ELEMENTARY HADAMARD DIFFERENCE SETS

by

John F. Dillon

Dissertation submitted to the Faculty of the Graduate School
of the University of Maryland in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
1974

APPROVAL SHEET

Title of Thesis : Elementary Hadamard Difference Sets

Name of Candidate : John F. Dillon

Doctor of Philosophy, 1974

Thesis and Abstract Approved : James C. Owings, Jr.

James C. Owings, Jr.
Associate Professor
Department of Mathematics

Date Approved : April 22, 1974

ABSTRACT

Title of Thesis: Elementary Hadamard Difference Sets

John F. Dillon, Doctor of Philosophy, 1974

Thesis directed by: Professor James C. Owings, Jr.

This paper is primarily a study of difference sets in elementary abelian 2-groups. It is, however, somewhat wider in scope and includes an exposition of the fundamental notions relating to the more general topics of difference sets and the Fourier analysis of Boolean functions.

A (v,k,λ,n)-difference set with $v=4n$, called a Hadamard difference set, necessarily has parameters of the form

$$(v,k,\lambda,n) = (4N^2,\ 2N^2-N,\ N^2-N,\ N^2) \quad \text{or} \quad (4N^2,\ 2N^2+N,\ N^2+N,\ N^2).$$

Every (nontrivial) difference set with v a power of 2 is Hadamard. A <u>partial spread</u> for a group G of order M^2 is a family of pairwise disjoint (except for 0) subgroups of order M.

THEOREM 1. <u>Let</u> $\{H_1, H_2, \ldots, H_r\}$ <u>be a partial spread for</u> G. $D = (\cup H_i)\setminus\{0\}$ (resp. $E = \cup H_i$) <u>is a difference set if and only if</u> G <u>has order</u> $4N^2$ <u>and</u> $r = N$ (resp. $N+1$). <u>These difference sets are Hadamard with parameters</u>

$$(4N^2,\ 2N^2-N,\ N^2-N,\ N^2) \text{ and } (4N^2, 2N^2+N,\ N^2+N,\ N^2), \text{ respectively.}$$

We call the difference sets D and E <u>partial spread difference sets</u> of types $PS^{(-)}$ and $PS^{(+)}$, respectively.

THEOREM 2. a) *The groups*

Z_4, $Z_2 \oplus Z_2 \oplus Z_4$, $Z_6 \oplus Z_6$, $Z_4 \oplus Z_4$, *and* Z_2^{2m}, $m \geq 1$,

all have $PS^{(-)}$ *difference sets.* b) *All but the first three of these groups have* $PS^{(+)}$ *difference sets.* c) *No other abelian group has a partial spread difference set.*

As a special case of our construction we obtain the family of difference sets in elementary abelian 2-groups given by

THEOREM 3. *The points* (resp. *nonzero points*) *lying on any* $2^{m-1}+1$ (resp. 2^{m-1}) *lines through the origin constitute a difference set in the affine plane* $L \oplus L$, $L = GF(2^m)$.

P. Kesava Menon and R. J. Turyn have shown that the set of zeros of the quadratic form

$$\Psi_m = X_1X_{m+1} + X_2X_{m+2} + \ldots + X_mX_{2m}$$

over Z_2 constitutes a difference set in Z_2^{2m}. We show that Turyn's "other" elementary difference set is equivalent to a partial spread difference set (given by Theorem 3) while Kesava Menon's "other" difference set is equivalent to the quadratic set which is itself a partial spread difference set (not given by Theorem 3) precisely when $m=1$ or m is even.

More generally, we define a *Pall partition* for a quadratic form over a field F to be a partition of the zeros of the form into pairwise disjoint (except for 0) maximal isotropic (singular if char F=2) F-linear subspaces.

THEOREM 4. a) *There exists a Pall partition for every nonsingular quadratic form over* $GF(2^r)$, *except for those equivalent to*

$$\Psi_m = X_1X_{m+1} + X_2X_{m+2} + \dots + X_mX_{2m}$$

with $m>1$ *odd, in which case no such partition exists.* b) *If* $m>1$ *is odd, then there does not exist a Pall partition for* Ψ_m *over any field whatsoever.*

The second part of this theorem generalizes a recent result of L. Couvillon.

It has been shown by J. A. Maiorana and R. L. McFarland, independently, that the quadratic difference set associated with the form

$$\Psi_m = X_1X_{m+1} + X_2X_{m+2} + \dots + X_mX_{2m}$$

on Z_2^{2m} may be generalized by replacing Ψ_m by a function on $Z_2^m \oplus Z_2^m$ of the form

$$f(X,Y) = \pi(X) \cdot Y + g(X),$$

where π is an arbitrary permutation of Z_2^m and g is an arbitrary function from Z_2^m to Z_2. We call this family of difference sets FAMILY $\mathcal{M}$.

THEOREM 5. *For* $m>3$ *there exist difference sets in* Z_2^{2m} *which are not equivalent to any difference set in* FAMILY $\mathcal{M}$.

We obtain this result and others on inequivalence by employing certain affine invariants which we develop here and which are useful in the more general study of Boolean functions.

ACKNOWLEDGEMENTS

It is a pleasure for me to acknowledge the generous assistance, guidance and encouragement provided by the following three men of mathematics: Professor David P. Roselle, Louisiana State University, who taught me how to do combinatorics and who started me out on the path toward my degree; Dr. Alvin I. Thaler, National Science Foundation, who guided me through some of the obstacles along that path; and Professor James C. Owings, Jr., University of Maryland, who led me to the path's end and who was particularly helpful during the preparation of this thesis.

To my wife, Marilyn, and my family I express my appreciation of their patience and encouragement.

I acknowledge the cooperation and support afforded by the Department of Defense, Fort George G. Meade, Maryland.

Finally, I am indebted to Miss Nancy Gartrell of the Department of Defense for her cheerful and expert typing of this thesis.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

Among the most beautiful of all combinatorial objects is the difference set, which is, at first blush, but a subset of a group with a certain peculiar property — namely, that all nonidentity group elements may be represented in the same number of ways as a difference of two elements of that subset. A closer examination, however, bares the equivalent property that the translates of that subset by all the group elements constitute a symmetric balanced incomplete block design, known also as a (v,k,λ)-configuration. Unlike many designs, those arising from a difference set have the desirable property of being completely determined by a single block (and the group which contains it). For this reason difference sets play a major role in the design of experiments [10].

Another oft exploited feature of a difference set is its characteristic function (and variations thereof) which is defined on the group and takes the value 1 on the difference set and 0 off the difference set. The autocorrelation function has just two levels, being uniformly small on the nonidentity elements of the group; consequently difference sets find much use in signal analysis and design [25].

Since any two translates of the characteristic function differ in the same number of places, these functions may be used as codewords in an error-correcting code. In certain cases functions corresponding to difference sets can be adjoined to a simple code to produce a much larger code with a relatively small loss in error-correcting power [3].

These applications may be considered as exploitations of the incidence matrix of the design of the difference set. It sometimes happens that the incidence matrix, with its 0's replaced by -1's, is Hadamard. This opens up another world of applications. We refer the interested reader to [26] for a comprehensive survey of Hadamard matrices.

The k-subset D of the (not necessarily abelian, but denoted additively) group G of order v is called a (v,k,λ,n)-difference set if every nonidentity element of G may be represented in exactly λ ways as the difference of two elements of D. The parameter n is defined to be equal to $k-\lambda$. If D is such a set then for any automorphism α of G and any element g of G, the set $D^{\alpha}+g$ is also a difference set with the same parameters. Two difference sets which are related in this way are said to be equivalent. In particular, if $D^{\alpha}+g = D$, the (nonidentity) automorphism α of G is called a multiplier of the difference set D. A multiplier which, for some integer t, maps each element g of G to tg, is called a numerical multiplier. The multipliers of a difference set D in G constitute a subgroup of the automorphism group of G and equivalent difference sets have isomorphic multiplier groups; equivalent cyclic difference sets have the same multipliers. H. B. Mann and R. L. McFarland [14] have shown that every multiplier of a difference set must fix some translate of that difference set. A very powerful theorem due to Marshall Hall, Jr. and several generalizations [15] provide multipliers for difference sets in a variety of groups. These multipliers, together with the result of Mann and McFarland, may then be used to establish the existence or nonexistence of a difference set (in the given group) with specified parameters or to test the equivalence of two difference sets in the same group. Unfortunately, all of the multipliers produced by these theorems are numerical multipliers — there is no general "Multiplier Theorem" for difference sets in groups which have no (nontrivial) numerical automorphisms.

Such groups include the elementary abelian 2-groups. The lack of a multiplier theorem for these groups may be one of the reasons that they have been largely ignored as a source of difference sets. In 1955 R. H. Bruck [4] gave an example of a (16,6,2,4)-difference set in the group Z_2^4. The early 60's saw a brief shower of attention given these groups. In 1960 P. Kesava Menon [18] gave a construction which yields for each $m \geq 1$ a difference set with parameters

$$(*) \qquad (v,k,\lambda,n) = (4^m,\ 2\cdot 4^{m-1}-2^{m-1},\ 4^{m-1}-2^{m-1},\ 4^{m-1})$$

in the elementary group Z_2^{2m}. In 1962 Kesava Menon [19] showed that any (v,k,λ,n)-difference set with $v=4n$ must have parameters of the form

$$(**) \qquad (v,k,\lambda,n) = (4N^2,\ 2N^2-N,\ N^2-N,\ N^2) \text{ or } (4N^2,\ 2N^2+N,\ N^2+N,\ N^2).$$

He observed that such difference sets D_1 in a group G_1 and D_2 in a group G_2 can be combined to produce a difference set of this type in the direct sum $G_1 \oplus G_2$. In particular, the trivial (singleton) difference set in $K_4 = Z_2^2$ may be used to produce via this process a (nontrivial) difference set in any group K_4^m. In 1965 R. J. Turyn [24] observed that the (± 1)-incidence matrix of a difference set with parameters of the form (**) is a Hadamard matrix and the composition theorem of Menon is a direct consequence of the fact that the Kronecker product of Hadamard matrices is again Hadamard. Consequently, such sets are now called Hadamard difference sets. Turyn also gave a new construction which provides another difference set in each group Z_2^{2m}. Also in 1965 H. B. Mann [13] showed that any nontrivial (v,k,λ)-configuration (and, in particular, any difference set) having v a power of 2 must have parameters of the form (**). Thus a difference set can exist in a 2-group only if it has square order, and any difference set (or its complement) in Z_2^{2m} must have parameters (*).

In unpublished work (completed in 1966 but only recently submitted for publication) O. S. Rothaus [22] generalized the Menon-Turyn construction and obtained, for each $m>2$, a "large" number of pairwise inequivalent difference sets in Z_2^{2m}. This construction was further generalized by J. A. Maiorana (also unpublished) around 1969. In 1973 R. L. McFarland [16] gave a very general construction for difference sets in certain non-cyclic groups. This construction applies to the groups Z_2^{2m}, in which case the difference sets produced are equivalent to those obtained by Maiorana. We thus accord to this family of difference sets the name FAMILY $\mathcal{M}$. It is a truly remarkable fact that every elementary Hadamard difference set known (before now!) is equivalent to one in FAMILY $\mathcal{M}$. Indeed, in [16] McFarland asks if <u>every</u> difference set in Z_2^{2m} is equivalent to one given by his construction.

This thesis provides a negative answer to McFarland's question. Indeed, our main result (Chapter 5) is a new construction which produces, for each $m>3$, a "large" number of pairwise inequivalent difference sets in Z_2^{2m} "most" of which are not equivalent to any difference set in FAMILY $\mathcal{M}$.

This paper is primarily a study of difference sets in elementary abelian 2-groups. It is, however, somewhat wider in scope and includes an exposition of the fundamental notions relating to the more general topics of difference sets and Boolean functions.

Chapter 2 contains a rather general discussion of difference sets and their incidence matrices with the emphasis being on Hadamard difference sets. In the last section of Chapter 2 we introduce the (complex) group algebra and its Fourier transform and derive quickly the useful characterizations of a difference set in terms of its "autocorrelation" and its Fourier transform.

We are mainly concerned with difference sets in elementary abelian 2-groups (which may be regarded as finite dimensional vector spaces over GF(2)), the characteristic functions of which may be regarded as certain strangely behaved Boolean functions. As a matter of fact, many properties of these difference sets are most easily discussed in the language of Boolean functions and polynomials. For example, the Fourier transform is a natural consideration in this setting. Also, two difference sets are equivalent precisely when their associated polynomials are equivalent under the action induced by the affine group on their variables. Thus, certain affine invariants (e.g. "degree") may be associated with each difference set. Chapter 3 is a general discussion of Boolean functions and their transforms. In sections 2 and 3 we develop the polynomial and Fourier transforms of a Boolean function, making explicit the Kronecker product nature of both of them. This last consideration is important because it permits via "Fast Fourier Transform" techniques (given in the introduction of Chapter 3) the actual computation of these transforms. In the last section of chapter 3 we introduce some new, more discriminating, affine invariants which are useful when the obvious ones fail. Indeed, it is this class of invariants which demonstrates the richness of our new family of difference sets.

In chapter 4 we define a Pall partition for a quadratic form over a field F to be a partition of the zeros of the form into pairwise disjoint (except for 0) maximal isotropic (singular if char $F=2$) subspaces. We prove that there exists a Pall partition for every nonsingular quadratic form over $GF(2^r)$, except for those equivalent to

$$\Psi_m = X_1X_{m+1} + X_2X_{m+2} + \dots + X_mX_{2m}$$

with $m>1$ odd. Further, if $m>1$ is odd, there does not exist a Pall partition for Ψ_m over any field whatsoever. This last result generalizes a recent theorem of L. Couvillon [5]. We demonstrate in chapter 6 the intimate connection between these forms over $GF(2)$ and difference sets.

Chapter 5 contains the main results of this paper. We define a partial spread for a group G of order M^2 to be a family of pairwise disjoint (except for identity) subgroups of order M. We prove that the elements (resp. nonidentity elements) in the union of a partial spread of cardinality r constitute a difference set in G if and only if G has order $4N^2$ and $r = N+1$ (resp. N). These difference sets are Hadamard with parameters $(4N^2, 2N^2+N, N^2+N, N^2)$ and $(4N^2, 2N^2-N, N^2-N, N^2)$ respectively.

that there are that many more which must be taken into account before we can determine just how many inequivalent ones there are. We hope that our present survey may arouse the interest of others in pursuing the fascinating charms of elementary Hadamard difference sets.

CHAPTER II

DIFFERENCE SETS AND THEIR INCIDENCE MATRICES

1. Introduction.

In this chapter we present a brief but rather comprehensive review of the fundamental notions concerning difference sets, the emphasis being on those aspects which shall concern us in later chapters. In particular, we include the basic results on Hadamard difference sets: the theorem of P. Kesava Menon to the effect that a (v,k,λ,n)-difference set with $v=4n$ must have the so-called "Hadamard parameters", and the theorem of H. B. Mann to the effect that any (v,k,λ,n)-difference set with v a power of 2 must be Hadamard; i.e. must have $v=4n$. We point out that Mann's proof also shows that there does not exist a (v,k,λ)-configuration with $v=2p^r$, p an odd prime. We incorporate this result in our statement of Mann's theorem. We also include a discussion of multipliers of difference sets and point out one of the difficulties encountered in studying difference sets in elementary abelian 2-groups.

The incidence matrix occupies a preeminent position in section 2. In section 3 we present the (complex) group algebra which is particularly well-suited to the study of difference sets. We introduce, for abelian groups, the "Fourier transform" on the algebra which leads immediately to the very useful characterization of difference sets in terms of group characters.

We refer the reader to [2] and [10] for more details on difference sets and to [15] for an excellent treatment of the (integral) group ring and its relation to difference sets.

2. Fundamental notions.

Let G be an arbitrary group of order v and let D be a k-subset of G. Here we denote the group operation additively.

DEFINITION. D *is a* (v,k,λ,n)-*difference set in* G *if for every nonzero element* g *in* G *the equation*

$$g = d_i - d_j$$

has exactly λ *solutions* (d_i,d_j) *with* d_i *and* d_j *in* D. *The parameter* n *is defined to be* $k-\lambda$ *(for convenience)*.

Since each of the $v-1$ nonzero elements of G occurs λ times among the $k(k-1)$ nonzero differences of elements of D, the parameters of a difference set must satisfy the fundamental relation given by

REMARK 2.2.1. $\lambda(v-1) = k(k-1)$

Every group of order $v>1$ contains difference sets with the parameters

v	k	λ	n
v	0	0	0
v	v	v	0
v	1	0	1
v	$v-1$	$v-2$	1 .

These difference sets are regarded as trivial; their consideration may be avoided by requiring that the parameter n be greater than one.

DEFINITION. *The incidence matrix associated with the subset* D *is the* $v \times v$ $(0,1)$*-matrix* $[D]$ *whose* (g,h)th *entry is* 1 *whenever* $g-h$ *is an element of* D; i.e.

$$[D](g,h) = \begin{cases} 1 & \text{if } g-h \varepsilon D \\ 0 & \text{otherwise} \end{cases} .$$

(here we assume some fixed order on the elements of G).

We then have the

REMARK 2.2.2. D *is a* (v,k,λ,n)*-difference set if and only if the incidence matrix* $[D]$ *satisfies*

$$[D][D]' = nI + \lambda J,$$

where J *is the* $v \times v$ *matrix with all entries* 1.

PROOF. The (g,h)th entry of $[D][D]'$ is the number of translates $D + \ell$ containing both g and h. But for elements d_i and d_j in D,

$$g=d_i+\ell \text{ and } h=d_j+\ell \text{ for some } \ell \varepsilon G \Longleftrightarrow g-h = d_i-d_j,$$

and the assertion follows immediately. qed.

We note here that Remark 2.2.2 shows that the translates $\{D+g : g \varepsilon G\}$ of a difference set D constitute a (v,k,λ)-configuration; i.e. an arrangement of v distinct objects into v blocks such that each block contains k objects and each pair of distinct objects appear together in λ blocks (equivalently, each pair of distinct blocks intersect in λ objects) [10].

We may now establish quite easily the

REMARK 2.2.3. *If* D *is a* (v,k,λ,n)*-difference set in* G, *then its complement* $\bar{D} = G\backslash D$ *is a* $(v,v-k,v-2k+\lambda,n)$*-difference set in* G.

PROOF. $[\bar{D}][\bar{D}]' = (J-[D])(J-[D]') = J^2-[D]J-J[D]'+[D][D]'$

$$= vJ - 2kJ + (nI + \lambda J)$$

$$= nI + (v - 2k + \lambda)\, J.$$ qed.

This result allows us to assume without loss of generality that $k < v/2$.

While the incidence matrix $[D]$ of a subset D is a very useful tool, it is sometimes more convenient to employ a matrix whose entries are ± 1.

DEFINITION. $[D^*] = J - 2[D]$.

This definition together with Remark 2.2.2 yields

REMARK 2.2.4 D *is a* (v,k,λ,n)*-difference set iff*

$$[D^*][D^*]' = 4nI + (v-4n)J.$$

DEFINITION. *The* $v \times v$ *matrix* H *is called a Hadamard matrix if its entries are* ± 1 *and it is orthogonal*; i.e. $HH' = vI$.

We note here for future reference the obvious

REMARK 2.2.5. *The* (± 1)*-matrix* H *is Hadamard iff* HH' *is scalar* (i.e. *of the form* cI *for some constant* c).

Collecting our foregoing observations we arrive at the very important

THEOREM 2.2.6. D *is a* (v,k,λ,n)-*difference set with* $v=4n$ *if any only if* $[D^*]$ *is a Hadamard matrix.*

In light of this last result we have the natural

DEFINITION. *A* (v,k,λ,n)-*difference set with* $v=4n$ *is called a Hadamard difference set.*

The Hadamard condition essentially determines the size of such a difference set in any group; P. Kesava Menon [19] was the first to note the rather surprising

REMARK 2.2.7. *A Hadamard difference set has parameters of the form*

$$(v,k,\lambda,n) = (4N^2,\ 2N^2-N,\ N^2-N,\ N^2) \text{ or } (4N^2,\ 2N^2+N,\ N^2+N,\ N^2).$$

PROOF. The fundamental relations $n = k-\lambda$ and $k(k-1) = \lambda(v-1)$, together with the Hadamard condition $v = 4n$, imply

$$\begin{aligned} 0 = k(k-1) - \lambda(v-1) &= k^2-k-(k-n)(4n-1) \\ &= k^2-4nk + n(4n-1) \\ &= (k-2n)^2 - n. \end{aligned}$$

Hence, $k = 2n \pm\sqrt{n}$, and the assertion follows. qed.

The corollary that a Hadamard difference set can exist only in a group of square order is actually a special case of the more general

REMARK 2.2.8. *If there exists a* (v,k,λ,n)-*difference set* D *with* v *even, then* n *is a square.*

PROOF. If D is a (v,k,λ,n)-difference set, then

$$[D][D]' = nI + \lambda J,$$

from which it follows quite easily that

$$(\det [D])^2 = \det ([D][D]') = k^2 n^{v-1},$$

and the result is immediate. qed.

The same proof establishes this result for an arbitrary (v,k,λ)-configuration or symmetric balanced incomplete block design; the general result was obtained by Schutzenberger [23] and Bruck and Ryser [10] independently.

Another general result which provides a restriction on parameters is the following remarkable theorem due to H. B. Mann [13].

