identities

$$\Delta\sigma_u(x) = (i-u+1)\sigma_{u-1}(x) \quad \text{and} \quad \Delta\sigma_r(y) = (n-i-r+1)\sigma_{r-1}(y) .$$

We now define

$$\phi(z) = \sum_{u=0}^{i} (-1)^u \binom{i}{u}^{-1} \binom{n-2i+u}{u} \phi_u(z) . \tag{4}$$

It follows readily from (2) that $\phi(z)$ is a solution of the Laplace equation $\Delta\phi(z) = 0$. Thus we have associated an eigenfunction $\phi \in \mathrm{harm}(i)$ with the given monomial $m \in \mathrm{hom}(i)$.

We next prove that $\phi(z)$ satisfies Eq. (1). First a simple counting argument yields

$$\sigma_u(x)\sigma_l(x) = \sum_{j=\max\{u,l\}}^{u+l} \binom{j}{u}\binom{u}{j-l} \sigma_j(x) , \tag{5}$$

for all u and l with $u + l \le i$. We then obtain the identity

$$\sigma_r(y) = \sum_{l=0}^{r} (-1)^l \binom{d-l}{r-l} \sigma_l(x) , \tag{6}$$

for $r \le i$. This can be proved by induction on r, as follows. We use the two relations

$$\sigma_1(y) = d - \sigma_1(x)$$

(which is the case $r = 1$ of (6)) and

$$\sigma_1(\cdot)\sigma_l(\cdot) \;=\; l\,\sigma_l(\cdot) \;+\; (l+1)\sigma_{l+1}(\cdot)$$

(which is a special case of (5)) together with (6) to obtain

$$(r+1)\sigma_{r+1}(y) \;=\; \sum_{l=0}^{r+1} (-1)^l \left[(d-r-l)\binom{d-l}{r-l} + l\binom{d+1-l}{r+1-l} \right] \sigma_l(x) \;,$$

which is (6) with r replaced by $r+1$.

Using (3)-(5) and the combinatorial identity

$$\sum_l \;(-1)^l \binom{d-l}{i-u-l}\binom{u}{j-l} = (-1)^{j-u}\binom{d-j}{i-j}$$

(which follows from [13], p. 58, Eq. (24)), we obtain a representation for $\phi_u(z)$ in the simple form

$$\phi_u(z) \;=\; \sum_{j=u}^{i} \;(-1)^{j-u}\binom{j}{u}\binom{d-j}{i-j}\sigma_j(x) \;. \tag{7}$$

Equation (1) now follows from (4) and (7), after applying the classical identity $\sum_u \binom{i-u}{j-u}\binom{n-2i+u}{u} = \binom{n-i+1}{j}$ ([12], Eq. (3.2)), together with $\binom{i}{j}\binom{j}{u} = \binom{i}{u}\binom{i-u}{j-u}$.

The set of all $\phi(z)$ associated with monomials m of degree i spans the whole space $\mathrm{harm}(i)$. For by construction the linear space spanned by these functions is invariant under the symmetric group S_n; and as the harmonic spaces $\mathrm{harm}(j)$ are the *irreducible* S_n-invariant subspaces of $\mathbb{R}^{\Omega}$, this implies that the space in question coincides with $\mathrm{harm}(i)$. This completes the proof of Theorem 4.

We conclude this section with an application of Theorem 4. (A stronger result will be given in Section 3.)

Theorem 5. *A classical* $(l-2)$*-design* $\mathcal{P}$ *is also an* $\{l\}$*-design if and only if for any l-subset x of* $[1,n]$ *the quantity*

$$L_x = \{ l(d-l+1) - (n-2l+2) \} \mu_{l,x} + (d-l+1)\mu_{l-1,x} , \tag{8}$$

where $\mu_{j,x}$ *is the number of blocks in* P *that have exactly* j *points in common with* x, *is independent of the choice of* x. (*We shall therefore call* L_x *an invariant linear form.*)

Proof. Let λ_j $(0 \le j \le l-2)$ be the number of blocks of P containing a particular set of j points. If x is any l-subset of $[1,n]$ then since P is an $(l-2)$-design we have

$$\langle \pi(\mathsf{P}),\ \sigma_j(x) \rangle = \binom{l}{j} \lambda_j , \quad j = 0, 1, \ldots, l-2 ,$$

$$\langle \pi(\mathsf{P}),\ \sigma_{l-1}(x) \rangle = l\, \mu_{l,x} + \mu_{l-1,x} ,$$

$$\langle \pi(\mathsf{P}),\ \sigma_l(x) \rangle = \mu_{l,x} .$$

Now P is an $\{l\}$-design if and only if $\langle \pi(\mathsf{P}),\ f \rangle = 0$ for all $f \in \mathrm{harm}(l)$, or equivalently (from Theorem 4) if and only if $\langle \pi(\mathsf{P}),\ \phi(x) \rangle = 0$ for all l-subsets x of $[1,n]$. Using (1) with $i = l$, and the trivial calculation that

