TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 330, Number 1, March 1992

HADAMARD MATRICES AND THEIR DESIGNS: A CODING-THEORETIC APPROACH

E. F. ASSMUS, JR. AND J. D. KEY

ABSTRACT. Given an $m \times m$ Hadamard matrix one can extract m^2 symmetric designs on $m-1$ points each of which extends uniquely to a 3-design. Further, when m is a square, certain Hadamard matrices yield symmetric designs on m points. We study these, and other classes of designs associated with Hadamard matrices, using the tools of algebraic coding theory and the customary association of linear codes with designs. This leads naturally to the notion, defined for any prime p, of p-equivalence for Hadamard matrices for which the standard equivalence of Hadamard matrices is, in general, a refinement: for example, the sixty 24×24 matrices fall into only six 2-equivalence classes. In the 16×16 case, 2-equivalence is identical to the standard equivalence, but our results illuminate this case also, explaining why only the Sylvester matrix can be obtained from a difference set in an elementary abelian 2-group, why two of the matrices cannot be obtained from a symmetric design on 16 points, and how the various designs may be viewed through the lens of the four-dimensional affine space over the two-element field.

1. INTRODUCTION

1.1 Historical background and motivation. The centennial of the debut of Hadamard matrices on the mathematical stage is hard upon us. They were introduced by Jacques Hadamard in 1893. And yet, despite much attention by numerous mathematicians, the central question of existence has not been answered: we do not know whether or not, for every integer n, there is an orthogonal $4n \times 4n$ matrix of ± 1's; this, notwithstanding that the number of such matrices seems to grow extremely rapidly with n—the combinatorial explosion coming perhaps as early as $n = 7$. Still less is known about the classification of Hadamard matrices for general n—but they have been enumerated for $n < 7$.

Hadamard introduced these matrices because they were solutions to an extremal problem in analysis and they since have found applications in many noncombinatorial contexts. A voluminous literature concerning both the applications and the combinatorial aspects of the subject now exists. The brief

Received by the editors December 20, 1989.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 05B20; Secondary 05B05, 05B10, 94B25.

Key words and phrases. Hadamard matrix, 3-design, symmetric design, oval, linear code, difference set, self-orthogonal code, self-dual code.

0002-9947/92 $1.00 + $.25 per page

bibliography that we give is no indication of that literature and pertains merely to the problems we are addressing here.

We have nothing *directly* to say about the existence question nor even a word to say about the applications. Our concern is with classification and we use the tools of algebraic coding theory to make a start in that direction, concentrating our attention on the combinatorial designs that are naturally associated with a Hadamard matrix.

Many authors have studied designs through codes associated with them and the outcome seems clear: coding theory can make a substantial contribution to the theory of designs. In [2] we employed coding theory to study finite planes, and, for example, introduced new ideas in hopes of aiding in the classification of affine planes and, in particular, affine translation planes. In this article we make use of the codes customarily associated with Hadamard designs to study these designs and the related Hadamard matrices. We pay special attention to the case where n is a power of 2, since here the so-called Sylvester matrices and affine geometries over the two-element field intervene in an interesting way and the associated codes, the Reed-Muller codes, have been heavily studied. Moreover, this case resembles that of translation planes—the first-order Reed-Muller code playing the role of the hull of the desarguesian affine plane—and here we have an easy-to-prove 'rigidity' theorem characterizing the Sylvester matrix.

1.2 Guide to the paper. The paper is divided into six sections and the work is organized as follows: in §2 we set down the standard definitions and our notation and we also interpret the codes associated with Hadamard matrices; §3 treats, for the most part, those designs with the parameters of affine-geometry designs whose blocks can be found amongst the supports of vectors in the Reed-Muller codes, but we also show how the special n-tuples introduced by Bhat and Shrikhande can be interpreted in the associated codes; §4 concerns, primarily, Hadamard designs that can be constructed from difference sets and, for expository completeness, we have included there statements of the 'rigidity' theorem first observed explicitly by Hamada and Ohmori and the Dillon-Schatz Theorem characterizing low-rank symmetric designs on 2^{2m} points; §5 describes a construction of Hadamard designs from another class of 2-designs, but in this case the 2-designs are Steiner systems; finally, in §6, we give a rather detailed discussion of the case $n = 6$.

2. Background and notation

The first two parts of this section explain our terminology for designs and their codes; everything is fairly standard here. The remaining parts develop our notation for the codes associated, through their designs, with Hadamard matrices: the notions and results presented there are, for the most part, new. Our definition of p-equivalence for Hadamard 3-designs is in §2.5.

2.1 Designs. Our notation for designs will be as in [20]: thus, an incidence structure $\mathscr{D} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$, where $\mathscr{P}$ and $\mathscr{B}$ are disjoint finite sets and $\mathscr{I} \subseteq \mathscr{P} \times \mathscr{B}$, is a $t-(v, k, \lambda)$ design if *the point set* $\mathscr{P}$ is of cardinality v, *the block set* $\mathscr{B}$ has members that are each incident with k points of $\mathscr{P}$, and any t distinct points of $\mathscr{P}$ are together incident with exactly λ blocks. We will generally suppress the incidence, $\mathscr{I}$, from the notation and simply write $\mathscr{D} = (\mathscr{P}, \mathscr{B})$. A t-design is an s-design for any $s \leq t$, and it is customary to

use λ_s to denote the number of blocks through s distinct points (so $\lambda_t = \lambda$). We write n for $\lambda_1 - \lambda_2$ and call this the *order* of the design. The designs we will be considering will all have $t = 2$ or $t = 3$ and we will refer to them as 2-designs or 3-designs when the other parameters are not relevant.

A 2-design $\mathscr{D}$ with $|\mathscr{P}| = |\mathscr{B}|$ is called a *symmetric* design, and we usually omit the '2-' when displaying the parameters, referring simply to (v, k, λ) designs. The order of such a design is $k - \lambda$ since there are precisely k blocks through each point. For a symmetric design $\mathscr{D}$, the related structures consisting of the *complementary design* $\overline{\mathscr{D}}$ (taking the complements of blocks for the new blocks), *the dual structure* $\mathscr{D}^t$ (taking the points for blocks and the blocks for points), and the complement of the dual, $\overline{\mathscr{D}^t}$, are also all symmetric designs, and will be considered along with $\mathscr{D}$.

Any 3-design with $v = 4n$, $k = 2n$, and $\lambda = n - 1$, is called a *Hadamard 3-design*, because of the association with Hadamard matrices, as we will explain presently. Further, if $\mathscr{T}$ is a Hadamard 3-design, then each of its *derived* designs, $\mathscr{T}_P$, obtained by omitting a point P and all the blocks that are not incident with P, is symmetric. Both $\mathscr{T}_P$ and $\overline{\mathscr{T}_P}$ are called *Hadamard 2-designs*. Their parameters are, respectively, $(4n - 1, 2n - 1, n - 1)$ and $(4n - 1, 2n, n)$. The order of $\mathscr{T}$ is $2n$, and the order of each of the derived designs is n. It is not hard to prove that a Hadamard $(4n - 1, 2n - 1, n - 1)$ design extends (uniquely up to isomorphism) to a Hadamard 3-design by including the blocks of the complementary design as the new blocks that are not incident with the added point: see [20, p. 132]. (Recall that the incidence structures $(\mathscr{P}, \mathscr{B})$ and $(\mathscr{Q}, \mathscr{C})$ are *isomorphic* if and only if there is a bijection σ taking $\mathscr{P}$ to $\mathscr{Q}$ and $\mathscr{B}$ to $\mathscr{C}$ such that incidence is preserved.)

The *classical* designs are those given by affine and projective spaces over finite fields. In the projective case the points of the design are the points of the projective space and the blocks the t-dimensional subspaces for some fixed t. Our concern will be almost exclusively with the design given by the points and hyperplanes, since it is a symmetric design. This symmetric design is isomorphic to its dual, of course, because of the duality intrinsic to projective spaces.

In the affine case the points are the points of the affine space and the blocks the t-flats for some fixed t. For affine designs appropriate to the study of Hadamard matrices and their designs, the two-element field plays a special rôle. As we shall see, the design of points and hyperplanes of the m-dimensional affine space over $\mathbf{F}_2$ is the Hadamard 3-design related to the Sylvester-Hadamard matrix. For a full discussion of these designs the reader may wish to consult [20].

When we speak of an *incidence matrix* A for a design $\mathscr{D}$, the rows of A will correspond to the blocks of $\mathscr{D}$ and the columns to the points. Thus A is a $|\mathscr{B}| \times |\mathscr{P}|$ matrix of 0's and 1's, with $a_{l,P} = 1$ if and only if l is incident with P. (This is the transpose of the incidence matrix of [20].)

2.2 The codes associated with a design. Let $\mathscr{D}$ be a design with point set $\mathscr{P}$. For any field F, let V denote the vector space $F^{\mathscr{P}}$ of functions from $\mathscr{P}$ to F. This space has a distinguished basis given by the characteristic functions of the singleton subsets of $\mathscr{P}$. We may thus appeal to algebraic coding theory, and we accordingly define the *code* of $\mathscr{D}$ over F to be the subspace $C_F(\mathscr{D})$ of V spanned by the vectors corresponding to the characteristic functions of the blocks of $\mathscr{D}$. If $X \subseteq \mathscr{P}$, we denote the characteristic function of X by

v^X. Thus

$$C_F(\mathscr{D}) = \langle v^l | l \in \mathscr{B} \rangle.$$

Further, for $v \in V$ and $P \in \mathscr{P}$, let $v(P)$ denote the image of P under v, or, equivalently, the coordinate of v at $\{P\}$ with respect to the distinguished basis. Then there is a natural inner product given by:

$$\sum_{P \in \mathscr{P}} u(P)v(P).$$

The *orthogonal* of $C = C_F(\mathscr{D})$ with respect to this inner product will be denoted by $C^\perp$: in the coding literature it is known as the *dual* of C. We define the *hull* of $\mathscr{D}$ to be the code

$$\text{Hull}_F(\mathscr{D}) = C_F(\mathscr{D}) \cap C_F(\mathscr{D})^\perp.$$

The relevance of the hull to the study of designs with the same parameters as $\mathscr{D}$ is discussed in [2]. For a shorter discussion see [1].

We will restrict our attention to finite fields of prime order p, where p divides the order n of $\mathscr{D}$, since it is well known (and simple to verify) that if p does not divide n the code will be either the full space V, or of codimension 1 in it. The subscript 'F' above will then be replaced by 'p', and frequently omitted altogether if p is clear from the context. The dimension of $C_p(\mathscr{D})$ is called the *rank* of $\mathscr{D}$, and is denoted by $\text{rank}_p(\mathscr{D})$. If $\mathscr{D}$ is a symmetric design of order n, then $\text{rank}_p(\mathscr{D}) \leq \frac{1}{2}(v+1)$ provided p divides n. Moreover, we have equality whenever p^2 does not divide n: see, for example, [27, Chapter 2 or 37].

The codes of certain classical designs are of particular importance in coding theory: the binary code of the design of points and lines of m-dimensional projective space over $\mathbf{F}_2$ is the Hamming code of length $2^{m+1}-1$ and of minimum weight 3 and the binary code of the points and t-flats of the m-dimensional affine space over $\mathbf{F}_2$ is the $(m-t)$th order Reed-Muller code, $\mathscr{R}(m-t, m)$, for any t such that $1 \leq t \leq m$. We refer the reader to [31] for a complete discussion of these linear codes. We simply note here that $\mathscr{R}(t, m)^\perp = \mathscr{R}(m-t-1, m)$, and that, for $s \leq t \leq m$, $\mathscr{R}(s, m) \subseteq \mathscr{R}(t, m)$.