THEOREM 2.2.9. *If there exists a nontrivial* (v,k,λ)-*configuration with* v *a power of* 2, *then* $(v,k,\lambda) = (4^{s+1}, 2\cdot 4^s-2^s, 4^s-2^s)$ *or* $(4^{s+1}, 2\cdot 4^s+2^s, 4^s+2^s)$.

Glenn F. Stahly (private communication) has observed that Mann's proof actually establishes the following more general

THEOREM 2.2.10. *If there exists a nontrivial* (v,k,λ)-*configuration with* $k < v/2$ *and* v *of the form* $2p^m$, p *prime, then*

$$(v,k,\lambda) = (4^{s+1}, 2\cdot 4^s-2^s, 4^s-2^s) \text{ for some } s.$$

PROOF. Since v is even, $n=k-\lambda$ must be a square which we write as

$$n = p^{2s}n_1^2, \quad (n_1, p) = 1.$$

The fundamental equation $\lambda(v-1) = k(k-1)$ may then be expressed as

$$(*) \qquad 2\lambda p^m = k^2 - p^{2s}n_1^2 .$$

Now $n < k < v/2 \Rightarrow p^{2s}|p^m \Rightarrow p^{2s}|k^2 \Rightarrow p^s|k$; so we may write

$$k = p^s k_1 .$$

It follows that p^s divides λ; we write

$$\lambda = p^s \lambda_1 .$$

Equation (*) then becomes

$$2p^s\lambda_1 p^m = p^{2s}k_1^2 - p^{2s}n_1^2$$

or

$$(**) \qquad 2\lambda_1 p^{m-s} = (k_1-n_1)(k_1+n_1).$$

Now $k_1-n_1 < k_1 < p^{m-s}$ and $k_1+n_1 < 2k_1 < 2p^{m-s}$. Thus, if p does not divide k_1-n_1 we must have

$$k_1+n_1 = p^{m-s}$$

and

$$k_1-n_1 = 2\lambda_1 ,$$

from which it follows that $p=2$. On the other hand, if p does divide k_1-n_1, then p must divide $(k_1+n_1)-(k_1-n_1) = 2n_1$ and since $(p,n_1)=1$

again we must have $p=2$. Thus, in any event, $p=2$ and n_1 is odd.

Now from (**) and the inequalities following (**) we see that $2 \cdot 2^{m-s}$ divides the product of (k_1-n_1) and (k_1+n_1), the larger of which is smaller than $2 \cdot 2^{m-s}$. Thus, each of these factors is even and, since n_1 is odd, no power of 2 greater than 2 can divide them both. It follows that

$$k_1+n_1 = 2^{m-s}$$

and
$$k_1-n_1 = 2\lambda_1 ,$$

which imply

$$4n = 4(k_1-\lambda_1)2^s = 2(2k_1-2\lambda_1)2^s = 2(2^{m-s})2^s = 2^{m+1} = v. \qquad \text{qed.}$$

We single out for future reference the

COROLLARY. *If* D *is a nontrivial difference set (with* $k < v/2$) *in the group* G *of order* 2^m, *then* D *is a Hadamard difference set with parameters of the form*

$$(v,k,\lambda,n) = (4^{s+1}, 2\cdot 4^s-2^s, 4^s-2^s, 4^s).$$

In particular, m *must be even.*

If D is a particular difference set in the group G, it is easy to obtain from D many other difference sets. Indeed, we have the easily verified

REMARK 2.2.11. *If* D *is a* (v,k,λ,n)-*difference set in the group* G, *then for all* $g \in G$ *and all automorphisms* α *of* G *the sets*

$$D+g = \{d+g : d \in D\}$$

and

$$D^{\alpha} = \{d^{\alpha} : d \in D\}$$

are also (v,k,λ,n)-*difference sets in* G.

This remark motivates the following

DEFINITION. *The difference sets* D_1 *and* D_2 *in the group* G *are said to be equivalent if there exists an automorphism* α *of* G *such that*

$$(*) \qquad D_1^{\alpha} = D_2 + g$$

for some g *in* G. *In particular, if* $(*)$ *holds with* $D_2 = D = D_1$ *then the group automorphism* α *is said to be a multiplier of* D. *A multiplier of the form*

$$\alpha : g \to g^t, \; t \text{ an integer},$$

is called a numerical multiplier.

H. B. Mann and R. L. McFarland [14] have shown that every multiplier of a difference set must fix at least one translate of that difference set. Indeed, if P and Q denote the permutation matrices effecting the action of the automorphism α on the points and blocks of the associated design, then

$$P[D]Q^{-1} = [D]$$

or

$$[D]^{-1} P[D] = Q .$$

Thus, the matrices P and Q are similar and it is not very hard to see that P and Q must be similar (i.e. conjugate) permutations. It follows that the permutations induced on the points and blocks of the design must have the same cycle structure. In particular, since a group automorphism always has a fixed point (the identity), a multiplier of a difference set must also fix at least one block (translate). In fact, the number of translates fixed by a multiplier must be the order of a subgroup of G and hence a divisor of v. We thus have

REMARK 2.2.12. *A multiplier α of a difference set D in G permutes the translates of D according to a permutation with the same cycle structure as the permutation induced on the points of G by α. In particular, the number of translates fixed by α divides the order of G.*

The multipliers of a difference set D in G constitute a subgroup $M(D)$ of the automorphism group of G. Equivalent difference sets have isomorphic multiplier groups; indeed, if

$$D_1^{\alpha} = D_2 + g,$$

then $M(D_1) = \alpha M(D_2)\alpha^{-1}$. To illustrate the equivalence of difference sets we prove

REMARK 2.2.13. *Every (16,6,2,4)-difference set in $G = Z_2^4$ is equivalent to*

$$D = \{0000,\ 1000,\ 0100,\ 0010,\ 0001,\ 1111\}.$$

PROOF. If D is a (16,6,2,4)-difference set in $G = Z_2^4$ we may (by translating D if necessary) assume that D contains 0000. Next, since every element of G appears as a difference of two elements of D, D must contain a basis for G which we may (by applying an automorphism, if necessary) assume is the unit basis 1000, 0100, 0010, 0001. The differences among these five elements already account for the two representations of each element of G containing either one or two 1's. Thus, the only choice for the sixth element of D is 1111, and it is clear that the resulting set D is indeed a difference set with the asserted parameters. qed.

This (16,6,2,4)-difference set, the best known example of a noncyclic difference set, was given by Bruck [4] in the first paper to treat difference sets in general groups. McFarland [17] has observed that the (16,6,2,4)-difference set in Z_2^4 has multiplier group of order 720. McFarland also observes [15] that, if D is such a difference set, there exists a group automorphism β such that D and D^β have <u>different</u> (although isomorphic) multiplier groups (this situation cannot arise for cyclic groups since they have abelian automorphism groups). A difference set D in G that is fixed under the multiplier α must be the union of orbits in G determined by α (the orbit containing the element g is the set $\{g, g\alpha, g\alpha^2, \ldots\}$). Thus, the existence of multipliers facilitates the investigation of a difference set. A very powerful theorem due to Marshall Hall, Jr. and several generalizations [15] provide multipliers for difference sets in a variety of groups; however, all multipliers given by these theorems are <u>numerical</u> multipliers; there is no general theorem which provides nonnumerical multipliers for difference sets in groups which have nonnumerical automorphisms. In particular, there is no general "Multiplier Theorem" for difference sets in elementary abelian 2-groups (such groups have no nontrivial numerical automorphisms).

3. The Group Algebra.

Let G be an arbitrary finite group which we denote multiplicatively. The *group algebra* $\mathbb{C}[G]$ of G over the field of complex numbers $\mathbb{C}$ is comprised of all formal sums

$$A = \sum_{g\varepsilon G} a_g g, \; a_g \varepsilon \mathbb{C},$$

with addition being defined component-wise; i.e.,

$$\sum a_g g + \sum b_g g = \sum (a_g + b_g) g,$$

and multiplication being defined by "convolution"; i.e.

$$(\sum_g a_g g)(\sum_g b_g g) = \sum_{g,h} a_g b_h gh = \sum_g \{ \sum_{hk=g} a_h b_k \} g.$$

Under these definitions $\mathbb{C}[G]$ is an associative ring with unity which is commutative precisely when the group G is abelian. Indeed defining scalar multiplication by $\alpha A = \sum (\alpha\, a_g) g$, we see that $\mathbb{C}[G]$ is a $\mathbb{C}$-algebra with basis consisting of the "sums"

$$C_g = \sum_{h\varepsilon G} c_{g,h} h, \; g\varepsilon G,$$

whose coefficients are all 0 except for the coefficient on g which is 1. Clearly, the map $g \to C_g$ is an isomorphism of G into the multiplicative structure of $\mathbb{C}[G]$; we therefore identify C_g with g and consider G to be the basis for $\mathbb{C}[G]$. In particular, for any subset S of G we use the same notation, S, to denote the element of $\mathbb{C}[G]$ which is the sum of the elements of S. 1 denotes the identity of G and the unity of $\mathbb{C}[G]$; for each $\alpha\varepsilon\mathbb{C}$ we denote simply by α the element of $\mathbb{C}[G]$ all of whose coefficients are 0 except the coefficient on 1 which is α. For any element $A = \sum a_g g$ in $\mathbb{C}[G]$ and any integer t, we denote by $A^{(t)}$ the element given by

$$A^{(t)} = \sum a_g g^t.$$

The group ring $Z[G]$ is the subring of $\mathbb{C}[G]$ consisting of all elements with rational integer coefficients.

The group ring $Z[G]$ (and more generally $\mathbb{C}[G]$) is particularly well suited to the study of difference sets. If G has order v and D is a k-subset of G, then D is a (v,k,λ,n)-difference set if each nonidentity element g in G has exactly λ representations of the form $d_i d_j^{-1}$, with d_i and d_j in D. But this is equivalent to saying that, in the group ring $Z[G]$,

$$DD^{(-1)} = n + \lambda G.$$

This is a very useful characterization of difference sets and will be used in later chapters.

Now suppose that G is abelian so that it is isomorphic to its character group; i.e., the group of homomorphisms from G into the multiplicative group of complex v^{*th} roots of unity, where v^* is the exponent of G. It is easy to see that any character χ of G

can be extended (linearly) to an algebra homomorphism on all of $\mathbb{C}[G]$; i.e.

$$\chi(\sum a_g g) = \sum a_g \chi(g).$$

In particular, χ maps $Z[G]$ homomorphically onto the ring of integers in the cyclotomic field $Q(\exp 2\pi i/v^*)$. Moreover, the orthogonality of group characters permits a Fourier analysis in $\mathbb{C}[G]$. For any

$$A = \sum a_g g$$

in $\mathbb{C}[G]$ we define its (unnormalized) Fourier transform $\hat{A}$ by

$$\hat{A} = \sum \chi_g(A) g.$$

Then the effect of the mapping

$$A \to \hat{A}$$

on $\mathbb{C}[G]$ is to transform it isomorphically into the algebra of complex-valued functions on G with component addition and multiplication. The coefficients of A are obtained from its transform $\hat{A}$ by

$$v\, a_g = \sum_h \chi_h(g^{-1}A), \text{ for all } g \in G.$$

Now let us reconsider the difference set D in G which satisfies in $Z[G]$ the equation

$$(*) \qquad D\, D^{(-1)} = n + \lambda G.$$

For any character χ of G we have from (*)

$$(**) \qquad |\chi(D)|^2 = \begin{cases} k^2 = n + \lambda v & \text{if } \chi \text{ is principal} \\ n & \text{if } \chi \text{ not principal.} \end{cases}$$

Moreover (**) is equivalent to (*). Thus, we have

REMARK 2.3.1. *Let* D *be a subset of the group* G. *Then the following are equivalent:*

1) D *is a difference set in* G;

2) $D\,D^{(-1)} = n + \lambda G$ *in the group ring* $Z[G]$.

If G *is abelian,* 1) *and* 2) *are equivalent to*

3) $|\chi(D)|^2 = n$ *for all nonprincipal characters* χ *of* G.

CHAPTER III

BOOLEAN FUNCTIONS AND THEIR TRANSFORMS

1. Introduction.

Let F denote the finite field with two elements.

DEFINITION. A Boolean function is a function from some finite dimensional F-linear space into F.

For concreteness we shall assume here that our functions have domain the space F^m of binary m-tuples. We recognize however that the fundamental notions developed in this chapter apply equally well to any isomorphic space, and in the following chapters we shall find it convenient to consider domains which are various direct sums of finite fields of characteristic 2. Formally, we may always choose a basis for the space and thereby reduce the domain to the space of m-tuples; as a matter of fact, this is usually the best procedure to follow when it becomes necessary to carry out computations of the type discussed in this chapter.

Let $\mathcal{F}_m$ denote the F-linear space of all functions from F^m into F. It is clear that the functions $\mathcal{F}_m$ on F^m are in 1-1 correspondence with the subsets of F^m, each function being associated with that subset of which it is the characteristic or indicator function. In later chapters we shall make extensive use of this correspondence. We shall characterize difference sets in the elementary abelian 2-groups F^m in terms of their characteristic functions and Fourier transforms thereof. Thus we shall have several representations of a given subset of F^m as a function on F^m; namely, the truth-table of the characteristic function (whose values may be interpreted as being real or as being in F), the polynomial in m coordinate variables which when evaluated on F^m is equal to the characteristic function (mod 2), and the Fourier transform of the real-valued characteristic function. It is most natural to associate with a given subset its truth-table function. We shall call the other functions the polynomial transform and the Fourier transform.

The next two sections contain a brief exposition of these important transforms. We stress the Kronecker product nature of both of them. In section 4 we consider the Boolean functions $\mathcal{F}_m$ under the (induced) action of the general affine group acting on F^m. We develop here a new class of "easily computed" affine invariants which we use later to demonstrate the inequivalence of certain difference sets.

The results of this chapter are certainly not limited to the study of difference sets. They apply equally well in the general analysis of Boolean functions, switching theory and binary error-correcting codes. The interested reader is referred to [12] for more details.

We have stated the importance of the polynomial and Fourier transforms of a Boolean function. In analyzing such functions it becomes necessary to compute these transforms. We shall see in the next two sections that each of these transforms on $\mathcal{F}_m$ is given by a $2^m \times 2^m$ matrix. The work involved in effecting a transformation by such a matrix might well be prohibitive were it not for one saving factor — each is the m-fold Kronecker product of a 2×2 matrix. Thus, standard "Fast Fourier Transform" techniques apply and our transforms are seen to be easily computed. At the heart of any such FFT algorithm lies a factorization of a "complicated" matrix into a product of "simple" matrices.

Multiplication by the complicated matrix is then effected by multiplying successively by the various simple factors. These ideas are so important and of such wide applicability that we present here the general results.

Let F be an arbitrary field and let $\mathcal{M}$ be the set of all matrices which have finitely many rows and columns and whose entries are elements of F. Let Z_n denote the ordered set $\{0, 1, 2, \ldots, n-1\}$ with the usual order, and let $Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_N}$ denote the Cartesian product of the Z_{n_i}'s, endowed with the lexicographic order. The correspondence

$$(*) \qquad t_1(n_2n_3 \ldots n_N) + t_2(n_3n_4 \ldots n_N) + \ldots + t_{N-1}(n_N) + t_N \leftrightarrow (t_1, t_2, \ldots, t_N)$$

is an order isomorphism between the ordered sets $Z_{n_1n_2\ldots n_N}$ and $Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_N}$. The rows (resp. columns) of a matrix with $n_1n_2 \ldots n_N$ rows (resp. columns) may be indexed by either of these sets and the correspondence (*) enables us to change from one indexing system to the other. For any matrices A and B in $\mathcal{M}$ the <u>Kronecker product</u> of A by B, denoted by $A \otimes B$, is given by

$$A \otimes B = \begin{bmatrix} a_{00}B & a_{01}B & \ldots & a_{0j}B & \ldots \\ a_{10}B & a_{11}B & \ldots & a_{1j}B & \ldots \\ \vdots & \vdots & & & \\ a_{i0}B & a_{i1}B & \ldots & a_{ij}B & \ldots \\ \vdots & \vdots & & & \end{bmatrix}.$$

More formally, if A (resp. B) has m_A rows and n_A columns (resp. m_B rows and n_B columns) then the Kronecker product $A \otimes B$ is the matrix with m_Am_B rows and n_Am_A columns such that

$$A \otimes B\ ((r,t),\ (s,u)) = A(r,s)\ B(t,u)$$

for all $(r,t) \in Z_{m_A} \times Z_{m_B}$ and $(s,u) \in Z_{n_A} \times Z_{n_B}$.

$\otimes$ is an associative binary operation on M, and if for each i, $1 \leq i \leq N$, A_i is an $m_i \times n_i$ matrix in M, then the Kronecker product $A_1 \otimes A_2 \otimes \ldots \otimes A_N$ is given by

$$A_1 \otimes A_2 \otimes \ldots \otimes A_N\ ((r_1,r_2, \ldots, r_N),(s_1,s_2, \ldots, s_N)) = \prod_{i=1}^{N} A_i(r_i,s_i)$$

for all $(r_1,r_2, \ldots, r_N) \in Z_{m_1} \times Z_{m_2} \times \ldots \times Z_{m_N}$ and $(s_1,s_2, \ldots, s_N) \in Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_N}$. In particular, if A is any $m \times n$ matrix in M we may form the Kronecker product of A with itself N times and obtain the matrix $\otimes^N A$ whose entries are given by

$$\otimes^N A\ ((r_1,r_2, \ldots, r_N),\ (s_1,s_2, \ldots, s_N)) = \prod_{i=1}^{N} A(r_i,s_i)$$

for all $(r_1,r_2, \ldots, r_N) \in Z_m^N$ and $(s_1,s_2, \ldots, s_N) \in Z_n^N$. We sometimes use the notation $\bigotimes_{i=1}^{N} A_i$ in place of $A_1 \otimes A_2 \otimes \ldots \otimes A_N$ and $\prod_{i=1}^{N} A_i$ in place of $A_1A_2 \ldots A_N$.

The following properties of the Kronecker product are classical.

REMARK 3.1.1. i) $(A\otimes B)' = A' \otimes B'$;

ii) $AB \otimes CD = (A\otimes C)(B\otimes D)$;

iii) $(A\otimes B)^{-1} = A^{-1} \otimes B^{-1}$, A, B nonsingular.

These properties are easily generalized to

REMARK 3.1.2. i) $\left(\bigotimes_{i=1}^{N} A_i\right)' = \bigotimes_{i=1}^{N} A_i'$;

ii) $\bigotimes_{i=1}^{N} \left(\prod_{j=1}^{M} A_{ij}\right) = \prod_{j=1}^{M} \left(\bigotimes_{i=1}^{N} A_{ij}\right)$;

iii) $(\otimes A_i)^{-1} = \otimes A_i^{-1}$, A_i's *nonsingular*.

Let I_n denote the n×n identity matrix. Part ii) of Remark 3.1.2, together with the obvious fact that $\bigotimes_{i=1}^{N} I_{n_i} = I_{n_1 n_2 \ldots n_N}$, now yields the well-known

FACTORIZATION THEOREM 3.1.3. *For each* i, $1 \le i \le N$, *let* A_i *be an* $m_i \times n_i$ *matrix. Then*

$$A_1 \otimes A_2 \otimes \ldots \otimes A_N = \prod_{i=1}^{N} (I_{n_1 n_2 \ldots n_{i-1}} \otimes A_i \otimes I_{m_{i+1} \ldots m_N}).$$

COROLLARY. *For any* n×n *matrix* A

$$\otimes^N A = \prod_{i=1}^{N} (I_{n^{i-1}} \otimes A \otimes I_{n^{N-i}}).$$

While this last result is a very effective factorization of a Kronecker N^{th} power, it is a remarkable fact that such a matrix is also a matrix N^{th} power.

FACTORIZATION THEOREM 3.1.4. *For any* n×n *matrix* A

$$\otimes^N A = \begin{bmatrix} I \otimes A(0,\cdot) \\ I \otimes A(1,\cdot) \\ \vdots \\ I \otimes A(n-1,\cdot) \end{bmatrix}^N$$

where I *denotes the* $n^{N-1} \times n^{N-1}$ *identity matrix and* $A(i,\cdot)$ *denotes the* i^{th} *row of* A.

This result was first given by I. J. Good; it follows directly from the previous corollary on observing that the N factors given there form a cycle under a similarity transformation by a permutation matrix of order N.

The final result we present here enables us to effect a transformation of a high dimensional space by means of several transformations of lower dimensional spaces.

BOX THEOREM 3.1.5. Let A and B be square matrices in M of dimensions $m_A \times m_A$ and $m_B \times m_B$, respectively. Let $\square$ denote the operator which transforms the $m_A m_B \times 1$ matrix (column vector) C into the $m_A \times m_B$ matrix $C^{\square}$ defined by

$$C^{\square}(i,j) = C(im_B+j) \quad 0 \leq i < m_A,\ 0 \leq j < m_B.$$

Then

$$[(A \otimes B)C]^{\square} = AC^{\square}B'.$$

This result is equivalent to the equation

$$A \otimes B = (A \otimes I_{m_B})(I_{m_A} \otimes B),$$

a special case of Factorization Theorem 3.1.3. It will be used extensively in chapter 6, where it makes transparent certain constructions of difference sets in noncyclic groups.

