19 NOVEMBER 2015

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 70103A
13 November 2015

JOHN L YOUNG
251 W 89th ST
NEW YORK NY 10024

Dear Mr. Young:

This is our final response to your Freedom of Information Act (FOIA) request of 13 March 2013 for a document by John Dillon entitled "Survey of Bent Functions", NSA Technical Journal, Special Fast Fourier Issue of August 1973. A copy of your request is enclosed. Your request has been processed under the FOIA and the document you requested is enclosed.

This agency is authorized by statute to protect certain information concerning its activities, as well as the names of its employees. Such information is exempt from disclosure pursuant to the third exemption of the FOIA which provides for the withholding of information specifically protected from disclosure by statute. The specific statute applicable in this case is Section 6, Public Law 86-36 (50 U.S. Code 3605). We have determined that such information exists in this document, and we have excised it accordingly.

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. The appeal must be in writing and addressed to the:

NSA/CSS FOIA/PA Appeal Authority (DJ4),
National Security Agency,
9800 Savage Road STE 6248,
Fort George G. Meade, MD 20755-6248

- It must be postmarked no later than 60 calendar days of the date of this letter.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of information was unwarranted.
- NSA will endeavor to respond within 20 working days of receiving your appeal, absent any unusual circumstances.

Blacker, Cindy S

From: John Young [jya@pipeline.com]
Sent: Wednesday, March 13, 2013 7:29 AM
To: foiarsc, foiarsc
Subject: FOIA Request

NSA FOIA REQUESTER SERVICE CENTER:
POC: Cindy Blacker
NSA FOIA Requester Service Center/DJ4
9800 Savage Road, Suite 6248
Ft. George G. Meade, MD 20755-6248

Dear Ms. Blacker,

This is a request under the FOIA for the following document:

NSA Technical Journal, Special Fast Fourier Issue, August 1973 (207 pages)

This document will be published on the public education website Cryptome.org

I agree to pay all associated costs.

Thank you very much.

John Young
Administrator
Cryptome.org
251 West 89th Street
New York, NY 10024
212-873-8700

A Survey of Bent Functions*

BY JOHN F. DILLON

Unclassified

A bent function is a Boolean function all of whose Fourier coefficients have the same magnitude; such a function is equivalent to a difference set in an elementary Abelian 2-group. This paper is a survey of the theory of bent functions and includes reviews of the major results relating to the more general topics of difference sets and the Fourier analysis of Boolean functions.

1. INTRODUCTION.

In a beautiful little paper [24] published in 1966 O. S. Rothaus invented a class of Boolean functions which he called "bent" functions and presented the basic properties and a large general family of these wonderful creatures. At about the same time Glenn F. Stahly pointed out that a bent function is equivalent to a difference set in an elementary Abelian 2-group. A few isolated examples of these difference sets had been constructed earlier, but Rothaus' construction was the first to produce non-equivalent difference sets in the same group. Recent investigations of bent functions have produced several new constructions and a number of interesting ideas which clarify and extend known results while raising questions for further research. Remarkably, however, no one has yet been able to exhibit a bent function known to be inequivalent to those considered by Rothaus. It is the opinion of many investigators that the class of bent functions obtained by J. A. Maiorana (and independently by R. L. McFarland) contains (up to affine equivalence) every possible bent function. A recent result of [redacted] implies that this conjecture is true for bent functions in six variables. Indeed, [redacted] has determined the pairwise inequivalent bent functions in six variables, and his representative functions turn out to be of the Maiorana type. They are also of the type considered by Rothaus. For functions in $2n > 6$ variables very little progress has been made toward the solutions of the central problem of determining the inequivalent bent functions and the lesser problem of constructing all bent functions.

This paper, which grew (and grew) out of notes prepared for a lecture presented to the CMI in August 1971, is intended to be primarily a survey of the theory of bent functions. It is, however, somewhat wider in scope and includes reviews of several major results relating to the more general topics of difference sets and Boolean functions.

Section 2 contains a rather general discussion of difference sets and their incidence matrices with the emphasis being on "Hadamard" difference sets, the incidence matrices of which correspond to certain highly structured Hadamard matrices. In Section 3 we present the fundamental notions from the theory of Boolean functions and their Fourier transforms. In Section 4 we derive quickly and painlessly all of the elementary properties of bent functions; these results are seen to follow easily from the fundamental results of the previous two sections. The main result of Section 4 is a theorem which characterizes bent functions in six different ways, each of which is particularly suited for some purposes. Section 5 contains the known "families" of bent functions, of which we have identified seven; however, some of these are not families in the usual sense of the word, but are merely classes of bent functions which share some particularly interesting structure and which it is not at all clear how to construct. Several questions arising from the consideration of these "families" are also presented in this section. Finally, in Section 6 we give a complete account of the bent functions in fewer than eight variables and point out an unfortunate (typographical) error which mars Rothaus' marvelous piece of work.

*For this paper Mr. Dillon won First Prize in the 1972 Crypto-Mathematics Institute Essay Contest.

As must be the case in any survey paper, many of the results contained herein are well known. Indeed, most of Section 4 is contained in Rothaus' pioneering paper. We have endeavored, however, to provide a number of new results as well as new proofs for most of our results, so that this survey may be of interest even to those well acquainted with the subject matter.

(b) (3) -P.L. 86-36

We are indebted to our colleagues in R41 who have created a stimulating environment in which bent functions thrive and from whose work we have benefited—especially [redacted] K. D. Lerche, [redacted] and G. F. Stahly. We particularly acknowledge the influence of our friend and colleague R. L. McFarland, who taught us all about difference sets in the first place. Finally, we thank the lovely ladies of R41 whose cryptanalytic bent has rendered straight our manuscript.

2. DIFFERENCE SETS AND THEIR INCIDENCE MATRICES.

Let G be an Abelian group of order v and let D be a k-subset of G.

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. For convenience we define the parameter n to be equal to $k - \lambda$.

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 2.1: $\lambda(v-1) = k(k-1)$.

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 (u, v)th entry is 1 whenever $u + v$ is an element in D; i.e.,

$$[D](u, v) = 1 \text{ iff } u + v \in D$$

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

We then have the easy

Remark 2.2: D is a (v, k, λ, n)- difference set if and only if the incidence matrix $[D]$ satisfies

$$[D]^2 = nI + \lambda J,$$

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

Proof: The (u, v)th entry of $[D]^2$ is the number of elements in both $D - u$ and $D - v$. But for elements d_i and d_j in D,

$$d_i - u = d_j - v \Leftrightarrow u - v = d_i - d_j,$$

and the assertion follows immediately. qed.