There are a few other notions we shall need from coding theory: if C is a subspace of the vector space V of dimension m over $\mathbf{F}_q$, and C has dimension k, then C is referred to as an $[m, k]$ q-ary code. For any vector v in V, the *weight* of v is the number of nonzero coordinates of v, and if the smallest nonzero weight of vectors in C is d, then C is referred to as an $[m, k, d]$ q-ary code. The *support* of a vector v is the set of those coordinate positions where v is nonzero: a vector is *constant* if it is a scalar multiple of a characteristic function, i.e., if it is constant on its support. Following [31], we will denote the *extended* code of C by $\widehat{C}$, and this is defined to have length one more than that of C, with the extra coordinate position for any $v \in C$ having the entry $-\sum_{P \in \mathscr{P}} v(P)$, where $\mathscr{P}$ is the set of coordinate positions for C. The *all-one vector* of the ambient space will be denoted by j, i.e. $j(P) = 1$ for all $P \in \mathscr{P}$: equivalently, $j = v^{\mathscr{P}}$.

2.3 Hadamard matrices and designs. Once again, a *Hadamard matrix* H of size m is an $m \times m$ matrix with all entries ± 1 that is orthogonal, i.e., satisfies $HH^t = mI_m$. It follows that $m = 1, 2$ or $4n$. Let H be a Hadamard matrix

of size $4n$ and let $r = (r_1, r_2, \ldots, r_{4n})$ be any row of H. Then for any other row s of H, $l_s = \{j | s_j = r_j\}$ is a $2n$-subset of $\mathscr{P} = \{1, 2, \ldots, 4n\}$, and the same is true for $\bar{l}_s = \mathscr{P} - l_s = \{j | s_j \neq r_j\}$. It is well known and elementary to verify (see [17 or 20]) that the collection

$$\mathscr{B}(H(r)) = \{l_s | s \neq r\} \cup \{\bar{l}_s | s \neq r\}$$

forms the block set of a Hadamard 3-design. To get a 2-design, we pick a point j, then retain the block l_s if $j \in l_s$, and $\bar{l}_s$ if not.

Conversely, given a Hadamard 3-design $\mathscr{D} = (\mathscr{P}, \mathscr{B})$, then any two distinct blocks are either disjoint or meet in n points. This allows a reversal of the above procedure to produce a Hadamard matrix of size $4n$: a pair of comlementary blocks, l and $\bar{l}$, forms a row s by setting $s_j = 1$ for $j \in l$ and $s_j = -1$ if $j \in \bar{l}$, where reversing the rôles of l and $\bar{l}$ simply changes s to $-s$. The $4n - 1$ complementary pairs, together with a constant row r (i.e. all entries equal to 1 or all entries equal to -1), yield a Hadamard matrix H of size $4n$. The arbitrariness involved in whether s or $-s$ is chosen, and the arbitrariness involved in the ordering of the points and blocks, is eliminated by the usual equivalence of Hadamard matrices, viz. H is *equivalent* to K if and only if there are monomial matrices P and Q whose nonzero entries are ± 1 with $K = PHQ$. Thus, with every Hadamard 3-design is associated an equivalence class of Hadamard matrices, and, moreover, isomorphic designs yield equivalent matrices.

When forming the design from the matrix, there are $4n$ choices for the row r, so that $4n$ Hadamard 3-designs are produced, and these designs need not be isomorphic. Moreover, an equivalence class of matrices may produce, in general, even more designs. These matters were investigated thoroughly by Norman [35] who showed, amongst other things, that two Hadamard matrices H and K are equivalent if and only if there is a row r of H and a row s of K with $\mathscr{B}(H(r))$ isomorphic to $\mathscr{B}(K(s))$. This prompted Norman to define a natural equivalence relation on Hadamard 3-designs: two Hadamard 3-designs are *equivalent* if they produce equivalent Hadamard matrices. Thus, for example, there are 130 Hadamard 3-(24, 12, 5) designs, but only 60 Hadamard matrices of size 24×24 (see Ito, Leon and Longyear [21] and Kimura [26]) and hence Norman's equivalence relation partitions the 130 designs into 60 equivalence classes.

We next discuss the usual process of 'normalization' of a Hadamard matrix. Given a Hadamard matrix H, pick a row r (respectively, column c): we can find matrices in the equivalence class of H with row r (respectively, column c) having all entries equal to 1, or, all entries equal to -1: for example, to achieve a row of -1's in row r, simply post-multiply H by a diagonal matrix with the negative of row r along the diagonal. Usually one normalizes the matrix in such a way that the first row and first column consist entirely of $+1$'s, but it is often more convenient to have a row of -1's. We will mostly be interested in *row normalization*, as this concerns the 3-designs. Because of the close connection between Hadamard matrices and binary codes and the obvious passage from the multiplicative group of order 2 to the additive one we usually choose to normalize to a row of -1's. Making the natural transition from the multiplicative group of order 2, $\{1, -1\}$, to the additive group, $\{0, 1\}$, we

make the following definition, where $H = (h_{i,j})$, is a Hadamard matrix:

$$\log_{-1} H = (\log_{-1}(h_{i,j})).$$

To go from an incidence matrix of the design to a Hadamard matrix, we reverse the procedure: let $B = (b_{i,j})$ be a matrix of 0's and 1's, then

$$\exp_{-1} B = (\exp_{-1}(b_{i,j})),$$

where $\exp_{-1}(x) = (-1)^x$. Thus, for example, if B is an incidence matrix of a symmetric $(4n-1, 2n-1, n-1)$ design, form $\exp_{-1}(B)$, add a row and column of -1's, and get a Hadamard matrix.

2.4 Codes of Hadamard designs and matrices. Consider first a Hadamard $(4n-1, 2n-1, n-1)$ design $\mathscr{D}$, and let p be a prime dividing n. It is easy to see (see [1]) that, in this case,

$$\text{Hull}_p(\mathscr{D}) = \langle v^l - v^{l_0} | l, l_0 \text{ blocks of } \mathscr{D} \rangle = C_p(\overline{\mathscr{D}}).$$

Now if we form the extended code $\widehat{C_p(\mathscr{D})}$, we simply get the code of the extended design, $\mathscr{T}$. Since blocks of $\mathscr{T}$ meet in 0 or n points, this code $C_p(\mathscr{T})$ is self-orthogonal, and, of course, $\text{rank}_p(\mathscr{T}) = \text{rank}_p(\mathscr{D}) \leq 2n$. In fact it also follows that

$$C_p(\mathscr{T})^{\perp} = (\widehat{\text{Hull}_p(\mathscr{D})})^{\perp}.$$

Before turning our attention to Hadamard matrices, we remark that when p, but not p^2, divides n, then the result we mentioned for symmetric designs implies that the code $C_p(\mathscr{T})$ is self-dual. Self-dual codes, especially for $p = 2$ and $p = 3$, have long been of great interest to coding theorists, and have been classified for certain block lengths.

Now suppose we are given a Hadamard matrix, H: what can we say about the codes of its related 3-designs? The case $p = 2$ is a little different and we consider it first. Set $B = \log_{-1} H$. Then it follows easily that, for any $\mathscr{T}$ coming from H,

$$C_2(\mathscr{T}) = \langle j \rangle + \langle a + b | a, b \text{ rows of } B \rangle.$$

Had H been normalized to have a row of -1's then this would reduce to the row span (over $\mathbf{F}_2$) of B. In the nonbinary case the code of the design comes more easily; if H is normalized, then $C_p(\mathscr{T})$ is simply the row span of H: if H is not normalized then $C_p(\mathscr{T})$ is code-equivalent to this row span (see below). We next examine how the codes change within an equivalence class of matrices and see that the answer is: not at all, up to natural equivalences.

2.5 Equivalence relations on codes, designs and matrices. We can now define our equivalence relations. For this we use equivalence amongst the $C(\mathscr{T})$'s, i.e., *code equivalence*. The finest such equivalence is obtained by allowing only the symmetric group, $\text{Sym}(\mathscr{P})$, to act on $F^{\mathscr{P}}$ in the natural way: $(v\sigma)(P) = v(\sigma(P))$ for $v \in F^{\mathscr{P}}$ and $\sigma \in \text{Sym}(\mathscr{P})$. But coarser equivalence relations can be obtained by introducing monomial actions. We begin by describing the general situation.

Let G be an arbitrary subgroup of $F^{\times}$, the multiplicative group of the field. Set $A = G^{\mathscr{P}}$, the group of all functions from $\mathscr{P}$ to G with the binary operation

of pointwise multiplication: $ab(P) = a(P)b(P)$ for $a, b \in A$. Let $\mathcal{G}$ be the semidirect product of A by $\mathrm{Sym}(\mathcal{P})$. Thus, for $\sigma, \tau \in \mathrm{Sym}(\mathcal{P})$ and $a, b \in A$, $(\sigma, a)(\tau, b) = (\sigma\tau, (a\tau)b)$, where the action of $\mathrm{Sym}(\mathcal{P})$ on A is defined by $(a\tau)(P) = a(\tau(P))$. Then $\mathcal{G}$ acts naturally on $F^{\mathcal{P}}$ by $(v(\sigma, a))(P) = v(\sigma(P))a(P)$. It is easy to check that $v((\sigma, a)(\tau, b)) = (v(\sigma, a))(\tau, b)$ and it is clear that $\mathcal{G}$ acts as a group of linear transformations of the vector space $F^{\mathcal{P}}$. In the distinguished basis of $F^{\mathcal{P}}$ the action is monomial. Taking G to be the trivial subgroup of $F^{\times}$ gives the finest equivalence—usually called *code isomorphism*—and taking $G = F^{\times}$ gives the coarsest—usually called *code equivalence*. For F of odd characteristic, taking $G = \{\pm 1\}$ is also interesting and obviously related to the Hadamard situation.

In our case we will be taking F to be a prime field, $\mathbf{F}_p$, so that for $p = 2$ the only choice is code isomorphism. In order to fix ideas we will take $G = \{\pm 1\}$ for p odd. Then two codes, C and D in $\mathbf{F}_p^{\mathcal{P}}$ are *equivalent* provided there is a (σ, a) in $\mathcal{G}$ with $D = C(\sigma, a)$.

Definition 1. Let $\mathcal{T}$ and $\mathcal{E}$ be two Hadamard 3-designs with parameters 3-$(4n, 2n, n-1)$ and let p be a prime dividing n. Then $\mathcal{T}$ and $\mathcal{E}$ are *p-equivalent* if $C_p(\mathcal{T})$ and $C_p(\mathcal{E})$ are equivalent codes in $\mathbf{F}_p^{\mathcal{P}}$.

Obviously if $\mathcal{T}$ and $\mathcal{E}$ are isomorphic designs they are p-equivalent for every prime p; in fact, $C_p(\mathcal{T})$ and $C_p(\mathcal{E})$ are code isomorphic. Further, $\mathcal{T}$ and $\mathcal{E}$ are p-equivalent provided that the Hadamard matrices determined by $\mathcal{T}$ and $\mathcal{E}$ are equivalent matrices, as we shall prove in the proposition below. We note that this implies that p-equivalence is a coarser equivalence relation than the equivalence introduced by Norman.