2. Polynomial transform.

Just as the functions in $\mathcal{F}_m$ may be regarded as subsets of F^m, so, too, the vectors in F^m may be regarded as subsets of the m-set $\{1, 2, 3, \ldots, m\}$; each vector $v = (v_1, v_2, \ldots, v_m)$ corresponds to the set of indices which index those coordinates of v containing its 1's (i.e. the set $\{i : v_i=1\}$). This identification then induces on F^m the following natural (partial) order which we call the inclusion order.

DEFINITION. For any vectors $v = (v_1, v_2, \ldots, v_m)$ and $u = (u_1, u_2, \ldots, u_m)$ in F^m we say that v is contained in u (and write $v \subset u$) if $v_i \leq u_i$ for all i, $1 \leq i \leq m$.

We may now prove a rather pretty inversion theorem which is a special case of "Möbius inversion in a partially ordered set" [10].

THEOREM 3.2.1. Let f and g be functions from F^m to F and let F^m be partially ordered by the inclusion order $\subset$. Then the following are equivalent:

$$\text{(I)} \quad f(v) = \sum_{u \subset v} g(u), \text{ for all } v \in F^m,$$

$$\text{(II)} \quad g(v) = \sum_{u \subset v} f(u), \text{ for all } v \in F^m.$$

PROOF. Applying (I) to the right side of (II) we obtain

$$\sum_{u\subset v} f(u) = \sum_{u\subset v} \sum_{w\subset u} g(w) = \sum_{w\subset u\subset v} g(w) = \sum_{w\subset v} 2^{|v-w|} g(w) = g(v),$$

the final equality a consequence of F having characteristic 2. Thus, (I) implies (II) and interchanging f and g shows that (II) implies (I). qed.

We now establish the important

THEOREM 3.2.2.

a) <u>To each function</u> $f : F^m \to F$ <u>there corresponds a unique function</u> $g : F^m \to F$ <u>such that</u> f <u>is given by the polynomial</u>

$$f(X) = \sum_{v\varepsilon F^m} g(v)X^v \equiv \sum_{v\varepsilon F^m} g(v)\, X_1^{v_1} X_2^{v_2} \cdots X_m^{v_m} ;$$

b) <u>The function</u> g <u>is given by</u>

$$g(v) = \sum_{u\subset v} f(u), \text{ for all } v\varepsilon F^m;$$

c) <u>With the functions</u> f <u>and</u> g <u>of part</u> a) <u>associate the vectors</u>

$$\mathbf{f} = (f(0), f(1), f(2), \ldots, f(2^m-1))'$$

and $\mathbf{g} = (g(0), g(1), g(2), \ldots, g(2^m-1))'$

<u>where the integers</u> $0, 1, 2, \ldots, 2^m-1$ <u>are used as a convenient means to denote their binary representations.</u>

<u>Then</u> $\mathbf{f} = U_m \mathbf{g}$ and $\mathbf{g} = U_m \mathbf{f}$

<u>where</u> $U_m = \otimes^m \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

PROOF. If f is any function from F^m into F it is clear (by Lagrange interpolation) that f is given by the polynomial

$$\sum_{v\varepsilon F^m} f(v) \prod_{i=1}^{m} (X_i + v_i + 1)$$

which can then be put into the form

$$\sum_{v\varepsilon F^m} g(v)\, X_1^{v_1} X_2^{v_2} \ldots X_m^{v_m} .$$

It is then easy to see that for all $v\varepsilon F^m$ we have

$$f(v) = \sum_{u\subset v} g(u).$$

But then our inversion theorem 3.2.1 gives b) and at the same time "uniqueness" in a). Now let U_m be the matrix effecting the linear transformation from f to g; i.e.

$$(g(0),\ g(1),\ \ldots,\ g(2^m-1))' = U_m(f(0),\ f(1),\ \ldots,\ f(2^m-1))'.$$

Then U_m is clearly the incidence matrix of the partial order relation $\subset$ on F^m; i.e. U_m is indexed by the vectors in F^m and

$$U_m(v,u) = \begin{cases} 1 & \text{if } u\subset v \\ 0 & \text{otherwise} \end{cases} .$$

Now clearly $U_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$; and by the definition of $\subset$

$$U_m(v,u) = 1 \Longleftrightarrow u\subset v$$

$$\Longleftrightarrow u_i \leq v_i \text{ for all } i,\ 1 \leq i \leq m$$

$$\Longleftrightarrow \prod_{i=1}^{m} U_1(v_i,u_i) = 1 .$$

Thus $U_m(v,u) = \prod_{i=1}^{m} U_1(v_i,u_i)$

and it follows that U_m is the Kronecker product $\otimes^m U_1$. qed.

The vectors f and g of part c) may be called the "truth-table" and "polynomial" representations of the function f. Since the matrix U_m effecting this transform is an involution, the same algorithm may be used to obtain the polynomial from the truth-table as is used to obtain the truth-table from the polynomial. The factorization theorems 3.1.3 & 4 yield algorithms which permit rapid computation of this transform.

Thus each function f in F_m is given by a polynomial $f(X) = f(X_1, X_2, \ldots, X_m)$. We shall usually identify the function f with the polynomial $f(X)$.

DEFINITION. The degree of a nonzero function f is the degree of its associated polynomial $f(X)$. We say that the zero function has degree -1.

DEFINITION. The functions $f(X)$ and $g(X)$ on F^m are called linearly (resp. affinely) equivalent if there exists a nonsingular linear (resp. affine) transformation T of the variables $X_1, X_2, \ldots, X_m$ such that

$$g(X) = g(X_1, X_2, \ldots, X_m) = f(X_1T, X_2T, \ldots, X_mT) = f(XT).$$

We note for future reference the well-known

REMARK 3.2.3. Affinely equivalent functions have the same cardinality and the same degree.

3. Fourier-Hadamard transform.

DEFINITION. *With each function* $f : F^m \to F$ *we associate the real-valued function*

$$f^* : F^m \to \{\pm 1\}$$

defined by $f^*(X) = (-1)^{f(X)}$. *Thus* f^* *is equal to the composition of* f *with the unique isomorphism between the additive group* F *and the multiplicative group of (complex) square-roots of unity.*

REMARK 2.3.1. *For each* $v \varepsilon F^m$, *let* $v \cdot x$ *denote the linear function* $\Sigma\, v_i X_i$. *The real functions* $(-1)^{v \cdot x}$, $v \varepsilon F^m$, *are precisely the group characters of* F^m.

It is familiar that the orthogonality of group characters permits a Fourier theory for abelian groups. In the present setting we have the important

THEOREM 3.3.1. *Let* C *denote the field of complex numbers.*

a) *To each function* $h : F^m \to C$ *there corresponds a unique function* $\hat{h} : F^m \to C$ *such that*

$$h(X) = \sum_{v \varepsilon F^m} \hat{h}(v)(-1)^{v \cdot x} .$$

b) *The function* $\hat{h} : F^m \to C$ *is given by*

$$2^m \hat{h}(x) = \sum_{v \varepsilon F^m} h(v)(-1)^{v \cdot x} .$$

c) *With the functions* h *and* $\hat{h}$ *of part* a) *associate the "truth-tables"*

$$h = (h(0), h(1), \ldots, h(2^m - 1))'$$

and $$\hat{h} = (\hat{h}(0), \hat{h}(1), \ldots, \hat{h}(2^m - 1))' .$$

Then we have

$$h = H_m \hat{h} \quad \text{and} \quad 2^m \hat{h} = H_m h,$$

where H_m is the m^{th} elementary Hadamard matrix given by

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ and } H_m = \otimes^m H_1 .$$

PROOF. Let M_m be the $2^m \times 2^m$ matrix whose rows and columns are indexed by the lexicographically ordered vectors in F^m and whose (u,v)th entry is $(-1)^{u \cdot v}$. Then $M_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H_1$ and, for all $u, v \varepsilon F^m$,

$$M_m(u,v) = (-1)^{u \cdot v} = (-1)^{\Sigma u_i v_i} = \prod_{i=1}^{m} (-1)^{u_i v_i} = \prod_{i=1}^{m} H_1(u_i, v_i).$$

Thus, $M_m = H_m$, the m^{th} elementary Hadamard matrix. The relations between the functions h and $\hat{h}$ in a) and b) can then be expressed in terms of H_m and the truth-tables of h and $\hat{h}$ as:

$$a') \quad h = H_m \hat{h}$$

$$\text{and} \quad b') \quad \hat{h} = \frac{1}{2^m} H_m h .$$

But $H_m^{-1} = \frac{1}{2^m} H_m$ so that a' and b' are obviously equivalent. qed.

The transform $h \to \hat{h}$ is formally known as the "discrete m-dimensional Fourier Transform mod 2"; because of its relationship to the Hadamard matrix (part c)) it is now usually called simply the Hadamard Transform or the Fourier-Hadamard Transform. The name "Walsh Transform" is also quite popular in engineering circles.

If the function h is of the form f^* for some Boolean function f, we write $\hat{f}$ in place of $\hat{f^*}$ and call $\hat{f}$ the Fourier transform of f (as well as f^*). We now note the important

REMARK 3.3.2. <u>If</u> $h(X) = g(XT+a)$ <u>for some vector</u> a <u>in</u> F^m <u>and some nonsingular</u> F-<u>linear transformation</u> T <u>of the variables</u> $X_1, X_2, \ldots, X_m$, <u>then</u>

$$\hat{h}(X) = (-1)^{a\cdot XL}\hat{g}(XL),$$

<u>where</u> $L' = T^{-1}$. <u>In particular, linearly (resp. affinely) equivalent Boolean functions have the same (resp. same in absolute value) Fourier spectrum.</u>

PROOF. If $h(X) = g(XT+a)$, then

$$\hat{h}(X) = \sum_v h(v)(-1)^{v\cdot x} = \sum_v g(vT+a)(-1)^{v\cdot x}$$

$$= \sum_v g(v)(-1)^{(vT^{-1}+aT^{-1})\cdot x}$$

$$= (-1)^{(aT^{-1})\cdot x} \sum_v g(v)(-1)^{(vT^{-1})\cdot x},$$

and the assertion is obtained by observing that for any vector u

$$(uT^{-1})\cdot X = uT^{-1}X' = (uT^{-1}X')' = X(T^{-1})'u' = (X(T^{-1})')\cdot u. \qquad \text{qed.}$$

DEFINITION. <u>With each function</u> $h : F^m \to C$ <u>we associate the</u> $2^m \times 2^m$ <u>matrix</u> [h] <u>whose</u> (u,v)th <u>entry is</u> $h(u+v)$.

THEOREM 3.3.3. $H_m[h]H_m^{-1} = 2^m \text{ diag } (\hat{h}(0), \hat{h}(1), \ldots, \hat{h}(2^m-1))$.

PROOF. The (u,v)th entry of the matrix on the left is

$$\frac{1}{2^m}\sum_{s,t} H_m(u,s)h(s+t)H_m(t,v) = \frac{1}{2^m}\sum_w h(w) \sum_s H_m(u,s)H_m(s+w,v)$$

$$= \frac{1}{2^m}\sum_w h(w)H_m(w,v)\sum_s H_m(u,s)H_m(v,s)$$

$$= \begin{cases} 2^m\hat{h}(v) & \text{if } u=v \\ 0 & \text{otherwise} \end{cases}.$$

qed.

COROLLARY. _Let_ $\overline{[h]}$ _denote the complex conjugate of_ [h].

$H_m[h]\overline{[h]}H_m^{-1} = 4^m \text{ diag } (|\hat{h}(0)|^2, |\hat{h}(1)|^2, \ldots, |\hat{h}(2^m-1)|^2)$.

Our next result has been called by Lechner [12] the "Poisson Summation Theorem".

THEOREM 3.3.4. _Let_ h _be an arbitrary complex-valued function on_ F^m _and let_ $\hat{h}$ _be its Fourier-transform. Let_ S _be an arbitrary subspace of_ F^m _and let_ $S^\perp$ _be the dual of_ S (i.e. $S^\perp = \{v \in F^m : v \cdot s = 0$ _for all_ $s \in S\}$. _Then_

$$\sum_{s\in S} h(s) = 2^{\dim S} \sum_{t \in S^\perp} \hat{h}(t) .$$

PROOF. $\sum_{s\in S} h(s) = \sum_{s\in S} \{ \sum_{v\in F^m} \hat{h}(v)(-1)^{v\cdot s} \} = \sum_{v\in F^m} \hat{h}(v) \{ \sum_{s\in S} (-1)^{v\cdot s} \}$

$$= 2^{\dim S} \sum_{v\in S^\perp} \hat{h}(v) \ . \qquad \text{qed.}$$

COROLLARY. <u>For any Boolean function</u> $f : F^m \to F$,

$$\sum_{u\subset v} f^*(u) = 2^{|v|} \sum_{u\subset \bar{v}} \hat{f}(u) \ .$$

The final result of this section is a special case of the Box Theorem of Chapter 1.

THEOREM 3.3.5. <u>Let</u> h <u>be any complex-valued function on</u> F^m. <u>Then for all integers</u> a, $0 \le a \le m$,

$$2^m \hat{h}^{\Box} = H_a h^{\Box} H_{m-a} \ ,$$

<u>where</u> $h^{\Box}$ (resp. $\hat{h}^{\Box}$) <u>is the</u> $2^a \times 2^{m-a}$ <u>matrix whose rows and columns are indexed by the lexicographically ordered vectors in</u> F^a <u>and</u> F^{m-a} <u>and whose</u> (u,v)th <u>entry is</u> $h(u,v)$ (resp. $\hat{h}(u,v)$).

4. Affine invariants for Boolean functions.

Let F denote the finite field $GF(2)$ and let V_m denote the m-dimensional F-linear space of m-tuples over F. Let $\mathcal{F}_m$ denote the F-algebra of functions from V_m to F. Each such function has a unique representation as a reduced (i.e. no variable appears to a power greater than one) polynomial $f(X) \equiv f(X_1, X_2, \ldots, X_m)$ in the m coordinate variables, and we find it convenient to identify the function

f with its polynomial $f(X)$. Let $\mathcal{A}_m$ denote the group of all nonsingular affine transformations A of V_m. $\mathcal{A}_m$ induces on $\mathcal{F}_m$ a group (also denoted by $\mathcal{A}_m$) of transformations given by

$$A : f(X) \to f(XA) \quad \text{for all} \quad f \varepsilon \mathcal{F}_m \, .$$

The orbits of $\mathcal{F}_m$ under the action of $\mathcal{A}_m$ then define an equivalence relation on $\mathcal{F}_m$; we say that two functions f and g in $\mathcal{F}_m$ are <u>affinely equivalent</u> if they lie in the same $\mathcal{A}_m$-orbit; i.e. if there exists a nonsingular affine transformation A of V_m such that $g(X) = f(XA)$. A fundamental problem in the study of Boolean functions is that of determining whether two given functions f and g in $\mathcal{F}_m$ are equivalent or inequivalent.

Let $\mathcal{P}$ be a mapping of $\mathcal{F}_m$ into some fixed but arbitrary set $\mathcal{S}$. We shall call $\mathcal{P}$ an <u>affine invariant</u> if $\mathcal{P}$ is constant on the equivalence classes of $\mathcal{F}_m$. The affine invariant $\mathcal{P}$ is called <u>complete</u> if it takes different values on different equivalence classes. We apply the fuzzy adjective "useful" to an affine invariant that is "easily" computed; for example, the complete affine invariant which maps a function to its equivalence class is definitely <u>not</u> a useful one.

There are several well-known affine invariants for the Boolean functions $\mathcal{F}_m$. Since a nonsingular affine transformation of variables preserves both the degree and the number of zeros of a Boolean function, the maps

$$f \to \delta(f) = \text{degree of } f$$

and $$f \to C(f) = \text{cardinality of } f^{-1}[1]$$

are both useful affine invariants which map $\mathcal{F}_m$ into Z. A less obvious but now classical and extremely useful affine invariant is the "power spectrum" of a function f; i.e. the multi-set $\{|\hat{f}(v)| : v \in V_m\}$, where $\hat{f}$ denotes the Fourier-Hadamard transform of f. Thus, the power spectrum is the absolute values of the Fourier spectrum. For many purposes these three affine invariants — cardinality, degree, and power spectrum — are sufficient to determine the inequivalence of two inequivalent functions. However, in the study of bent functions, which (as we shall see in the next chapter) are the characteristic functions of difference sets, these invariants are almost worthless. For all bent functions have exactly the same (constant) power spectrum. Furthermore, there are only two cardinalities possible for bent functions on V_{2m}, namely $2^{2m-1} \pm 2^{m-1}$ and we usually restrict our attention (by considering complements if necessary) to those having the smaller cardinality. Thus, if we wish to check two bent functions f and g for inequivalence, all we have left at our disposal is the degree criterion. If the functions in question happen to have the same degree we are lost. We need a more discriminating test function. We now proceed to fill that need.

Let f be an arbitrary function in $\mathcal{F}_m$. For any subspace S of V_m we define the derivative of f with respect to S, denoted f_S, by

$$f_S(X) = \sum_{s \in S} f(X+s) .$$

We say that f_S is an e-dimensional derivative if the subspace S has dimension e. If the 1-dimensional subspace S contains the nonzero vector s, than we denote the derivative by f_s and call this derivative

$$f_s(X) = f(X) + f(X+s)$$

simply the directional derivative of f in the direction s.

We now make a simple observation which has far-reaching consequences.

THEOREM 3.4.1. For any function f in $\mathcal{F}_m$ let $\mathcal{D}_e(f)$ denote the multi-set of all e-dimensional derivatives of f. If f and g in $\mathcal{F}_m$ are affinely equivalent, then $\mathcal{D}_e(f)$ and $\mathcal{D}_e(g)$ are affinely equivalent. Indeed, if the nonsingular affine transformation A (operating on $\mathcal{F}_m$) maps f onto g then it also maps $\mathcal{D}_e(f)$ onto $\mathcal{D}_e(g)$.

PROOF. Suppose that $g(X) = f(XA) = f(XL+a)$ where L is a nonsingular linear transformation of V_m and a is some fixed vector in V_m. Let S be an arbitrary e-dimensional subspace of V_m. Then

$$g_S(X) = \sum_{s\varepsilon S} g(X+s) = \sum_{s\varepsilon S} f(XL + sL + a) = f_{SL}(XA).$$

Since the map $S \to SL$ is a permutation of the family of all e-dimensional subspace S of V_m, the result follows. qed.

COROLLARY. *If $\mathcal{P}$ is any affine invariant for $\mathcal{F}_m$, then*

$$f \to \mathcal{P}\{\mathcal{D}_e(f)\}$$

is also an affine invariant for $\mathcal{F}_m$.

A consequence worth stating explicitly is the

THEOREM 3.4.2. *For any function f in $\mathcal{F}_m$ let $\mathcal{D}_e(f)$ denote the multi-set of all e-dimensional derivatives of f. Suppose that f and g in $\mathcal{F}_m$ are affinely equivalent. Then it must be true that*

1) $C\{\mathcal{D}_e(f)\} = C\{\mathcal{D}_e(g)\}$;

2) $\delta\{\mathcal{D}_e(f)\} = \delta\{\mathcal{D}_e(g)\}$;

3) $PS\{\mathcal{D}_e(f)\} = PS\{\mathcal{D}_e(g)\}$,

where C, δ, and PS denote the "cardinality", "degree", and "power spectrum" affine invariants, respectively.

We note that $\delta(f)$ and $PS(f)$ are trivially obtained from the polynomial representation of f and the Fourier transform of f, respectively; and both the polynomial and Fourier transforms are easily computed from the truth-table of f via familiar fast transform algorithms. Furthermore, the directional derivatives of a function f are also easily computed (via "fast" algorithms) from the truth-table of f; and the invariant $C\{\mathcal{D}_1(f)\}$ may be obtained directly from the Fourier transform of f via the convolution theorem.

When $e=0$ the set $\mathcal{D}_e(f)$ is comprised of just f itself and our invariants given by Theorem 3.4.2 are simply the classical invariants C, δ, and PS. Our invariants with $e>0$ will prove to be extremely useful in the sequel.

CHAPTER IV

PALL PARTITIONS FOR QUADRATIC FORMS

1. Introduction.

Gordon Pall [21] has introduced the fruitful notion of partitioning the zeros of a nonsingular quadratic form over a field F into pairwise disjoint (except for 0) maximal isotropic subspaces. These subspaces are all of the same dimension, called the index of the form [1]. We shall call such a partition P a Pall partition of the associated quadric; we also say that P is a Pall partition for the quadratic form. Pall exhibited such partitions for the forms

$$\Psi_n = \sum_{i=1}^{n} X_i X_{n+i} \text{ (equivalent to } \sum_{i=1}^{n} (X_i^2 - X_{n+i}^2) \text{ if char } F \neq 2)$$

over formally real fields for $n = 1, 2, 4, 8$ and for the form

$$X_1^2 + X_2^2 + X_3^2 + X_4^2$$

over any finite field GF(p), p an odd prime. Pall's student L. Couvillon [5] showed that a Pall partition exists for Ψ_2 over any field, while if n is odd and greater than 1 then there does not exist a Pall partition for Ψ_n over any field which is formally real or finite of odd characteristic. Couvillon also exhibited a Pall partition for the form

$$X_1X_2 + X_3X_4 + X_5^2$$

over GF(2).