We note here that Remark 2.2 shows that the translates $\{D + g : g \in G\}$ 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) [11].

We may now establish quite easily the

Remark 2.3: If D is a (v, k, λ, n)-difference set in G, then its complement $\overline{D} = G - D$ is a $(v, v - k, v - 2k + \lambda, n)$-difference set in G.

Proof: $[\overline{D}]^2 = (J - [D])^2 = J^2 - 2[D]J + [D]^2$

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

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

Remark 2.4: D is a (v, k, λ, n)-difference set if and only if $[D^*]^2 = 4nI + (v - 4n)J$.

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 2.5: The (± 1)-matrix H is Hadamard if and only if HH' is scalar (i.e., of the form cI for some constant c).

Collecting our foregoing observations, we arrive at the very important

Theorem 2.1: D is a (v, k, λ, n)-difference set with $v = 4n$ if and only if $[D^*]$ is a Hadamard matrix.

In light of Theorem 2.1 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 [23] was the first to note the rather surprising

Remark 2.6: 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 2.7: 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

$$[D]^2 = nI + \lambda J,$$

from which it follows quite easily that

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

and the result is immediate. qed.

The same proof establishes this result for an arbitrary (v, k, λ)-configuration (symmetric balanced incomplete block design); the general result was obtained by Schutzenberger [25] and Bruck and Ryser [11] independently. Another general result which provides a restriction on parameters is the following remarkable theorem due to H. B. Mann [16].

Theorem 2.2: 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 2.3: If there exists a nontrivial (v, k, λ)-configuration with $k < v/2$ and v of the form $2p^m$, p prime, then $(v, k, \lambda) = (4^{s+1}, 2 \cdot 4^s - 2^s, 4^s - 2^s)$ for some s.

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

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

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

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

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

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

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.

It now follows easily from (**) that

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

and

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

which imply

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

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 2.8: 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

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

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 [17] have shown that every multiplier of a difference set must fix at least one translate of that difference set. 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 2.9: 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 0 0 0 0. 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 1 0 0 0, 0 1 0 0, 0 0 1 0, 0 0 0 1. Finally, it is easy to verify that the sixth element of D must be 1 1 1 1. That the resulting set D is indeed a difference set is obvious. 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 [21] has observed that the (16, 6, 2, 4)-difference set in Z_2^4 has multiplier group of order 720. McFarland also observes [19] that, if D is such a difference set, there exists a group automorphism β such that D and D^β have *different* (although isomorphic) multiplier groups. (Note: this situation cannot arise for cyclic groups because such groups 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 $\{g, g\alpha, g\alpha^2, \ldots, g\alpha^t, \ldots\}$). Thus, the existence of a multiplier facilitates the investigation of a difference set. A very powerful theorem due to Marshall Hall, Jr. and several generalizations [19] provide multipliers for difference sets in a variety of groups; however, all multipliers given by these theorems are *numerical* 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. BOOLEAN FUNCTIONS AND THEIR FOURIER TRANSFORMS.

In this section we shall denote by F the field $GF(2)$ with two elements.

Definition: A Boolean function is a function from some space F^n of binary n-tuples into F. The space F^n is denoted by V_n.

The following result is well known (see, for example, [7]):

Theorem 3.1: Every Boolean function

$$f: V_n \to F$$

is given by a unique "reduced" polynomial

$$f(x) = \sum_{v \in V_n} g(v)\, x_1^{v_1} x_2^{v_2} \cdots x_n^{v_n}$$

in the n "coordinate variables" $x_1, x_2, \ldots, x_n$.

The coefficients g(v) are given by

$$g(v) = \sum_{u \subset v} f(u) \text{ for all } v \in V_n,$$

where "$u \subset v$" means "$u_i = 1 \Rightarrow v_i = 1, 1 \leq i \leq n$".

We shall usually identify the function f with the polynomial $f(x)$.

Definition: The functions $f(x)$ and $g(x)$ on V_n are linearly (resp. affinely) equivalent if there exists a nonsingular linear (resp. affine) transformation T of the coordinate variables $x_1, x_2, \ldots, x_n$ such that $g(x_1, x_2, \ldots, x_n) = g(x) = f(xT) = f(x_1 T, x_2 T, \ldots, x_n T)$.

Definition: The "truth-table" of a function g defined on V_n is the 2^n-long column vector $g = (g(0), g(1), g(2), \ldots, g(2^n - 1))'$ where we use the integer i as convenient notation for the binary n-tuple which is the binary representation of i.

Definition: With each Boolean function $f: V_n \to F$ we associate the real-valued function $f^*: V_n \to \{\pm 1\}$ defined by $f^*(x) = (-1)^{f(x)}$.

Remark 3.1: The real functions $(-1)^{v \cdot x}$ corresponding to the linear Boolean functions $v \cdot x$ are precisely the group characters of V_n.

Theorem 3.2: Each function $g: V_n \to R$ may be expressed as

$$g(x) = \sum_{v \in V_n} \hat{g}(v) (-1)^{v \cdot x}.$$

The function $\hat{g}: V_n \to R$ is the (n-dimensional mod 2) Fourier transform or Hadamard transform of g and is uniquely given by

$$\hat{g}(x) = \frac{1}{2^n} \sum_{u \in V_n} g(u) (-1)^{u \cdot x}.$$

If $g = f^*$, f Boolean, we write $\hat{f}$ in the place of $\hat{f^*}$ and call $\hat{f}$ the Fourier transform of f as well as f^*. It is straightforward to verify

Remark 3.2: If $g(x) = f(xT + a)$, T a nonsingular linear transformation, then

$$\hat{g}(x) = (-1)^{a \cdot xL} \hat{f}(xL),$$

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

Definition: The elementary Hadamard matrix H_n is defined by

$$H_0 = 1; H_{n+1} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}, n \geq 0.$$

Remark 3.3: $H_n = \otimes^n \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ (i.e., *the n-fold Kronecker product of $H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ with itself*) *and $H_n(u, v) = (-1)^{u \cdot v}$ for all $u, v \in V_n$. Also, $H_n^{-1} = \frac{1}{2^n} H_n$.*

We may combine Theorem 3.2 and Remark 3.3 to obtain

Remark 3.4: Let g be (the truth-table of) a real-valued function on V_n and let $\hat{g}$ be (the truth-table of) its Fourier (Hadamard) transform. Then

$$g = H_n \hat{g}$$

and

$$\hat{g} = \frac{1}{2^n} H_n g.$$

Definition: With each function $g: V_n \to R$ *we associate the* $2^n \times 2^n$ *matrix* $[g]$ *whose* (u, v)th *entry is* $g(u + v)$.