$$\frac{(-1)^l \binom{d-l}{0} \binom{n-l+1}{l} \Big/ \binom{l}{l}}{(-1)^{l-1} \binom{d-l+1}{1} \binom{n-l+1}{l-1} \Big/ \binom{l}{l-1}} = - \frac{n-2l+2}{d-l+1}$$

we see that $\langle \pi(\mathsf{P}),\ \phi(x) \rangle = 0$ for all x implies that L_x is independent of x. Conversely, if L_x is independent of x, the inner product

$$\langle \pi(\mathsf{P}),\ \sum_{j=0}^{l} (-1)^j \binom{l}{j}^{-1} \binom{d-j}{l-j} \binom{n-l+1}{j} \sigma_j(x) \rangle = A ,$$

for some constant A independent of x. Since

$$\sum_x \sigma_j(x) \in \mathrm{hom}(0) , \quad \text{for all} \quad j ,$$

$$\sum_{j=0}^{l} (-1)^j \binom{l}{j}^{-1} \binom{d-j}{l-j} \binom{n-l+1}{j} \sigma_j(x) \in \mathrm{harm}(l) , \quad \text{for all} \quad x ,$$

we have

$$\sum_{x} \sum_{j=0}^{l} (-1)^j \binom{l}{j}^{-1} \binom{d-j}{l-j} \binom{n-l+1}{j} \sigma_j(x) \in \mathrm{hom}(0) \cap \mathrm{harm}(l) = \{0\} ,$$

and so $A = 0$. This completes the proof.

3. Invariant linear forms

Any S_n-invariant subspace ζ of $\mathbb{R}^{\Omega}$ is the sum of harmonic subspaces:

$$\zeta = \sum_{i \in T} \mathrm{harm}(i) , \tag{9}$$

where T is a well-defined subset of $\{0, 1, \ldots, d\}$, and $\sum$ denotes an orthogonal sum. There are 2^{d+1} such subspaces ζ.

Let $\mathcal{P}$ be a subset of Ω. A subspace ζ of $\mathbb{R}^{\Omega}$ will be said to be $\mathcal{P}$-*regular* if

$$\langle \pi(\mathcal{P}), \psi \rangle = \frac{|\mathcal{P}|}{|\Omega|} \langle \pi(\Omega), \psi \rangle , \quad \text{for all} \quad \psi \in \zeta . \tag{10}$$

Note that since $\pi(\Omega)$ is the function 1 (which spans $\mathrm{harm}(0)$), the inner product $\langle \pi(\Omega), \psi \rangle$ vanishes for all $\psi \in \mathrm{harm}(j)$ with $j \geq 1$.

Theorem 6. *A non-empty subset $\mathcal{P} \subseteq \Omega$ is a T-design if and only if the subspace ζ defined by* (9) *is $\mathcal{P}$-regular.*

Proof. If ζ is $\mathcal{P}$-regular it follows from (9) and (10) that

$$\langle \pi(\mathcal{P}), \psi \rangle = 0, \quad \text{for all} \quad \psi \in \mathrm{harm}(j) \quad \text{with} \quad j \in T,\ j \neq 0 , \tag{11}$$

i.e. $\mathcal{P}$ is a T-design. Conversely, if $\mathcal{P}$ is a T-design with $0 \notin T$ then

$$\pi(\mathcal{P}) \in \sum_{i \notin T} \mathrm{harm}(i) \tag{12}$$

and so $\zeta = \sum_{i \in T} \mathrm{harm}(i)$ is $\mathcal{P}$-regular.

We can now give the generalization of Theorem 5 that will be used to prove the main theorem. We replace (8) by a more general invariant form, (13).

Theorem 7. *Let* $\mathcal{P}$ *be a non-empty subset of* Ω. *Suppose that for some integer* l *with* $1 \le l \le d$ *there exist real numbers* a, b, c, *not all zero, such that*

$$a \, \mu_{l,x} + b \, \mu_{l-1,x} = c \tag{13}$$

for all l*-subsets* x *of* $\{1, 2, \ldots, n\}$ ($\mu_{j,x}$ *was defined in Theorem* 5). *Then*

$$\begin{aligned} &\mathcal{P} \text{ is an } \{l\}\text{-design}, && \text{if} \quad a \ne lb , \\ &\mathcal{P} \text{ is an } \{l-1\}\text{-design}, && \text{if} \quad a = lb . \end{aligned} \tag{14}$$

In particular, if $\mathcal{P}$ *is not an* $\{l-1\}$*-design then* $\mathcal{P}$ *is an* $\{l\}$*-design.*

Proof. For a given l-set $x = \{p_1, \ldots, p_l\}$ let us define a function $\psi_x \in \mathbb{R}^{\Omega}$ by

$$\begin{aligned} \psi_x(\xi_1, \ldots, \xi_n) = {} & a \, \xi_{p_1} \xi_{p_2} \cdots \xi_{p_l} + \\ & b[(1-\xi_{p_1})\xi_{p_2} \cdots \xi_{p_l} + \xi_{p_1}(1-\xi_{p_2})\xi_{p_3} \cdots \xi_{p_l} + \cdots + \xi_{p_1} \cdots \xi_{p_{l-1}}(1-\xi_{p_l})] . \end{aligned} \tag{15}$$