In this chapter we settle completely the question of the existence of a Pall partition for any nonsingular quadratic form over a finite field of characteristic 2. If $F = GF(q)$, q a power of 2, then a classical result of Dickson [8] guarantees that any nonsingular m-ary quadratic form $Q(X) \equiv Q(X_1, X_2, \ldots, X_m)$ over F is equivalent (under some nonsingular F-linear transformation of variables) to one of the canonical forms

I. $\Psi_n = X_1X_{n+1} + X_2X_{n+2} + \ldots + X_nX_{2n}$

II. $\Phi_n = \Psi_{n-1} + \alpha X_n^2 + X_nX_{2n} + \alpha X_{2n}^2$

if $m = 2n$, or

III. $\rho_n = \Psi_n + X_{2n+1}^2$

if $m = 2n + 1$.

For forms of Type II α may be chosen to be any nonzero element of F which makes the polynomial $\alpha z^2+z+\alpha$ irreducible over F (equivalently, α has trace 1 with respect to the extension F over GF(2)). The forms of Types I, II, and III have index n, n-1, and n respectively [9], and the associated quadrics have cardinalities $1 + (q^{n-1}+1)(q^n-1)$, $1 + (q^n+1)(q^{n-1}-1)$, and $q^{2n}=1 + (q^n+1)(q^n-1)$, respectively. Thus the cardinality of a nonsingular quadric over F determines its canonical form.

It turns out that Couvillon's result on the nonexistence of a Pall partition for the forms Ψ_n with $n>1$ odd remains true over the fields $GF(2^N)$ (in fact, it's true over any field!). In every other case, however, a Pall partition does exist. We can therefore state the

THEOREM 4.1.1. *There exists a Pall partition for every nonsingular quadratic form over* $GF(2^N)$, *except those equivalent to*

$$\Psi_n = X_1X_{n+1} + X_2X_{n+2} + \ldots + X_nX_{2n}$$

with $n>1$ *odd in which case no such partition exists.*

In the next two sections we exhibit Pall partitions for forms of Types II and III. The most interesting case, Type I, is treated in sections 4 and 5. In section 4 we exhibit a Pall partition for those forms of Type I with n even. In the special case of $F = GF(2)$ our construction is very closely related to a recent result of A. M. Kerdock in the theory of error-correcting codes [11]. Our results also show that the quadric associated with Ψ_n on F^{2n}, $F = GF(2)$, belongs to the family of "partial spread" difference sets which are discussed in the next chapter. Furthermore, our construction for difference sets comprising our FAMILY H of the last chapter was in fact suggested by our Pall partition of the forms of Type II.

In the last section we generalize the result of Couvillon by showing in an extremely simple manner that for $n>1$ odd there does not exist a Pall partition for the form Ψ_n over any field whatsoever.

Caveat lector: Given a quadratic form Q on an F-linear space V, we say that a subspace $W \subset V$ is *isotropic* if $Q(W) = \{0\}$. This definition is equivalent to the usual one [1] if char $F \neq 2$. Dieudonné [9] uses the term "singular".

2. A Pall partition for forms of Type II.

The nonsingular quadratic forms of Type II over $F = GF(q)$, $q = 2^N$, are equivalent to the canoncial form

$$\Phi_n = X_1X_{n+1} + X_2X_{n+2} + \ldots + X_{n-1}X_{2n-1} + \alpha X_n^2 + X_nX_{2n} + \alpha X_{2n}^2 ,$$

where α is any nonzero element of F which makes the polynomial $\alpha z^2+z+\alpha$ irreducible over F (equivalently, α has trace 1 with respect to the extension F over GF(2)). This form has index n-1 and the associated quadric has cardinality $1 + (q^n+1)(q^{n-1}-1)$. Thus, any Pall partition of the quadric must be comprised of q^n+1 pairwise "disjoint" F-linear subspaces of dimension n-1.

Now let $L = GF(q^n)$ be the degree n extension of F and let $K = GF(q^{2n})$ be the quadratic extension of L. Let $Q: K \to L$ be the map given by

$$Q(X) = Tr_{L/F}\{X^{q^n+1}\} ,$$

where $Tr_{L/F}\{\cdot\}$ denotes the trace with respect to the extension L/F; i.e.

$$Tr_{L/F}\{z\} = z + z^q + \ldots + z^{q^{n-1}} .$$

Then Q is a quadratic map on the 2n-dimensional F-linear space K and Q has $1 + (q^n+1)(q^{n-1}-1)$ zeros on K.

NOTE. Formally, for any basis $B_1, B_2, \ldots, B_{2n}$ for K over F, the map Q is given by the polynomial

$$Q(X) = Q(\Sigma X_i B_i) = Tr_{L/F}\{(\Sigma X_i B_i)^{q^n+1}\} = \Sigma(Tr_{L/F}\{B_i^{q^n} B_j\}) X_i X_j$$

which is a quadratic form in the coordinate variables $X_1, X_2, \ldots, X_{2n}$. Alternatively, we may simply observe that Q satisfies the quadratic criteria [1]:

1) $Q(\alpha X) = \alpha^2 Q(X), \alpha\varepsilon F$;

2) $Q(X+Y) - Q(X) - Q(Y)$ bilinear on $K \times K$.

Thus, Q is equivalent to Φ_n and it suffices to exhibit a Pall partition for Q. But this is very easy to do.

If S denotes the kernel of the trace $Tr_{L/F}$ on L, then S is invariant under the map

$$z \to z^2$$

and it is clear that Q vanishes on each of the (n-1)-dimensional F-linear subspaces θS of K where θ is any $(q^n+1)^{th}$ root of unity in K; i.e. for any $s\varepsilon S$

$$Q(\theta s) = Tr_{L/F}\{(\theta s)^{q^n+1}\} = Tr_{L/F}\{s^2\} = (Tr_{L/F}\{s\})^2 = 0.$$

These q^n+1 subspaces are disjoint (except for 0) since their nonzero elements are subsets of the q^n+1 distinct multiplicative cosets of

$L^* = L\backslash\{0\}$ in $K^* = K\backslash\{0\}$. It follows that for any primitive $(q^n+1)^{th}$ root of unity θ the spaces

$$\mathcal{P} = \{\theta^t S\colon 0 \leq t \leq q^n\} \text{ constitute a Pall partition for } Q.$$

3. A Pall partition for form of Type III.

The nonsingular quadratic forms of Type III over $F = GF(q)$, $q = 2^N$, are equivalent to the canonical form

$$\rho_n = X_1X_{n+1} + X_2X_{n+2} + \ldots + X_nX_{2n} + X_{2n+1}^2$$

which has index n and whose associated quadric has cardinality $q^{2n} = 1 + (q^n+1)(q^n-1)$. Thus, any Pall partition for such a form must be comprised of q^n+1 pairwise "disjoint" F-linear subspaces of dimension n.

Now the quadratic map

$$Q(X,Y,Z) = \mathrm{Tr}_{L/F}\{XY\} + Z^2$$

on the (2n+1)-dimensional F-linear space $V = L \oplus L \oplus F$, $L = GF(q^n)$, clearly has q^{2n} zeros. Furthermore, the linear map

$$Q(X+a,\ Y+b,\ Z+c) - Q(X,Y,Z) - Q(a,b,c) = \mathrm{Tr}_{L/F}\{bX+aY\}$$

vanishes identically on V precisely when $a = 0 = b$, so that Q has defect 1 and is therefore nonsingular. Thus, the forms of Type III are equivalent to Q and it suffices to exhibit a Pall partition of its zeros. The family P consisting of the subspaces

$$X = 0 = Z$$

and

$$Y = a^2X; \; Z = Tr_{L/F}\{aX\}, \; a \in L,$$

is easily seen to have all the necessary properties.

4. A Pall partition for forms of Type I, n even.

The nonsingular quadratic forms of Type I over $F = GF(q)$, $q = 2^N$, are equivalent to the canonical form

$$\Psi_n = X_1X_{n+1} + X_2X_{n+2} + \ldots + X_nX_{2n}$$

which has index n and whose associated quadric has cardinality $1 + (q^{n-1}+1)(q^n-1)$. Thus, any Pall partition of the quadric must be comprised of $q^{n-1}+1$ pairwise "disjoint" F-linear subspaces of dimension n. We shall show in the next section that such a partition cannot exist if $n>1$ is odd. Thus, we shall assume here that n is even.

The quadratic map Q given by

$$Q(X,x,Y,y) = Tr_{M/F}\{XY\} + xy$$

on the 2n-dimensional F-linear space $M \oplus F \oplus M \oplus F$, $M = GF(q^{n-1})$, has $1 + (q^{n-1}+1)(q^n-1)$ zeros, so that Ψ_n is equivalent to Q and it suffices to exhibit a Pall partition for the zeros of Q.

THEOREM 4.4.1. *For each* $\alpha \in M$, *let* L_α *be the endomorphism of* $V = M \oplus F$ *given by*

$$L_\alpha(X,x) = (\alpha^2 X + \alpha\tau\{\alpha X\} + \alpha x,\ \tau\{\alpha X\}),$$

where $\tau \equiv Tr_{M/F}$, *the trace with respect to the extension* M/F, *and let* S_α *be the subspace of* $V \oplus V$ *given by*

$$S_\alpha = \{(X,x,Y,y) : (Y,y) = L_\alpha(X,x)\}.$$

Then the $q^{n-1}+1$ *subspaces*

$$S_\infty = \{(X,x,Y,y) : X = 0 = x\};\quad S_\alpha\ ,\ \alpha \in M$$

constitute a Pall partition for the quadratic form

$$Q(X,x,Y,y) = \tau\{XY\} + xy \quad \textit{on} \quad V \oplus V\ .$$

PROOF. It is clear that Q vanishes on each of these subspaces and that they all have dimension n. Thus we need only show that they are pairwise "disjoint". The subspace S_∞ is certainly disjoint from each of the subspaces S_α, $\alpha \in M$, so it suffices to show that the subspaces S_α are pairwise "disjoint".

To this end we suppose that the point (X,x,Y,y) lies in both S_α and S_β, $\alpha \neq \beta$; i.e.

$$(\alpha^2 X + \alpha\tau\{\alpha X\} + \alpha x,\ \tau\{\alpha X\}) = (\beta^2 X + \beta\tau\{\beta X\} + \beta x,\ \tau\{\beta X\}).$$

Then equating second coordinates yields

$$\tau\{\alpha X\} = \tau\{\beta X\},$$

while equating first coordinates yields

$$(\alpha+\beta)((\alpha+\beta)X + \tau\{\alpha X\} + x) = 0$$

or (since $\alpha \neq \beta$)

$$(*) \quad (\alpha+\beta)X = \tau\{\alpha X\} + x.$$

Since the right side of (*) is an element of F, so must be the left side. Furthermore, since $n-1$, the degree of M over F, is odd we may write

$$(\alpha+\beta)X = \tau\{(\alpha+\beta)X\} = 0.$$

Thus, $X = 0$ which implies by (*) that $x = 0$. Hence, S_α and S_β do indeed intersect only in the zero vector and our proof is complete. qed.

5. A nonexistence theorem.

Consider the quadratic form

$$\Psi_n = X_1X_{n+1} + X_2X_{n+2} + \dots + X_nX_{2n}, \quad n>1 \text{ odd},$$

over an arbitrary field F. Again the index is n so that a Pall partition certainly must contain at least three subspaces (the maximal isotropic subspaces $X_1 = X_2 = \dots = X_n = 0$ and $X_{n+1} = X_{n+2} = \dots = X_{2n} = 0$ do not account for all the zeros of Ψ_n). The nonexistence of a Pall partition will follow from the following generalization of Couvillon's theorem.

THEOREM 4.5.1. *For odd* n *there does not exist a family of three pairwise "disjoint"* n*-dimensional subspaces of* F^{2n} *on which* Ψ_n *vanishes.*

PROOF. Consider the equivalent form

$$Q(X,Y) = X_1Y_1 + X_2Y_2 + \dots + X_nY_n$$

on $F^n \oplus F^n$, and suppose that Q vanishes on the pairwise "disjoint" subspaces A, B, and C. By Witt's Theorem [9] we may assume that A is the subspace $X = 0$. Since B and C are disjoint from A, they must be given by

$$B = \{(X, XL_B) : X \varepsilon F^n\}; \quad C = \{(X, XL_C) : X \varepsilon F^n\},$$

where L_B and L_C are $n \times n$ matrices over F. Since B and C are disjoint, $L_C - L_B$ is nonsingular. But B and C isotropic implies that the forms

$$XL_BX' \quad \text{and} \quad XL_CX'$$

vanish identically on F^n, so that L_B and L_C are skew-symmetric (with 0 diagonal). Thus, $L_C - L_B$ is a nonsingular skew-symmetric matrix of order n. It follows that n must be even. qed.

COROLLARY. *There does not exist a Pall partition for any nonsingular quadratic form over* $GF(2^N)$ *which is of Type* I *with* $n>1$ *odd*.

This corollary, together with the results of sections 2, 3, and 4, completes the proof of our theorem stated in the introduction.

CHAPTER V

PARTIAL SPREADS AND HADAMARD DIFFERENCE SETS

1. Introduction.

It seems quite reasonable to try to construct a difference set in a group by fitting together some large pieces which behave well, individually and in pairs. An obvious choice is to pick pieces which are subgroups. To insure that they behave well in pairs we might require that any two of these subgroups generate the whole group. But surely mustn't such a naive approach come to nought? Surprisingly, the answer is, "No!". This simple idea leads to a very rich family of Hadamard difference sets.

In section 2 we formalize our ideas sketched above and determine the conditions necessary for the existence of such a difference set. In section 3 we find all abelian groups which meet the conditions — but for some small exceptions these are precisely the elementary abelian 2-groups. In section 4 we show that the elementary 2-groups contain an enormous number of these difference sets and we exhibit several classes of them. These new difference sets are examined more closely in the next chapter.

2. Partial spreads and Hadamard difference sets.

We now suppose that G is a group of square order $v = M^2$. In this section we use multiplicative notation for the group operation and we do not assume that G is abelian. We define a partial spread for G to be a family of pairwise disjoint (except for 1) subgroups of order M. These subgroups are called the components of the partial spread. A partial spread containing $M + 1$ components (so that every element $g \neq 1$ of G is in exactly one component) is called simply a spread. This terminology is consistent with that used in the theory of finite translation planes [20] where the group G is an even-dimensional vector space over a finite field.

Now let

$$\mathcal{H} : H_1, H_2, \ldots, H_N$$

be a partial spread for G, and for i, $1 \leq i \leq N$, let H_i^* denote the set of nonidentity elements of H_i. Then, employing the notation of the group ring $Z[G]$, we have the easy

REMARK 5.2.1. For all i,j, $1 \leq i, j \leq N$,

$$H_i^* H_j^* = \begin{cases} 1 + (M-2)H_i & \text{if } i=j \\ 1 + G - H_i - H_j & \text{if } i \neq j \end{cases} .$$

Let D be the set of nonidentity elements in the union of the partial spread $\mathcal{H}$; i.e.

$$D = \sum_{i=1}^{N} H_i^* .$$

Then, using Remark 5.2.1, we obtain

$$D^{(-1)}D = D^2 = \{\sum H_i^*\}^2$$

$$= \sum_i H_i^{*2} + \sum_{i\neq j} H_i^* H_j^*$$

$$= \sum_i \{1+(M-2)H_i\} + \sum_{i\neq j} \{1+G-H_i-H_j\}$$

$$= N+(M-2)\sum H_i + N(N-1)(1+G) - 2(N-1)\sum H_i$$

$$= N^2 + N(N-1)G + (M-2N)\sum H_i .$$

Thus, D is a (nontrivial) difference set precisely when $M=2N$, in which case D has parameters

$$v=M^2=4N^2, \quad k=N(M-1)=2N^2-N, \quad \lambda=\frac{k(k-1)}{v-1}=N^2-N, \quad n=N^2.$$

Consequently, all difference sets constructed in this way are Hadamard.

Suppose that the partial spread $\mathcal{H}$ can be extended to a partial spread $\mathcal{H}'$ by the adjunction of another component H_{N+1}. Let E be the union of all components in $\mathcal{H}'$; i.e.

$$E = D + H_{N+1}.$$

Then for all i, $1 \le i \le N$, we have

$$H_i^* H_{N+1} = G - H_{N+1} = H_{N+1}H_i^*,$$

so that

$$E^{(-1)}E = E^2 = (D + H_{N+1})^2$$

$$= D^2 + DH_{N+1} + H_{N+1}D + H_{N+1}^2$$

$$= D^2 + \sum_i \{H_i^* H_{N+1} + H_{N+1} H_i^*\} + MH_{N+1}$$

$$= D^2 + 2\sum_i \{G - H_{N+1}\} + MH_{N+1}$$

$$= D^2 + 2NG + (M - 2N) H_{N+1}$$

$$= N^2 + N(N+1)G + (M - 2N) \sum_{i=1}^{N+1} H_i .$$

Thus, again, we see that E is a difference set precisely when $M = 2N$; this set has parameters

$$v=M^2=4N^2, \quad k=N(M-1)+M=2N^2+N, \quad \lambda=\frac{k(k-1)}{v-1}=N^2+N, \quad n=N^2.$$

We summarize the above results in the

THEOREM 5.2.2. Let $H_1, H_2, \ldots, H_r$ be a partial spread for G. Then

$$D = (\cup H_i)\setminus\{1\} \quad (\text{resp. } D = \cup H_i)$$

is a difference set if and only if G has order $4N^2$ and $r=N$ (resp. $r = N+1$). These difference sets are Hadamard with parameters

$$(4N^2,\ 2N^2-N,\ N^2-N,\ N^2) \text{ and } (4N^2,\ 2N^2+N,\ N^2+N,\ N^2), \text{ respectively.}$$

We note here that these difference sets are fixed by the "inverse" mapping on G even though this map may not be an automorphism. Consequently, the (± 1)-incidence matrix $[\mathcal{D}^*]$, defined by

$$[\mathcal{D}^*](x,y) = \begin{cases} -1 & \text{if } xy^{-1} \varepsilon D \\ 1 & \text{otherwise} \end{cases},$$

is a regular, symmetric Hadamard matrix with constant diagonal.

We call the difference sets of Theorem 5.2.2 partial spread difference sets; those of cardinality $2N^2-N$ (resp. $2N^2+N$) are said to be of type $PS^{(-)}$ (resp. $PS^{(+)}$). Clearly, any $PS^{(+)}$ set contains $PS^{(-)}$ sets, obtained by deleting a component. However, not every $PS^{(-)}$ set can be extended to one of type $PS^{(+)}$. Also, while the difference sets of types $PS^{(-)}$ and $PS^{(+)}$ have complementary parameters (i.e. each type has the parameters of the complement of the other type), not every $PS^{(+)}$ set is equivalent to the complement of a $PS^{(-)}$ set. Examples given in the next section attest these assertions.

3. Groups having partial spread difference sets.

We now proceed to determine all abelian groups which have partial spread difference sets. For the remainder of this chapter we use additive notation for all groups. We assume G is abelian of order $4N^2$; we seek those groups G which have a partial spread of cardinality N or $N+1$. Equivalently, we seek those groups of order $4N^2$ which have either N or $N+1$ pairwise "disjoint" subgroups of order $2N$.

When $N=1$ the group G, of order 4, must be either the cyclic group, denoted Z_4, or the Klein 4-group which we (following Turyn [24]) denote be K_4. K_4 has three (pairwise disjoint) subgroups of order 2, while Z_4 has a unique subgroup of order 2. Thus, K_4 contains difference sets of both types $PS^{(-)}$ and $PS^{(+)}$ while Z_4 has a unique $PS^{(-)}$ difference set. Of course, all of these sets are singletons or complements of singletons, and are therefore trivial.

In the case $N=2$ G has order $4N^2=16$. If G has two disjoint subgroups of order 4, say H_1 and H_2, then

$$G = H_1 \oplus H_2 ,$$

where each of H_1 and H_2 may be either Z_4 or K_4.

$$K_4 \oplus K_4,\ K_4 \oplus Z_4,\ \text{and } Z_4 \oplus Z_4$$

all have difference sets of type $PS^{(-)}$. If G contains a third subgroup H_3 disjoint from both H_1 and H_2, then clearly

$$G = H_1 \oplus H_2 = H_1 \oplus H_3 = H_2 \oplus H_3$$

and it follows that H_1, H_2, and H_3 are all isomorphic. Thus, we may write

$$G = H \oplus H$$

where H is either K_4 or Z_4; and, in either case,

$$H_1 = \{(0,h):h\varepsilon H\},\ H_2 = \{(h,0):h\varepsilon H\},\ H_3 = \{(h,h):h\varepsilon H\}$$

is a partial spread of cardinality $3 = N+1$. Thus, for $N=2$ $K_4 \oplus K_4$, $Z_4 \oplus Z_4$, and $K_4 \oplus Z_4$ all have $PS^{(-)}$ difference sets, while only the first two of these groups have a $PS^{(+)}$ difference set.

In the case $N=3$ a group G of order $4N^2=36$ which contains two disjoint subgroups of order 6 can only be

$$G = Z_6 \oplus Z_6,$$

which does have a partial spread of $N=3$ components; namely,

$$\{(0,X):X\varepsilon Z_6\},\ \{(X,0):X\varepsilon Z_6\},\ \{(X,X):X\varepsilon Z_6\},$$

the nonzero elements in the union of which do consequently constitute a (36,15,6,9)-difference set in G. Since $G = Z_6 \oplus Z_6$ has only three elements of order 2, G cannot have a partial spread with $N+1=4$ components.

We have so far determined all groups of order $4N^2$, $N \leq 3$, which have *PS* difference sets. So that we may more easily investigate the question for larger N we now develop a very useful characterization of partial spreads having at least three components. Again, these ideas are an obvious extension of well-known results in the theory of finite translation planes [20].