We now prove a very pretty result which the present writer learned from R. L. McFarland [18].

Theorem 3.3: $H_n [g] H_n^{-1} = 2^n \operatorname{diag}(\hat{g}(0), \hat{g}(1), \ldots, \hat{g}(2^n - 1))$.

Proof: The (u, v)th entry of the matrix on the left is

$$\frac{1}{2^n} \sum_{s,t} H_n(u, s)\, g(s + t)\, H_n(t, v) = \frac{1}{2^n} \sum_{w} g(w) \sum_{s} H_n(u, s)\, H_n(s + w, v)$$

$$= \frac{1}{2^n} \sum_{w} g(w)\, H_n(w, v) \sum_{s} H_n(u, s)\, H_n(v, s)$$

$$= \begin{cases} 2^n \hat{g}(v) & \text{if } u = v \\ 0 & \text{otherwise.} \end{cases} \quad \text{qed.}$$

Corollary: $H_n [g]^2 H_n^{-1} = (2^n)^2 \operatorname{diag}(\hat{g}^2(0), \hat{g}^2(1), \ldots, \hat{g}^2(2^n - 1))$.

The next result has been called by Lechner [13] the "Poisson Summation Formula."

Remark 3.5: Let g *be a real-valued function on* V_n *and let* g *be its Fourier (Hadamard) transform. Let* S *be an arbitrary subspace of* V_n *and let* $S^\perp$ *be the dual (annihilator) of* S (i.e., $S^\perp = \{v \in V_n$: $v \cdot s = 0$ *for all* s *in* $S\}$). *Then*

$$\sum_{u \in S} g(u) = 2^{\dim S} \sum_{u \in S^\perp} \hat{g}(u).$$

Proof: $\sum_{u \in S} g(u) = \sum_{u \in S} \left\{ \sum_{v \in V_n} \hat{g}(v)\, (-1)^{u \cdot v} \right\} = \sum_{v \in V_n} \hat{g}(v) \left\{ \sum_{u \in S} (-1)^{u \cdot v} \right\} = 2^{\dim S} \sum_{v \in S^\perp} \hat{g}(v)$. qed.

The following corollary was discovered independently by [redacted]

Corollary: For any Boolean function $f: V_n \to F$,

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

where $\overline{v}$ *denotes the complement of the vector* v, *and* $|v|$ *denotes the density* (i.e., *number of* 1's) *of* v.

The final result of this section we call the "Box Theorem" [9].

Theorem 3.4. (Box Theorem). Let g *be a real-valued function on* V_n. *Then for all integers* a, $0 \le a \le n$,

$$2^n \hat{g}^\square = H_a g^\square H_{n-a},$$

where $g^\square$ (resp. $\hat{g}^\square$) *is the* $2^a \times 2^{n-a}$ *matrix whose rows and columns are indexed by the lexicographically ordered vectors in* V_a *and* V_{n-a} *and whose* (u, v)th *entry is* $g(u, v)$ (*resp.* $\hat{g}(u, v)$).

Proof: The (u, v)th entry of the matrix on the right is

$$\sum_{s,t} H_a(u, s)\, g^\square(s, t)\, H_{n-a}(t, v)$$

$$= \sum_{(s,t) \in V_n} H_a(u, s)\, H_{n-a}(v, t)\, g(s, t)$$

$$= \sum_{(s,t) \in V_n} H_n((u, v), (s, t))\, g(s, t)$$

$$= 2^n \hat{g}(u, v). \quad \text{qed.}$$

4. BENT FUNCTIONS.

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

We may immediately establish the

Theorem 4.1: f is bent iff $[f^*]$ is Hadamard.

Proof: By the corollary to Theorem 3.3 we have

$$H_n [f^*]^2 H_n^{-1} = (2^n)^2 \operatorname{diag}(\hat{f}^2(0), \hat{f}^2(1), \ldots, \hat{f}^2(2^n - 1)).$$

Thus, f is bent $\Leftrightarrow H_n [f^*]^2 H_n^{-1}$ is scalar
$\Leftrightarrow [f^*]^2$ is scalar
$\Leftrightarrow [f^*]$ is Hadamard,
the last equivalence a consequence of Remark 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 2.1 and 4.1 then combine to yield

Theorem 4.2: f is bent iff $D = f^{-1}[1]$ is a Hadamard difference set in V_n.

Definition: For $f: V_n \to F$ and $v \in V_n$, $v \neq 0$, we define the function $f_v: V_n \to F$ by

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

f_v is called the (directional) derivative of f in the direction v.

It is now very easy to establish the following theorem first enunciated by [redacted] who proved it in a vastly different manner.

Theorem 4.3: f is bent iff f_v is balanced for all $v \neq 0$.

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

(b) (3)-P.L. 86-36

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

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

$$H_n [f^*]^2 H_n^{-1} = (2^n)^2 \operatorname{diag}(\hat{f}^2(0)), \hat{f}^2(1), \ldots, \hat{f}^2(2^n - 1))$$

of the Corollary to Theorem 3.3 becomes for bent functions

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

which implies immediately the

Remark 4.1: If f is bent on V_n, the Fourier coefficients of f are all equal to $\pm 2^{-n/2}$.

Since the Fourier coefficients of a Boolean function are rational numbers, Remark 4.1 implies

Remark 4.2: Bent functions exist on V_n only if n is even.

We may restate Remark 4.1 as

Remark 4.3: $f: V_{2n} \to F$ is bent iff there exists $\tilde{f}: V_{2n} \to F$ such that $\hat{f} = \frac{1}{2^n} f^*$. In this case, $\tilde{f}$ is also bent and $\hat{\tilde{f}} = \frac{1}{2^n} f^*$.

We shall refer to the bent function $\tilde{f}$ as the "Fourier transform" of f. There is thus a natural pairing of bent functions which we express (loosely) in the

Remark 4.4: The "Fourier transform" of a bent function is bent.

Next, if we let N_v denote the number of 0's of the function $f(x) + v \cdot x$ on V_{2n}, we have

$$2^{2n}\hat{f}(v) = \sum_{u \in V_{2n}} (-1)^{f(u)+v \cdot u} = N_v - (2^{2n} - N_v) = 2N_v - 2^{2n}$$

or

$$N_v = 2 \cdot 4^{n-1} + 2 \cdot 4^{n-1}\hat{f}(v).$$

It then follows that

Remark 4.5: $f: V_{2n} \to F$ is bent iff $f(x) + v \cdot x$ has $2 \cdot 4^{n-1} \pm 2^{n-1}$ zeros for all v in V_{2n}.