Proposition 1. *Let $\mathcal{T}$ and $\mathcal{E}$ be Hadamard 3-designs with parameters 3-$(4n, 2n, n-1)$. If the Hadamard matrices given by $\mathcal{T}$ and $\mathcal{E}$ are equivalent, then $\mathcal{T}$ and $\mathcal{E}$ are p-equivalent for every prime p.*

Proof. We first show that $C_p(\mathcal{T})$ is determined, up to code equivalence, by the Hadamard matrix H determined by $\mathcal{T}$. For p odd this is clear, since $C_p(\mathcal{T})$ is generated by the rows of H. For $p = 2$, we change, as we explained above, from multiplicative to additive notation, and for this purpose it is best to use a row of -1's (rather than 1's) as the added row when producing H from $\mathcal{T}$. Then the rows of $\log_{-1} H$ generate $C_2(\mathcal{D})$.

Now suppose that H and K are equivalent Hadamard matrices with $K = PHQ$. Then for p odd the monomial matrix P merely permutes the rows of H, possibly also multiplying by -1, and this clearly does not change the row space of H. Further, post-multiplication by Q amounts to a code equivalence, since Q is a monomial matrix with non-zero entries ± 1.

The situation is different for $p = 2$: in this case it follows that the binary code of any design from PH is actually identical to that from H, and that the binary code of any design from PHQ is isomorphic to that from H.

In view of this equivalence, we will write $C_p(H)$ for the p-ary code associated with any 3-design defined by H, and we will refer to this as the *p-ary code of H*.

2.6 Difference sets and their designs. Let $\mathcal{G}$ be an arbitrary finite group. A subset D of $\mathcal{G}$ is said to be a *difference set* for $\mathcal{G}$ if every nonidentity element of $\mathcal{G}$ can be written in precisely λ ways in the form ab^{-1} where both a

and b are in D. One normally insists that D contain the identity element of $\mathcal{G}$, since the interest is in the collection of all subsets of $\mathcal{G}$ of the form $gD = \{ga | a \in D\}$. If $|\mathcal{G}| = v$ and $|D| = d$, then this collection forms a (v, d, λ) design [27] of order $n = d - \lambda$. It is clear that $\mathcal{G}$ acts regularly on the symmetric design given by the difference set and as a group of isomorphisms of the codes of the symmetric design. In fact, if F is a field and $\mathcal{D}$ is the symmetric design given by a difference set D of $\mathcal{G}$, then $\mathcal{G}$ acts on $F^{\mathcal{G}}$ by $(u\sigma)(P) = u(\sigma P)$, where $u \in F^{\mathcal{G}}$, both σ and P are in $\mathcal{G}$, and $C_F(\mathcal{D})$ is generated by all $(u^D)\sigma$, $\sigma \in \mathcal{G}$.

If a difference set yields a design of order n with $v = 4n$, the difference set is called a *Hadamard difference set*, since then $n = k^2$ and $d = 2k^2 \pm k$ with $\exp_{-1}(A)$ a Hadamard matrix (A being the incidence matrix of the symmetric design) [12]. Moreover, since a $(2^m, k, \lambda)$ design of order n must have $2^m = 4n$ [33, p. 72], if $\mathcal{G}$ is an elementary abelian 2-group, the difference set must be Hadamard; hence our particular interest in the case where $\mathcal{G}$ is an elementary abelian 2-group (normally taken to be $\mathbf{F}_2^{2m}$).

Let $\mathcal{G}$ be the elementary abelian 2-group of order 2^{2m}; then $\mathbf{F}_2^{\mathcal{G}}$ can be viewed as the vector space of all suitably restricted polynomial functions in $2m$ boolean variables and this is precisely the setting for the Reed-Muller codes. In this case, the difference sets in $\mathcal{G}$ have characteristic functions that are bent functions. The bent functions are certain reduced polynomial functions of degree m or less and thus contained in the Reed-Muller code $\mathcal{R}(m, 2m)$: see [31, Chapter 14]. These functions correspond to cosets of the first-order Reed-Muller code of highest possible weight and the minimal-weight vectors in such a coset also yield a symmetric design, but not usually the design given by the corresponding difference set. The situation is quite complex and will be discussed in §4. We simply note here that the parameters of the symmetric designs produced in this way are $(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$ and $(2^{2m}, 2^{2m-1} + 2^{m-1}, 2^{2m-2} + 2^{m-1})$, complementary parameters.

As remarked above *Hadamard difference sets* yield Hadamard matrices. In fact, something slightly more general is true, as we next explain.

2.7 Other designs from Hadamard matrices. We describe one final connection between designs and Hadamard matrices that applies to a particular class of Hadamard matrices. Suppose H is a Hadamard matrix with the property that the sum of the entries in each row is constant. Then it is straightforward to verify that H must have size $4k^2$, and that the rows of $\log_{-1} H$ form the blocks of either a $(4k^2, 2k^2 - k, k^2 - k)$ design or a $(4k^2, 2k^2 + k, k^2 + k)$ design, depending on whether there are more or fewer $+1$'s than -1's in each row, the excess or shortfall being constant because of the assumption on H. As before, the procedure is reversible. Nonisomorphic designs may yield equivalent Hadamard matrices; put another way, an equivalence class of a Hadamard matrix may yield many of these designs. In fact the Sylvester matrices do and the number of inequivalent designs grows very fast as the size of the Sylvester matrix grows. The codes of these designs will not necessarily (indeed not usually) be equivalent, even though they come from the same equivalence class of matrices. This accounts for part, at least, of the subtlety of this aspect of the theory.

The parameters above are the parameters of the designs arising from Hadamard difference sets, but there are designs with these parameters that are not obtained from difference sets.

In summary, every pair—a Hadamard matrix of size $4n$ together with a row—yields a Hadamard 3-design on $4n$ points and hence $4n$ symmetric designs on $4n-1$ points (of order n): further, certain Hadamard matrices yield symmetric designs on $4n$ points. These latter symmetric designs can occur only when n is a square and they also are of order n. They conjecturally exist for all square orders but not every equivalence class of Hadamard matrices of size four times a square can be produced by such a design. Moreover, there are equivalence classes that can be produced by such a design but not by a difference set in an elementary abelian 2-group. We examine these designs, and the associated Hadamard designs, in §4.

3. Hadamard 3-designs contained in $\mathscr{R}(m-2, m)$

3.1 Introduction. In [2] we suggested studying 2-(v, k, λ) designs through the weight-k vectors of codes contained in the orthogonal of the hull of the design. In particular, affine translation planes of order p^s, where p is a prime, were studied using certain p-ary codes introduced by Delsarte [10]. For the case at hand the codes involved are the Reed-Muller codes, an intensively studied class of binary codes.

This fact informs the discussion in this section where the designs we consider are, of course, Hadamard designs. The natural geometric design arises for $4n = 2^m$ and is the design of points and hyperplanes of a projective space over $\mathbf{F}_2$. This design is a Hadamard 2-design and the associated Hadamard 3-design is the design of points and hyperplanes of the affine space of one greater dimension. The binary code of this 3-design is precisely the first-order Reed-Muller code $\mathscr{R}(1, m)$. This situation is peculiar to the two-element field and we do not know of a p-ary analogue.

As we mentioned before, if $\mathscr{D}$ is a Hadamard 2-$(4n-1, 2n-1, n-1)$ design, and $\mathscr{T}$ the extended 3-design, then the extended orthogonal of the hull of $\mathscr{D}$ is equal to the orthogonal of the code of $\mathscr{T}$ over $\mathbf{F}_p$, for any p dividing n. Thus we may concentrate our attention on the 3-designs, in particular, when $4n = 2^m$, on those whose binary codes are inside the orthogonal of $\mathscr{R}(1, m)$, i.e. the Reed-Muller code $\mathscr{R}(m-2, m)$. For the 2-designs this corresponds to those designs whose codes are in the binary Hamming code.

3.2 Kronecker product constructions. The following is a standard construction (see, for example [20, p. 104]): if $H = (h_{ij})$ is any $n \times n$ Hadamard matrix, and $B_1, B_2, \ldots, B_n$ are any $m \times m$ Hadamard matrices, then the matrix obtained from the Kronecker product, viz.

$$H \otimes [B_1, B_2, \ldots, B_n] = \begin{pmatrix} h_{11}B_1 & h_{12}B_1 & \cdots & h_{1n}B_1 \\ h_{21}B_2 & h_{22}B_2 & \cdots & h_{2n}B_2 \\ \vdots & \vdots & & \vdots \\ h_{n1}B_n & h_{n2}B_n & \cdots & h_{nn}B_n \end{pmatrix},$$

is an $nm \times nm$ Hadamard matrix. This is a well-known method for creating new Hadamard matrices, especially in the case $B_1 = B_2 = \cdots = B_n = B$, when $H \otimes [B_1, B_2, \ldots, B_n] = H \otimes B$, which is the more familiar form of the Kronecker product.

For our purposes we need to consider the representatives of the equivalence classes of matrices that we use in the construction. This is important, since different representatives can produce inequivalent Kronecker products, as the case $n = 2$, $m = 8$ will illustrate below (cf. §3.4). Thus we will normalize our matrices to have a row of 1's or -1's and, in this section, all our codes will be binary unless otherwise stated. We are indebted to R. D. Baker for several discussions that helped formulate and prove the next two proposition.

Proposition 2. *Suppose that* $H, B_1, \ldots, B_n, C_1, \ldots, C_n$ *are normalized Hadamard matrices, and that* H *has size* n, *and the* B_i *and* C_i *have size* m, *where* $n \geq 2$, $m \geq 4$. *Then*

$$C(H \otimes [B_1, \ldots, B_n]) \subseteq C(H \otimes [C_1, \ldots, C_n])^{\perp}.$$

Proof. This is easy to see by noting that, since we have normalized all the matrices, $C(H \otimes [B_1, B_2, \ldots, B_n])$ will be the space spanned by

$$\log_{-1}(H \otimes [B_1, B_2, \ldots, B_n]),$$

possibly together with the all-one vector j. This is also a Kronecker product, with entries $\log_{-1} B_i$ or $j + \log_{-1} B_i$, and the conditions $n \geq 2$ and $m \geq 4$ will ensure the result.

The particular case we will concentrate on has for H the 2×2 Sylvester matrix, which we will denote by H_1, i.e.

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Then we also have the following:

Proposition 3. *Let* H_1 *be as defined above, and let* K *and* L *be normalized Hadamard matrices of size* $m \geq 4$. *Then*

1. $\operatorname{rank}(H_1 \otimes [K, L]) = \operatorname{rank}(K) + \operatorname{rank}(L) + 1 - \dim(\langle \log_{-1} K, j \rangle \cap \langle \log_{-1} L, j \rangle)$;
2. $C(H_1 \otimes [K, K]) \subseteq C(H_1 \otimes [K, L])$.

Proof. Straightforward.