Suppose that

$$\mathcal{H} : H_1, H_2, H_3, \ldots, H_{r+2}$$

is a partial spread for G containing $r + 2 \geq 3$ components. It is clear that

$$G = H_i \oplus H_j$$

for all $i \neq j$, and it follows that all components H_i are isomorphic to the same group, say H. Thus, G is isomorphic to $H \oplus H$ and there exists an isomorphism α of G onto $H \oplus H$ which takes the partial spread $\mathcal{H}$ of G onto a partial spread $\mathcal{H}^\alpha$ of $H \oplus H$, and, in particular, takes the two components H_{r+1} and H_{r+2} of $\mathcal{H}$ onto

$$H^\alpha_{r+1} = \{(0,h):h\varepsilon H\} \text{ and } H^\alpha_{r+2} = \{(h,0):h\varepsilon H\}.$$

We shall identify G with its image $H \oplus H$ and relabel the components of the partial spread, so that we may assume without loss of generality that $G = H \oplus H$ has the partial spread

$$\mathcal{H} : H_\infty, H_0, H_1, \ldots, H_r$$

where $H_\infty = \{(0,X):X\varepsilon H\}$ and $H_0 = \{(X,0):X\varepsilon H\}$.

Now consider any component H_i, $i \geq 1$, and let (X_1,Y_1) and (X_2,Y_2) be elements of H_i. Then H_i, being a group, contains (X_2-X_1, Y_2-Y_1). Since

$$H_i \cap H_\infty = \{(0,0)\} = H_i \cap H_0,$$

it is clear that

$$X_1 = X_2 \Longleftrightarrow Y_1 = Y_2 .$$

In other words, there exists a permutation α_i of H such that

$$H_i = \{(X,X\alpha_i):X\varepsilon H\}.$$

Furthermore, since, for all X_1,X_2 in H, the element

$$(X_1+X_2, (X_1+X_2)\alpha_i) - (X_1,X_1\alpha_i) - (X_2,X_2\alpha_i)$$

$$= (0, (X_1+X_2)\alpha_i - X_1\alpha_i - X_2\alpha_i)$$

belongs to H_i, it follows that

$$(X_1+X_2)\alpha_i = X_1\alpha_i + X_2\alpha_i;$$

thus α_i is in fact an automorphism of H. Since, for any $i \neq j$, the components H_i and H_j intersect only in $(0,0)$, the corresponding automorphisms α_i and α_j cannot take the same value on any nonzero element of H. Thus, the endomorphisms $\alpha_i - \alpha_j$ of H given by

$$\alpha_i - \alpha_j : X \to (X\alpha_i) - (X\alpha_j)$$

are also automorphisms of H. We thus have the

THEOREM 5.3.1. *Let H be an abelian group and let*

$$\alpha_1, \alpha_2, \ldots, \alpha_r, \; r \geq 1,$$

be automorphisms of H with the property that no two take the same value on any nonzero element of H. Let

$$\mathcal{H} : H_\infty, H_0, H_1, \ldots, H_r$$

be the family of subgroups of $G = H \oplus H$ *given by*

$$H_\infty = \{(0,X) : X \varepsilon H\}; \; H_0 = \{(X,0) : X \varepsilon H\}; \; H_i = \{(X, X\alpha_i) : X \varepsilon H\}, \; 1 \leq i \leq r.$$

Then $\mathcal{H}$ *is a partial spread for G. Further, any partial spread for G of cardinality r+2 is equivalent under some automorphism of G to a partial spread of this type.*

REMARK 5.3.2. *By applying if necessary the automorphism*

$$(X,Y) \to (X, Y\alpha_1^{-1})$$

of G we may obtain an equivalent partial spread for G in which α_1 *is the identity automorphism. The other automorphisms* α_i, $2 \leq i \leq r$, *must then have no nonzero fixed points.*

NOTE: In the first part of Theorem 5.3.1 the group H need not be abelian. Indeed, if we take H to be the symmetric group S_3 we obtain for the group $G = S_3 \oplus S_3$ the partial spread

$$\{(0,X):X\varepsilon S_3\},\ \{(X,0):X\varepsilon S_3\},\ \{(X,X):X\varepsilon S_3\},$$

the nonidentity elements in whose union constitute a (36,15,6,9)-difference set in G.

We are now in a position to determine the abelian groups G of order $4N^2$, N>3, which have a partial spread of cardinality N (and consequently a partial spread difference set). We first show that such a group must be a 2-group.

THEOREM 5.3.3. *If the abelian group G of order $4N^2$, N>3, has a partial spread of cardinality N, then $N = 2^{m-1}$ for some $m \geq 3$.*

PROOF. Put $N = 2^{m-1}N_1$ with $m \geq 1$ and N_1 odd. Then G, of order $4N^2=2^{2m}N_1^2$, has $2^{2m}-1$ elements of order a power of 2; while any subgroup of order $2N=2^mN_1$ has 2^m-1 elements of order a power of 2. It follows that a partial spread for G can have at most 2^m+1 components.

If G has a partial spread with N components we must have

$$2^{m-1}N_1 = N \leq 2^m+1.$$

The only solutions to this inequality are

$$N_1 = 3 = N;\ m=1,$$

which violates our hypothesis on N, and qed.

$$N_1 = 1;\quad m \text{ arbitrary.}$$

THEOREM 5.3.4. *Let* G *be an abelian group of order* 4^m, $m > 2$. *Then* G *has a partial spread of cardinality* 2^{m-1} *only if* G *is elementary*.

PROOF. We may assume that $G = H \oplus H$, where H is a subgroup of order 2^m isomorphic to each component of the partial spread. According to our Theorem 5.3.1 there must exist $2^{m-1}-2$ automorphisms of H with the property that no two of these automorphisms agree on any nonzero element of H. In particular, for any element θ in H of order 2, the $2^{m-1}-2$ automorphisms of H map θ to $2^{m-1}-2$ distinct elements of order 2. Thus, the group H must contain at least $2^{m-1}-2$ elements of order 2.

But suppose that

$$H \cong Z_{2^{a_1}} \oplus Z_{2^{a_2}} \oplus \ldots + Z_{2^{a_s}},$$

where $a_i \geq 1$, $1 \leq i \leq s$, and $\Sigma a_i = m$. Then each direct summand $Z_{2^{a_i}}$ has a unique element of order 2 and the entire group H contains precisely 2^s-1 elements of order 2. We thus have

$$2^{m-1}-2 \leq 2^s-1,$$

which implies that only the following two possibilities exist:

Case I. $s=m-1$ and $H \cong Z_4 \oplus Z_2^{m-2}$

Case II. $s=m$ and $H \cong Z_2^m$.

We complete our proof by showing that Case I cannot occur. According to our Remark 5.3.2 H must have $2^{m-1}-3 > 1$ automorphisms which fix no nonzero element of H. We show that

$$H = Z_4 \oplus Z_2^{m-2}$$

has no such automorphism. For let a be a generator of Z_4. Any automorphism α of H must map (a,0) to an element of one of the forms

$$(a,b) \quad \text{or} \quad (-a,b)$$

where b is in Z_2^{m-2}. But, in either case, α maps (2a,0) onto $2(a,0) = (2a,2b) = (2a,0)$. Thus, every automorphism of $Z_4 \oplus Z_2^{m-2}$ has a (nonzero) fixed point and Case I is impossible. qed.

In the next section we exhibit partial spreads of cardinality 2^{m-1} and $2^{m-1}+1$ for all elementary abelian groups $G = Z_2^{2m}$. We may thus combine the results of sections 3 and 4 and state the

THEOREM 5.3.5 a) *The groups*

$$Z_4;\ Z_2 \oplus Z_2 \oplus Z_4;\ Z_6 \oplus Z_6;\ Z_4 \oplus Z_4;\ \text{and}\ Z_2^{2m},\ m \geq 1,$$

all have $PS^{(-)}$ difference sets. b) *All but the first three of these groups have $PS^{(+)}$ difference sets.* c) *No other abelian group has a partial spread difference set.*

4. Elementary abelian 2-groups.

In this section we restrict our attention to elementary abelian 2-groups. We usually take such a group G of order 2^{2m} to be Z_2^{2m}, but it is sometimes convenient to regard G as one or another of several (2m)-dimensional linear spaces over the field of two elements. We have seen in chapter 2 that a difference set in G must have parameters

$$(v,k,\lambda,n) = (4N^2,\ 2N^2-N,\ N^2-N,\ N^2) \text{ or } (4N^2,\ 2N^2+N,\ N^2+N,\ N^2),$$

where $N = 2^{m-1}$. Thus the cardinality of a difference set in G completely determines its parameters. We also saw in Chapter 2 that the subset D of G is a difference set if and only if

$$\chi(D) = \pm N$$

for all nonprincipal characters χ of G.

Recall that a <u>partial spread</u> for Z_2^{2m} is a collection of pairwise disjoint (except for 0) subgroups of order 2^m. A partial spread containing 2^m+1 components is called simply a <u>spread</u>.

We restate here, for the group Z_2^{2m}, our construction theorem for partial spread difference sets (Theorem 5.2.2). We give here a different (shorter) proof which uses the group character characterization of difference sets.

THEOREM 5.4.1. <u>Let</u> $G = Z_2^{2m}$ <u>and let</u> $\mathcal{A}$ <u>and</u> $\mathcal{B}$ <u>be partial spreads for</u> G <u>of cardinality</u> N <u>and</u> $N+1$ <u>respectively</u>, $N = 2^{m-1}$. <u>Then the sets</u>

$$D = \left(\bigcup_{A\in\mathcal{A}} A\right) \setminus \{0\} \quad \text{and} \quad E = \bigcup_{B\in\mathcal{B}} B$$

<u>are difference sets in</u> G <u>with parameters</u>

$$(4N^2,\ 2N^2-N,\ N^2-N,\ N^2) \quad \text{and} \quad (4N^2,\ 2N^2+N,\ N^2+N,\ N^2), \text{ respectively.}$$

PROOF. We have $D = \bigcup_{A \varepsilon \mathcal{A}} A^*$, $A^* = A \setminus \{0\}$.

For any subgroup S of G, let $\tilde{S}$ denote the subgroup of characters of G which induce the principal character on S. Then for any nonprincipal character χ of G

$$\chi(D) = \sum \chi(A^*) = \begin{cases} N(-1) & \text{if } \chi \notin \tilde{A} \text{ for all } A \varepsilon \mathcal{A} \\ (N-1)(-1) + (2N-1) = N & \text{otherwise.} \end{cases}$$

Thus, $\chi(D) = \pm N$ for all nonprincipal characters χ of G and it follows that D is a difference set.

Now suppose that $\mathcal{B} = \mathcal{A} \cup \{B\}$, so that $E = D \cup B$. Then for any nonprincipal character χ of G

$$\chi(E) = \chi(D) + \chi(B) = \begin{cases} \chi(D) & \text{if } \chi \notin \tilde{B} \\ -N+2N = N & \text{if } \chi \varepsilon \tilde{B} \end{cases} .$$

Since D is a difference set, so is E. qed.

We shall say that the partial spread difference sets D and E of Theorem 5.4.1 are of type $PS^{(-)}$ and $PS^{(+)}$, respectively. We shall call partial spreads of cardinality N or $N+1$ <u>Hadamard partial spreads</u> (since they give rise to Hadamard difference sets). Thus, in order to obtain (partial spread) difference sets in G, all we need do is find some Hadamard partial spreads. The following well-known result shows that Hadamard partial spreads abound in Z_2^{2m}.

REMARK 5.4.2. <u>The 2^m+1 lines through the origin constitute a spread for the affine plane</u> $L \oplus L$, $L = GF(2^m)$.

PROOF. The affine plane $L \oplus L$ consists of all points (X,Y) with X and Y in L. As an additive group it is isomorphic to $Z^m \oplus Z^m \cong Z_2^{2m}$. A line in the plane is a set of points (X,Y) determined by an equation of the form

$$X = b,\ b\varepsilon L$$

or

$$Y = mX+b,\ m,b\varepsilon L.$$

The lines through the origin are those with $b=0$, i.e.

$$L_\infty : X = 0$$

$$L_m : Y = mX,\ m\varepsilon L.$$

Thus, $L_\infty = \{(0,Y):Y\varepsilon L\}$ and $L_m = \{(X,mX):X\varepsilon L\}$, $m\varepsilon L$. It is clear that these lines are all isomorphic to L as additive groups so that they are indeed subgroups of $L \oplus L$ of order 2^m. That any two of these lines intersect only in the origin (i.e. $(0,0)$) is obvious. qed.

Combining Theorem 5.4.1 with Remark 5.4.2, we arrive at the very important

THEOREM 5.4.3. <u>The points (resp. nonzero points) lying on any $2^{m-1}+1$ (resp. 2^{m-1}) lines through the origin form a difference set in the affine plane</u> $L \oplus L$, $L = GF(2^m)$.

We observe here that the $PS^{(+)}$ difference sets given by Theorem 5.4.3 are precisely the complements of the $PS^{(-)}$ sets given by the theorem. We shall see in the next chapter, however, that there exist $PS^{(+)}$ difference sets which are not equivalent to the complement of any $PS^{(-)}$ difference set. We also show in the next chapter that for $m>3$ there are many pairwise inequivalent $PS^{(-)}$ difference sets in Z_2^{2m}. This contrasts sharply with

THEOREM 5.4.4. <u>For</u> $m \leq 3$ <u>there is, up to equivalence, exactly one</u> $PS^{(-)}$ <u>difference set in</u> Z_2^{2m}.

PROOF. The result is trivial for $m=1$, while for $m=2$ we have already seen (Remark 2.2.13) that the (16,6,2,4) difference set in Z_2^4 is unique. Thus we need consider only $m=3$.

Let $\{H_\infty, H_0, H_1, H_2\}$ be a partial spread for $G = Z_2^6$ which we regard as $H \oplus H$, $H = Z_2^3$. By Theorem 5.3.1 we may assume that $H_\infty = \{(0,X):X\varepsilon H\}$, $H_0 = \{(X,0):X\varepsilon H\}$, $H_1 = \{(X,X):X\varepsilon H\}$, $H_2 = \{(X,X\alpha):X\varepsilon H\}$ where α is an automorphism of H with no nonzero fixed point. Thus, α is a nonsingular Z_2-linear transformation of $H = Z_2^3$. Let L be the matrix effecting this transformation, so that

$$H_2 = \{(X,XL):X\varepsilon H\}.$$

Since α has no fixed point, L has minimum polynomial either $f(X) = X^3 + X + 1$ or $f(X) = X^3 + X^2 + 1$. By applying if necessary the automorphism

$$(X,Y) \rightarrow (Y,X)$$

of G, we may assume the former case. Thus L has rational canonical form

$$C = \begin{bmatrix} & & 1 \\ 1 & & 1 \\ & 1 & \end{bmatrix}.$$

Let $L = S^{-1}C\,S$ for some nonsingular matrix S. Then

$$
\begin{aligned}
H_2 &= \{(X,XL):X\varepsilon H\} \\
&= \{(X,XS^{-1}CS):X\varepsilon H\} \\
&= \{(XS,XCS):X\varepsilon H\},
\end{aligned}
$$

and the automorphism

$$(X,Y) \rightarrow (XS^{-1},\ YS^{-1})$$

of $G = H \oplus H$ then takes the partial spread into the "canonical" partial spread

$H_\infty = \{(0,X):X\varepsilon H\}$, $H_0 = \{X,0):X\varepsilon H\}$, $H_1 = \{(X,X):X\varepsilon H\}$, $H_2 = \{(X,XC):X\varepsilon H\}$. qed.

There is another family of partial spread difference sets which we have already encountered in chapter 4. Recall (from that chapter) that a Pall partition for a quadratic form

$$Q(X) \equiv Q(X_1, X_2, \ldots, X_t)$$

over a field F is a partition of the zeros of the form into pairwise disjoint (except for 0) maximal isotropic subspaces. We proved (Theorem 4.1.1) that such a partition exists for every nonsingular quadratic form of characteristic 2, except for those over a finite field $F = GF(q)$ equivalent to

$$\Psi_m = X_1X_{m+1} + X_2X_{m+2} + \ldots + X_mX_{2m}$$

with $m > 1$ odd. Thus, whenever m is even (or $m=1$) the

$1 + (q^{m-1}+1)(q^m-1)$ zeros of Ψ_m on F^{2m} may be partitioned into $q^{m-1}+1$ pairwise "disjoint" m-dimensional subspaces of F^{2m}. These subspaces clearly constitute a partial spread for F^{2m}; and if (and only if) q=2 this partial spread is Hadamard. Thus, we have

THEOREM 5.4.5. <u>The zeros of the quadratic form</u>

$$\Psi_m = X_1X_{m+1} + X_2X_{m+2} + \ldots + X_mX_{2m}$$

<u>over $F = GF(2)$ constitute a partial spread difference set of type $PS^{(+)}$ in F^{2m} if and only if $m=1$ or m is even.</u>

We note here the interesting fact [20] that a spread for Z_2^{2m} is equivalent to a Veblen-Wedderburn system with additive group Z_2^m. Our difference sets given in Theorem 5.4.3 arise from the special case in which the V-W system is a field. But any other system will do as well.

REMARK 5.4.6. <u>Every V-W system with additive group Z_2^m gives rise to $\binom{2^m+1}{2^{m-1}}$ $PS^{(-)}$ difference sets in $Z_2^m \oplus Z_2^m \cong Z_2^{2m}$. The complements of these difference sets are of type $PS^{(+)}$.</u>

CHAPTER VI

DIFFERENCE SETS IN ELEMENTARY ABELIAN 2-GROUPS

1. Introduction.

This chapter is a survey of difference sets in elementary abelian 2-groups. We begin with the idea of a Boolean function whose Fourier transform has constant magnitude. Following Rothaus [22] we call such functions bent functions. In section 2 we quickly show that the bent functions are precisely the characteristic functions of elementary Hadamard difference sets and go on to derive quite painlessly all of the familiar properties of these difference sets, along with some others perhaps not so familiar.

In section 3 we give a thorough account of all the known constructions for bent functions (elementary Hadamard difference sets). We take particular care to relate the various families to one another and we endeavor to point out any equivalences of which we are aware. We also give examples of inequivalences which demonstrate that some families do not contain others.

This chapter serves as the focal point of the entire paper. Every other chapter is represented here — its results stripped of their generality to reveal some truth about elementary Hadamard difference sets.

The terminology and notation follows that of earlier chapters, except that here we denote by V_m the space of m-tuples over $F = GF(2)$. Also we say that a Boolean function $f: V_m \to F$ is <u>balanced</u> if it takes the values 0 and 1 equally often.

2. Bent functions.

DEFINITION. *The Boolean function $f : V_m \to F$ is bent if its Fourier coefficients are all of the same magnitude; i.e. $|\hat{f}|^2$ is constant.*

We may immediately establish the

THEOREM 6.2.1. *f is bent iff $[f^*]$ is Hadamard.*

PROOF. By the corollary to Theorem 3.3.3 we have

$$H_m[f^*]^2H_m^{-1} = 4^m \operatorname{diag}(|\hat{f}(0)|^2, |\hat{f}(1)|^2, \ldots, |\hat{f}(2^m-1)|^2).$$

$$\begin{aligned} \text{Thus, } f \text{ is bent} &\Longleftrightarrow H_m[f^*]^2H_m^{-1} && \text{is scalar} \\ &\Longleftrightarrow [f^*]^2 && \text{is scalar} \\ &\Longleftrightarrow [f^*] && \text{is Hadamard,} \end{aligned}$$

the last equivalence being a consequence of Remark 2.2.5. qed.

Now if we regard the Boolean function f as the characteristic function of the set $D = f^{-1}[1]$, then the matrices $[f]$ and $[f^*]$ coincide with the incidence matrix $[D]$ and its associate $[D^*]$, respectively. Theorems 2.2.6 and 6.2.1 then combine to yield

THEOREM 6.2.2. *f is bent iff $D = f^{-1}[1]$ is a Hadamard difference set in V_m.*

Recall that the (directional) derivative of f in the direction v is given by

$$f_v(X) = f(X+v) + f(X).$$

It is now easy to establish the following very useful characterization first noticed by D. Lieberman (private communication) who proved it in a vastly different manner.

THEOREM 6.2.3. <u>f is bent iff f_v is balanced for all</u> $v \neq 0$,

PROOF. We have $[f^*] = ((-1)^{f(u+v)})$. Thus,

$$\begin{aligned} f \text{ is bent} &\Leftrightarrow [f^*] \text{ is Hadamard} \\ &\Leftrightarrow \sum_w (-1)^{f(u+w)+f(v+w)} = 0 \quad \text{for all } u \neq v \\ &\Leftrightarrow f_{u+v} \text{ is balanced for all } u+v \neq 0. \end{aligned}$$

qed.

We now pause to collect several elementary results consequent to f being bent on V_m. First the general equation

$$H_m[f^*][\bar{\bar{f}}^*] H_m^{-1} = 4^m \operatorname{diag}(|\hat{f}(0)|^2, |\hat{f}(1)|^2, \ldots, |\hat{f}(2^m-1)|^2)$$

of the corollary to Theorem 3.3.3 becomes for bent functions

$$I = 2^m \operatorname{diag}(|\hat{f}(0)|^2, |\hat{f}(1)|^2, \ldots, |\hat{f}(2^m-1)|^2),$$

which implies immediately the

REMARK 6.2.4. <u>If f is bent on V_m, the Fourier coefficients of f are all equal to</u> $\pm 2^{-m/2}$.