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_{2n}. Since, by Theorem 4.2, 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 2.3. Finally we note that if $\chi = (-1)^{v \cdot x}$ is a nonprincipal character of V_{2n} (i.e., $v \neq 0$), then for any $f: V_{2n} \to F$

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

We then have the

Remark 4.6: $f: V_{2n} \to F$ is bent iff $\chi(f^{-1}[1]) = \pm 2^{n-1}$ for all nonprincipal characters χ of V_{2n}.

We now collect the various characterizations of bent functions in the

Theorem 4.4: The following are equivalent:

1) *$f: V_{2n} \to F$ is bent;*
2) *$f(v) = \pm\dfrac{1}{2^n}$ for all $v \in V_{2n}$;*
3) *$f(x) + v \cdot x$ has $2 \cdot 4^{n-1} \pm 2^{n-1}$ zeros for all v in V_{2n};*
4) *$f_v(x) = f(x + v) + f(x)$ is balanced for all nonzero v in V_{2n};*
5) *$[f^*] = (f^*(u + v))$ is Hadamard;*
6) *$f^{-1}[1]$ is a Hadamard (equivalent to "nontrivial" for $n > 1$) difference set in V_{2n};*
7) *$\chi(f^{-1}[1]) = \pm 2^{n-1}$ for all nonprincipal characters χ of V_{2n}.*

The Poisson Summation Formula (Remark 3.5) may be combined with Theorem 3.1 to yield information about the degree of a bent function. Let $f: V_{2n} \to F$ be bent and let $\bar{f}: V_{2n} \to F$ be such that $\hat{f} = \dfrac{1}{2^n} f^*$. Thus, the Boolean function $\bar{f}$ is also bent and has Fourier transform $\hat{\bar{f}} = \dfrac{1}{2^n} f^*$. By the corollary to Remark 3.5 we have

$$\sum_{u \subset v} f^*(u) = 2^{|v|} \sum_{u \subset \bar{v}} \hat{f}(u) = 2^{|v|-n} \sum_{u \subset \bar{v}} \bar{f}^*(u) \tag{4.1}$$

for all v in V_{2n}. We now write $f^*(u) = 1 - 2f(u)$ and $\bar{f}^*(u) = 1 - 2\bar{f}(u)$, where we interpret f and $\bar{f}$ as functions taking the *real* values 0 and 1. Equation (4.1) then becomes

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

We restate this fruitful result in the

Remark 4.7: Let f and $\bar{f}$ be bent functions on V_{2n} such that $2^n\hat{f} = \bar{f}^*$ (equivalently, $2^n\hat{\bar{f}} = f^*$). Then, interpreting f and $\bar{f}$ as real-valued functions, we have

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

for all v in V_{2n}.

Several corollaries follow immediately from Remark 4.7.

Theorem 4.5: If n is greater than 1, a bent function on V_{2n} has degree at most n.

Proof: Let $f(x) = \sum_{v \in V_{2n}} g(v) x_1^{v_1} x_2^{v_2} \ldots x_{2n}^{v_{2n}}$ be a bent function.

According to Theorem 3.1 the monomial $x_1^{v_1} x_2^{v_2} \ldots x_{2n}^{v_{2n}}$ is present in the polynomial $f(x)$ if and only if $\sum_{u \subset v} f(u)$ is odd.

But Remark 4.7 assures us that

$$\sum_{u \subset v} f(u) = 2^{n-1}(2^{|v|-n} - 1) + 2^{|v|-n} \sum_{u \subset \bar{v}} f(u). \tag{4.2}$$

If $n > 1$ and $|v| > n$, the right side of (4.2) is even. Thus, $\sum_{u \subset v} f(u)$ is even and $f(x)$ does not contain the monomial $x_1^{v_1} x_2^{v_2} \ldots x_{2n}^{v_{2n}}$. qed.

Remark 4.8. If $f: V_{2n} \to F$ is bent of degree n, then its "Fourier transform" $\tilde{f}$ is also of degree n.

Proof: We prove a slightly stronger result. By Remark 4.7 we have

$$\sum_{u \subset v} f(u) = \sum_{u \subset \bar{v}} \tilde{f}(u) \quad \text{for all } v \text{ with } |v| = n.$$

Thus, $f(x)$ contains the degree n monomial $x^v \iff \sum_{u \subset v} f(u)$ is odd $\iff \sum_{u \subset \bar{v}} \tilde{f}(u)$ is odd $\iff \tilde{f}(x)$ contains the degree n monomial $x^{\bar{v}}$. qed.

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

Remark 4.9: 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 iff the individual factors are Hadamard. qed.

Functions of the type constructed in Remark 4.9 are rather uninteresting because they may be "decomposed" into simpler functions.

Definition: The Boolean function f(x) 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 $x_1, x_2, \ldots, x_n$ such that $f(xT) = g(x_1, x_2, \ldots, x_m) + h(x_{m+1}, x_{m+2}, \ldots, x_n)$ for some m, $1 \leq m < n$.*

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

$$f(x) \equiv f(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4.$$

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 4.10: For $n > 2$, every bent function of degree n on V_{2n} is indecomposable.

Proof: Let the bent function $f(x_1, x_2, \ldots, x_{2n})$ of degree n be linearly equivalent to

$$g(x_1, x_2, \ldots, x_{2m}) + h(x_{2m+1}, x_{2m+2}, \ldots, x_{2n}), 1 \leq m \leq n-1.$$

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 n. By Remark 4.9 g is bent, and by Theorem 4.5 g has degree at most m (unless $m = 1$, in which case g has degree 2). Since g has degree n which is greater than m, we must have $m = 1$ and $n = 2$. qed.

5. FAMILIES OF BENT FUNCTIONS.

The simplest bent function of all is the function

$$f(x, y) = xy$$

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

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

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 the rows and columns) known Hadamard circulix, and it has been conjectured that no larger one exists. The conjecture has been verified [1] for matrices of order less than 12,100. This trivial bent function in two variables yields via Remark 4.9 the simplest general family of bent functions; this result was discovered independently by P. Kesava Menon [23] and R. J. Turyn [26] around 1960.