The assumption (13) can be written as

$$\langle \pi(\mathcal{P}), \psi_x \rangle = c , \quad \text{for all} \quad l\text{-sets} \quad x . \tag{16}$$

The value of c can be deduced from a and b by summing (13) over all l-sets x; this yields

$$\left[a \binom{d}{l} + b \binom{d}{l-1} \binom{n-d}{1} \right] |\mathcal{P}| = c \binom{n}{l} . \tag{17}$$

Now $\langle \pi(\Omega), \psi_x \rangle$ is clearly constant, and this constant, c' say, is given by

$$\left[a \binom{d}{l} + b \binom{d}{l-1} \binom{n-d}{1} \right] |\Omega| = c' \binom{n}{l} . \tag{18}$$

It follows from (17), (18) that (16) amounts to

$$\langle \pi(\mathcal{P}), \psi_x \rangle = \frac{|\mathcal{P}|}{|\Omega|} \langle \pi(\Omega), \psi_x \rangle , \quad \text{for all} \quad l\text{-sets} \quad x . \tag{19}$$

Consider the linear space ζ spanned by the functions ψ_x (for all l-sets x). By definition, ζ is S_n-invariant. Furthermore it follows from (19) that ζ is P-regular. Hence P is a T-design with respect to the set T defined from the harmonic decomposition (9) of ζ. In view of (15) we have

$$\psi_x(\xi) \;=\; (a - lb)\,\xi_{p_1} \;\cdots\; \xi_{p_l} \;+\; \theta_{l-1} \;, \tag{20}$$

where θ_{l-1} is a member of $\hom(l-1)$. Hence ζ is a subspace of $\hom(l)$, and ζ is a subspace of $\hom(l-1)$ if and only if $a = lb$. Furthermore it is easily seen from (15) that (assuming a, b, c are not all zero) ζ is not a subspace of $\hom(l-2)$. (This is obvious if $a \neq lb$. When $a = lb$,

$$\begin{aligned}
\sum_{\substack{x \,=\, \{1,\, \ldots,\, l-1,\, i\} \\ \text{where } i \,=\, l,\, \ldots,\, n}} \psi_x(\xi) \;&=\; b \sum_{i=l}^{n} [\xi_2\,\xi_3 \cdots \xi_{l-1} + \xi_1\,\xi_3 \cdots \xi_{l-1} + \;\cdots\; + \xi_1\,\xi_2 \cdots \xi_{l-2}]\,\xi_i \\
&\qquad + \; b(n - l + 1)\,\xi_1 \cdots \xi_{l-1} \\
&= \; b[\xi_2 \cdots \xi_{l-1} \;+\; \cdots \;+ \xi_1 \cdots \xi_{l-2}] \left(d - \sum_{i=1}^{l-1} \xi_i \right) \\
&\qquad + \; b(n - l + 1)\,\xi_1 \cdots \xi_{l-1} \\
&= \; b(n - 2l + 2)\,\xi_1 \cdots \xi_{l-1} \\
&\qquad + \; b(d - l + 2)[\xi_2 \cdots \xi_{l-1} \;+\; \cdots \;+ \xi_1 \cdots \xi_{l-2}] \;,
\end{aligned}$$

and since $n - 2l + 2$ is not zero, this sum cannot belong to $\hom(l-2)$ unless b, and hence a and c, are zero.) Thus if $a \neq lb$ then P is an $\{l\}$-design, and if $a = lb$ then P is an $\{l-1\}$-design. This completes the proof.

4. Proof of Theorem 2

Suppose C satisfies the hypotheses of Theorem 2. By Theorem 1 the codewords of any weight w_i in C form a t-design. If $k = \dim C = 1$, only the repetition code yields a t-design. In this case $C^{\perp}$ consists of all even weight vectors and gives trivial designs. So from now on we assume $k > 1$.

It is easy to see (the argument is given on page 165 of [17]) that there are no codewords of $C^{\perp}$ with weight w' satisfying $n - t < w' < n$, and hence that there are two cases: (i) C is even, $w'_{s'} = n$, $s' = d - t + 1$, or (ii) C is not even, $w'_{s'} \neq n$, $s' = d - t$. Thus we can write

$$s' = d - t + 1 - \delta , \tag{21}$$

where $\delta = 0$ if C is even, $\delta = 1$ if C is not even.

We work in the framework of the Hamming association scheme $H(n,2)$ – see [8], [9], [11], [17, Chap. 21] for background. The *Krawtchouk polynomial* of degree i is defined to be

$$P_i(\xi) = \sum_{j=0}^{i} (-1)^j \binom{\xi}{j} \binom{n-\xi}{i-j} \quad (0 \le i \le n) ,$$

and the *annihilator polynomial* of C is

$$\alpha(\xi) = 2^{n-k} \prod_{i=1}^{s'} \left(1 - \frac{\xi}{w'_i} \right) .$$

Let us expand

$$\xi^m \alpha(\xi) = \sum_{i=0}^{s'+m} \alpha_i^{(m)} P_i(\xi) , \qquad m = 0, 1, \ldots .$$

We set $\alpha_i^{(0)} = \alpha_i$. Note that $\alpha_{s'+m}^{(m)} \neq 0$ for all m.