Since the Fourier coefficients of a Boolean function are rational numbers, the preceding remark implies

REMARK 6.2.5. <u>Bent functions exist on V_m only if m is even.</u>

We may restate Remark 6.2.4 as

REMARK 6.2.6. *The function*

$$f : V_{2m} \to F$$

is bent iff there exists a function

$$\mathfrak{f} : V_{2m} \to F$$

such that $\hat{f} = \frac{1}{2^m}\, \mathfrak{f}^*$. *In this case,* $\mathfrak{f}$ *is also bent and* $\hat{\mathfrak{f}} = \frac{1}{2^m} f^*$.

We shall refer to the bent function $\mathfrak{f}$ as the "Fourier transform" of f. There is thus a natural pairing of bent functions expressed by

REMARK 6.2.7. *The "Fourier transform" of a bent function is bent.*

Remark 3.3.2 now implies for bent functions

REMARK 6.2.7. *If* f_1, f_2 *are bent on* V_{2m} *with*

$$f_2(X) = f_1(XT+a)$$

for some a *in* V_{2m} *and some nonsingular F-linear transformation* T *of variables then*

$$\mathfrak{f}_2(XT') = \mathfrak{f}_1(X) + a \cdot X.$$

Thus, linearly equivalent bent functions have "Fourier transforms" which are themselves linearly equivalent. Affinely equivalent bent functions have "Fourier transforms" of the same degree.

Next, if we let N_v denote the number of zeros of the function $f(X) + v \cdot X$ on V_{2m}, we have

$$2^{2m}\,\hat{f}(v) = \sum_u (-1)^{f(u)+v\cdot u} = N_v - (2^{2m} - N_v) = 2N_v - 2^{2m}$$

or $\quad N_v = 2 \cdot 4^{m-1} + 2 \cdot 4^{m-1}\,\hat{f}(v).$

It then follows that

REMARK 6.2.8. $f : V_{2m} \to F$ <u>is bent iff</u> $f(X) + v \cdot X$ <u>has</u> $2 \cdot 4^{m-1} \pm 2^{m-1}$ <u>zeros for all</u> v in V_{2m}.

We note that if $g(X) = f(X) + v \cdot X$, then $\hat{g}(X) = \hat{f}(X+v)$; thus, if $f(X)$ is bent, then $f(X) + v \cdot X$ is bent for all v in V_{2m}. Since, by Theorem 6.2.2, f is bent iff $f^{-1}[1]$ (and $f^{-1}[0]$) is a Hadamard difference set, all of the foregoing remarks are trivial consequences of the corollary to Mann's Theorem 2.2.10. Finally, we note that if

$$\chi = (-1)^{v \cdot X}$$

is a nonprincipal character of V_{2m} (i.e. $v \neq 0$), then for any

$$f : V_{2m} \to F$$

$$2^{2m}\,\hat{f}(v) = \sum_u (-1)^{f(u)+v\cdot u} = \chi(f^{-1}[0]) - \chi(f^{-1}[1]) = -2\chi(f^{-1}[1]).$$

We then have the

REMARK 6.2.9. $f : V_{2m} \to F$ <u>is bent iff</u>

$$\chi(f^{-1}[1]) = \pm\, 2^{m-1}$$

<u>for all nonprincipal group characters</u> χ <u>of</u> V_{2m}.

We now collect the various characterizations of bent functions in the

THEOREM 6.2.10. <u>The following are equivalent</u>:

1) $f : V_{2m} \to F$ <u>is bent</u>;

2) $\hat{f}(v) = \pm(1/2^m)$ <u>for all</u> v <u>in</u> V_{2m};

3) $f(X) + v \cdot x$ <u>has</u> $2 \cdot 4^{m-1} \pm 2^{m-1}$ <u>zeros for all</u> v <u>in</u> V_{2m};

4) $f_v(X) = f(X+v) + f(X)$ <u>is balanced for all nonzero</u> v <u>in</u> V_{2m};

5) $[f^*] = (f^*(u+v))$ <u>is Hadamard</u>;

6) $f^{-1}[1]$ <u>is a (Hadamard) difference set in</u> V_{2m};

7) $\chi(f^{-1}[1]) = \pm 2^{m-1}$ <u>for all nonprincipal characters</u> χ <u>of</u> V_{2m}.

The Poisson summation Theorem 3.3.4 may be combined with Theorem 3.2.2 to yield information about the degree of a bent function.

Let $f : V_{2m} \to F$ be bent

and let $\mathfrak{f} : V_{2m} \to F$ be such that

$$\hat{f} = \frac{1}{2^m} \mathfrak{f}^* .$$

Thus, the Boolean function $\mathfrak{f}$ is also bent and has Fourier transform

$$\hat{\mathfrak{f}} = \frac{1}{2^m} f^* .$$

By Theorem 3.3.4 we have

$$(*) \qquad \sum_{s\in S} f^*(s) = 2^{\dim S} \sum_{s\in S^\perp} \hat{f}(s) = 2^{\dim S-m} \sum_{s\in S^\perp} \mathfrak{f}^*(s)$$

for any subspace S of V_{2m}. We now write

$$f^* = 1 - 2f$$

$$\text{and} \quad \mathfrak{f}^* = 1 - 2\mathfrak{f},$$

where we interpret f and $\mathfrak{f}$ as functions taking the <u>real</u> values 0 and 1. Equation (*) then becomes

$$\sum_{s\in S} f(s) = 2^{m-1}(2^{\dim S-m}-1) + 2^{\dim S-m} \sum_{s\in S^\perp} \mathfrak{f}(s).$$

We restate this fruitful result in the

THEOREM 6.2.11. *Let f and $\mathfrak{f}$ be bent functions on V_{2m} such that $2^m\hat{f} = \mathfrak{f}^*$ (equivalently, $2^n\hat{\mathfrak{f}} = f^*$). Then, interpreting f and $\mathfrak{f}$ as real-valued functions, we have*

$$\sum_{s\in S} f(s) = 2^{m-1}(2^{\dim S-m}-1) + 2^{\dim S-m} \sum_{s\in S^\perp} \mathfrak{f}(s)$$

for any subspace S of V_{2m}.

COROLLARY. For any v in V_{2m},

$$\sum_{u\subset v} f(u) = 2^{m-1}(2^{|v|-m}-1) + 2^{|v|-m} \sum_{u\subset \bar{v}} \mathfrak{f}(u).$$

This last result has several important consequences.

THEOREM 6.2.12. *If m is greater than 1, a bent function on V_{2m} has degree at most m.*

PROOF. Let $f(X) = \Sigma\, g(v) X_1^{v_1} X_2^{v_2} \cdots X_{2m}^{v_{2m}}$ be bent. According to Theorem 3.2.2 the monomial

$$X^v \equiv X_1^{v_1} X_2^{v_2} \cdots X_{2m}^{v_{2m}}$$

is present in the polynomial $f(X)$ if and only if $\sum_{u \subset v} f(u)$ is odd. But the corollary to Theorem 6.2.11 assures us that

$$\sum_{u \subset v} f(u) = 2^{m-1}(2^{|v|-m}-1) + 2^{|v|-m} \sum_{u \subset \bar{v}} \hat{f}(u)$$

If $m>1$ and $|v|>m$, the right side of this equation is even. Thus, $\sum_{u \subset v} f(u)$ is even and $f(X)$ does not contain the monomial

$$X^v = X_1^{v_1} X_2^{v_2} \cdots X_{2m}^{v_{2m}} .$$

qed.

REMARK 6.2.13. *If* $f : V_{2m} \to F$ *is bent of degree* m, *then its "Fourier transform"* $\hat{f}$ *is also of degree* m.

PROOF. We prove a slightly stronger result. By the corollary to Theorem 6.2.11 we have

$$\sum_{u \subset v} f(u) = \sum_{u \subset \bar{v}} \hat{f}(u)$$

for all v with $|v| = m$. Thus, $f(X)$ contains the degree m monomial X^v

$$\Longleftrightarrow \sum_{u \subset v} f(u) \text{ is odd}$$

$$\Longleftrightarrow \sum_{u \subset \bar{v}} \hat{f}(u) \text{ is odd}$$

$$\Longleftrightarrow \hat{f}(X) \text{ contains the degree } m \text{ monomial } X^{\bar{v}}.$$

qed.

REMARK 6.2.14. *If* $f : V_{2m} \to F$ *is bent, then*

$$|S \cap f^{-1}[1]| = 2^{\dim S-1} - 2^{m-1} + 2^{\dim S-m} |S^{\perp} \cap \mathfrak{f}^{-1}[1]|$$

for all subspaces S *of* V_{2m}.

PROOF. This is just a restatement of Remark 6.2.11.

COROLLARY. *If* $\dim S \geq m$, *then*

$$2^{\dim S-1} - 2^{m-1} \leq |S \cap f^{-1}[1]| \leq 2^{\dim S-1} + 2^{m-1}.$$

COROLLARY. *Let the difference set* D *in* V_{2m} *contain the subspace* S *of* V_{2m}. *Then* $\dim S \leq m$. *If* $\dim S = m$, *then* D *contains exactly half the points of each proper coset of* S *in* V_{2m}. *Hence,* $|D| = 2^{2m-1} + 2^{m-1}$.

PROOF. We have for any subspace T of V_{2m}

$$|T \cap D| = 2^{\dim T-1} - 2^{m-1} + 2^{\dim T-m} |T^{\perp} \cap E|,$$

where E is the difference set corresponding to the "Fourier transform" of D. If $\dim T \geq m$,

$$|T \cap D| \leq 2^{\dim T-1} + 2^{m-1} \leq 2^{\dim T}$$

with equality only if $\dim T = m$. Thus D contains the subspace S only if S has dimension at most m. The proof of the second assertion is contained in the proof of the

REMARK 6.2.15. Let E be a subset of V_{2m} containing the m-dimensional subspace S and let $D = E\backslash S$. Then E is a (nontrivial) difference set if and only if D is a (nontrivial) difference set.

PROOF. We interpret the space V_{2m} as the direct sum $V_m \oplus V_m$ and assume (by applying an automorphism if necessary) that $S = 0 \oplus V_m$. We use the Box Theorem 3.3.5 of chapter 3. Let $e^{\square}$ and $d^{\square}$ be the $2^m \times 2^m$ (± 1)-matrices corresponding to the characteristic functions of E and D and let $\hat{e}^{\square}$ and $\hat{d}^{\square}$ be the matrices corresponding to the associated Fourier transforms. Then

$$2^m \hat{e}^{\square} = H_m e^{\square} H_m^{-1}$$

and $$2^m \hat{d}^{\square} = H_m d^{\square} H_m^{-1} .$$

Now $e^{\square}$ and $d^{\square}$ differ only in the first row where $e^{\square}$ is constant -1 and $d^{\square}$ is constant 1. Since the rows of $e^{\square} H_m^{-1}$ and $d^{\square} H_m^{-1}$ are the Fourier transforms of the rows of $e^{\square}$ and $d^{\square}$ we see that $e^{\square} H_m^{-1}$ and $d^{\square} H_m^{-1}$ differ only in the (0,0)-position where the former is -1 and the latter 1. Now e (resp. d) is bent if and only if the columns of $e^{\square} H_m^{-1}$ (resp. $d^{\square} H_m^{-1}$) are Fourier transforms of Boolean functions. Furthermore, in that case the first column must have 0's in all but the first row. The result is then clear. qed.

If we have bent functions on the spaces V_m and V_n, we may construct bent functions on V_{m+n} according to the

REMARK 6.2.16. *Let* f *and* g *be Boolean functions on* V_m *and* V_n, *respectively. Let* $h : V_{m+n} \to F$ *be defined by*

$$h(X,Y) = f(X) + g(Y).$$

Then h *is bent iff* f *and* g *are bent.*

PROOF. We have $[h^*] = [f^*] \otimes [g^*]$, and the assertion follows from the fact that a Kronecker product of matrices is Hadamard if and only if the individual factors are Hadamard. qed.

Functions of the type constructed in Remark 6.2.16 are rather uninteresting because they may be "decomposed" into simpler functions.

DEFINITION. *The Boolean function* $f(X) = f(X_1, X_2, \ldots, X_m)$ *is decomposable if it is linearly equivalent to a sum of functions in disjoint sets of variables*; i.e. *there exists a nonsingular linear transformation* T *of the variables* $X_1, X_2, \ldots, X_m$ *such that*

$$f(XT) = g(X_1, X_2, \ldots, X_r) + h(X_{r+1}, X_{r+2}, \ldots, X_m)$$

for some r, $1 \leq r < m$.

As an example of a decomposable function we consider the elementary symmetric function of degree 2 in four variables; i.e.

$$f(X) = f(X_1, X_2, X_3, X_4) = X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 \; .$$

The transformation

$$T: \begin{cases} X_1 \to X_1 + X_3 + X_4 \\ X_2 \to X_2 + X_3 + X_4 \\ X_3 \to X_3 \\ X_4 \to X_4 \end{cases}$$

transforms $f(X)$ into

$$f(XT) = X_1X_2 + (X_3X_4 + X_3 + X_4) = g(X_1,X_2) + h(X_3,X_4);$$

thus, $f(X)$ is decomposable.

The next result provides a means for recognizing some indecomposable bent functions.

REMARK 6.2.17. For $m>2$, every bent function of degree m on V_{2m} is indecomposable.

PROOF. Let the bent function $f(X_1, X_2, \ldots, X_{2m})$ of degree m be linearly equivalent to

$$g(X_1, X_2, \ldots, X_{2r}) + h(X_{2r+1}, X_{2r+2}, \ldots, X_{2m}),\ 1 \leq r \leq m-1.$$

Since the degree of a polynomial is invariant under a nonsingular linear transformation of its variables, one of these addends, say g, must have degree m. By Remark 6.2.16 g is bent, and by Theorem 6.2.12 g has degree at most r (unless $r=1$, in which case g has degree 2). Since g has degree m which is greater than r, we must have $r=1$ and $m=2$. qed.

3. Families of bent functions.

The simplest bent function of all is the function

$$f(X,Y) = XY$$

in two variables. This is a "trival" bent function which vanishes on all of V_2 except on the single point (1,1) where it takes the value 1. The ($\pm$1)-matrix corresponding to f is

$$[f^*] = \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix} \quad .$$

This matrix, being a circulix, may be interpreted as the incidence matrix of a "trivial" difference set in the cyclic group Z_4. In fact, $[f^*]$ is the only (up to permutation and complementation of rows and columns) known Hadamard circulix, and it has been conjectured that no larger one exists. The conjecture has been verified [2] for matrices of order up to 12,100. This trivial bent function in two variables yields via Remark 6.2.16 the simplest general family of bent functions; this result was discovered independently by P. Kesava Menon [19] and R. J. Turyn [24] around 1960.

FAMILY $\mathcal{Q}$. $f(X,Y) = X\cdot Y = X_1Y_1 + X_2Y_2 + \ldots + X_mY_m$ is bent on V_{2m}.

Indeed, as both Kesava Menon and Turyn have observed, the matrix $[f^*]$ corresponding to a function in FAMILY $\mathcal{Q}$ may be interpreted as the incidence matrix of a Hadamard difference set in any group of order 4^m which is the direct sum of m groups of order 4 (each of which may be either cyclic or the Klein 4-group).

We observe that the bent function

$$f(X,Y) = X \cdot Y$$

of FAMILY $\mathcal{Q}$ is a nondefective quadratic form on V_{2m}. A classical result of Dickson [8] states that every quadratic polynomial in n Boolean variables $X_1, X_2, \ldots, X_n$ is affinely equivalent to a polynomial of the form

$$X_1X_{k+1} + X_2X_{k+2} + \ldots + X_kX_{2k} + aX_{2k+1} + b,$$

where $1 \leq k \leq n/2$ and $a,b \varepsilon F$ with $ab=0$. But it is clear that such a polynomial defines a bent function on V_n if and only if $n = 2k$ (in which case $a=0$). Thus, the quadratic bent functions on V_{2m} are precisely the nondefective forms and their complements. We have

REMARK 6.3.1. Every quadratic bent function on V_{2m} is equivalent (up to complementation) to the canonical nondefective form $X \cdot Y$. Thus, $X \cdot Y$ is the "only" quadratic bent function on V_{2m}.

The $2^m \times 2^m (\pm 1)$-matrix $f^{*\square}$ whose (u,v)th entry is $f^*(u,v)$ is given by

$$f^{*\square} = (f^*(u,v)) = ((-1)^{u \cdot v}),$$

which is precisely the elementary Hadamard matrix H_m. By the Box Theorem 3.3.5, the Fourier transform $\hat{f}$ of f is given by

$$2^m \hat{f}^{\square} = H_m f^{*\square} H_m^{-1}$$

$$= H_m \,.$$

Thus, the functions f^* and $2^m\hat{f}$ are identical, and we have

REMARK 6.3.2. *The canonical quadratic bent function* $X \cdot Y$ *of FAMILY* $\mathcal{Q}$ *is its own "Fourier transform".*

In an earlier paper [18] submitted for publication in 1958 P. Kesava Menon established

REMARK 6.3.3. *The set* D *of all vectors containing a number of 1's congruent to 2 or 3 (mod 4) is a difference set in* V_{2m}.

Let

$$S_2(X) = \sum_{1 \le i < j \le 2m} X_i X_j$$

denote the elementary symmetric function of degree 2 on V_{2m}. Then for all v in V_{2m}, $S_2(v)$ is congruent (mod 2) to the binomial coefficient

$$\binom{|v|}{2}$$

which is odd precisely when $|v| \equiv 2$ or $3 \pmod 4$. Thus, $S_2(X)$ is the characteristic function of Kesava Menon's set D and Remark 6.3.3 is equivalent to

REMARK 6.3.4. *The elementary symmetric function of degree 2 is a bent function on* V_{2m}.

The truth of both Remarks is implied by the more general

REMARK 6.3.5. Let T be the linear transformation of the n Boolean variables $X_1, X_2, \ldots, X_n$ given by

$$T: \begin{cases} X_{2i-1} \to X_{2i-1} + \sum_{j>2i} X_j \\ X_{2i} \to X_{2i} + \sum_{j>2i} X_j \end{cases} .$$

Then the elementary symmetric function of degree 2 in $X_1, X_2, \ldots, X_n$ is transformed via

$$A: \begin{cases} \begin{cases} X_{2i-1} \to T(X_{2i-1}) \\ X_{2i} \to T(X_{2i}) \end{cases} & \text{if } i \text{ is odd or } 2i-1=n \\ \\ \begin{cases} X_{2i-1} \to T(X_{2i-1})+1 \\ X_{2i} \to T(X_{2i})+1 \end{cases} & \text{if } i \text{ is even and } 2i-1\neq n \end{cases}$$

into

$$\begin{cases} G(X) = X_1X_2 + X_3X_4 + \ldots + X_{2t-1}X_{2t} & \text{if } n=2t\equiv 0,2 \pmod 8 \\ & \text{or } n=2t+1\equiv 1,5 \pmod 8 \\ G(X) + 1 & \text{if } n=2t\equiv 4,6 \pmod 8 \\ G(X) + X_{2t+1} & \text{if } n=2t+1\equiv 3 \pmod 8 \\ G(X) + X_{2t+1} + 1 & \text{if } n=2t+1\equiv 7 \pmod 8). \end{cases}$$

We omit the straightforward proof of this Remark.

COROLLARY. Kesava Menon's difference sets (bent functions) given in FAMILY Q and Remark 6.3.3 are equivalent.

In his 1966 paper Rothaus [22] generalized the quadratic bent function to

FAMILY $\mathcal{R}$. $f(X,Y) = X \cdot Y + g(X)$, g <u>arbitrary, is bent on</u> V_{2m}.

PROOF. In this case

$$f^{*\square} = \Delta H_m$$

where $\Delta = \text{diag}\ (g^*(0), g^*(1), \ldots, g^*(2^m-1))$. Thus, by the Box Theorem 3.3.4

$$2^m \hat{f}^{\square} = H_m f^{*\square} H_m^{-1}$$

$$= H_m \Delta \ .$$

Since this matrix has entries ± 1, the assertion follows. qed.

COROLLARY. <u>The "Fourier transform" of</u>

$$f(X,Y) = X \cdot Y + g(X)$$

<u>is</u> $\mathfrak{f}(X,Y) = X \cdot Y + g(Y)$.

COROLLARY. FAMILY $\mathcal{R}$ <u>bent functions have "Fourier transforms" of the same degree</u>.

Since $g(X)$ is an arbitrary polynomial in the m variables $X_1, X_2, \ldots, X_m$ we have the

REMARK 6.3.6. <u>There exist bent functions on</u> V_{2m} <u>of every degree</u> d, $2 \leq d \leq m$.

Also, since affinely equivalent functions have the same degree we have the

REMARK 6.3.7. *The functions*

$$f_2(X,Y) = X\cdot Y$$

$$f_3(X,Y) = X\cdot Y + X_1X_2X_3$$

$$f_4(X,Y) = X\cdot Y + X_1X_2X_3X_4$$

$$\vdots$$

$$f_m(X,Y) = X\cdot Y + X_1X_2X_3X_4\ldots X_m$$

are pairwise inequivalent bent functions on V_{2m}.

The next family, a natural generalization of Rothaus' FAMILY $\mathcal{R}$, was discovered independently by J. A. Maiorana (private communication) and R. L. McFarland [16].

