

Block Designs with the Symmetric Difference Property

J. F. DILLON

AND

J. R. SCHATZ

Department of Defense

ABSTRACT

If f is the characteristic function of a difference set in F^{2m} , $F = GF(2)$, then the words of minimum weight in the code spanned by f and the 1st order Reed-Muller code give rise to a Hadamard design $R(f)$ with parameters $(v, k, \lambda) = (2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$, the same as those of the translate design. W. M. Kantor and others have investigated block designs with the property that the symmetric difference of any three blocks is itself either a block or the complement of a block.

In this paper we show that any design with this symmetric difference property is, up to complementation, equivalent to an $R(f)$ design.

1. INTRODUCTION

A combinatorial *block design* with parameters (v, k, λ, r, b) is a collection D of b k -subsets (blocks) of a v -set V (points) such that any pair of points is contained in exactly λ blocks and any single point is contained in exactly r blocks. Such a design is completely specified by its *incidence matrix* whose rows and columns are indexed by the blocks and points respectively, an entry in the matrix being 1 or 0 according to whether the corresponding block and point are incident or not incident. A *symmetric block design* is a block design with $b = v$; that is, the number of blocks equals the number of points. Symmetric designs are characterized by the property that the number of points in the intersection of any two blocks is independent of the pair of blocks chosen. In fact, if D is symmetric then any pair of blocks must meet in exactly λ points. The symmetric design arises from a *difference set* if the incidence matrix is of the form $[f(g_j - g_i)]$ for some $(0, 1)$ -valued function f on a group $G = \{g_0, g_1, g_2, \dots, g_{v-1}\}$. In this case the blocks of the design are the v translates in G of the subset D of which f is the characteristic function. These facts may be found in any good combinatorics book; e.g. [3].

A symmetric design is said to have the *symmetric difference property* if the symmetric difference of any three blocks is either a block or the complement of a block. A design with this property is called an *SDP-design*. In this paper we determine all symmetric designs with the symmetric difference property. Our characterization of *SDP*-designs employs several well-known properties of difference sets D in F^{2m} , $F = GF(2)$. We shall identify these with their characteristic functions which in the context of Coding Theory are sometimes called bent functions and which are characterized as being those functions on F^{2m} which are of covering radius distance from the 1st order Reed-Muller code $RM(1, 2m)$. In particular, associated with any difference set f_D there are *two* symmetric designs, both having parameters

$$v = 2^{2m}, k = 2^{2m-1} - 2^{m-1}, \lambda = 2^{2m-2} - 2^{m-1}. \quad (*)$$

We denote by $T(f_D)$ the usual translate design which has incidence matrix

$$[f_D(x+y)]$$

and we denote by $R(f_D)$ the design whose incidence matrix has rows given by the words of minimum weight in the code spanned by f_D and $RM(1, 2m)$.

Our main result asserts that the symmetric difference property precisely characterizes the $R(f_D)$ designs. Specifically, we prove the following theorem and corollaries.

THEOREM. *Let D be any symmetric (v, k, λ) block design with $k \leq v/2$, $v > 2$. D has the symmetric difference property if and only if D is isomorphic to $R(f_D)$ for some difference set D .*

COROLLARY 1. *Let D be any symmetric design with the Hadamard parameters (*) and let M be an incidence matrix for D . If the 2-rank of M is $2m + 2$ and the row space of M over $GF(2)$ contains the all-1 vector then D is isomorphic to $R(f_D)$ for some difference set D .*

COROLLARY 2. *Let D be a difference set in F^{2m} . The incidence matrix $[T(f_D)]$ of the design $T(f_D)$ has rank $2m + 2$ if and only if there is a difference set E in F^{2m} such that $T(f_D)$ is isomorphic to $R(f_E)$ or its complement.*

The symmetric difference property was introduced by W. M. Kantor [4]. Kantor derived a number of necessary conditions on designs that satisfy the symmetric difference property. He proved that an *SDP*-design, or its complement, must have the Hadamard parameters (*), and he associated an incidence geometry with each such design. The primary examples of *SDP*-designs that Kantor studied and which he called *symplectic designs* correspond to the designs $R(f_D)$ obtained when f_D is a quadratic form on F^{2m} . In this case the (± 1) -incidence matrix may be taken to be

$$\otimes^m \begin{bmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \\ 1 & 1 & 1 & - \end{bmatrix}$$

and the difference set is the well-known Menon-Turyn set obtained from singleton sets in 4-groups via the tensor product of Hadamard matrices.