It was shown in [9] that for all $x \in \mathbb{F}_2^n$,

$$\sum_{i=0}^{s'+m} \alpha_i^{(m)} b_i(x) = \begin{cases} 1, & m = 0, \\ 0, & m \ge 1, \end{cases} \tag{22}$$

where $b_i(x)$ is the number of codewords in C at distance i from x.

We next prove a lemma.

Lemma 8. *Let C be a binary $[n, k, d]$ code with nonzero weights $w_1 = d$, $w_2, \ldots, w_s$, and let $w'_1, \ldots, w'_{s'}$ be the nonzero weights in the dual code $C^{\perp}$. Let t be the greatest integer in the range $0 < t < d$ such that there are at most $d - t$ weights w'_i with $0 < w'_i \le n - t$, and suppose $w_2 \ge d + 4$. If the codewords of minimal weight form a $(t+1)$-design then so do the codewords of any nonzero weight w_i.*

Proof. Let x be an arbitrary subset of $\{1, 2, \ldots, n\}$ of size $l = t + 1$. Setting $m = w_2 - d - 2 + \delta > 0$ in (22) we obtain

$$\sum_{i=0}^{w_2 - t - 1} \alpha_i^{(m)} \, b_i(x) = 0 \, . \tag{23}$$

The zero codeword contributes to the sum in (23) if and only if $l \le w_2 - t - 1$. The contributions from the codewords of weight d are independent of x, since by hypothesis these words form a $(t+1)$-design. Codewords of weight greater than w_2 do not contribute to the sum at all, since

$$w_3 - l > w_2 - l = w_2 - t - 1 \, . \tag{24}$$

We now consider the contributions from the codewords c of weight w_2. Suppose c intersects x in j points. Then

$$\mathrm{dist}(c, x) = w_2 + l - 2j \le w_2 - t - 1 \, , \tag{25}$$

implying $j = t + 1$, i.e. codewords of weight w_2 contribute to the sum in (23) if and only if they contain x. Therefore (23) implies that the number of codewords of weight w_2 containing x is independent of x, or in other words the codewords of weight w_2 form a $(t+1)$-design. Similarly, by taking $m = w_j - d - 2 + \delta$ in (22), we find that the words of weight w_j form a $(t+1)$-design. This proves the lemma.

We now complete the proof of Theorem 2. The set of minimal weight words in C will be denoted by P, and $\mu_{j,x}$ is the number of words in P that have exactly j points in common with a given l-set x.

Case (i), C even, $s' = d - t + 1$. Suppose first that there is a smallest integer f in the range $0 \le f \le [(d-t)/2]$ such that $\alpha_{d-t-2f} \ne 0$. Let x be an arbitrary subset of $\{1, 2, \ldots, n\}$ of size $l = t + 2f$. Since C is even, the distances from x to C are all congruent to t (modulo 2), and from (22) we have

$$\sum_{\substack{i=0 \\ i \equiv t \ (\mathrm{mod}\ 2)}}^{d-t-2f} \alpha_i \, b_i(x) = 1 \, . \tag{26}$$

Proceeding as in the proof of the lemma, we find that only the zero codeword and the codewords of weight d contribute to the sum in (26), and the words of weight d contribute if and only if they contain x. Equation (26) then reads

$$\alpha_{d-t-2f} \, \mu_{t+2f,x} = 1 - \alpha_{t+2f} \, \varepsilon_{d-2t-2f-2} \, , \tag{27}$$

where we set

$$\varepsilon_p = \begin{cases} 0 & p < 0, \\ 1 & p \ge 0. \end{cases}$$

If $f \ge 1$ we conclude from (27) that P is a $(t+2f)$-design, in particular a $(t+1)$-design, and therefore by Lemma 8 that the codewords of every nonzero weight form $(t+1)$-designs.

On the other hand suppose $f = 0$. We take x to have weight $l = t + 2$, and find that (22) becomes

$$\alpha_{d-t-2} \, \mu_{t+2,x} + \alpha_{d-t} \, \mu_{t+1,x} = 1 - \alpha_{t+2} \, \varepsilon_{d-2t-2} \, , \tag{28}$$

where both coefficients on the left side are nonzero. From Theorem 7 we conclude that P is a $\{t+1\}$-design or a $\{t+2\}$-design, and hence either a $(t+1)$-design or a $\{1, \ldots, t, t+2\}$-design. In the former case Lemma 8 extends this to codewords of every nonzero weight.

The third possibility is that no such f exists, and all coefficients α_{d-t-2i} are zero. But in this case taking x in (22) to have weight t leads to a contradiction (that left side of (26) vanishes but the right side does not).

Case (ii), C not even, $s' = d-t$. Let x have weight $t+2$. Equation (22) implies

$$\alpha_{d-t-2}\,\mu_{t+2,x} + \alpha_{d-t}\,\mu_{t+1,x} = 1 - \alpha_{t+2}\,\varepsilon_{d-2t-2}\ ,$$

where $\alpha_{d-t} \neq 0$. From Theorem 7 we conclude that P is a $\{t+1\}$-design or a $\{t+2\}$-design, and Lemma 8 completes the proof.