FAMILY $\mathcal{M}$. $f(X,Y) = \pi(X)\cdot Y + g(X)$, *g arbitrary and* π *an arbitrary permutation of* V_m, *is bent on* V_{2m}.

PROOF. Let P be the $2^m \times 2^m$ permutation matrix such that $P(X,\pi(X)) = 1$ for all $x \varepsilon V_m$; and let Δ be the diagonal matrix diag $(g^*(0), g^*(1), \ldots, g^*(2^m-1))$. Then

$$f^{*\Box} = \Delta P H_m ,$$

so that, by the Box Theorem 3.3.5, f has Fourier transform

$$2^m\hat{f}^{\Box} = H_m f^{*\Box} H_m^{-1}$$

$$= H_m \Delta P.$$

Since this matrix has entries ± 1, the assertion follows. qed.

There are several different proofs for this last result; the beautiful proof presented here which graphically illustrates the constant magnitude of the Fourier coefficients is due to D. P. Cargo (private communication).

COROLLARY. The "Fourier transform" of

$$f(X,Y) = \pi(X)\cdot Y + g(X)$$

is

$$\mathfrak{f}(X,Y) = X\cdot\pi^{-1}(Y) + g(\pi^{-1}(Y)).$$

We note here the useful characterization of permutations on V_m (also given by Maiorana).

REMARK 6.3.7. The function

$$\pi : X \to (P_1(X), P_2(X), \ldots, P_m(X))$$

is a permutation of V_m if and only if for every nonzero vector e in V_m the function

$$e\cdot\pi = e_1P_1(X) + e_2P_2(X) + \ldots + e_mP_m(X)$$

is balanced on V_m.

PROOF. For each v in V_m let $G_\pi(v)$ be the number of vectors u such that $\pi(u)=v$. Then the excess of 0's over 1's of the function $e\cdot\pi$ may be written

$$B_\pi(e) = \sum_{v\varepsilon V_m} G_\pi(v)(-1)^{e\cdot v},$$

from which we see that the function B_π is the (unnormalized) Fourier-Hadamard transform of G_π. Thus, π is a permutation

$$\Longleftrightarrow G_\pi \text{ is the constant 1 function}$$

$$\Longleftrightarrow B_\pi \text{ is the function } 2^m\delta_{0,X}$$

$$\Longleftrightarrow e\cdot\pi \text{ is balanced for all } e\neq 0. \qquad \text{qed.}$$

We now demonstrate that FAMILY $\mathcal{M}$ is truly a generalization of FAMILY $\mathcal{R}$. First we observe

REMARK 6.3.8. Let f be bent on V_{2m} and let $\mathfrak{f}$ be its "Fourier transform".

a) If $m<5$, then f and $\mathfrak{f}$ have the same degree;

b) For any $m\geq 5$, f and $\mathfrak{f}$ need not have the same degree.

PROOF. We have already proved that a bent function of degree 2 or of degree m must have a "Fourier transform" of the same degree. This establishes part a).

Now suppose that $m=5$ and consider the function on $V_{10} = V_5 \oplus V_5$ given by

$$f(X,Y) = \pi(X)\cdot Y$$

where

$$\pi(X) = (X_1 + X_2X_3,\ X_2 + X_4X_5,\ X_3,\ X_4,\ X_5).$$

Then $f(X,Y)$ has "Fourier transform"

$$g(X,Y) = X\cdot\pi^{-1}(Y)$$

where

$$\pi^{-1}(X) = (X_1 + X_2X_3 + X_3X_4X_5,\ X_2 + X_4X_5,\ X_3,\ X_4,\ X_5).$$

Thus, f has degree 3 while g has degree 4. This establishes part b) for $m=5$; the same example may be extended to an arbitrary $m\geq 5$ by taking $V_m = V_5 \oplus V_{m-5}$ and defining π to be the identity permutation on the component V_{m-5}. qed.

Since these examples are in FAMILY $\mathcal{M}$ we have

COROLLARY. FAMILY $\mathcal{M}$ *contains bent functions which are not equivalent to any bent function in* FAMILY $\mathcal{R}$.

The family of difference sets corresponding to the bent functions in FAMILY $\mathcal{M}$ is actually a special case of a very general construction obtained recently by R. L. McFarland [16].

THEOREM 6.3.9. *Let* E *be (the additive group of) a vector space of dimension* s+1 *over the finite field* GF(q). *Let* $H_1, H_2, \ldots, H_r$, $r = (q^{s+1}-1)/(q-1)$, *be the hyperplanes in* E, *and let* $e_1, e_2, \ldots, e_r$ *be any* r *elements of* E. *Let* K *be an arbitrary (not necessarily abelian) group of order* r+1 *and let* $k_1, k_2, \ldots, k_r$ *be any* r *distinct elements of* K. *Let* $C_i = H_i + (e_i,k_i)$ *denote the coset of* H_i *in the direct sum* $G = E \oplus K$ *which contains the element* (e_i,k_i). *Then* $D = C_1 \cup C_2 \cup \cdots \cup C_r$ *is a difference set in* G *with parameters*

$$(v,k,\lambda,n) = \left(q^{s+1}\left[\frac{q^{s+1}-1}{q-1}+1\right],\ q^s\left[\frac{q^{s+1}-1}{q-1}\right],\ q^s\left[\frac{q^s-1}{q-1}\right],\ q^{2s}\right).$$

Though the proof of McFarland's theorem is elementary, we shall prove only the following special case, which yields to a simple generalization of our proof of FAMILY $\mathcal{M}$.

COROLLARY. *Let* $G = Z_2^m \oplus K$ *be the direct sum of the elementary abelian group* Z_2^m *and the arbitrary abelian group* K *of order* 2^m. *For any subset* D *of* G *let* $g_D^{\square}$ *denote the* $2^m \times 2^m$ (± 1)*-matrix whose* (X,Y)th *entry is* -1 *if* (X,Y) *is in* D. *If the matrix* $g_D^{\square}$ *satisfies*

$$g_D^{\square} = H_m P \Delta,$$

with Δ *a diagonal matrix with diagonal entries* ± 1 *and* P *a permutation matrix, then the corresponding subset* D *is a difference set in* G.

PROOF. The matrix F_G effecting the Fourier transform on G is equal to the Kronecker product

$$\frac{1}{4^m}\,(H_m \otimes F_K)$$

where F_K is the group character table for K. By the Box Theorem 3.3.5 the Fourier transform of the "characteristic function" g_D is given by

$$\begin{aligned} \hat{g}_D^{\square} &= \frac{1}{4^m}\, H_m\, g_D^{\square}\, F_K \\ &= \frac{1}{4^m}\, H_m\, (H_m P \Delta) F_K \\ &= \frac{1}{2^m}\, P \Delta F_K\,. \end{aligned}$$

Since each entry of this matrix has absolute value $\frac{1}{2^m}$, the assertion follows. qed.

We observe that taking K to be cyclic yields difference sets in the group $G = Z_2^m \oplus Z_{2m}$ which has exponent 2^m — within a factor of 2 of the upper bound given by a theorem of Turyn [24].

We now come to the important family of bent functions corresponding to the partial spread difference sets constructed in Chapter V, section 4.

FAMILY $PS^{(-)}$. *Let* $H_1, H_2, \ldots, H_{2^{m-1}}$ *be m-dimensional subspaces of* V_{2m} *such that*

$$H_i \cap H_j = \{0\},\ 1 \le i < j \le 2^{m-1},$$

and let

$$H_i^* = H_i \setminus \{0\},\quad 1 \le i \le 2^{m-1}.$$

Then $D = \bigcup H_i^*$ *is a difference set in* V_{2m} *and the characteristic function of* D *is a bent function on* V_{2m}.

FAMILY $PS^{(+)}$. *The union of any* $2^{m-1}+1$ *pairwise "disjoint" m-dimensional subspaces of* V_{2m} *is a difference set in* V_{2m}.

REMARK 6.3.10. *The "Fourier transform" of (the characteristic function of)* $\bigcup H_i$ *is (the characteristic function of)* $\bigcup H_i^\perp$. *Thus,* FAMILY PS *is closed under the taking of Fourier transforms.*

The next result shows that all bent functions of FAMILY $PS^{(-)}$ (and many of those of FAMILY $PS^{(+)}$) are indecomposable.

REMARK 6.3.11. *Every bent function in* FAMILY $PS^{(-)}$ *has degree* m.

PROOF. By applying (if necessary) a nonsingular linear transformation of V_{2m} we may assume that

$$H_1 = \{(v,0)\varepsilon V_{2m} : v\varepsilon V_m\}$$

and

$$H_2 = \{(0,v)\varepsilon V_{2m} : v\varepsilon V_m\} .$$

Then by Theorem 3.2.2 the characteristic function of $D = \bigcup H_i^*$ contains the monomials $X_1 X_2 \cdots X_m$ and $X_{m+1} X_{m+2} \cdots X_{2m}$. qed.

We observe that if E is a $PS^{(+)}$ difference set which is the union of a *nonmaximal* partial spread (i.e. one which can be extended by adjunction of another m-dimensional subspace) then the same argument applied to the complement $\bar{E}$ of E shows that $\bar{E}$, and hence E, has degree m. That this need not be the case is shown by

THEOREM 6.3.12. *If* m *is even, then* FAMILY $PS^{(+)}$ *contains "the" quadratic bent function.*

PROOF. We showed in Chapter 4 that, whenever m is even, the quadratic form

$$\Psi_m = X_1 X_{m+1} + X_2 X_{m+2} + \cdots + X_m X_{2m}$$

over any finite field F = GF(q), q a power of 2, has a Pall partition. Equivalently, the set Q of zeros of Ψ_m is the union of $q^{m-1}+1$ pairwise "disjoint" m-dimensional subspaces of F^{2m}. Thus, Q is the union of a partial spread containing $q^{m-1}+1$ components. The special case q=2 then shows that Q is a difference set in $PS^{(+)}$ whose characteristic function is the (complement of the) canonical quadratic Ψ_m on V_{2m}. qed.

COROLLARY. *Not every bent function in* FAMILY $PS^{(+)}$ *is equivalent to the complement of a bent function in* FAMILY $PS^{(-)}$.

We now restrict our attention to the subfamily of FAMILY PS obtained (in accordance with Theorem 5.4.3) from the affine plane over $GF(2^m)$. For this subfamily, every $PS^{(+)}$ set is the complement of a $PS^{(-)}$ set.

FAMILY PS/ap. *The nonzero points lying on any* 2^{m-1} *lines through the origin constitute a difference set in the affine plane* $L \oplus L$, $L = GF(2^m)$. *The bent functions* (i.e. *characteristic functions*) *corresponding to these difference sets are equivalent to functions of the form*

$$f(X,Y) = \tau\{\pi(X^{2^m-2}Y)\},$$

where $\tau\{\cdot\}$ *is the trace with respect to* L/F *and* $\pi: L \to L$ *is any function for which* $\tau\{\pi(z)\}$ *is a balanced function on* L *which vanishes at* 0 (*in particular,* π *may be taken to be any permutation fixing* 0).

PROOF. We need only verify the assertion about the characteristic polynomial $f(X,Y)$.

If our difference set D consists of the nonzero points on the 2^{m-1} lines

$$L_1, L_2, \ldots L_{2^{m-1}},$$

We may assume (since $GL(2,2^m)$ is doubly transitive on the 2^m+1 lines through the origin in $L \oplus L$) that neither of the lines $X=0$ and $Y=0$ is among the L_i's. Suppose $L_i = \{(X, a_iX) : X \in L\}$, $1 \leq i \leq 2^{m-1}$.

Let S be the subset of L containing the 2^{m-1} elements which have trace 1 with respect to L/F. Let π be any permutation of L which fixes 0 and maps $A = \{a_1, a_2, \ldots, a_{2^{m-1}}\}$ onto S. Put

$f(X,Y) = \tau\{\pi(X^{2^m-2}Y)\}$.

$$\text{Then}\quad f(X,Y) = 1 \iff \tau\{\pi(X^{2^m-2}Y)\} = 1$$

$$\iff \pi(X^{2^m-2}Y) \varepsilon S$$

$$\iff X^{2^m-2}Y \varepsilon A$$

$$\iff Y = a_i X \text{ for some } a_i \varepsilon A \text{ and } XY \neq 0.$$

Thus, $f(X,Y)$ is precisely the characteristic function of D. It is not necessary to use a permutation for the map π; any map π with $\pi^{-1}[S]=A$ will do as well. qed.

COROLLARY. <u>For any integer</u> d, $(d,2^m-1)=1$,

$$f(X,Y) = \tau\{X^{2^m-1-d}Y^d\}$$

<u>is a bent function on</u> $L \oplus L$, $L = GF(2^m)$.

Note that for $d = 1$ we get the function

$$f(X,Y) = \tau\{X^{2^m-2}Y\}$$

which is also in FAMILY M, the permutation of that representation being the permutation of L which fixes 0 and maps each nonzero element to its multiplicative inverse.

This particular bent function has appeared in the literature in disguise. In his remarkable paper [24] of 1965 R. J. Turyn gave the following result.

REMARK 6.3.13. *Let* G *be the direct sum* $L \oplus L$, *where* $L = GF(2^m)$. *Then the subset*

$$D = \{(m_1+m_2,\ m_1m_2) : m_1, m_2 \varepsilon L\}$$

is a $(4^m,\ 2\cdot 4^{m-1}+2^{m-1},\ 4^{m-1}+2^{m-1},\ 4^{m-1})$*-difference set in* G.

PROOF. The set D is precisely the set of points of the affine plane $L \oplus L$ lying on the lines

$$Y = mX + m^2,\ m\varepsilon L.$$

Thus, $D = \bigcup\limits_m \bigcup\limits_X \{(X,\ mX+m^2)\}$

$$= \bigcup_X \bigcup_m \{(X,\ mX+m^2)\}$$

$$= (0 \oplus L) \bigcup_{X\neq 0} (\bigcup_m \{(X,\ mX+m^2)\})$$

$$= (0 \oplus L) \bigcup_{X\neq 0} (\bigcup_m \{(X,\ (m^2+m)X^2)\}),$$

which is equivalent under the automorphism

$$(X,Y) \to (X^2,Y)$$

to the set of points lying on the lines

$$X = 0$$

and $$Y = (m^2+m)X,\ m\varepsilon L.$$

But the map $m \to m^2+m$ is a 2-1 (F-linear) mapping of L onto the kernel of the trace map $\tau : L \to F$ and we see that Turyn's "second bent function" is equivalent to the set of zeros of

$$f(X,Y) = \tau\{X^{2^m-2}Y\}$$

on $L \oplus L$. This bent function is the simplest member of FAMILY *PS*/ap, obtained by taking the map π to be the identity map. qed.

REMARK 6.3.14. Turyn's "second bent function" is in FAMILY $\mathcal{M}$ and FAMILY *PS*.

REMARK 6.3.15. All difference sets in FAMILY *PS*/ap are fixed under the multipliers

$$(X,Y) \to (aX,aY), \quad a \in L^* = L\setminus\{0\}.$$

Thus, the multiplier group of any difference set equivalent to one in FAMILY *PS*/ap must contain an element of order 2^m-1.

We now consider a different description of the difference sets in FAMILY *PS*/ap. Let K be a quadratic extension of L and let ω be an element in $K\setminus L$. Then the (additive group) isomorphism

$$(X,Y) \leftrightarrow X + Y\omega$$

between $L \oplus L$ and $K = L(\omega)$ carries the spread for $L \oplus L$ consisting of the lines through the origin onto the spread for K consisting of the subspaces

$$H_0 = L, \; H_1 = \theta L, \; H_2 = \theta^2 L, \; \ldots, \; H_{2^m} = \theta^{2^m} L$$

where θ is a (2^m+1)th root of unity in K. The sets of nonzero elements

$$H_i^* = H_i\setminus\{0\}, \; 0 \leq i \leq 2^m,$$

are precisely the (multiplicative) cosets of L^* in K^*.

Thus, we have the alternative description

FAMILY *PS*/ap (cyclotomic form). The union of any 2^{m-1} cosets of $L^* = (K^*)^{2^m+1}$ in K^* is a difference set in $K = GF(4^m)$. These difference sets are fixed by the (multipliers) automorphisms

$$X \to aX, \ a \in L^*.$$

The bent functions corresponding to these difference sets are of the form

$$g(X^{2^m-1}),$$

where $g : K \to F$ is any function satisfying i) $g(0)=0$ and ii) $g(h)=1$ for exactly 2^{m-1} elements of H, $K^* = L^*H$.

We consider an example of this construction. We take $m=4$ so that

$$K = GF(2^8).$$

It is easy to see that the trace map

$$\tau(Z) \equiv Tr_{K/F}\{Z\}$$

takes the value 1 on exactly 8 elements of H; indeed, the element 1 has trace 0 and the set $H\backslash\{1\}$ is the union of exactly two conjugate classes on which $\tau(Z)$ must take different values (if θ generates H, the elements $\theta^i(1+\theta)$, $1 \leq i \leq 8$, form a basis for K over F so that $\tau\{\theta^i\} \neq \tau\{\theta^{i+1}\}$ for some i.)

Thus, we have the

EXAMPLE 6.3.16. _The function_

$$f(X) = \tau\{X^{15}\}$$

is a bent function on $K = GF(2^8)$.

REMARK 6.3.17. _The bent function in_ EXAMPLE 6.3.16 _is not affinely equivalent to any bent function in_ FAMILY M.

PROOF. We first observe that any FAMILY M bent function

$$\pi(X)\cdot Y + g(X)$$

on $V_{2m} = V_m \oplus V_m$ has the property that any derivative with respect to a 2-dimensional subspace of $0 \oplus V_m$ must vanish identically on V_{2m}. From our results on affine invariants obtained in Chapter 3, it follows that any bent function on V_{2m} which is equivalent to one in FAMILY M must have the property that for some m-dimensional subspace W of V_{2m} the derivative with respect to every 2-dimensional subspace of W must be identically zero on V_{2m}.

We now consider our example

$$f(X) = \tau\{X^{15}\}$$

on $K = GF(2^8)$. We shall show that, contrary to the behavior of FAMILY M bent functions, _no_ 2-dimensional derivative of $f(X)$ can vanish. For let a,b be distinct nonzero elements of K. The derivative of f with respect to the space spanned by a and b is

$$g(X) = f(X) + f(X+a) + f(X+b) + f(X+a+b)$$

$$= \tau\{X^{15} + (X+a)^{15} + (X+b)^{15} + (X+a+b)^{15}\}.$$

$$= \sum_{t=1}^{12} \tau\{[a^{15-t} + b^{15-t} + (a+b)^{15-t}]\ X^t\}$$

$$= \tau\{C_8X^8\} + \tau\{C_{12}X^{12}\} + \tau\{C_{10}X^{10}\} + \tau\{C_9X^9\},$$

where
$$C_8 = [a^7+b^7+(a+b)^7] + [a^{11}+b^{11}+(a+b)^{11}]^2 + [a^{13}+b^{13}+(a+b)^{13}]^4 + [a^{14}+b^{14}+(a+b)^{14}]^8$$

$$C_{12} = [a^3+b^3+(a+b)^3] + [a^9+b^9+(a+b)^9]^2 + [a^{12}+b^{12}+(a+b)^{12}]^4$$

$$C_{10} = [a^5+b^5+(a+b)^5] + [a^{10}+b^{10}+(a+b)^{10}]^2$$

$$C_9 = [a^6+b^6+(a+b)^6].$$

Now $g(X)$ vanishes identically if and only if

$$C_8 = C_{12} = C_{10} = C_9 = 0.$$

In particular, $g(X)$ vanishes only when

$$0 = C_9 = [a^6+b^6+(a+b)^6]$$

$$= [a^3+b^3+(a+b)^3]^2.$$

$$= [ab(a+b)]^2.$$

Since a and b were assumed to be distinct and nonzero, we see that $g(X)$ cannot be the zero function. qed.

This example thus establishes the

THEOREM 6.3.18. <u>There exist bent functions in</u> FAMILY $\mathcal{PS}$ <u>which are not equivalent to any bent function in</u> FAMILY $\mathcal{M}$.

COROLLARY. <u>For all</u> $m > 3$ <u>there exist bent functions on</u> V_{2m} <u>which are not equivalent to any bent function in</u> FAMILY $\mathcal{M}$.

PROOF. Consider V_{2m} as the direct sum $V_8 \oplus V_{2m-8}$. The bent function $g(X,Y) = f(X) + q(Y)$, with f equivalent to our EXAMPLE 6.3.16 on V_8 and q the quadratic on V_{2m-8}, will do the job. qed.

We point out here that several years ago K. D. Lerche (private communication) posed the question of whether elementary-2 difference sets could be constructed by cyclotomy in $K = GF(2^{2m})$ — more specifically as the union of 2^{m-1} multiplicative cosets of the subgroup of e^{th} powers in K^*, with $e = 2^m \pm 1$. Lerche (with the help of a computer) had found such sets for $m = 3$.

Our FAMILY $\mathcal{PS}$/ap settles completely the case $e = 2^m+1$; here the subgroup of e^{th} powers is precisely the multiplicative group L^* of the subfield $L = GF(2^m)$ and any choice of cosets yields a difference set. The case $e = 2^m-1$ is not so happily resolved. Such a difference set has characteristic function

$$G : K \to F$$

given by

$$G(X) = g(X^{2^m+1}),$$

where

$$g : L \to F$$

satisfies

i) $g(0)=0$, and ii) g is balanced.