3.3 Affine and projective geometry designs over $\mathbf{F}_2$. Starting with H_1, define recursively $H_m = H_1 \otimes [H_{m-1}, H_{m-1}] = H_1 \otimes H_{m-1}$, for $m \geq 2$. Then H_m is a $2^m \times 2^m$ Hadamard matrix (Sylvester matrix) and gives the unique Hadamard 3-design of points and hyperplanes ($(m-1)$-flats) of the affine geometry of dimension m over $\mathbf{F}_2$. Thus $C(H_m) = \mathscr{R}(1, m)$, a $[2^m, m+1, 2^{m-1}]$ binary code. We have, therefore, $C(H_m)^{\perp} = \mathscr{R}(m-2, m)$ and, for $m \geq 3$, $C(H_m) \subseteq C(H_m)^{\perp}$.

Now it is clear from the two propositions above that we can employ recursive constructions to obtain 3-$(2^m, 2^{m-1}, 2^{m-2} - 1)$ designs for $m \geq 3$, whose binary codes contain $\mathscr{R}(1, m)$ and are contained in $\mathscr{R}(m-2, m)$. We illustrate this for $m = 4$ (since for $m = 3$ the design is unique) in the next section.

3.4 The five Hadamard 3-(16, 8, 3) designs. The Hadamard matrix H_4 has rank 5 over $\mathbf{F}_2$ and is constructed from H_3 as described above. It has been shown (see Todd [39]) that there are precisely five inequivalent 16×16 Hadamard matrices, and five nonisomorphic 3-(16, 8, 3) designs: see also [6, 16].

On the other hand, there is only one equivalence class of 8×8 Hadamard matrices, so if we use the Kronecker construction, we must use equivalent matrices. This is done in the following way: we start with H_3 as given, a symmetric matrix with first row and column entries all equal to 1. Then we can find three other members of H_3's equivalence class, K_1, K_2, K_3, having the property that each has first row j, and that K_1 has three other rows in common with H_3, K_2 has one other row in common with H_3, and K_3 has no other row in common with H_3. (This can, possibly, be more easily seen in the underlying Fano plane, by simply constructing three new Fano planes with three, one or zero lines in common with the original.) Arrange matters to make the first column of each K_i all 1's.

Now let $B_i = H_1 \times [H_3, K_i]$ for $i = 1, 2, 3$; let B_0 denote H_4, and B_4 denote the transpose of B_3. Let the design defined by the first row of B_i be denoted by $\mathscr{D}_i$, for $i = 0, 1, 2, 3, 4$. Then, since the rank of H_3 is 4, the propositions of §3.2 show that $\operatorname{rank}(B_0)$ is 5, $\operatorname{rank}(B_1)$ is 6, $\operatorname{rank}(B_2)$ is 7, and $\operatorname{rank}(B_3)$ is 8, and that $C(B_0) \subseteq C(B_i) \subseteq C(B_0)^\perp$. This clearly accounts for four of the five inequivalent matrices. For the last, we look at B_4; now H_3 was defined to be symmetric, and the transpose, $(K_3)^t$, of K_3 is just a matrix obtained from H_3 by permuting its rows. Since $C(H_3)$ is a self-dual code, we get $C(B_4) \subset C(H_4)^\perp$; since H_4 is symmetric and $C(H_4) \subset C(B_3)$, we get also $C(H_4) \subset C(B_4)$, i.e. again

$$C(B_0) \subseteq C(B_4) \subseteq C(B_0)^\perp.$$

Of course, $\operatorname{rank}(B_4)$ is also 8, and it is not clear that either the designs or the codes are not isomorphic. To see that they are not we look at the weight-4 vectors that occur in the codes of the new designs. All the codes are self-orthogonal, generated by weight-8 vectors, and hence are doubly-even. They all contain j, and all, except $C(B_0)$, must have vectors of weight other than 8, i.e. weight-4 vectors must occur.

In fact, an analysis of the vectors arising from the defining Hadamard matrix, shows that $C(B_1)$ can be obtained by adding a single weight-4 vector of $C(B_0)^\perp$ to $C(B_0)$. All the complements in the three 3-flats that contain this 2-flat must occur too, so $C(B_1)$ has weight distribution

$$x^0 + 4(x^4 + x^{12}) + 54x^8 + x^{16}.$$

Similarly, for $C(B_2)$, two weight-4 vectors, corresponding to two 2-flats through a line or 1-flat, are added, from which a further 2-flat through that line will also appear. With the complements as well, the weight distribution of $C(B_2)$ becomes

$$x^0 + 12(x^4 + x^{12}) + 102x^8 + x^{16}.$$

For $C(B_3)$ seven weight-4 vectors (corresponding to seven planes, or 2-flats, through a line) are added, giving in all 28 weight-4 vectors, and weight distribution

$$x^0 + 28(x^4 + x^{12}) + 198x^8 + x^{16}.$$

(All of these weight distributions can quite easily be obtained by examining the codewords that must appear when the defining Hadamard matrix is used to generate the code.)

For $C(B_4)$, the weight distribution is the same as that for $C(B_3)$, but the supports of the weight-4 vectors do not have the same configuration as in the

case of B_3, but form a 3-(8, 4, 1) design. Thus the codes are distinct; hence the designs are nonisomorphic and the matrices inequivalent. A view of the five 2-designs through a projective lens can be seen in [1].

3.5 Special n-tuples. The occurrence of weight-4 vectors in the codes of the design can be interpreted more generally in terms of *special n-tuples* in the 3-$(4n, 2n, n-1)$ design $\mathscr{T}$, using the terminology of [6]: a *special n-tuple* of $\mathscr{T}$ is a set of n points that is the intersection of three blocks of $\mathscr{T}$. The *characteristic number* of $\mathscr{T}$ is the number of special n-tuples of $\mathscr{T}$. Bhat and Shrikhande classified the 3-(16, 8, 3) designs through their characteristic numbers and intersection properties of the special n-tuples in case the characteristic numbers were the same. We will show how these special n-tuples manifest themselves in the codes related to the designs.

Proposition 4. *Let $\mathscr{T} = (\mathscr{P}, \mathscr{B})$ be a 3-$(4n, 2n, n-1)$ design, and let X be a special n-tuple. Then $X = l_1 \cap l_2 \cap l_3$, for $l_i \in \mathscr{B}$ for $i = 1, 2, 3$ and we have:*

1. *$l_i - X$ is a special n-tuple for $i = 1, 2, 3$ and hence $\mathscr{P}$ is the disjoint union of these four special n-tuples;*
2. *a block of $\mathscr{T}$ that neither contains X nor is disjoint from it meets X in $n/2$ points; thus special n-tuples can exist, for $n > 1$, only when n is even;*
3. *if p is a prime dividing $n/2$ then $v^X \in C_p(\mathscr{T})^\perp$;*
4. *if $n = 2p$ where p is a prime, then, conversely, the special n-tuples are precisely the supports of the constant weight-n vectors of $C_p(\mathscr{T})^\perp$ and, moreover, when p is odd, $C_p(\mathscr{T}) = C_p(\mathscr{T})^\perp$.*

Proof. (1) $\mathscr{P} - l_i$ is a block for each i, and $l_i - X = l_i \cap (\mathscr{P} - l_j) \cap (\mathscr{P} - l_k)$, where l_j and l_k are the other two blocks containing X. (2) Blocks in $\mathscr{T}$ meet in 0 or n points. Let $l \in \mathscr{B}$, and suppose $l \neq l_i$ for $i = 1, 2, 3$, and let $x = |l \cap X|$. If $x \neq 0$ then $|l| = 2n = x + 3(n - x)$, i.e. $2x = n$. Since if $n > 1$ there will exist blocks other than the l_i meeting X, we must have n even for special n-tuples to exist. (3) If p divides $n/2$ and $l \in \mathscr{T}$, then $|l \cap X| \equiv 0 \pmod{p}$ by (2) above. Hence $v^X \in C_p(\mathscr{T})^\perp$. (4) Suppose $X \subset \mathscr{P}$ with $|X| = n$, and $v^X \in C_p(\mathscr{T})^\perp$. Then $|l \cap X| \equiv 0 \pmod{p}$ for every $l \in \mathscr{T}$. Thus, $|l \cap X|$ must meet X in 0, p or $2p = n$ points. Let X_i be the number of blocks meeting X in i points. Then counting incidences gives

$$X_0 + X_p + X_{2p} = 8n - 2 = 16p - 2,$$
$$pX_p + 2pX_{2p} = n(4n-1) = 2p(8p-1),$$
$$p(p-1)X_p + 2p(2p-1)X_{2p} = n(n-1)(2n-1) = 2p(2p-1)(4p-1).$$

These equations imply that $X_{2p} = 3$ and hence that X is a special n-tuple. That $C_p(\mathscr{T})^\perp = C_p(\mathscr{T})$ follows from the fact that p divides the order n to the first power (see §2.2).

Consider again the five nonisomorphic 3-(16, 8, 3) designs, $\mathscr{D}_i$, for $i = 0$ to 4. Here $n = 4 = 2p$, and the Proposition on n-tuples applies. Thus the weight-4 vectors in $C(\mathscr{D}_i)^\perp$ simply give the supports of the special 4-tuples in $\mathscr{D}_i$: 140 for $\mathscr{D}_0$, 78 for $\mathscr{D}_1$, 44 for $\mathscr{D}_2$, and 28 for $\mathscr{D}_3$ or $\mathscr{D}_4$, the latter being in the codes of $\mathscr{D}_3$ and $\mathscr{D}_4$, since they are self-dual.

3.6 General constructions. The geometrical device used in 3.4 to produce new designs, which amounted to using existing weight-8 vectors in the Reed-

Muller code $\mathscr{R}(2, 4)$, can easily be generalized to weight-2^{m-1} vectors in $\mathscr{R}(m-2, m)$. It is most likely that, for any dimension between $m+1$ and 2^{m-1}, a design of that rank whose blocks are the supports of weight-2^{m-1} vectors of this Reed-Muller code can be found. Certainly nonisomorphic designs of the same dimension can be produced in many ways: see Dillon [11]. We will describe here just one of these methods.

Recall that $\mathscr{R}(m-1, m)$, viewed as the code of the design of points and 2-flats of the m-dimensional affine geometry over $\mathbf{F}_2$, contains amongst its weight-2^t vectors, for any t such that $2 \leq t \leq m$, vectors corresponding to the characteristic functions of all t-flats. These will produce weight-2^{m-1} vectors in $\mathscr{R}(m-2, m)$, whose supports are not hyperplanes, in the following way: if T is a t-dimensional subspace and X is a hyperplane, then the vector $v^T + v^X = v^{X \oplus T}$ is a weight-2^{m-1} vector with support $X \oplus T$, the symmetric difference of X and T. If $t = m-1$ then $X \oplus T$ is a hyperplane, but if $t < (m-1)$ we get new vectors. Adding v^T to $\mathscr{R}(1, m)$ will then give a code of dimension $m+2$, and it is only a matter of deciding which weight-2^{m-1} vectors to take for the blocks to produce a 3-$(2^m, 2^{m-1}, 2^{m-2}-1)$ design with this as its code. The following proposition describes the obvious choice:

Proposition 5. *Let T be a subspace of dimension t of the affine geometry of dimension m over $\mathbf{F}_2$ where $2 \leq t < (m-1)$. Let $\mathscr{B}$ denote the set of subspaces of dimension $m-1$. Then the collection of subsets*

$$\{X \oplus T | T \not\subset X \in \mathscr{B}\} \cup \{X | T \subset X \in \mathscr{B}\},$$

together with their complements form the blocks of a 3-design whose code is $\langle v^T, \mathscr{R}(1, m)\rangle$.