An alternative proof of Theorem 2. The above argument shows only that an invariant linear form of the type (13) exists; by Theorem 7 this is enough to prove the desired result. However it is possible to give a proof in which a ‘‘computation miracle’’ produces an explicit invariant linear form. We give this direct proof in the case when C is even. We suppose that P is not a $(t+1)$-design.

By applying (22) with $m=0$ and 1 to a $(t+1)$-set x we obtain

$$\alpha_{d-t-1}\,\mu_{t+1,x} + \alpha_{d-t+1}\,\mu_{t,x} = 1 - \alpha_{t+1}\,\varepsilon_{d-2t}\ , \tag{29}$$

$$\alpha^{(1)}_{d-t-1}\,\mu_{t+1,x} + \alpha^{(1)}_{d-t+1}\,\mu_{t,x} = -\,\alpha^{(1)}_{t+1}\,\varepsilon_{d-2t+1}\ , \tag{30}$$

where $\alpha_{d-t+1} \neq 0$. Since P is a t-design,

$$(t+1)\,\mu_{t+1,x} + \mu_{t,x} = (t+1)\,\lambda_t\ , \tag{31}$$

where λ_t is the number of blocks through t given points. Since P is not a $(t+1)$-design, the left sides of (29)-(31) must be proportional (or else $m_{t+1,x}$ would be independent of x). Therefore

$$\alpha_{d-t-1} = (t+1)\,\alpha_{d-t+1}\ , \tag{32}$$

$$\alpha^{(1)}_{d-t-1} = (t+1)\,\alpha^{(1)}_{d-t+1}\ , \tag{33}$$

and so $\alpha_{d-t-1} \neq 0$. From the Krawtchouk recurrence [17, p. 152]

$$(i+1)\ P_i(\xi)\ =\ (n-2\xi)\ P_i(\xi)\ -\ (n-i+1)\ P_{i-1}(\xi)$$

($i \geq 1$), with $P_0(\xi) = 1$, $P_1(\xi) = n-2\xi$, we obtain

$$2\alpha_i^{(1)}\ =\ -\ (n-i)\,\alpha_{i+1}\ +\ n\alpha_i\ -\ i\alpha_{i-1} \tag{34}$$

($i \geq 1$). In particular,

$$2\alpha_{d-t+1}^{(1)}\ =\ n\alpha_{d-t+1}\ -\ (d-t+1)\,\alpha_{d-t}\ , \tag{35}$$

$$2\alpha_{d-t-1}^{(1)}\ =\ -\ (n-d+t+1)\,\alpha_{d-t}\ +\ n\alpha_{d-t-1}\ -\ (d-t-1)\,\alpha_{d-t-2}\ . \tag{36}$$

Furthermore $\alpha_{d-t} \neq 0$, or else (as shown in the first proof) P is a $(t+1)$-design. From (32), (33), (35), (36) we obtain

$$\alpha_{d-t-2}\ =\ \frac{(t+2)(d-t-1)\ -\ (n-2t-2)}{d-t-1}\ \alpha_{d-t}\ . \tag{37}$$

We now apply (22) with $m=0$ to a $(t+2)$-set x and find

$$\begin{aligned} &\{(t+2)(d-t-1)\ -\ (n-2t-2)\}\ \mu_{t+2,x}\ +\ (d-t-1)\,\mu_{t+1,x} \\ &\qquad =\ \frac{d-t-1}{\alpha_{d-t}}\ (1-\alpha_{t+2}\ \varepsilon_{d-2t-1})\ . \end{aligned} \tag{38}$$

The left-hand side of (38) is the desired linear form, independent of x. Theorem 7 and Lemma 8 complete the proof. The most interesting aspect of this argument is the leverage provided by the assumption that P is *not* a $(t+1)$-design.

Examples. An example with $t=5$ is provided by the set of 759 minimal weight words in the $[24, 12, 8]$ Golay code. In this case we have the identity $\mu_{7,x} + \mu_{6,x} = 1$ for any 7-set x. (There are only two possibilities, $(\mu_{7,x}, \mu_{6,x}) = (0,1)$ or $(1,0)$, corresponding to the two kinds of 7-subsets of $[1,\ 24]$ under the action of the Mathieu group M_{24} – cf. [6, Fig. 10.1].) The 759 words form a $\{1,\ 2,\ 3,\ 4,\ 5,\ 7\}$-design.

A second example with $t = 5$ is provided by the 17296 minimal weight words in the $[48, 24, 12]$ extended quadratic-residue code (or in any self-dual doubly even $[48, 24, 12]$ code). In this case we have the identity $\mu_{7,x} + \mu_{6,x} = 8$ for any 7-set x. (There are only two possibilities: $(\mu_{7,x}, \mu_{6,x}) = (0,8)$ or $(1,7)$.) Again the minimal weight words form a $\{1, 2, 3, 4, 5, 7\}$-design.