We have already encountered (in Chapter 4) an example of such a bent function; we restate the result as

REMARK 6.3.19. *If* K *has degree* 2 *over* L *which has degree* m *over* $F = GF(2)$, *then the function*

$$f(X) = Tr_{L/F}\{X^{2^m+1}\}$$

is a quadratic bent function on K.

PROOF. For any nonzero θ in K the derivative of f with respect to θ is given by

$$f_\theta(X) = Tr_{L/F}\{(X+\theta)^{2^m+1} + X^{2^m+1}\}$$

$$= Tr_{L/F}\{\theta X^{2^m} + \theta^{2^m}X\} + f(\theta)$$

$$= Tr_{L/F}\{\theta^{2^m}X\} + f(\theta),$$

which, being a nonconstant (affine) linear function, is balanced on K.

Equivalently, we may observe that the map

$$B(X,Y) = f(X+Y) + f(X) + f(Y)$$

$$= Tr_{K/F}\{X^{2^m}Y\}$$

is a nondegenerate bilinear form on $K \times K$ so that $f(X)$ is a nondefective quadratic on K.

qed.

It is useful here to note the connection between the Fourier-Hadamard transform and Singer difference sets [10]. If f is any function to $F = GF(2)$ from $L = GF(2^m)$, the Fourier transform $\hat{f}$ is given by

$$2^m \hat{f}(X) = \sum f^*(Y) \tau^*_{L/F}(XY),$$

this sum being taken over all Y in L. If $f(0) = 0$ then it is straightforward to verify that for any $X \neq 0$

$$2^m \hat{f}(X) = 4A(X) - 2|f|$$

where $|f|$ denotes the cardinality of f and $A(X)$ is the number of Y in L satisfying $f(Y) = 1 = \tau_{L/F}\{XY\}$. Alternatively, if we let Δ denote the 2^{m-1}-subset of L^* given by

$$\Delta = \{X \varepsilon L^* : \tau_{L/F}\{X\} = 1\},$$

we may observe that for all $x \varepsilon L^*$ $A(X)$ is precisely the coefficient on X in the element $f^{(-1)}\Delta$ of the group ring $Z[L^*]$. Then $2^m \hat{f}(0) = 2^m - 2|f|$; and, if we let $(\hat{f})$ denote the restriction of $\hat{f}$ to L^*, we have $2^m(\hat{f}) = 4f^{(-1)}\Delta - 2|f|L^*$ in $Z[L^*]$. The set Δ is a Singer difference set in the cyclic group L^*; it has parameters

$$(2^m - 1,\ 2^{m-1},\ 2^{m-2},\ 2^{m-2})$$

so that

$$\Delta^{(-1)}\Delta = 2^{m-2} + 2^{m-2} L^*$$

in the group ring $Z[L^*]$.

Now let K be the quadratic extension of L and let D be the corresponding Singer difference set in K^*; i.e.

$$D = \{Z \varepsilon K^* : \tau_{K/F}\{Z\} = 1\}.$$

Let E be the 2^m-subset of K^* given by

$$E = \{Y \varepsilon K^* : \tau_{K/L}(Y) = 1\}$$

and let H be the subgroup of K^* such that $K^* = L^*H$. Then it is not hard to verify that $D = \Delta E$ and $EH = 2\Delta H$ in $Z[K^*]$. A subset G of K^* comprised of 2^{m-1} cosets of H may be represented as $G = gH$ in $Z[K^*]$ where g is a 2^{m-1}-subset of L^*. By the preceding observations it follows that G is bent iff

$$G^{(-1)}D = 2^{m-1}fH + 4^{m-1}K^*$$

where f is again a 2^{m-1}-subset of L^*; indeed, fH is the "Fourier transform" of $G = gH$. But now we may write

$$G^{(-1)}D = (g^{(-1)}H)(\Delta E) = (g^{(-1)}\Delta)(HE) = 2g^{(-1)}\Delta^2 H,$$

which implies

$$g^{(-1)}\Delta^2 = 2^{m-2}(f + 2^{m-1}L^*).$$

Multiplying this last equation by $\Delta^{(-1)}$, we obtain

$$g^{(-1)}\Delta = f\Delta^{(-1)}.$$

We are thus able to characterize this second class of cyclotomic bent functions as follows.

FAMILY C^+. *Let* g *be a balanced function from* $L = GF(2^m)$ *to* $F = GF(2)$ *which vanishes at* 0. *Let* G *be the function on* $K = GF(2^{2m})$ *given by*

$$G(Z) = g(Z^{2^m+1}).$$

Then G *is bent iff there exists a balanced function*

$$h : L \to F$$

such that

$$\hat{h}(Y) = \hat{g}(Y^{-1})$$

for all $Y \in L^*$, *where*

$$2^m \hat{f}(Y) = \sum_{X \in L} f^*(X) \, Tr^*_{L/F} \{YX\}$$

for all $Y \in L$.

Remark 6.3.19 shows that FAMILY C^+ contains "the" quadratic bent function which arises from a linear g (if $g(X) = Tr_{L/F}\{\alpha X\}$, the corresponding h is $h(X) = Tr_{L/F}\{\alpha^{-1}X\}$). We know of no other bent function of this type; we thus pose the

QUESTION. *Does FAMILY* C^+ *contain a bent function of degree greater than 2? Equivalently, do there exist nonlinear functions* $g, h : L \to F$ *satisfying* i) $g(0)=0=h(0)$; ii) $\hat{g}(0)=0=\hat{h}(0)$, *and* iii) $\hat{g}(X)=\hat{h}(X^{-1})$ *for all* $X \in L^*$?

Notice that the difference set which is the set of zeros of the quadratic function

$$f(X) = \mathrm{Tr}_{L/F}\{X^{2^m+1}\}$$

on $K = GF(2^{2m})$ can be expressed as the union of 2^m+1 pairwise "disjoint" subgroups of order 2^{m-1}; namely, the Pall partition

$$P : S, \theta S, \theta^2 S, \ldots, \theta^{2^m} S,$$

where θ is a primitive (2^m+1)th root of unity in K^* and S is the kernel of $\mathrm{Tr}_{L/F}$ on L. This suggests a method by which we may be able to obtain other difference sets.

REMARK 6.3.20. Let $H_1, H_2, \ldots, H_{2^m+1}$ be pairwise "disjoint" $(m-1)$-dimensional subspaces of Z_2^{2m}. Then $D = \cup H_i$ is a difference set in Z_2^{2m} iff every hyperplane of Z_2^{2m} contains exactly one H_i or exactly three H_i's.

PROOF. In the group ring notation we have

$$D = 1 + \sum H_i^*, \quad H_i^* = H_i \backslash \{0\}.$$

Then, for any nonprincipal character χ of Z_2^{2m},

$$\begin{aligned} \chi(D) &= 1 + \sum \chi(H_i^*) \\ &= 1 + t(2^{m-1}-1) + (2^m+1-t)(-1) \\ &= 2^{m-1}(t-2), \end{aligned}$$

where t is the number of H_i's contained in the hyperplane corresponding to χ (i.e. the hyperplane on which χ is the principal character). The result is then clear. qed.

Now consider the spread for the affine plane $L \oplus L$, $L = GF(2^m)$, given by the lines

$$X = 0; \quad Y = mX, \quad m\varepsilon L.$$

For each of these m-dimensional spaces, we choose an (m-1)-dimensional subspace; in particular, suppose we pick the subspaces

$$H_\infty = \{(0,Y):\tau\{Y\}=0\}; \quad H_m = \{(X,mX):\tau\{\rho(m)X\}=0\}, \ m\varepsilon L.$$

It is not hard to verify that these subspaces meet the conditions of Remark 6.3.20 as long as the map $\rho:L\to L$ satisfies i) $\rho(z)$ does not vanish; ii) $\rho(z)+z$ is one-to-one; iii) $\rho(z)+\beta(z)$ is two-to-one for all $\beta\neq 1$ in L. The resulting set is then the set of zeros of the function

$$f(X,Y) = \tau\{Y+X\sigma(X^{2^m-2}Y)\}$$

on $L \oplus L$. We restate this result as

FAMILY $\mathcal{H}$. Let $\sigma : L \to L$ be a permutation such that $\sigma(z)+z$ does not vanish on L and $\sigma(z)+\beta z$ is two-to-one for every $\beta\varepsilon L^*$. Then the points in the subspaces $H_\infty=\{(0,Y):\tau\{Y\}=0\}$, $H_m=\{(X,mX):\tau\{(\sigma(m)+m)X\}=0\}, m\varepsilon L$, constitute a difference set in $L \oplus L$, $L = GF(2^m)$. This set is the set of zeros of the function

$$f(X,Y) = \tau\{Y + X\sigma(X^{2^m-2}Y)\}.$$

We remark that choosing $\sigma(z) = z^{2^{n-r}}+\theta$, with $(r,n)=1$ and θ not in the range of $z^{2^{n-r}}+z$ yields the bent function $f(X,Y) = \tau\{\theta X+Y+X^{2^r-1}Y\}$ which has degree r and is also in FAMILY $\mathcal{M}$.

The final "family" we present here is actually a characterization of bent functions having a certain restricted polynomial form. In his beautiful paper [22] of 1966 Rothaus included the

FAMILY $\mathcal{O}'$. *If* A, B, C, *and* $A+B+C$ *are all bent functions on* V_{2m}, *then*

$$f(X,y,z) = A(X)B(X) + A(X)C(X) + B(X)C(X) + [A(X)+B(X)]y + [A(X)+C(X)]z+yz$$

is a bent function on V_{2m+2}.

At the end of his paper [22] Rothaus stated without proof the

REMARK 6.3.21. *The bent function in* FAMILY $\mathcal{O}'$ *is the most general bent function of the form*

$$f(X,y,z) = R(X) + S(X)y + T(X)z + yz.$$

We shall now present another characterization of the above class of bent functions; a curious property of the Hadamard transform will then be used to establish FAMILY $\mathcal{O}'$ and Remark 6.3.21. In what follows we employ several typographical shortcuts. First we use $\bar{g}$ to denote the complement $g+1$ of the function g. Secondly, we suppress the variable X in functions which depend only on X; the capital letters A, B, C, R, S, T denote such functions. Finally, we use $g^{\wedge}$ as an alternative to $\hat{g}$ to denote the Fourier transform of g.

FAMILY $\mathcal{O}$. $f(X,y,z) = R + Sy + Tz + yz$ *is bent on* V_{2m+2} *if and only if* $R + ST$, $R + S\bar{T}$, $R + \bar{S}T$, *and* $R + \overline{ST}$ *are all bent on* V_{2m}.

PROOF. We regard V_{2m+2} as the direct sum $V_{2m} \oplus V_2$ and use the "Box Theorem" (Theorem 3.3.5). Letting $f^{*\square}$ (resp. $\hat{f}^{\square}$) denote the $2^{2m} \times 4$ matrix whose rows and columns are indexed by the lexicographically orders vectors in V_{2m} and V_2 and whose (u,v)th entry is $f^*(u,v)$ (resp. $\hat{f}(u,v)$), we may write

$$\hat{f}^{\square} = H_{2m}^{-1} f^{*\square} H_2^{-1} .$$

The columns of $f^{*\square}$ correspond to the functions

$$f_{00} = f(X,0,0) = R$$

$$f_{01} = f(X,0,1) = R + T$$

$$f_{10} = f(X,1,0) = R + S$$

$$f_{11} = f(X,1,1) = R + S + T + 1,$$

so that the columns of $H_{2m}^{-1} f^{*\square}$ are simply the Fourier transforms of the columns of $f^{*\square}$; i.e.

$$H_{2m}^{-1} f^{*\square} = [\hat{f}_{00}, \hat{f}_{01}, \hat{f}_{10}, \hat{f}_{11}].$$

It follows that

$$\hat{f}^{\square}(X,y,z) = \tfrac{1}{4}(\hat{f}_{00}(X) + (-1)^z \hat{f}_{01}(X) + (-1)^y \hat{f}_{10}(X) + (-1)^{y+z} \hat{f}_{11}(X)).$$

But it is easily seen that if $S_2(x_1,x_2,x_3) = x_1x_2 + x_1x_3 + x_2x_3$ and A, B, C are arbitrary Boolean functions on V_n then the composite function $S_2(A,B,C)$ has Fourier transform

$$[S_2(A,B,C)]^\wedge = \tfrac{1}{2}[\hat{A} + \hat{B} + \hat{C} - (A+B+C)^\wedge].$$

Thus, we have

$$\hat{f}^{\square} = \tfrac{1}{2}[(S_2(f_{00},f_{01},f_{10}))^\wedge, (S_2(f_{00},\bar{f}_{01},f_{10}))^\wedge, (S_2(f_{00},f_{01},\bar{f}_{10}))^\wedge, (\bar{S}_2(\bar{f}_{00},f_{01},f_{10}))^\wedge$$

which may be expressed in terms of R, S, and T by

$$\hat{f}^{\square} = \tfrac{1}{2}[(R+ST)^\wedge,\ (R+S\bar{T})^\wedge,\ (R+\bar{S}T)^\wedge,\ (R+\bar{S}\bar{T})^\wedge].$$

The assertion of the theorem is now obvious. qed.

We now observe a curious property of Boolean functions.

REMARK 6.3.22. *Let* a, b, c *be arbitrary Boolean functions on* V_n. *Then there exist unique functions* A, B, C *such that*

$$a = \bar{A}B + \bar{A}C + BC$$

$$b = A\bar{B} + AC + \bar{B}C$$

$$c = AB + A\bar{C} + B\bar{C}.$$

Indeed, the functions A, B, C *are given by*

$$A = \bar{a}b + \bar{a}c + bc$$

$$B = a\bar{b} + ac + \bar{b}c$$

$$C = ab + a\bar{c} + b\bar{c}.$$

PROOF. Taking Fourier transforms, we need

$$(a^\wedge, b^\wedge, c^\wedge, (a+b+c)^\wedge) = (A^\wedge, B^\wedge, C^\wedge, (A+B+C)^\wedge)H,$$

where $H = \frac{1}{2}\begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}$.

But (since H is involutory) this is equivalent to

$$(A^\wedge, B^\wedge, C^\wedge, (A+B+C)^\wedge) = (a^\wedge, b^\wedge, c^\wedge, (a+b+c)^\wedge)H.$$ qed.

We may use this result to establish Rothaus' Remark 6.3.21. According to FAMILY $\mathcal{O}$ the most general bent function of the form

$$f(X,y,z) = R(X) + S(X)y + T(X)z + yz$$

is the function for which

$$A = f_{00}f_{01} + f_{00}f_{10} + f_{01}f_{10}$$

$$B = f_{00}\bar{f}_{01} + f_{00}f_{10} + \bar{f}_{01}f_{10}$$

$$C = f_{00}f_{01} + f_{00}\bar{f}_{10} + f_{01}\bar{f}_{10}$$

$$A+B+C = \bar{f}_{00}f_{01} + \bar{f}_{00}f_{10} + f_{01}f_{10}$$

are all bent, where

$$f_{00} = R$$

$$f_{01} = R + T$$

$$f_{10} = R + S.$$

But by Remark 6.3.22 we have

$$f_{00} = AB + AC + BC$$

$$f_{01} = A\bar{B} + AC + \bar{B}C = f_{00} + A + C$$

$$f_{10} = AB + A\bar{C} + B\bar{C} = f_{00} + A + B,$$

so that R, S, and T are given by

$$R = AB + AC + BC$$

$$S = A + B$$

$$T = A + C.$$

It follows that the most general bent function of the form $f(X,y,z) = R + Sy + Tz + yz$ on V_{2m+2} is, indeed, given by $f(X,y,z) = AB + AC + BC + (A+B)y + (A+C)z + yz$, where A, B, C, and $A+B+C$ are all bent on V_{2m}.

Note that, if A, B, C, and $A+B+C$ are all bent on V_{2m}, we have immediately that the "box"

$$[g^*] = 2^m[A^{\wedge}, B^{\wedge}, C^{\wedge}, (A+B+C+1)^{\wedge}]$$

represents a bent function on V_{2m+2}. Indeed, transforming the columns of $[g^*]$ yields

$$[A^*, B^*, C^*, (A+B+C+1)^*]$$

every row of which is necessarily a bent function on V_2. Of course, these bent functions are just the "Fourier transforms" of the bent functions in FAMILY $\mathcal{O}$. Thus, we have

FAMILY $\hat{\mathcal{O}}$. *If* $A,B,C,$ *and* $A+B+C$ *are bent on* V_{2m}, *then*

$$g(X,y,z) = a(X)\bar{y}\bar{z} + b(X)\bar{y}z + c(X)y\bar{z} + d(X)yz$$

is bent on V_{2m+2}, *where* $a,b,c,$ *and* d *are the "Fourier transforms" of* $A,B,C,$ *and* $A+B+C+1$, *respectively. These bent functions are the "Fourier transforms" of those in* FAMILY $\mathcal{O}$.

REFERENCES

[1] E. Artin, _Geometric Algebra_, Interscience, New York, 1957.

[2] L. D. Baumert, _Cyclic Difference Sets_, Lecture Notes in Mathematics 182, Springer-Verlag, Berlin-Heidelberg-New York, 1971.

[3] E. R. Berlekamp, _Algebraic Coding Theory_, McGraw-Hill, New York, 1968.

[4] R. H. Bruck, Difference Sets in a Finite Group, Trans. A.M.S. 78 (1955), 464-481.

[5] L. Couvillon, _Partitionings by Means of Maximal Isotropic Spaces_, Ph.D. Thesis, Louisiana State U., 1971.

[6] J. F. Dillon, Singer Difference Sets and Bent Functions, unpublished, 1972.

[7] __________, The Kerdock Codes and Bent Functions, unpublished, 1973.

[8] L. E. Dickson, _Linear Groups with an Exposition of the Galois Field Theory_, Dover, New York, 1958.

[9] J. Dieudonné, _La Géométrie des Groupes Classiques_, second ed., Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.

[10] Marshall Hall, Jr., _Combinatorial Theory_, Ginn-Blaisdell, Waltham, 1967.

[11] A. M. Kerdock, A Class of Low-Rate Nonlinear Binary Codes, Information and Control 20 (1972), 182-187.

[12] R. J. Lechner, Harmonic Analysis of Switching Functions, in _Recent Developments in Switching Theory_, edited by Amar Mukhopadhyay, Academic Press, New York, 1971.

[13] H. B. Mann, _Addition Theorems_, Interscience, New York, 1965.

[14] __________ and R. L. McFarland, On Multipliers of Difference Sets, Canadian J. Math. 17 (1965), 541-542.

[15] R. L. McFarland, On Multipliers of Abelian Difference Sets, Ph.D. Thesis, Ohio State U., 1970.

[16] __________, A Family of Noncyclic Difference Sets, J. Comb. Th. (Series A) 15 (1973), 1-10.

[17] __________, The Multipliers of the Difference Set in the Elementary Abelian Group of Order 16, unpublished, 1971.

[18] P. Kesava Menon, Difference Sets in Abelian Groups, Proc. A.M.S. 11 (1960), 368-377.

[19] _______________, On Difference Sets Whose Parameters Satisfy a Certain Relation, Proc. A.M.S. 13 (1962), 739-745.

[20] T. G. Ostrom, Finite Translation Planes, Lecture Notes in Mathematics 158, Springer-Verlag, Berlin-Heidelberg-New York, 1970.

[21] G. Pall, Partitioning by Means of Maximal Isotropic Subspaces, Linear Algebra and its Applications 5 (1972), 173-180.

[22] O. S. Rothaus, On Bent Functions, preprint.

[23] M. P. Schutzenberger, A Non-existence Theorem for an Infinite Family of Symmetrical Block Designs, Annals of Eugenics 14 (1949), 286-287.

[24] R. J. Turyn, Character Sums and Difference Sets, Pacific J. Math 15 (1965), 319-346.

[25] ___________, Sequences With Small Correlation, in Error-Correcting Codes, edited by H. B. Mann, Wiley, New York, 1968.

[26] W. D. Wallis, Anne Penfold Street, Jennifer Seberry Wallis, Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices, Lecture Notes in Mathematics 292, Springer-Verlag, Berlin-Heidelberg-New York, 1972.

VITA

Name: John Francis Dillon.

Permanent address: 85^{th} Avenue, New Carrollton, Maryland, 20784.

Degree and date to be conferred: Ph.D., 1974.

Date of birth: August 18, 1941.

Place of birth: Willimantic, Connecticut.

Secondary education: Windham High School, 1959.

Collegiate institutions attended	Dates	Degree	Date of Degree
Villanova University	1959-1963	B.S.	1963
University of Maryland	1964-1967	M.A.	1967
University of Maryland	1967-1974	Ph.D.	1974

Major: Mathematics (Algebra)

Minor: Mathematics (Analysis)

Publications:

with D. P. Roselle, Eulerian Numbers of Higher Order, Duke Math. J. 35 (1968)

with D. P. Roselle, Simon Newcomb's Problem, SIAM J. Appl. Math. 17 (1969)

The Generalized Langford-Skolem Problem, in _Proceedings of the Fourth Southeastern Conference on Combinatorics, Graph Theory, and Computing_, F. Hoffman, R. B. Levow and R. S. D. Thomas, Eds., Utilitas Mathematica Publishing Inc., Winnipeg, 1973

with R. A. Morris, A Skew Room Square of Side 257, Utilitas Math. 4 (1973)

with R. A. Morris, On a Paper of Berlekamp, Fredricksen, and Proto, Utilitas Math. 5 (1974)

Position held: Mathematician, Department of Defense, Fort George G. Meade, Maryland.