FAMILY I. *$f(x, y) = x_1y_1 + x_2y_2 + \ldots + x_ny_n$ is a bent function on V_{2n}, $n \geq 1$.*

Indeed, as both Kesava Menon and Turyn have observed, the matrix $[f^*]$ corresponding to a function of FAMILY I may be interpreted as the incidence matrix of a Hadamard difference set in any group of order 4^n which is the direct sum of n groups of order 4 (each of which must be either cyclic or the Klein 4-group). The function in FAMILY I is usually called the "dot product" and is written as

$$f(x, y) = x \cdot y.$$

The $2^n \times 2^n$ (± 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_n. By the Box Theorem (Theorem 3.4), the Fourier transform $\hat{f}$ of f is given by

$$\begin{aligned} 2^n \hat{f}^{\square} &= H_n f^{*\square} H_n^{-1} \\ &= H_n. \end{aligned}$$

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

Remark 5.1: The "dot product" bent function of FAMILY I *is its own "Fourier transform."*

In an earlier paper [22] submitted for publication in 1958 P. Kesava Menon established

Remark 5.2: 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_{2n}.*

Let $S_2(x) = \sum_{1 \le i < j \le 2n} x_i x_j$ denote the elementary symmetric function of degree 2 on V_{2n} and let $|v|$ denote the density of a vector v. Then for all v in V_{2n}, $S_2(v)$ is congruent (mod 2) to the binomial coefficient $\binom{|v|}{2}$, which is odd if and only if $|v| \equiv 2$ or 3 (mod 4). Thus, $S_2(x)$ is precisely the characteristic function of Menon's set D and Remark 5.2 is seen to be equivalent to

Remark 5.3: The elementary symmetric function of degree 2 is a bent function on V_{2n}.

The truth of both remarks is implied by the following more general

Remark 5.4: Let T be the linear transformation of the m Boolean variables $x_1, x_2, \ldots, x_m$ 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 $x_1, x_2, \ldots, x_m$ is transformed via

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

into

$$\begin{cases} G(x) = x_1x_2 + x_3x_4 + \ldots + x_{2t-1}x_{2t} & \text{if } m = 2t \equiv 0, 2 \bmod 8 \text{ or } m = 2t+1 \equiv 1, 5 \bmod 8 \\ G(x) + 1 & \text{if } m = 2t \equiv 4, 6 \bmod 8 \\ G(x) + x_{2t+1} & \text{if } m = 2t+1 \equiv 3 \bmod 8 \\ G(x) + x_{2t+1} + 1 & \text{if } m = 2t+1 \equiv 7 \bmod 8. \end{cases}$$

The proof of Remark 5.4 is straightforward and is omitted. We thus have the

Corollary: Kesava Menon's difference sets (bent functions) given in FAMILY I *and Remark 5.2 are equivalent.*

Indeed, P. J. Chase [6] has observed

Remark 5.5: Every quadratic bent function is equivalent (up to complementation) to the "dot product" bent function of FAMILY I. *Thus, the "dot product" is the "only" quadratic bent function on V_{2n}.*

Proof: A classical result of Dickson [3] states that every quadratic polynomial in m Boolean variables $x_1, x_2, \ldots, x_m$ is affinely equivalent to a polynomial of the form

$$x_1x_2 + x_3x_4 + \ldots + x_{2k-1}x_{2k} + ax_{2k+1} + b$$

where $1 \le k \le m/2$ and $a, b \in GF(2)$. But it is clear that such a polynomial defines a bent function on V_m if and only if $m = 2k$ (in which case $a = 0$). qed.

In his 1966 paper Rothaus generalized the quadratic bent function to

FAMILY II. *$f(x, y) = x \cdot y + g(x)$, g arbitrary, is a bent function on V_{2n}, $n \ge 1$.*

Proof: In this case

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

where $\Delta = \operatorname{diag}(g^*(0), g^*(1), \ldots, g^*(2^n - 1))$. Thus, by the Box Theorem 3.4

$$\begin{aligned} 2^n \hat{f}^{\square} &= H_n f^{*\square} H_n^{-1} \\ &= H_n \Delta. \end{aligned}$$

Since this matrix has entries ± 1, the assertion follows. qed. (b) (3)-P.L. 86-36

Corollary: The "Fourier transform" of

$$f(x, y) = x \cdot y + g(x)$$

is

$$f(x, y) = x \cdot y + g(y).$$

Since the $g(x)$ of FAMILY II is an arbitrary polynomial in the n variables $x_1, x_2, \ldots, x_n$, we have the

Remark 5.6: There exist bent functions on V_{2n} of every degree d, $2 \leq d \leq n$.

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

Remark 5.7: The functions

$$\begin{aligned} f_2(x, y) &= x \cdot y \\ f_3(x, y) &= x \cdot y + x_1 x_2 x_3 \\ f_4(x, y) &= x \cdot y + x_1 x_2 x_3 x_4 \\ &\vdots \\ f_n(x, y) &= x \cdot y + x_1 x_2 x_3 x_4 \ldots x_n \end{aligned}$$

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

The next family, a natural generalization of Rothaus' FAMILY II, was discovered by J. A. Maiorana [15] in 1969.

FAMILY III. *$f(x, y) = \Pi(x) \cdot y + g(x)$, g arbitrary and Π an arbitrary permutation of V_n, is a bent function on V_{2n}.*

Proof: Let P be the $2^n \times 2^n$ permutation matrix such that $P(x, \Pi(x)) = 1$ for all $x \in V_n$ and let Δ be the diagonal matrix diag $(g^*(0), g^*(1), \ldots, g^*(2^n - 1))$. Then $f^{*\square} = \Delta P H_n$ so that, by the Box Theorem 3.4, f has Fourier transform

$$\begin{aligned} 2^n \hat{f}^{\square} &= H_n f^{*\square} H_n^{-1} \\ &= H_n \Delta P. \end{aligned}$$

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

The usual proof of this result consists of showing that the derivatives of such a function are balanced. The beautiful proof presented here which graphically illustrates the constant magnitude of the Fourier coefficients is due to [redacted] private communication).

Corollary: The "Fourier transform" of

$$f(x, y) = \Pi(x) \cdot y + g(x)$$

is

$$f(x, y) = x \cdot \Pi^{-1}(y) + g(\Pi^{-1}(y)).$$

We note here the useful characterization of permutations also given by Maiorana.