A more trivial example with $t = 1$ is provided by the $[n = 2m, 2, m]$ code $\{0^{2m}, 0^m 1^m, 1^m 0^m, 1^{2m}\}$. The two words of weight m form a $\{1,3\}$-design.

A further example: complementation. The $\{1, 2, \ldots, l, l+2\}$-design property is preserved when the blocks of $\mathcal{P}$ are complemented. To see this, let $\overline{\mathcal{P}} = \{[1,n] \setminus B \mid B \in \mathcal{P}\}$, and let $\nu_{j,x}$ be the number of blocks in $\overline{\mathcal{P}}$ meeting a given $(l+2)$-set x in exactly j points. Then $\nu_{j,x} = \mu_{l+2-j,x}$, and we must therefore show that

$$\bar{a}\, \mu_{0,x} + \bar{b}\, \mu_{1,x} = \bar{c} \tag{39}$$

for all x, for suitable real numbers $\bar{a}$, $\bar{b}$, $\bar{c}$ not all zero. Since $\overline{\mathcal{P}}$ is a $\{1, 2, \ldots, l, l+2\}$-design we have invariant linear forms

$$a\, \mu_{l+2,x} + b\, \mu_{l+1,x} = c\ , \quad \text{where} \quad b \neq 0\ , \tag{40}$$

$$\sum_{i=j}^{l+2} \binom{i}{j} \mu_{i,x} = \binom{l+2}{j} \lambda_j\ , \quad j = 0, 1, \ldots, l\ , \tag{41}$$

where λ_j is the number of blocks of $\mathcal{P}$ through j given points. Equations (40), (41) form a triangular system of $l+2$ equations in the $l+3$ quantities $\mu_{j,x}$, $j = 0, \ldots, l+2$. From this we obtain

$$\mu_{0,x} = \alpha\, \mu_{l+2,x} + \beta\ , \quad (\alpha, \beta \text{ not both zero})\ ,$$

$$\mu_{1,x} = \gamma\, \mu_{l+2,x} + \delta\ , \quad (\gamma, \delta \text{ not both zero})\ ,$$

for suitable real numbers α, β, γ, δ, and Equation (39) follows.

5. Extension to codewords of higher weight and the proof of Theorem 3

Lemma 8 shows that if the codewords of minimal weight form a $(t+1)$-design then so do the codewords of any nonzero weight. To extend the $\{1, 2, \ldots, t, t+2\}$-design property to codewords of higher weight it is necessary to make some assumptions about the gap sizes $w_i - w_{i-1}$ for $i \geq 3$. In the sequel we shall only consider self-dual codes with all weights divisible by 4, even though the arguments apply to a wider class of codes.

We begin with an example, the $[24,\ 12,\ 8]$ Golay code. The annihilator polynomial is

$$\begin{aligned} \alpha(\xi) \ &= \ 2^{12} \left(1 - \frac{\xi}{8}\right)\left(1 - \frac{\xi}{12}\right)\left(1 - \frac{\xi}{16}\right)\left(1 - \frac{\xi}{24}\right) \\ &= \ \sum_{i=0}^{3} P_i(\xi) \ + \ \frac{1}{6} \, P_4(\xi) \ . \end{aligned} \tag{42}$$

Given an arbitrary 7-set x, let $M_{j,x}^{w}$ be the number of codewords of weight w that meet x in exactly j points. From (38), (41) we obtain the invariant linear forms

$$M_{7,x}^{8} \ + \ M_{6,x}^{8} \ , \tag{43}$$

$$21 M_{7,x}^{8} \ + \ 6 M_{6,x}^{8} \ + \ M_{5,x}^{8} \ . \tag{44}$$

Next we apply (22) with $m = 1$ to obtain the invariant form

$$\alpha_1^{(1)} \ M_{7,x}^{8} \ + \ \alpha_3^{(1)} \ M_{6,x}^{8} \ + \ \alpha_5^{(1)} \ M_{5,x}^{8} \ + \ \alpha_5^{(1)} \ M_{7,x}^{12} \ . \tag{45}$$

Before calculating the shifted Krawtchouk coefficients $\alpha_j^{(1)}$ we can see that there are two possibilities. The first is that the form

$$\alpha_1^{(1)} \ M_{7,x}^{8} \ + \ \alpha_3^{(1)} \ M_{6,x}^{8} \ + \ \alpha_5^{(1)} \ M_{5,x}^{8} \tag{46}$$

is a linear combination of (43) and (44). Since $\alpha_5^{(1)} \neq 0$, we may conclude that in this case the codewords of weight 12 form a 7-design. The second possibility is that (43), (44), (46) form a basis for the space of linear forms in the variables $M_{j,x}^{8}$ $j = 5,\ 6,\ 7$. Now we understand the Golay code well enough to know that the first possibility does not occur, but it is precisely this argument that we will apply to an arbitrary doubly-even code. We may in fact calculate the shifted Krawtchouk coefficients from (34), finding that $\alpha_0^{(1)} = \alpha_1^{(1)} = \alpha_2^{(1)} = 0$, $\alpha_3^{(1)} = \frac{35}{4}$, $\alpha_4^{(1)} = 0$, $\alpha_5^{(1)} = -\frac{5}{12}$, so (45) becomes