SDP-designs were also the topic of a recent doctoral dissertation [1] in which P. J. Bush studied *SDP*-designs on 64 points with the aim of finding all such designs. The examples of *SDP*-designs that Bush investigated were constructed using inductive methods. The complete classification of *SDP*-designs on 64 points is now a consequence of the main theorem of the present paper together with the known theory of $R(f)$ designs. It is easy to see [5] that $R(f_D)$ and $R(f_E)$ are isomorphic designs if and only if f_D and f_E are weakly affinely equivalent functions; i.e.

$$\exists \sigma \in GA(2m, 2) \ni f_D^\sigma = f_E \pmod{RM(1, 2m)}.$$

Rothaus [7] proved that up to weak affine equivalence there are exactly four distinct bent functions on F^6 . Hence, there are exactly four distinct *SDP*-designs on 64 points.

We will henceforth assume that the reader is familiar with the basic definitions and facts on codes and designs. If D is a symmetric design then blocks of D are denoted by capital letters. An incidence matrix for D is a $v \times v$ matrix in which the rows are indexed by the blocks of D and the columns are indexed by the points and the (B, p) entry is 1 if $p \in B$, 0 otherwise. A block B is identified with the corresponding row of the incidence matrix. This row is called an incidence vector of B . The symmetric difference of blocks corresponds to the mod 2 sum of their incidence vectors and is therefore denoted by addition. A function f on F^{2m} is identified with the incidence vector $(f(0), f(1), \dots, f(2^{2m}-1))$ where $f(i)$ denotes the value of f on the binary expansion of i . The code $C(f)$ is defined to be the space spanned by the incidence vector of f and the first order Reed-Muller code $RM(1, 2m)$.

2. MAIN RESULTS

The proof of the main theorem requires one lemma. This lemma is actually a reformulation of a familiar result from geometry. It may also be found as Problem 41 on p. 28 of [6] where it is stated in terms of the extended Hamming Code which is the dual of $RM(1, m)$.

LEMMA. *If a binary linear code C has the same parameters and weight distribution as the first order Reed-Muller code $RM(1, m)$ then C is equivalent to $RM(1, m)$.*

Proof. Let C be a code of length 2^m , dimension $m+1$, minimum distance 2^{m-1} and weight distribution

$$A_0 = 1 = A_{2^m}, \quad A_{2^{m-1}} = 2^{m+1} - 2.$$

Form a new code C' by first selecting all codewords of C with a zero in the first coordinate, and then deleting this zero coordinate from each codeword. Then C' has

the same parameters as the binary simplex code $S(m)$: length $n = 2^m - 1$, dimension $k = m$, minimum distance $d = 2^{m-1}$, and weight distribution

$$B_0 = 1, B_{2^{m-1}} = 2^m - 1.$$

Let M be an $m \times n$ generator matrix for C . Since the dual of $S(m)$ has minimum weight 3 so must the dual of C , and so the columns of M must be distinct and nonzero. The permutation which places the columns of M in lexicographic order defines an equivalence between C and $S(m)$. Moreover, it is now clear that C is equivalent to $RM(1, m)$.

We are now in a position to prove the Theorem.

Assume that D has the symmetric difference property. Denote the all-1 vector of length v by 1 . Following Kantor [4], we define a hyperplane to be any point set of the form $B+C$, or $1+B+C$, where $B, C \in D, B \neq C$. First we prove that the number of hyperplanes is $2(v-1)$. Note that for any fixed hyperplane H every block B determines a unique block C such that $H = B+C$ or $H = 1+B+C$. Now consider the set

$$T = \{(H, B, C): H \text{ is a hyperplane, } B, C \in D, H = B+C \text{ or } H = 1+B+C\}.$$

Suppose there are N distinct hyperplanes. Then there are N choices for H , and v choices for B , so $|T| = Nv$. On the other hand, there are v choices for B , $v-1$ choices for C and 2 choices for H . Hence $|T| = 2v(v-1)$ and $N = 2(v-1)$.

Next we prove that there are three blocks whose sum is the complement of a block. Assume that this is not the case. Then it follows that the intersection of any three blocks has constant cardinality. But in this case we see that the derived design D_B on any fixed block B has the property that the intersection of any two blocks has constant cardinality. Thus, D_B must be a symmetric design. Equating the number of points and blocks in D_B we obtain $k = v-1$. This is a contradiction because $k \leq v/2$ and $v > 2$. Hence, there exist three blocks whose sum is the complement of a block, and so the space spanned by the blocks of D contains the all-1 vector.

Now let C denote the collection of hyperplanes together with 0 and 1 . We claim that C is a binary linear code and that C is equivalent to $RM(1, 2m)$ for some m . If B, C, D , and E are blocks and $B \neq C, D \neq E$, and $B+C \neq D+E$ then

$$(B+C) + (D+E) = (B+C+D) + E = F+E \text{ or } 1+F+E$$

for some block F . Hence, the sum of two hyperplanes is a hyperplane. Thus, C is a code and $|C| = 2(v-1) + 2 = 2v$. It follows that v is a power of 2. A familiar result of H.B. Mann [2] asserts that if D is a nontrivial symmetric (v, k, λ) design in which v is a power of 2 and $k \leq v/2$ then D has parameters

$$v = 2^{2m}, k = 2^{2m-1} - 2^{m-1}, \lambda = 2^{2m-2} - 2^{m-1}$$

for some m . Now $|C| = 2^{2m+1}$ so C has dimension $2m+1$. Also, every hyperplane has $2(k-\lambda) = 2^{2m-1}$ points, so C has the weight distribution of $RM(1, 2m)$. Thus, by the Lemma, C is equivalent to $RM(1, 2m)$.