Remark 5.8: 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 every nonzero linear combination of the P_i's is a balanced function 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 bias of the function $e_1 P_1(x) + e_2 P_2(x) + \ldots + e_m P_m(x)$ on V_m may be written as

$$B_\Pi(e) = \sum_{v \in V_m} G_\Pi(v) (-1)^{e \cdot v}$$

from which we see that the function B_Π is the (unnormalized) Hadamard transform of G_Π.

Thus, Π is a permutation $\Leftrightarrow$ G_Π is the constant 1 function
$\Leftrightarrow$ B_Π is the function $2^m \delta_{0,x}$
$\Leftrightarrow$ $\Sigma e_i P_i(x)$ is balanced for all $e \neq 0$. qed.

Note that if $\Pi: x \to (P_1(x), P_2(x), \ldots, P_m(x))$ is a permutation, then for each unit vector $e_i = (\delta_{1,i}, \delta_{2,i}, \ldots, \delta_{m,i})$ we have

$$(P_1(e_i), P_2(e_i), \ldots, P_m(e_i)) = \Pi(e_i) \neq \Pi(0) = (P_1(0), P_2(0), \ldots, P_m(0)),$$

(b) (3)-P.L. 86-36

which implies that $P_j(e_i) \neq P_j(0)$ for some j. We thus have the useful

Remark 5.9: If $\Pi: x \to (P_1(x), P_2(x), \ldots, P_m(x))$ is a permutation of V_m, then each variable x_i appears linearly in some $P_j(x)$.

At the end of his otherwise fine paper [15] Maiorana combined his results with characterization of bent functions (our Theorem 4.3) and somehow arrived at the erroneous

"Corollary": $f(x_1, x_2, \ldots, x_n)$ is bent if and only if the map $T: x \to (f_{b_1}(x), f_{b_2}(x), \ldots, f_{b_n}(x))$ is a permutation of V_n, where $f_{b_i}(x)$ is the derivative $f(x + b_i) + f(x)$ and $b_1, b_2, \ldots, b_n$ is a basis for V_n.

The following is an easy consequence of Remark 5.9.

Remark 5.10: If $f(x_1, x_2, \ldots, x_m)$ has the property that

$$T: x \to (f_{e_1}(x), f_{e_2}(x), \ldots, f_{e_m}(x))$$

is a permutation of V_m where $e_1, e_2, \ldots, e_m$ is the unit basis of V_m, then each variable x_i appears in some quadratic term of $f(x_1, \ldots, x_m)$.

The bent function

$$f(x_1, x_2, x_3, y_1, y_2, y_3) = (x_1x_2 + x_1x_3 + x_2x_3)y_1 + (x_1 + x_3)y_2 + (x_1 + x_2)y_3,$$

which has no quadratic term containing y_1, then shows the falsity of Maiorana's "corollary" even for the unit basis $e_1, e_2, \ldots, e_n$. In fact, it is not difficult to prove

Remark 5.11: For any bent function $f(x_1, \ldots, x_m)$ of degree greater than 2, there exists a basis $b_1, b_2, \ldots, b_m$ of V_m such that the map

$$T: x \to (f_{b_1}(x), f_{b_2}(x), \ldots, f_{b_m}(x))$$

is not a permutation of V_m.

That the converse of Maiorana's "corollary" is also false is demonstrated by the function

$$f(x_1, x_2, x_3, x_4, x_5) = (x_1 + x_2)x_4 + (x_1 + x_3)x_5 + x_1x_2x_3$$

whose derivatives (with respect to the unit basis) have the "permutation property," but which is certainly not a bent function.

The family of difference sets corresponding to the Maiorana bent functions of FAMILY III is actually a special case of a very general construction obtained recently by R. L. McFarland [20].

Theorem: Let E be (the additive group of) a vector space of dimension $s + 1$ over the finite field $GF(q)$, let $H_1, H_2, \ldots, H_r$, $r = \dfrac{q^{s+1} - 1}{q - 1}$, 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 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 product $G = E \times K$ which contains the element (e_i, k_i). Then $D = C_1 \cup C_2 \cup \ldots \cup C_r$ 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 III.

Corollary: Let $G = Z_2^n \oplus K$ be the direct sum of the elementary Abelian 2-group Z_2^n and the arbitrary Abelian group K of order 2^n. For any subset D of G let $g_D^{\square}$ denote the $2^n \times 2^n$ (± 1)-matrix whose (x, y)th entry is -1 if (x, y) is in D. Then if the matrix $g_D^{\square}$ satisfies

$$g_D^{\square} = H_n P \Delta$$

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 is equal to the Kronecker product

$$\frac{1}{4^n} (H_n \otimes F_K)$$

where F_K is the group character table for K. By the Box Theorem 3.4 the Fourier transform of the "characteristic function" g_D is given by

$$\hat{g}_D^{\square} = \frac{1}{4^n} H_n g_D^{\square} F_K = \frac{1}{4^n} H_n (H_n P \Delta) F_K = \frac{1}{2^n} P \Delta F_K .$$

Since each entry of this matrix has absolute value $\frac{1}{2^n}$, it follows that D is a difference set in G. qed.

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

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

and let

$$H_i^* = H_i - \{0\}, 1 \leq i \leq 2^{n-1}.$$

Then $D = \cup H_i^*$ is a $(4^n, 2 \cdot 4^{n-1} - 2^{n-1}, 4^{n-1} - 2^{n-1}, 4^{n-1})$-difference set in V_{2n} and the characteristic function of D is a bent function on V_{2n}.

Proof: For each i let $\tilde{H}_i$ be the dual of H_i; i.e., the subgroup of characters of V_{2n} which induce the principal character on H_i. Then for all nonprincipal characters χ of V_{2n}

$$\chi(D) = \Sigma \chi(H_i^*) = \begin{cases} 2^{n-1}(-1) \text{ if } \chi \notin \tilde{H}_i \text{ for all } i \\ (2^{n-1} - 1)(-1) + 2^n - 1 \text{ otherwise.} \end{cases}$$

Thus, $\chi(D) = \pm 2^{n-1}$ for all nonprincipal characters χ of V_{2n}, and it follows from Remark 4.6 that D is a difference set. qed.

Corollary: The "Fourier transform" of the characteristic function of $\cup H_i$ is the characteristic function of $\cup H_i^{\perp}$, where $H_i^{\perp}$ is the annihilator of H_i (i.e., $H_i^{\perp} = \{v \in V_{2n} : v \cdot u = 0$ for all u in $H_i\}$).

While it is not clear just how the bent functions of FAMILY IV are related to those of FAMILY III, the following result shows that they are at least indecomposable.