$$21\, M_{6,x}^{8} - M_{5,x}^{8} - M_{7,x}^{12} \ . \tag{47}$$

Next we apply (22) with $m = 3$ to obtain the invariant form

$$\alpha_1^{(3)}\, M_{7,x}^{8} + \alpha_3^{(3)}\, M_{6,x}^{8} + \alpha_5^{(3)}\, M_{5,x}^{8} + \alpha_7^{(3)}\, M_{4,x}^{8} + \alpha_5^{(3)}\, M_{7,x}^{12} + \alpha_7^{(3)}\, M_{6,x}^{12} \ , \tag{48}$$

where $\alpha_7^{(3)} \neq 0$. From (41) we have a second invariant form involving the new variable $M_{4,x}^{8}$, namely

$$35\, M_{7,x}^{8} + 15\, M_{6,x}^{8} + 5\, M_{5,x}^{8} + M_{4,x}^{8} \ . \tag{49}$$

Since (43), (44), (46), (47) are a basis for the space of linear forms in the variables $M_{j,x}^{8}$ $j = 4,\ 5,\ 6,\ 7$, we may eliminate these variables from (48) and obtain an invariant form

$$a\, M_{7,x}^{12} + b\, M_{6,x}^{12} \ ,$$

of type (13). In this case $a/b = 5$, and so the codewords of weight 12 in the Golay code form a $\{1,\ 2,\ 3,\ 4,\ 5,\ 7\}$-design.

The proof of Theorem 3 is a straightforward generalization of this example. From Theorem 1 the codewords of any given weight w_p form a t-design, so (generalizing (41)) we have invariant linear forms

$$L_{w_p,\, j} = \sum_{h=1}^{t+2} \binom{h}{j} M_{h,x}^{w_p} \ , \quad j = 0,\ 1,\ \ldots,\ t, \quad p = 1,\ \ldots,\ d-t \ , \tag{50}$$

where x is an arbitrary $(t+2)$-subset of $[1,\ n]$. From (22) we also have invariant forms (generalizing (45) and (48)):

$$H_m = \sum_{\substack{w_i,\, j \\ w_i + t + 2 - 2j \le d - t + 1 + m}} \alpha^{(m)}_{w_i + t + 2 - 2j} \; M^{w_i}_{j,x} \;, \qquad m = 1,\, 3,\, 5,\, \ldots \; . \tag{51}$$

Finally Theorem 2 provides an invariant form

$$a\, M^d_{t+2,x} \;+\; b\, M^d_{t+1,x} \;, \qquad b \neq 0 \; . \tag{52}$$

The theorem is proved by induction. For $i = 2$, ..., let $\Gamma(i)$ be the linear system in the variables $\{ M^{w_p}_{j,x} \,:\, p < i,\, w_p + t + 2 - 2j < w_i - t - 2 \}$ consisting of (52) and the linear forms

$$L_{w_p,\, j} \quad \text{for} \quad p < i, \quad w_p + t + 2 - 2j < w_i - t - 2 \;, \quad \text{and}$$

$$H_m \quad \text{for} \quad m < w_i - d - 3 \;, \quad m \quad \text{odd} \; .$$

The inductive hypothesis is that the corank of the linear system $\Gamma(i)$ is at most 1. This is certainly true for $i = 2$, since $\Gamma(2)$ includes the triangular system consisting of (52) and $L_{d,j}$ for $d + t + 2 - 2j < w_2 - t - 2$.

The linear system $\Gamma(i+1)$ involves variables $M^{w_p}_{j,x}$ that do not appear in $\Gamma(i)$. For each new variable $M^{w_p}_{j,x}$ with $w_p < w_{i+1}$ we have a linear form $L_{w_p,\, f}$, so these new variables do not change the corank. The linear form

$$H_{w_{i+1} - d - 3} \;-\; \alpha^{(w_{i+1} - d - 3)}_{w_{i+1} - t - 2} \; M^{w_{i+1}}_{t+2,x} \tag{53}$$

only involves variables $M^{w_p}_{j,x}$ with $w_p < w_{i+1}$. We distinguish two cases.

The first is that (53) is a linear combination of forms from $\Gamma(i)$ and forms $L_{w_p, f}$ involving variables $M^{w_p}_{j,x}$ not appearing in $\Gamma(i)$. Then $M^{w_{i+1}}_{t+2,x}$ is independent of *x*, that is the codewords of weight w_{i+1} form a $(t+2)$-design. Now $\Gamma(i+1)$ includes the triangular system

$$M^{w_{i+1}}_{t+2,x},\; (t+2)\; M^{w_{i+1}}_{t+2,x} \;+\; M^{w_{i+1}}_{t+1,x},\; L_{w_{i+1},\, j}$$

in the variables $M^{w_p}_{j,x}$, so the corank of $\Gamma(i+1)$ is at most 1.