Let C' denote the code generated by all the blocks in D , and fix a block B_0 in D . Then C' contains:

- 1) 2^{2m} codewords of the form $B, B \in D$,
- 2) 2^{2m} codewords of the form $1+B, B \in D$,
- 3) $2^{2m}-1$ codewords of the form $B_0+B, B \in D, B \neq B_0$,
- 4) $2^{2m}-1$ codewords of the form $1+B_0+B, B \in D, B \neq B_0$,
- 5) 0 and 1.

The codewords of type 3 and 4 account for all hyperplanes so C' contains C . Moreover, the symmetric difference property insures that every codeword in C' is among the codewords listed above, so C' has dimension $2m+2$. Hence, C' coincides with the code spanned by C and B_0 .

Denote the permutation of coordinate positions which maps C to $RM(1, 2m)$ by π . It is clear that B_0 meets every hyperplane in C in $2^{2m-2} - 2^{m-1}$ points or 2^{2m-2} points. Therefore, by the geometric characterization of elementary Hadamard difference sets [2] we see that the image of B_0 under π is the incidence vector of the characteristic function f_D of a difference set D in F^{2m} . Moreover, π defines an equivalence between the code C' and the code $C(f_D)$ spanned by f_D and $RM(1, 2m)$. In particular, the minimum weight codewords of C' are mapped onto the minimum weight codewords of $C(f_D)$ by π . Thus, D is isomorphic to $R(f_D)$.

Conversely, we must show that every design $R(f_D)$ has the symmetric difference property. But every block of $R(f_D)$ has a characteristic function of the form $f_D(y) + x \cdot y + u_x$ where x is fixed, y varies, and u_x is 0 or 1. Hence, the sum of the three blocks $f_D(y) + a \cdot y + u_a$, $f_D(y) + b \cdot y + u_b$, and $f_D(y) + c \cdot y + u_c$ is clearly a block or the complement of a block. This completes the proof of the Theorem. \blacksquare

We shall prove Corollary 1 by showing that D has the symmetric difference property. Let C be the code generated by the rows of M . C contains 2^{2m} codewords of weight $2^{2m-1} - 2^{m-1}$ corresponding to the blocks of D and 2^{2m} codewords of weight $2^{2m-1} + 2^{m-1}$ corresponding to the complements of the blocks. Fix a block B_0 . Then, for any block $B \neq B_0$ we obtain a codeword B_0+B of weight 2^{2m-1} . Moreover, the complement of such a codeword has weight 2^{2m-1} . If $B_0+A = B_0+B+1$ then $A+B = 1$, which is a contradiction. Hence C has $2^{2m+1} - 2$ distinct codewords of weight 2^{2m-1} . Since C has rank $2m+2$ we have now accounted for all codewords in C .

Now it is easy to see that the codewords of weight 2^{2m-1} together with 0 and 1 form a subcode of C . For, the sum of any two codewords of the form $B_0+B+\varepsilon$, ($\varepsilon = 0$ or 1) clearly has weight 2^{2m-1} . Hence, given any three blocks A, B, C in D there exists a block D such that

$$(B_0+A) + (B_0+B) + (B_0+C) = (B_0+D) + \varepsilon,$$

where ε is 0 or 1. Therefore, $A+B+C = D+\varepsilon$, so D has the symmetric difference property, and the result follows.

Finally Corollary 2 follows from Corollary 1 and the elementary observations that if D is any difference set in F^{2m} then the incidence matrix of the translate design $T(f_D)$ has row space containing the all 1 vector while the incidence matrix of $R(f_D)$ has rank $2m + 2$. ■

REFERENCES

1. P. J. BUSH, "On 2-Designs With The Symmetric Difference Property," Thesis, Northeastern U., 1980.
 2. J. F. DILLON, "Elementary Hadamard Difference Sets," Thesis, U. of Maryland, 1974.
 3. MARSHALL HALL, JR., "Combinatorial Theory," 2nd edition, Wiley, 1986.
 4. W. M. KANTOR, Symplectic Groups, Symmetric Designs and Line Ovals, *J. Algebra* 33 (1975).
 5. W. M. KANTOR, Exponential Numbers of Two-Weight Codes, Difference Sets and Symmetric Designs, *Discrete Math.* 46 (1983).
 6. F. J. MACWILLIAMS AND N. J. A. SLOANE, "The Theory of Error-Correcting Codes," North Holland, 1977.
 7. O. S. ROTH AUS, On Bent Functions, *J. Combinatorial Theory (A)* 20 (1976).
-