Proof. Straightforward.

It is also quite straightforward to show that the code of this new design contains $\mathscr{R}(1, m)$. It is clear that different values of t will give different codes and hence different designs; there are also many other possibilities for constructions in this way, some of them involving a variety of subspaces and producing designs of larger 2-rank.

3.7 *Remarks.* We have yet to find an example of a 3-$(2^m, 2^{m-1}, 2^{m-2}-1)$ design whose binary code C cannot be placed in the range

$$\mathscr{R}(1, m) \subseteq C \subseteq \mathscr{R}(m-2, m),$$

For such a code C, the dimension of C *does* lie within the range $m+1$ and 2^{m-1}, with $C = \mathscr{R}(1, m)$ if the rank is $m+1$: see [18]. (The upper bound follows from the fact that C is self-orthogonal; it is achieved, of course, if and only if C is self-dual.) Clearly, an enormous number of these Hadamard 3-designs do have binary codes that can be placed in the given range: even the extended quadratic-residue codes, when $2^m - 1$ is a prime, will occur here. The situation is somewhat analogous to the case of affine planes where the majority of planes appear to lie in a similar range and are translation planes—in this case the codes are not necessarily binary.

Confining ourselves to those Hadamard 3-designs whose codes contain $\mathscr{R}(1, m)$, we will still be treating a large subclass of the designs with parameters 3-$(2^m, 2^{m-1}, 2^{m-2}-1)$ and possibly all such designs. Moreover, as Proposition 5 makes clear, for each d with $1 \leq d \leq m-2$ there will be a design

whose code is contained in $\mathscr{R}(d, m)$ but is not contained in $\mathscr{R}(k, m)$ for any $k < d$. Natural questions immediately arise: (1) For the self-orthogonal codes coming from such designs does every possible minimum weight occur? That is to say, is there, for every multiple of 4 less than or equal to 2^{m-1}, a design whose code has this minimum weight? (2) Does every possible dimension occur? (3) Is there anything special about the Hadamard matrices that give rise to "extremal" codes. (At one extreme, maximum minimum weight, we have the Sylvester matrices, but what about the other extreme: is there anything special about the matrices giving rise to self-dual codes with the maximal minimum weight?) Of course, what one would really like is a helpful characterization of those doubly-even, self-orthogonal codes that are binary codes of Hadamard matrices: the would amount to a characterization up to linear equivalence of the designs. There are, for example, things that can be said about the vectors of a given weight in such a code: an instance of this is how the vectors of weight four must be deployed in the case $m = 4$.

All dimensions and minimum weights occur in the case $m = 4$ as we saw in §3.4. Moreover the two [16, 8] self-dual codes obtained are the only two that exist. This case is too small to be decisive, of course, but the next case, $m = 5$, should be a better testing ground since here there is no shortage of designs and, moreover, there are five extremal [32, 16] codes (i.e. [32, 16, 8] codes).

The Reed-Muller codes already give a very rough classification of the matrices and it might be interesting to investigate those whose codes are contained in $\mathscr{R}(2, m)$, for example.

Finally we note that, were it true that *all* designs with these parameters had binary codes in the given range, then a conjecture of Dillon and Schatz (see [13]) would be proven. We have more to say of this in §§4.2 and 4.3 below.

4. Designs with parameters $(4k^2, 2k^2 - k, k^2 - k)$

Much of the material in this section is due to John Dillon and all of it has benefited from conversations with him. Many of the results herein were developed with an eye to investigating the curiously difficult problem of determining when the all-one vector is in the code of a symmetric design over $\mathbf{F}_2$—in the case where all the parameters are even.

4.1 General incidence structures, their duals and their complements. Given an incidence structure $\mathscr{D} = (\mathscr{P}, \mathscr{B})$ and a field F we denote by $F^{\mathscr{B}}$ the vector space of all functions from $\mathscr{B}$ to F: as before, $F^{\mathscr{P}}$ is the space of all functions from $\mathscr{P}$ to F. Define $S: F^{\mathscr{B}} \to F^{\mathscr{P}}$ by $S(f) = \sum_{l \in \mathscr{B}} f(l) v^l$. Here v^l denotes the function on $\mathscr{P}$ which is 1 when $P \in \mathscr{P}$ is incident with l and 0 otherwise, which, by an abuse of language, is the characteristic function of l. The mapping S is clearly linear and its image is, obviously, $C_F(\mathscr{D}) = \langle v^l | l \in \mathscr{B} \rangle$. A minute's reflection (think of the incidence matrix) should convince the reader that the *kernel* of S is $C_F(\mathscr{D}^t)^\perp$. Next, define $s: F^{\mathscr{B}} \to F$ by $s(f) = \sum_{l \in \mathscr{B}} f(l)$. Clearly s is onto with kernel $\langle j_{\mathscr{B}} \rangle^\perp$, where we are denoting the constant function taking the value 1 by $j_{\mathscr{B}}$—the all-one vector, if you will. We have, immediately, that $j_{\mathscr{B}} \in C_F(\mathscr{D}^t)$ if and only if $\mathrm{Ker}(S) \subseteq \mathrm{Ker}(s)$.

There is one last bit of notation that will prove useful: for an incidence structure $\mathscr{D} = (\mathscr{P}, \mathscr{B})$ set $E_F(\mathscr{D}) = \langle v^{l_1} - v^{l_2} | l_1, l_2 \in \mathscr{B} \rangle$: clearly

$$E_F(\mathscr{D}) = \langle v^l - v^{l_0} | l \in \mathscr{B} \rangle.$$

Proposition 6. *Let $\mathscr{D} = (\mathscr{P}, \mathscr{B})$ be an incidence structure and F a field. Then, $E_F(\mathscr{D})$ has codimension at most 1 in $C_F(\mathscr{D})$ and $E_F(\mathscr{D}) = C_F(\mathscr{D})$ if and only if $j_{\mathscr{B}} \notin C_F(\mathscr{D}^t)$.*

Proof. That $E_F(\mathscr{D})$ has codimension at most 1 is obvious from the fact that $E_F(\mathscr{D}) = \langle v^l - v^{l_0} | l \in \mathscr{B} \rangle$. If $j_{\mathscr{B}} \in C_F(\mathscr{D}^t)$, then $\mathrm{Ker}(S) \subseteq \mathrm{Ker}(s)$ and, since $\mathrm{Ker}(s)$ is of codimension 1 in $F^{\mathscr{B}}$, its image under S is of codimension 1 in the image of S, namely, $C_F(\mathscr{D})$. But $E_F(\mathscr{D})$ is the image of $\mathrm{Ker}(s)$ under S. If $j_{\mathscr{B}} \notin C_F(\mathscr{D}^t)$, then $F^{\mathscr{B}} = \mathrm{Ker}(S) + \mathrm{Ker}(s)$. For $w \in C_F(\mathscr{D})$ and $u \in F^{\mathscr{B}}$ with $S(u) = w$ express u as $x + y$ with $x \in \mathrm{Ker}(S)$ and $y \in \mathrm{Ker}(s)$. Then, $w = S(y) \in E_F(\mathscr{D})$ and therefore $E_F(\mathscr{D}) = C_F(\mathscr{D})$.

For an arbitrary incidence structure $\mathscr{D} = (\mathscr{P}, \mathscr{B})$ consider the complementary structure $\overline{\mathscr{D}}$. Let $j_{\mathscr{P}}$ denote the all-one vector. Now, if l is a block of $\mathscr{D}$ and $\bar{l}$ the complementary block, then $v^{\bar{l}} = j_{\mathscr{P}} - v^l$ and it follows immediately that $E_F(\mathscr{D}) = E_F(\overline{\mathscr{D}})$ and we denote this code simply by E. Moreover, it is clear that $C_F(\mathscr{D}) = C_F(\overline{\mathscr{D}})$ if and only if $j_{\mathscr{P}} \in C_F(\mathscr{D}) \cap C_F(\overline{\mathscr{D}})$. We use these easy facts to give conditions sufficient to ensure that the all-one vector is in various codes given by a design. Here is our first example:

Proposition 7. *$C_2(\mathscr{D}) = C_2(\overline{\mathscr{D}})$ if and only if $j_{\mathscr{P}} \in E$.*

Proof. If $j_{\mathscr{P}} \in E$, then clearly $j_{\mathscr{P}} \in C_F(\mathscr{D}) \cap C_F(\overline{\mathscr{D}})$ and by the above remarks $C_F(\mathscr{D}) = C_F(\overline{\mathscr{D}})$. On the other hand, when $C_F(\mathscr{D}) = C_F(\overline{\mathscr{D}})$, if $E = C_2(\mathscr{D})$, then $j_{\mathscr{P}} \in E$. Suppose $E \subset C_2(\mathscr{D})$ and $j_{\mathscr{P}} \notin E$. Then, since it is of codimension 1 in $C_2(\mathscr{D})$, $C_2(\mathscr{D}) = \langle j_{\mathscr{P}} \rangle + E$ and for any block l of $\mathscr{D}$ we have that $v^l = j_{\mathscr{P}} + e$ where $e \in E$. But then, $v^{\bar{l}} = j_{\mathscr{P}} + v^l = e \in E$ and $E = C_2(\overline{\mathscr{D}})$, a contradiction.

Bagchi and Sastry [5] have shown that in an incidence system with a polarity, the characteristic function of the set of absolute points is in the binary code of the system. John Dillon has given an easy proof of this result which we state and prove in its matrix form.

Proposition 8. *Let $A = (a_{ij})$ be an $m \times m$ symmetric matrix with entries from $\mathbf{F}_2$. Then the vector $(a_{11}, a_{22}, \ldots, a_{mm})$ is in the row space of A.*

Proof. For any vector $\mathbf{x} = (x_1, x_2, \ldots, x_m) \in \mathbf{F}_2^m$, the fact that we are over a field of characteristic two yields

$$\mathbf{x}A\mathbf{x}^t = \sum_{i=1}^{m} x_i a_{ii}.$$

Thus $\mathbf{x}A\mathbf{x}^t = 0$ if and only if $\mathbf{x} \in \langle \mathbf{a} \rangle^\perp$, where we have set $(a_{11}, a_{22}, \ldots, a_{mm}) = \mathbf{a}$. But, if C is the row space of A, then $\mathbf{x} \in C^\perp$ if and only if $A\mathbf{x}^t = 0$. Thus, $C^\perp \subseteq \langle \mathbf{a} \rangle^\perp$ or $\langle \mathbf{a} \rangle \subseteq C$ and the proposition follows.

Now an incidence structure with a polarity is necessarily self-dual (i.e. it is isomorphic to its dual) and a design given by a difference set in an elementary abelian 2-group possesses a polarity all of whose points are absolute [27]. From what we have already proved, therefore, we have the following:

Corollary 1. *If $\mathscr{D}$ is the design given by a difference set in an elementary abelian 2-group, then the all-one vector is in E and E is of codimension 1 in $C_2(\mathscr{D}) = C_2(\overline{\mathscr{D}})$; moreover, $C_2(\mathscr{D}^t) = C_2(\overline{\mathscr{D}}^t)$ is isomorphic to $C_2(\mathscr{D}) = C_2(\overline{\mathscr{D}})$.*

4.2 The designs of order k^2. Recall that we are interested in designs with parameters $(4k^2, 2k^2 - k, k^2 - k)$. The complementary design has parameters $(4k^2, 2k^2 + k, k^2 + k)$. When p divides the order, k^2, the codes of these designs are obviously self-orthogonal. If M is the incidence matrix of such a design, then it is well-known [17] that $\exp_{-1} M$ is a Hadamard matrix. The associated Hadamard 3-*designs* are obtained by choosing a block of the design, l_0 say, and taking all symmetric differences, $l_0 \oplus l$ for $l \neq l_0$, and their complements.