Remark 5.12: Every bent function in FAMILY IV *has degree n.*

Proof: By applying (if necessary) a linear transformation of V_{2n} we may assume that

$$H_1 = \{(v, 0) \in V_{2n} : v \in V_n\}$$

and

$$H_2 = \{(0, v) \in V_{2n} : v \in V_n\}.$$

Then by Theorem 3.1 the characteristic function of $D = \cup H_i^*$ contains the monomials $x_1 x_2 \ldots x_n$ and $x_{n+1} x_{n+2} \ldots x_{2n}$. qed.

Consideration of the difference sets of FAMILY IV leads to some basic questions concerning the geometry of V_{2n}. We shall say that two subspaces of V_{2n} are "disjoint" (in quotes) if they intersect in the zero subspace. It is easy to see that if $D = \cup H_i^*$ is a difference set in FAMILY IV and if $H_{2^{n-1}+1}$ is an n-dimensional subspace of V_{2n} which is "disjoint" from each H_i, $1 \le i \le 2^{n-1}$, (i.e., $H_{2^{n-1}+1}$ is contained in $\overline{D} = V_{2n} - D$), then $D \cup H_{2^{n-1}+1}$ is also a difference set in V_{2n}. We thus have

FAMILY IV′. *The union of* $2^{n-1} + 1$ *pairwise "disjoint" n-dimensional subspaces of* V_{2n} *is a* $(4^n, 2 \cdot 4^{n-1} + 2^{n-1}, 4^{n-1} + 2^{n-1}, 4^{n-1})$*-difference set in* V_{2n}.

Question 1: Are the difference sets of FAMILY IV′ *simply the complements of the difference sets of* FAMILY IV?

This question is equivalent to the

Question 1′: Can every family of 2^{n-1} *pairwise "disjoint" n-dimensional subspaces of* V_{2n} *be extended to a complete family of* $2^n + 1$ *such subspaces?*

Question 2: What is the least integer $E(n)$ *for which there exists a family of* $E(n)$ *pairwise "disjoint" n-dimensional subspaces of* V_{2n} *which cannot be extended to a complete family?; cannot be extended at all?*

Benson and Dillon [2] have shown that a complete family of $2^n + 1$ "disjoint" n-dimensional subspaces of V_{2n} is equivalent to a Veblen-Wedderburn System with additive group V_n. A special case in which the V-W system is in fact a field provides the next family of bent functions.

In [6] K. D. Lerche suggested that there might exist $(4^n, 2 \cdot 4^{n-1} - 2^{n-1}, 4^{n-1} - 2^{n-1}, 4^{n-1})$-difference sets in (the additive group of) $K = GF(4^n)$ which are the union of 2^{n-1} cosets of $(K^*)^{2^n+1}$ in the multiplicative group K^*. Lerche showed via computer techniques that for $n = 3$ any 4 cosets of the group of 9th powers yield such a difference set in $GF(64)$. In [6] we showed that this result is true in general. Since $(K^*)^{2^n+1}$ is precisely the multiplicative group L^* of the unique subfield L of K having dimension n over $F = GF(2)$, each coset θL^* is the set of nonzero elements of an n-dimensional subspace θL of K. Thus, these "cyclotomic" difference sets constitute a subfamily of FAMILY IV which we single out as

FAMILY IVC. *The union of any* 2^{n-1} *cosets of* $L^* = (K^*)^{2^n+1}$ *in* K^* *is a difference set in* $K = GF(4^n)$ *with parameters* $(4^n, 2 \cdot 4^{n-1} - 2^{n-1}, 4^{n-1} - 2^{n-1}, 4^{n-1})$. *These difference sets have as multipliers all automorphisms of the form*

$$\alpha: x \to ax, \; a \in L^*.$$

Furthermore, the (additive group) isomorphism

$$(x, y) \leftrightarrow x + y\theta$$

between $L \oplus L$ and $K = L(\theta)$, which allows us to interpret K as the 2-dimensional Euclidean geometry over L, also allows us to interpret the difference sets of FAMILY IVC as

FAMILY IVC (Geometric Form): *The nonzero points lying on any* 2^{n-1} *lines through the origin constitute a* $(4^n, 2 \cdot 4^{n-1} - 2^{n-1}, 4^{n-1} - 2^{n-1}, 4^{n-1})$*-difference set in the 2-dimensional Euclidean geometry* $L \oplus L$, $L = GF(2^n)$.

Lerche also asked in [6] whether there exists a difference set in $K = GF(4^n)$ which is the union of 2^{n-1} cosets of the subgroup $(K^*)^{2^n-1}$ in K^*. Such a difference set is equivalent to a bent function

$$G: K \to F$$

given by

$$G(x) = g(x^{2^n+1}),$$

where

$g: L \to F$ satisfies

i) $g(0) = 0$, and

ii) g is balanced.

Lerche's computer search had shown that there is essentially only one such bent function for $n = 3$. In [6] we showed that any nontrivial linear function g on L yields in this way a bent function G on K. Indeed, any such bent function is equivalent to that in the following

Remark 5.13: If K has degree 2 over L which has degree n over $F = GF(2)$, the function

$$f: x \to Tr_{L/F}(x^{2^n+1})$$

is a bent function on K. This bent function, being of degree 2 (as a Boolean function), is equivalent to the "dot-product" bent function of FAMILY I.

Proof: For any nonzero θ in K the derivative $f_\theta(x)$ is given by

$$\begin{aligned} f_\theta(x) &= f(x+\theta) + f(x) = Tr_{L/F}\{(x+\theta)^{2^n+1}\} + Tr_{L/F}\{x^{2^n+1}\} \\ &= Tr_{L/F}\{\theta x^{2^n} + \theta^{2^n} x\} + Tr_{L/F}\{\theta^{2^n+1}\} = Tr_{K/F}\{\theta^{2^n} x\} + Tr_{L/F}\{\theta^{2^n+1}\} \end{aligned}$$

which, being a nonconstant affine linear function, is balanced on K. qed.

In [8] we have obtained the following characterization of this second class of "cyclotomic" bent functions.