The second case is that the linear form (53), together with the forms in $\Gamma(i)$ and the forms $L_{w_p, f}$ involving variables $M_{j,x}^{w_p}$ not appearing in $\Gamma(i)$, form a basis for the space of linear forms in the variables appearing in (53). Now consider $H_{w_{i+1}-d-1}$. We may eliminate variables from $H_{w_{i+1}-d-1}$ to obtain a linear form

$$a\, M_{t+2,x}^{w_{i+1}} \;+\; b\, M_{t+1,x}^{w_{i+1}}\;, \tag{54}$$

where $b \neq 0$. By Theorem 7 we may conclude that the codewords of weight w_{i+1} form a $(t+1)$-design or a $\{1, 2, ..., t, t+2\}$-design. The rank of $\Gamma(i+1)$ restricted to variables $M_{j,x}^{w_p}$ for $p < i+1$ is full. Since $\Gamma(i+1)$ includes the triangular system {(54), $L_{w_{i+1}, j}$} in the variables $M_{j,x}^{w_{i+1}}$, the corank of $\Gamma(i+1)$ is at most 1.

Remarks. The proof leaves open the possibility that the codewords of weight w_i might form a $(t+1)$-design while the codewords of weight w_j $(j \neq i)$ form a $\{1, ..., t, t+2\}$-design.

Acknowledgements

We thank the referees for several helpful comments.

REFERENCES

[1] M. Abramowitz and I. A. Stegun, ‘‘Handbook of Mathematical Functions’’, National Bureau of Standards Appl. Math. Series, vol. 55, U.S. Dept. Commerce, Wash. D.C., 1972.

[2] E. F. Assmus, Jr., and H. F. Mattson, Jr., ‘‘New 5-designs’’, J. Comb. Theory, vol. 6 (1969), 122-151.

[3] A. R. Calderbank and P. Delsarte, ‘‘On error-correcting codes and invariant linear forms’’, SIAM J. Discrete Math., to appear.

[4] A. R. Calderbank and P. Delsarte, ‘‘The concept of a (t, r)-regular design as an extension of the classical concept of a t-design’’, preprint.

[5] J. H. Conway and V. Pless, ‘‘On the enumeration of self-dual codes’’, J. Comb. Theory, vol. 28A (1980), 26-53.

[6] J. H. Conway and N. J. A. Sloane, ‘‘Sphere Packings, Lattices and Groups’’, Springer-Verlag, N.Y. 1988.

[7] J. H. Conway and N. J. A. Sloane, ‘‘A new upper bound on the minimal distance of self-dual codes’’, IEEE Trans. Information Theory, vol. 36 (1990), 1319-1333.

[8] P. Delsarte, ‘‘An algebraic approach to the association schemes of coding theory’’, Philips Research Reports Supplements, vol. 10 (1973).

[9] P. Delsarte, ‘‘Four fundamental parameters of a code and their combinatorial significance’’, Info. Control, vol. 23 (1973), 407-438.

[10] P. Delsarte, ‘‘Hahn polynomials, discrete harmonics, and t-designs’’, SIAM J. Appl. Math., vol. 34 (1978), 157-166.

[11] J.-M. Goethals, ‘‘Association schemes’’, in ‘‘Algebraic Coding Theory and Applications’’, edited by G. Longo, CISM Courses and Lectures 258, Springer-Verlag, Vienna, 1979, 243-283.

[12] H. W. Gould, ‘‘Combinatorial Identities’’, Morgantown, W. Va., Revised edition, 1972.

[13] D. E. Knuth, ‘‘The Art of Computer Programming’’, vol. 1, 2nd edition, Addison-Wesley, Reading, Mass., 1973.

[14] H. V. Koch, ‘‘On self-dual, doubly-even codes of length 32’’, Report R-Math-32/84, Institüt f. Math., Akad. Wiss. DDR, Berlin, 1984.

[15] H. Koch, ‘‘Unimodular lattices and self-dual codes’’, in ‘‘Proc. Intern. Congress Math., Berkeley 1986’’, Amer. Math. Soc., Providence R.I., 1987, vol. 1, pp. 457-465.

[16] H. Koch and B. B. Venkov, ‘‘Über ganzzahlige euklidische Gitter’’, J. Reine Angew. Math., vol. **398** (1989), 144-168.

[17] F. M. MacWilliams and N. J. A. Sloane, ‘‘The Theory of Error-Correcting Codes’’, North Holland, Amsterdam, 1979.

[18] C. L. Mallows and N. J. A. Sloane, ‘‘An upper bound for self-dual codes’’, Inform. Control, vol. 22 (1973), 188-200.

[19] N. J. A. Sloane, ‘‘A Handbook of Integer Sequences’’, Academic Press, N.Y. 1973.

[20] N. J. A. Sloane, ‘‘Binary codes, lattices and sphere packings’’, in ‘‘Combinatorial Surveys’’, edited P. J. Cameron, Academic Press, N.Y. 1977, pp. 117-164.

[21] B. B. Venkov, ‘‘On even unimodular extremal lattices’’ (in Russian), Trudy Mat. Inst. Steklov, vol. 165 (1984), 43-48. English translation in Proc. Steklov Inst. Math., vol. 165 (1984), 47-52.