It is clear that for k even the binary code of the associated Hadamard 3-design contains E and is, in fact, E provided E contains the all-one vector.

We do not have an example for which the all-one vector is not in E. By the results above, that could only happen for such a design $\mathscr{D}$ if $C_2(\mathscr{D})$ and $C_2(\overline{\mathscr{D}})$ had different dimensions with the smaller of the two codes equal to E. This fact allows us to restate an interesting result due to Dillon and Schatz [13].

Theorem 1. *Suppose $\mathscr{D}$ is a design with parameters $(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$ with both $C_2(\mathscr{D})$ and $C_2(\overline{\mathscr{D}})$ of dimension $2m + 2$. Then there is a difference set D in the elementary abelian 2-group corresponding to the first-order Reed-Muller code $\mathscr{R}(1, 2m)$ with*

$$C_2(\mathscr{D}) = C_2(\overline{\mathscr{D}}) = \langle v^D \rangle \oplus \mathscr{R}(1, 2m)$$

and the design $\mathscr{D}$ is the design of minimal-weight vectors of this binary code.

Observe that the theorem shows that an equivalence class of Hadamard matrices may yield nonisomorphic designs; in fact, the Sylvester-Hadamard matrix does. Put in terms of the matrices, this means that an equivalence class may contain many matrices with constant row sums, each such matrix yielding a design and all these designs distinct—that is, not isomorphic.

The assumption in the theorem that both $\mathscr{D}$ and $\overline{\mathscr{D}}$ have the same rank could be eliminated if the answer to the following were yes.

Question 1. *Does the code of a design with parameter $(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$ contain the all-one vector?*

The rank given in the theorem is the smallest possible rank for a design with parameters $(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$. We know of no design with parameters $(4k^2, 2k^2 - k, k^2 - k)$ whose code over any field does not contain the all-one vector. That the $(16, 6, 2)$ designs do is obvious since we have them all, but this can also be "proved": see [4]. Jungnickel and Tonchev [22] have recently managed to give a short proof that also settles the case $(64, 28, 12)$, but the general problem appears to be quite difficult. The reader may want to consult [1] for another discussion of the all-one problem and the Dillon-Schatz Theorem. One should be aware of the fact that the design given by the theorem is not necessarily isomorphic to the design (called the translate design) given by the difference set.

Suppose next that we are given a design that is the design given by a difference set in an elementary abelian 2-group. Thus $\mathscr{D}$ has parameters $(2^{2m}, 2^{2m-1} -$

$2^{m-1}, 2^{2m-2} - 2^{m-1})$ and is given by the translates of a difference set in an elementary abelian 2-group. Moreover, we know that the all-one vector is present in its binary code by the Corollary above. Thus the rank of $\mathscr{D}$ is $1 + \dim(E)$. If C is the binary code of $\mathscr{D}$, then since the difference set is given by a bent function, we have that $C \subseteq \mathscr{R}(m, 2m)$ and E is in the code orthogonal to $\mathscr{R}(m, 2m)$. This allows one to upperbound the dimension of C. The upper bound is of the same nature as those given in [2] and [3] in that any two designs whose ranks meet the bound are linearly equivalent. In this case that means that the bindary codes of the designs are isomorphic. Here is the result.

Theorem 2. *Let $\mathscr{D}$ be the design given by a difference set in an elementary abelian 2-group of order 2^{2m}. Then the 2-rank of $\mathscr{D}$ is at most $2^{2m-1} + 1 - \frac{1}{2}\binom{2m}{m}$. Moreover, any two such designs with 2-ranks meeting the bound have isomorphic binary codes.*

Observe that for $m = 2$ the upper bound is 6. This explains the fact that although there are three designs with parameters $(16, 6, 2)$ and all of them are difference sets in groups of order 16, only the one of rank six is a difference set in an elementary abelian 2-group: see [4]. The proposition also yields a proof of the uniqueness of a $(16, 6, 2)$ design of 2-rank six since the minimal-weight vectors of the code are precisely the vectors given by the blocks of the design. The two 16×16 Hadamard matrices of rank 8 cannot be produced by such a design since all three designs contain the all-one vector and hence can only produce matrices of 2-rank at most 7. It follows from rank considerations alone, therefore, that three of the five matrices are produced by $(16, 6, 2)$ designs and two are not. More precisely, neither of the two equivalence classes of 16×16 Hadamard matrices of rank 8 possess matrices with constant row sums while the other three equivalence classes do: moreover, in each of these three cases the design can be chosen to be a difference set design.

It must be said, however, that the bound does not appear to be useful for $m > 2$ although it is better than the bound coming from self-orthogonality, that bound being 2^{2m-1}. But this fact does, at least, imply that no Hadamard matrix of size 2^{2m} and rank 2^{2m-1} can be produced by an elementary Hadamard difference set.

4.3 The lower bound for the 2-rank of Hadamard designs. We choose to work with Hadamard 3-designs, but, of course, one immediately gets the ranks of the associated 2-designs from the rank of the 3-design. So, let $\mathscr{T}$ be a 3-$(4n, 2n, n-1)$ design with n even. We wish to lowerbound the dimension of $C_2(\mathscr{T}) = C$. We know that C is a self-orthogonal, doubly-even binary code and that the all-one vector is in C. Thus $C^{\perp}$ has only even-weight vectors and since given any two points of the design there is a block containing one but not the other, we know that $C^{\perp}$ has minimum weight at least 4. Using the sphere-packing bound gives the following result.

Theorem 3. *The 2-rank of a Hadamard 3-design of order $2n$, where n is a power of 2, is at least $3 + \log_2 n$.*

Theorem 3 proves half of the following result. The fact that the design of points and hyperplanes of the affine geometry has the bounding dimension is well-known and it is easy to show that in the case of equality one has the classical

design. This result was first observed by Hamada and Ohmori and we call it a 'rigidity' theorem because of the topological analogy; it says that among the structures $\mathscr{D}$ of a certain class the invariant $C_2(\mathscr{D})$ determines the structure uniquely. It is a rather easy example of such a theorem in design theory since it is really the dimension of the invariant that determines the structure—provided the dimension is as small as possible. The analogous result for translation planes [2, §6] is not as easy and, at present at least, more than the dimension of the invariant is necessary for the characterization.

Theorem 4. *The 2-rank of a design with parameters* $3\text{-}(2^{m+1}, 2^m, 2^{m-1}-1)$ *is at least* $m+2$ *with equality if and only if it is the design of points and hyperplanes in the affine geometry of dimension* $m+1$ *over* $\mathbf{F}_2$.

The binary code of the Hadamard $3\text{-}(2^{m+1}, 2^m, 2^{m-1}-1)$ design of smallest rank is, of course, the first-order Reed-Muller code. As we remarked in §3 we have not been able to find a Hadamard $3\text{-}(2^{m+1}, 2^m, 2^{m-1}-1)$ design whose binary code does not contain a copy of a first-order Reed-Muller code of the appropriate length and for $m = 3$ all the designs do, as we have seen. We thus ask the following:

Question 2. *Does the binary code of a* $3\text{-}(2^{m+1}, 2^m, 2^{m-1}-1)$ *design always contain a copy of* $\mathscr{R}(1, m+1)$*?*

One must be careful about what is being asked here. Even if the Hadamard 3-design is obtained using a design coming from a difference set in an elementary abelian 2-group one cannot expect the Reed-Muller code to be the one associated with that 2-group. However, if the answer to this question is yes, then the answer to Question 1 is yes also by the general discussion given above. We have checked that the designs coming from the four inequivalent bent functions, viewed as difference sets, of $\mathscr{R}(3, 6)$ each contain a copy of a first order Reed-Muller code. Only the quadratic bent function contains the 'natural' Reed-Muller code.

5. A class of $3\text{-}(4k^2, 2k^2, k^2-1)$ designs

5.1 The construction. The construction of Hadamard designs that we describe here was first discovered by Shrikhande and Singh [38], and then later by Goethals and Seidel [15]. Given a $2\text{-}(v, k, 1)$ design $\mathscr{D}$, let A be any $b \times v$ incidence matrix for $\mathscr{D}$, where b is the number of blocks of $\mathscr{D}$. Consider the symmetric matrix $B = AA^t - kI$, where I is the $b \times b$ identity matrix. Shrikhande and Singh observed that, when $v = 2k^2 - k$, B is an incidence matrix of a Hadamard $2\text{-}(4k^2-1, 2k^2, k^2)$ design, the complement of a Hadamard $2\text{-}(4k^2-1, 2k^2-1, k^2-1)$ design. Clearly, both these Hadamard designs are self dual, B being symmetric. Extending the complementary design yields a Hadamard 3-design and hence an equivalence class of Hadamard matrices of size $4k^2$ containing a symmetric matrix with constant entries on the diagonal. We note that it is quite easy to prove that a $2\text{-}(v, k, 1)$ design with incidence matrix A for which $AA^t - kI$ is an incidence matrix of a symmetric design must have $v = 2k^2 - k$. In this section we study the codes of the Hadamard 3-designs that can be constructed in this way, especially in relationship to those of the Steiner systems.

5.2 The associated codes. Given a $2\text{-}(2k^2-k, k, 1)$ design $\mathscr{D}$, let $\mathscr{E}$ be the

Hadamard 2-design given by the construction; then the order of $\mathscr{D}$ is $2k$, and the other of both $\mathscr{E}$ and its complementary design is k^2. Thus, for nontriviality, we take primes p dividing k.

Theorem 5. *Let $\mathscr{D}$ be a 2-$(2k^2-k, k, 1)$ design and $\mathscr{E}$ the symmetric $(4k^2-1, 2k^2, k^2)$ design that it produces. Then for any prime p dividing k, there is an exact sequence*

$$0 \to \mathrm{Hull}_p(\mathscr{D}) \to C_p(\mathscr{D}) \to C_p(\mathscr{E}) \to 0.$$

In particular,

$$\mathrm{rank}_p(\mathscr{E}) = \mathrm{rank}_p(\mathscr{D}) - \dim(\mathrm{Hull}_p(\mathscr{D})).$$

Proof. If A is an incidence matrix for $\mathscr{D}$, then A^t maps the space of row vectors, $\mathbf{F}^{2k^2-k}$, into the space of row vectors, $\mathbf{F}^{4k^2-1}$. Then $C_p(\mathscr{D})$ is mapped onto $C_p(\mathscr{E})$, and the kernel of the mapping is $C_p(\mathscr{D})^\perp$. Thus the kernel of the restriction of the mapping to $C_p(\mathscr{D})$ is the hull, $C_p(\mathscr{D}) \cap C_p(\mathscr{D})^\perp$.

Corollary 2. *If $\mathscr{T}$ is the Hadamard 3-design defined by $\mathscr{E}$, then*

$$\mathrm{rank}_p(\mathscr{T}) = \mathrm{rank}_p(\mathscr{D}) - \dim(\mathrm{Hull}_p(\mathscr{D})) + 1.$$

We next examine examples of the construction; this will amount to finding examples of the designs $\mathscr{D}$. We can then use the theorem to help determine the designs $\mathscr{E}$ that can occur, and hence the classes of Hadamard matrices that arise. We start with a well-known class.

5.3 Oval designs. Bose and Shrikhande [7] first described these designs in the geometrical setting that we will give here: let Π be a projective plane of order $n = 2k$ (i.e. a 2-$(n^2+n+1, n+1, 1)$ design) with an oval $\mathscr{O}$ (i.e. an $(n+2)$-arc, also called a hyperoval in the literature). Construct the design $W(\Pi, \mathscr{O})$ by taking for the point set $\mathscr{P}$ the set of all exterior (i.e. nonsecant) lines to $\mathscr{O}$, and for the block set $\mathscr{B}$ the set of all points of Π off the oval $\mathscr{O}$, with incidence given by the incidence in the ambient plane. Then $W(\Pi, \mathscr{O})$ is a 2-$(2k^2-k, k, 1)$ design, with the same order, $n = 2k$, as the ambient plane. Following Wertheimer [41], we will call these oval designs.

All known planes of even order have ovals, and, equally true, all known planes of even order n have n a power of 2. The $W(\Pi, \mathscr{O})$, particularly when Π is desarguesian and $\mathscr{O}$ is a regular oval, i.e. a conic plus nucleus, have been studied by many authors, and their p-ary codes, for p dividing k (but mostly for $p = 2$), have received some attention: see [23, 30, 41, 42]. In [30] it is shown, simply by considering the projection of the code of the plane onto the coordinate positions of the oval, that

$$\mathrm{rank}_p(W(\Pi, \mathscr{O})) \le \mathrm{rank}_p(\Pi) - (n+1).$$

If Π is desarguesian with $n = 2^m$, then $\mathrm{rank}_2(\Pi) = 3^m + 1$, and hence

$$\mathrm{rank}_2(W(\Pi, \mathscr{O}))) \le 3^m - 2^m.$$

If Π is nondesarguesian there is no known general formula for the dimension, although some bounds are known, in particular for translation planes: see [2, 3].

What can we say about the Hadamard designs and matrices that arise in this way? Before looking at special cases, we remark that Maschietti [34] rediscovered this construction in a slightly different context: for the points take all those

points of Π not on the oval, and for the blocks, construct one for each point of Π off $\mathscr{O}$, given as the sum (modulo 2) of the exterior lines through the given point. This gives the symmetric $(4k^2 - 1, 2k^2, k^2)$ design directly, and it is exactly the same as the design $\mathscr{E}$ we get from $W(\Pi, \mathscr{O})$. Also notice that each point on $\mathscr{O}$ defines a distinct resolution for $W(\Pi, \mathscr{O})$ by taking the secants through the point to define the parallel classes of blocks. It follows then from [15] that the derived Hadamard matrix has a matrix of constant row (and column) sum in its equivalence class, and hence that the designs we discussed in §4 are present.

In the case when Π is desarguesian with $n = 2^m$ and $\mathscr{O}$ is regular, we will use the customary notation $W(2^m)$ for $W(\Pi, \mathscr{O})$. Since all the known even-order planes have $n = 2^m$, all our codes will be binary for the remainder of this section. The first nontrivial case is for $n = 4$, $k = 2$. Here $W(4)$ is the unique $2 - (6, 2, 1)$ design, i.e. all 2-subsets of a 6-set. Clearly $C(W(4))$ has dimension 5, and has $\langle j \rangle$ for its hull, so $\operatorname{rank}_2(\mathscr{T}) = 5$. Since $\mathscr{T}$ is a 3-(16, 8, 3) design of rank five it must be (see §3) the design of points and hyperplanes of a 4-dimensional affine space over $\mathbf{F}_2$. Moreover, $C(\mathscr{T}) = \mathscr{R}(1, 4)$. This was first observed by Maschietti [34]: his Theorem 4.1 shows, however, that $C(\mathscr{T}) \neq \mathscr{R}(1, 2m)$ for $m \geq 3$. We had discovered this for $m = 3$ via computations with CAYLEY on the Birmingham University VAX (in the course of examining the codes coming from the Hadamard matrices in some detail).

For the case $m = 3$ we have that $n = 8$ and $k = 4$: the plane is still necessarily desarguesian and the oval regular. The design $W(8)$ is well known to be the familiar smallest Ree unital, i.e. a 2-(28, 4, 1) design. The corresponding Hadamard 3-design $\mathscr{T}$ is a 3-(64, 32, 15) design. The dimension of $C(W(8))$ is 19, and its hull has dimension 7 (see [2]) so $\operatorname{rank}(\mathscr{T}) = 13$, verifying again that $\mathscr{T}$ is not the design of points and hyperplanes of the 6-dimensional affine space over $\mathbf{F}_2$ and its binary code not $\mathscr{R}(1, 6)$. In fact, in order to compare this design with those mentioned in §4 with respect to bent functions, we computed the weight distribution of the code $C(\mathscr{T})$, viz.

$$x^0 + 588(x^{24} + x^{40}) + 1680(x^{28} + x^{36}) + 3654x^{32} + x^{64}.$$

The observation that the weight-24 vectors cannot form a 1-design (since 8 does not divide 588) shows that $\mathscr{T}$ cannot have a transitive automorphism group, and hence that it does not arise from a (64, 28, 12) design coming from a difference set.

For higher values of n the 3-designs were too large to examine with CAYLEY. However, computations related to oval designs made in [23, 30] suggest a general formula for the dimension of the hull in the case of a regular oval. These computations led to the following:

Conjecture 1. If $\mathscr{T}$ is a 3-design constructed from an oval design $W(\Pi, \mathscr{O})$ where Π is desarguesian of order 2^m, and $\mathscr{O}$ is regular, then $\operatorname{rank}_2(\mathscr{T}) = 2^{m-1}m + 1$.

The situation for nondesarguesian planes, or nonregular ovals in desarguesian planes, seems to be quite different. For example, the nonregular oval in the plane of order 16, i.e. the Hall oval (see [19, p. 177]), gives a 3-(256, 128, 63) design of 2-rank 65 (as opposed to that from the regular oval, which has 2-rank 33).

We remark that the Ree unital is by no means the only unital on 28 points; apart from the Hermitian unital, Brouwer [8] has constructed many others, and examined their codes. All of these give 3-(64, 32, 15) designs in the way described, but Brouwer's computations on the codes of the 2-designs show that none of these has rank less than 13. We have not checked these sporadic designs to try to determine whether or not they might provide a negative answer to Question 2.

5.4 Other examples. A class of examples of $2\text{-}(2k^2-k, k, 1)$ designs for all k would yield Hadamard matrices for all sizes of the form $4k^2$; we are not aware of such a class. Apart from $k = 2^m$ (discussed in the last section) we know of no further infinite classes; however, such designs are known to exist for all values of k through 8; see [17, pp. 408–417] and note that the design given for $k = 9$ appears to be in error. For $k = 3$, the 2-designs are the Steiner triple systems on 15 points, of which there are 80. For the codes to assist in classification, we need p to divide k, i.e. we must choose $p = 3$. The 3-rank of the Steiner triple systems is always 14 (see [14]) and the hull is $\langle j \rangle$, the one-dimensional code generated by the all-one vector. Thus, the 3-(36, 18, 8) designs will all have 3-rank 14, and their 3-ranks will not distinguish them. We do not know if the corresponding Hadamard matrices are equivalent or not: cf. [15], where a finer equivalence relation seems to be intended.

6. Hadamard matrices of size 24

6.1 Hadamard designs of small order. The number of equivalence classes of Hadamard matrices of size $4n \leq 24$ is known: there is only one equivalence class for each $n < 4$ and the designs are also unique (up to isomorphism) since the matrices have transitive automorphism groups. The sharply 5-fold transitive Mathieu group and the celebrated ternary Golay code occur for $n = 3$. For $n = 4$ there are five matrices, each with transitive automorphism groups, and hence five 3-designs and five 2-designs, as we discussed in §3.4. For $n = 5$ there are three matrices and six designs. In this section we examine the case $n = 6$; the binary and ternary codes arising from the 3-design (and hence form the matrices) will be self-dual and of maximum rank 12.

6.2 The binary self-dual [24, 12] codes. There are exactly 60 equivalence classes of Hadamard matrices of size 24 (see [21 and 26]) and, up to isomorphism, 130 Hadamard 3-(24, 12, 5) designs. Each such design produces a binary doubly-even [24, 12] code and also a self-dual ternary [24, 12] code (see §2). We look first at the binary case, since these codes have been classified. In fact, following Conway, Pless and Sloane show in [36] that there are precisely nine binary doubly-even [24, 12] codes. Here we first prove that three of the nine cannot occur as the binary code of a Hadamard 3-(24, 12, 5) design.

Proposition 9. *If C is a binary doubly-even [24, 12] code with the property that there exist seven coordinate places such that the projection onto these seven coordinates is the [7, 4] Hamming code, then C is not the binary code of a Hadamard 3-(24, 12, 5) design.*

Proof. Suppose that C is a binary doubly-even [24, 12] code that is generated by the characteristic functions of the blocks of a Hadamard 3-(24, 12, 5) design and let $\mathscr{S}$ be a set of seven coordinates with the property that C', the

projection of C to $\mathscr{S}$, is a [7, 4] Hamming code. We must now reach a contradiction. Every 3-subset of $\mathscr{S}$ is covered by five blocks of the design, each of which, viewed in C, is a weight-12 vector. These weight-12 vectors project to nonzero vectors of C'. Since two blocks of the design meet either in six points or not at all, the all-one vector of C' is the projection of at most one block. Therefore each of the other nonzero vectors of C' must be the projection of at least four blocks, since no 3-subset of $\mathscr{S}$ is covered by two of the fourteen weight-3 and weight-4 vectors of C'. But then there would be at least $4 \times 14 = 56$ blocks of the design. Since there are only 46, we have the contradiction.

Corollary 3. *At most six of the nine binary doubly-even* [24, 12] *codes can be the binary codes of Hadamard* 3-(24, 12, 5) *designs.*

Proof. Each of the two decomposable codes are built from a Hamming code and are thus eliminated by the proposition above. Moreover, B_{24} (in the notation of Pless and Sloane) is also so built (but with *glue*) and the proposition eliminates it also.

We have used CAYLEY on the Birmingham University VAX to classify the 130 Hadamard 3-(24, 12, 5) designs through their binary codes by finding the codes associated with each of the 60 equivalence classes of matrices. All of the six posssible [24, 12] codes appeared. The results are given in Table 1, where the equivalence classes of matrices are as listed in [21], with $1, 2, \ldots, 59$ representing $H1, H2, \ldots, H59$ and K representing the 60th class (found by Kimura). Also we use the notation of [36] for the six codes that occur. Each entry in the table also gives information about the equivalence class of the transpose of that entry; the superscript denotes the matrix equivalence class of the transpose, and the subscript denotes the 2-equivalence class of the transpose. Thus 5^9_E in the row corresponding to A_{24} indicates that $H5$ has code A_{24}, and that its transpose is in the class of $H9$ which has binary code E_{24}. The twelve classes that contain both a matrix and its transpose are entered in boldface, and the superscripts and subscripts are omitted.

TABLE 1. Binary codes of the 24×24 Hadamard matrices

Code	Hadamard Matrices
A_{24}	5^9_E, **10**, 18^{11}_C, 19^{12}_C, 36^{13}_D, 37^{14}_D, 51^{15}_F, 52^{16}_F
C_{24}	3^{17}_E, 11^{18}_A, 12^{19}_A, **20**, **22**, **25**, **27**, **33**, 38^{21}_D, 39^{24}_D, 40^{28}_D, 41^{30}_D, 53^{23}_F, 54^{26}_F, 55^{29}_F, 56^{31}_F
D_{24}	2^{34}_E, 7^{35}_E, 13^{36}_A, 14^{37}_A, 21^{38}_C, 24^{39}_C, 28^{40}_C, 30^{41}_C, 32^{42}_D, 42^{32}_D, 43^{44}_D, 44^{43}_D, **45**, **46**, **48**, 57^{47}_F
E_{24}	**1**, 9^5_A, 17^3_C, 34^2_D, 35^7_D, 49^4_F, 50^6_F, 58^8_G
F_{24}	4^{49}_E, 6^{50}_E, 15^{51}_A, 16^{52}_A, 23^{53}_C, 26^{54}_C, 29^{55}_C, 31^{56}_C, 47^{57}_D, **K**
G_{24}	8^{58}_E, **59**

6.3 *Remarks.* (1) G_{24} is the [24, 12] extended Golay code. The two Hadamard matrices, $H8$ and $H59$ (the latter representing the class of the Paley-Hadamard matrix) that generate this binary code have transitive automorphism groups and hence only one $3-(24, 12, 5)$ design is involved with each case. The Paley-Hadamard matrix also generates the extremal [24, 12, 9] ternary extended quadratic-residue code. There are two extremal [24, 12, 9] ternary codes (see [28] and note that we have checked that K's ternary code has weight-6 vectors and hence cannot be extremal) and curiously it is not $H8$ that generates the other, but $H8$'s transpose, $H58$. We do not have an explanation for this fact.

(2) Observe that 2-equivalence distinguishes among $H8$, $H58$ and $H59$ and between the two extremal [24, 12, 9] ternary codes, thus yielding a nongroup-theoretic proof that the two codes are inequivalent: if, for any arbitrary 24×24 Hadamard matrix H, both H and its transpose generate G_{24} then H is the Paley-Hadamard matrix: on the other hand if H generates G_{24} and its transpose does not, then H is $H8$ and its transpose is $H58$. In all, twelve 24×24 Hadamard matrices are characterized by their two 2-equivalence classes (of the matrix and its transpose) but note that 2-equivalence will not distinguish between $H18$ and $H19$, for example. It is possible that 2-equivalence and 3-equivalence, together with transpose information, would completely characterize each of the 24×24 Hadamard matrices. Since there are at most ten ternary self-dual [24, 12] codes (see [28], but note that the authors of that paper were not aware of the error in [21], nor of Kimura's matrix) there will be matrices (generating the codes C_{24} and D_{24}) that are both 2-equivalent and 3-equivalent.

(3) Since $H58$ and $H59$ both generate extremal ternary codes these codes do not have any weight-6 vectors at all. It follows from part 4 of Proposition 4 in §3 that the two associated 3-designs do not have special 6-tuples. Put another way, any three distinct blocks of either design intersect in at most five points.

(4) It is an easy computational matter to decide the 2-equivalence class of a 3-(24, 12, 5) design, or of a 24×24 Hadamard matrix, since the six [24, 12] binary codes involved have different weight distributions—indeed, different numbers of weight-4 vectors.

(5) The next binary case to consider is order 8, i.e., 3-(32, 16, 7) designs. This case has been considered intractable by combinatorialists, since there are millions of these designs [35]. But the [32, 16] binary doubly-even codes have been classified [9] and, since the binary code of a 32×32 Hadamard matrix is doubly-even (but not necessarily self-dual), it follows (see [32]) that it is contained in one of the 85 binary doubly-even [32, 16] codes. Even an examination of the five extremal binary doubly-even [32, 16, 8] codes might prove interesting. In this case we have only 2-equivalence.

(6) The 20×20 (or 3-(20, 10, 4)) case must be treated over $\mathbf{F}_5$. Leon, Pless and Sloane [29] have investigated the self-dual codes over $\mathbf{F}_5$, but the [20, 10]'s were not classified. It is possible that the three designs and three matrices reduce to two 5-equivalence classes. The 28×28 case will have to be treated over $\mathbf{F}_7$; we do not have any coding-theoretic information on this case, but Tonchev [40] has classified those matrices having transitive automorphism groups with the help of coding theory; there are seven. It appears, however, that the number of matrices goes up sharply and 487 have been found: see [24 and 25]; Hiroshi Kimura has conjectured that there are no others. Clearly much

more computer work could, and probably should, be undertaken.

We have, obviously, left many questions unanswered, but we hope the results we have presented will stimulate others to rethink the subject in coding-theoretic terms and we believe that there is further progress to be made in this direction—and that it will come before the sesquicentennial.

References

1. E. F. Assmus, Jr., *On the theory of designs*, Surveys in Combinatorics, 1989 (J. Siemons, Ed.), London Math. Soc. Lecture Note Series no. 141, Cambridge Univ. Press, 1989.
2. E. F. Assmus, Jr. and J. D. Key, *Affine and projective planes*, Discrete Math. **83** (1990), 161–187.
3. ——, *Translation planes and derivation sets*, J. Geom. **37** (1990), 3–16.
4. E. F. Assmus, Jr. and Chester J. Salwach, *The* (16, 6, 2) *designs*, Internat. J. Math. Sci. **2** (1979), 261–281.
5. Bashkar Bagchi and N. S. Narasimha Sastry, *Even order inversive planes, generalized quadrangles and codes*, Geom. Dedicata **22** (1987), 137–147.
6. Vasanti N. Bhat and S. S. Shrikhande, *Non-isomorphic solutions of some balanced incomplete block designs*. I, J. Combin. Theory **9** (1970), 174–191.
7. R. C. Bose and S. S. Shrikhande, *On the construction of sets of mutually orthogonal latin squares and the falsity of a conjecture of Euler*, Trans. Amer. Math. Soc. **95** (1960), 191–209.
8. A. E. Brouwer, *Some unitals on* 28 *points and their embeddings in projective planes of order* 9, Geometries and Groups (M. Aigner and D. Jungnickel, Eds.), Lecture Notes in Math., vol. 893, Springer-Verlag, Berlin and New York, 1981, pp. 183–188.
9. J. H. Conway and Vera Pless, *On the enumeration of self-dual codes*, J. Combin. Theory Ser. A **28** (1980), 26–53.
10. P. Delsarte, *A geometric approach to a class of cyclic codes*, J. Combin. Theory **6** (1969), 340–358.
11. J. F. Dillon, Private communication.
12. ——, *Elementary Hadamard difference sets*, Congr. Numer. **14** (1975), 237–249.
13. J. F. Dillon and J. R. Schatz, *Block designs with the symmetric difference property*, (Robert L. Ward, Ed.), Proc. NSA Mathematical Sciences Meetings, The United States Government, 1987, pp. 159–164.
14. J. Doyen, X. Hubaut, and M. Vandensavel, *Ranks of incidence matrices of Steiner triple systems*, Math. Z. **163** (1978), 251–259.
15. J. M. Goethals and J. J. Seidel, *Strongly regular graphs derived from combinatorial designs*, Canad. J. Math. **22** (1970), 597–614.
16. Ken Grey, *Further results on designs carried by a code*, Ars Combin. **26B** (1988), 133–152.
17. Marshall Hall, Jr., *Combinatorial theory*, 2nd ed., Wiley, 1986.
18. N. Hamada and H. Ohmori, *On the BIB design having the minimum p-rank*, J. Combin. Theory Ser. A **18** (1975), 131–140.
19. J. W. P. Hirschfeld, *Projective geometries over finite fields*, Oxford, 1979.
20. D. R. Hughes and F. C. Piper, *Design theory*, Cambridge Univ. Press, 1985.
21. Noboru Ito, Jeffrey S. Leon, and Judith Q. Longyear, *Classification of* 3-(24, 12, 5) *designs and* 24*-dimensional Hadamard matrices*, J. Combin. Theory Ser. A **31** (1981), 66–93.
22. Dieter Jungnickel and Vladimir Tonchev, *On symmetric and quasi-symmetric designs with the symmetric difference property and their codes*, J. Combin. Theory. Ser. A (to appear).
23. J. D. Key and K. Mackenzie, *Ovals in the designs* $W(2^m)$, Tech. Rep. 568, Department of Mathematical Sciences, Clemson Univ., November 1988; Ars Combinatoria (to appear).
24. Hiroshi Kimura, *Classification of Hadamard matrices of order* 28 *with Hall sets and new matrices*, Preprint.

25. ____, *On equivalence of Hadamard matrices*, Hokkaido Math. J. **17** (1988), 139–146.

26. ____, *New Hadamard matrix of order* 24, Graphs and Combinatorics **5** (1989), 235–242.

27. Eric S. Lander, *Symmetric designs: an algebraic approach*, London Math. Soc. Lecture Notes Series, no. 74, Cambridge Univ. Press, 1983.

28. Jeffrey S. Leon, Vera Pless, and N. J. A. Sloane, *On ternary self-dual codes of length* 24, IEEE Trans. Inform. Theory **IT-27** (1981), 176–180.

29. ____, *Self-dual codes over* GF(5), J. Combin. Theory Ser. A **32** (1982), 178–194.

30. K. Mackenzie, *Codes of designs*, Ph.D. thesis, Univ. of Birmingham, 1989.

31. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, 1983.

32. F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, *Good self-dual codes exist*, Discrete Math. **3** (1972), 153–162.

33. Henry B. Mann, *Addition theorems: The addition theorems of group theory and number theory*, Interscience Tracts in Pure and Appl. Math., 18, Interscience, a division of Wiley, 1965.

34. A. Maschietti, *c-sets, hyperovals and Hadamard designs*, Preprint.

35. C. W. Norman, *Nonisomorphic Hadamard designs*, J. Combin. Theory Ser. A **21** (1976), 336–344.

36. Vera Pless and N. J. A. Sloane, *Binary self-dual codes of length* 24, Bull. Amer. Math. Soc. **80** (1974), 1173–1178.

37. C. J. Salwach, *Planes, biplanes, and their codes*, Amer. Math. Monthly **88** (1981), 106–125.

38. S. S. Shrikhande and N. K. Singh, *On a method of constructing incomplete block designs*, Sankhyā Sér. A **24** (1962), 25–32.

39. J. A. Todd, *A combinatorial problem*, J. Math. Phys. **12** (1933), 321–333.

40. Vladimir D. Tonchev, *Hadamard matrices of order* 28 *with automorphisms of order* 7, J. Combin. Theory Ser. A **40** (1985), 62–81.

41. M. A. Wertheimer, *Oval designs in quadrics*, Contemp. Math. **111** (1990), 287–297.

42. ____, *Designs in quadrics*, Ph.D. thesis, Univ. of Pennsylvania, 1986.

DEPARTMENT OF MATHEMATICS, LEHIGH UNIVERSITY, BETHLEHEM, PENNSYLVANIA 18015

DEPARTMENT OF MATHEMATICAL SCIENCES, CLEMSON UNIVERSITY, CLEMSON, SOUTH CAROLINA 29634