FAMILY V. *Let $g(x)$ be a balanced function from $L = GF(2^n)$ to $F = GF(2)$ which vanishes on 0. Let G be the function on $K = GF(2^{2n})$ defined by*

$$G(z) = g(z^{2^n+1}).$$

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

$$\hat{f}(u) = \frac{1}{2^n} \sum_{x \in L} f^*(x)\, Tr^*_{L/F}(ux) \quad \text{for all } u \text{ in } L.$$

Remark 5.13 shows that FAMILY V 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 ask the

Question 3: Does FAMILY V *contain a bent function of degree greater than 2? Equivalently, do there exist nonlinear functions g and h from $L = GF(2^n)$ to $F = GF(2)$ which satisfy i) $g(0) = 0 = h(0)$; ii) $\hat{g}(0) = 0 = \hat{h}(0)$; and iii) $\hat{g}(u) = \hat{h}(u^{-1})$ for all u in L^*?*

The cardinality $2^{n-1}(2^n - 1)$ of difference sets in V_{2n} suggests that they may be obtained as the disjoint union of certain "nice" $(2^n - 1)$-subsets of V_{2n}. Indeed, FAMILY IV was obtained by taking the $(2^n - 1)$-subset to be the set of nonzero elements in an n-dimensional subspace of V_{2n}. Similarly, we may try to obtain these difference sets as the disjoint union of certain "nice" 2^{n-1}-subsets of V_{2n}. [redacted] (private communication) has given the following characterization of such difference sets for which the 2^{n-1}-subset is an $(n-1)$-dimensional affine subspace of V_{2n}.

FAMILY VI. *Let $A_1, A_2, \ldots, A_{2^n-1}$ be pairwise disjoint $(n-1)$-dimensional affine subspaces of V_{2n}. Then $D = \cup A_i$ is a $(4^n, 2\cdot 4^{n-1} - 2^{n-1}, 4^{n-1} - 2^{n-1}, 4^{n-1})$-difference set in V_{2n} if and only if for each nonzero linear functional l on V_{2n}:*

i) l annihilates an odd number $L_{i_1}, L_{i_2}, \ldots, L_{i_{2k-1}}$ of L_i's,
and ii) l is "almost balanced" on the corresponding a_i's; i.e., l vanishes on k or $k-1$ of $a_{i_1}, a_{i_2}, \ldots, a_{i_{2k-1}}$
where for each i, $1 \le i \le 2^n - 1$, A_i is the translation by a_i of the linear space L_i.

Proof: For each nonprincipal character $\chi = (-1)^l$ of V_{2n}.

$$\chi(D) \Leftrightarrow \sum_{i=1}^{2^n-1} \chi(A_i) = \sum_{i=1}^{2^n-1} \chi(a_i)\,\chi(L_i) = 2^{n-1} \sum{}' \chi(a_j),$$

the last sum being over those j for which l annihilates L_j. By Remark 4.6, D is a difference set $\Leftrightarrow \Sigma' \chi(a_j) = \pm 1$, and the assertion follows. qed.

FAMILY VI contains the Maiorana bent functions of FAMILY III. Indeed, if

$$f(x, y) = \Pi(x) \cdot y + g(x)$$

is a Maiorana bent function (with $g(\Pi^{-1}(0)) = 0$ so that card $f^{-1}[1] = 2^{n-1}(2^n - 1)$), the corresponding difference set $D = f^{-1}[1]$ is given by

$$\begin{aligned} D &= \{(u, v) \in V_n \oplus V_n : \Pi(u) \cdot v = g(u) + 1\} \\ &= \bigcup_{\Pi(u) \neq 0} \{u \oplus [H_{\Pi(u)^\perp} + b_u]\}, \end{aligned}$$

where $H_{\Pi(u)^\perp}$ is the annihilator of $\Pi(u)$ in V_n and b_u is in $H_{\Pi(u)^\perp}$ or its complement $V_n - H_{\Pi(u)^\perp}$, depending on whether $g(u) = 1$ or $g(u) = 0$. Thus, D is the union of the $2^n - 1$ disjoint $(n-1)$-dimensional affine subspaces $[0 \oplus H_{\Pi(u)^\perp}] + (u, b_u)$ of $V_{2n} = V_n \oplus V_n$ where $\Pi(u) \neq 0$. For these difference sets every nonzero linear functional $a \cdot x + b \cdot y$ annihilates either exactly one subspace $0 \oplus H_{\Pi(u)^\perp}$ (in case $b \neq 0$) or all $(2^n - 1)$ subspaces $0 \oplus H_{\Pi(u)^\perp}$ (in case $b = 0$) so that the necessary conditions on the affine subspaces are trivially satisfied. Indeed, for the FAMILY III difference sets, the $2^n - 1$ affine subspaces have the property that their corresponding linear subspaces are precisely the hyperplanes of a single n-dimensional subspace of V_{2n}.

Question 4: Does FAMILY VI contain a difference set that is not equivalent to one contained in FAMILY III?

At least one other class of bent functions has appeared in the literature. In his remarkable paper [26] of 1965 R. J. Turyn gave the following result.
Remark 5.14: Let G be the direct sum $L \oplus L$ where $L = GF(2^n)$. Then the subset

$$D = \{(m_1 + m_2, m_1 m_2) : m_1, m_2 \in L\}$$

is a $(4^n, 2\cdot 4^{n-1} + 2^{n-1}, 4^{n-1} + 2^{n-1}, 4^{n-1})$-difference set in G.

Proof: Observe that (x, y) is in D if and only if $y = mx + m^2$ for some $m \in L$; i.e.,

$$D = \bigcup_{x \in L} \{x \oplus S_x\},$$

where $S_x = \{mx + m^2 : m \in L\}$. Now $S_0 = L$ and as x ranges over L^*, S_x rages over the hyperplanes in L. Indeed, for $x \neq 0$ we have

$$\begin{aligned} S_x &= \{(mx)x + (mx)^2 ; m \in L\} \\ &= x^2 \{m + m^2 : m \in L\} \\ &= x^2 S, \end{aligned}$$

where $S = \{Z \in L: Tr(Z) = 0\}$ and Tr denotes the trace from L to $GF(2)$. Thus

$$D = (0 \oplus L) \cup \{ \bigcup_{x \in L^*} (x \oplus x^2 S) \},$$

and, applying the automorphism

$$(x, y) \to (x^2, y) \text{ of } G$$

shows that D is equivalent to

$$D' = \bigcup_{x \in L^*} (x \oplus x S) \cup (0 \oplus L). \qquad (*)$$

But this set is clearly a difference set of FAMILY III; its characteristic function is precisely

$$f(x, y) = Tr\{\Pi(x)\, y\} + 1,$$

where $\Pi: L \to L$ is the permutation which fixes 0 and maps each nonzero element onto its multiplicative inverse. Furthermore, the (additive group) isomorphism

$$(x, y) \leftrightarrow x + y\theta, \ \theta \text{ fixed of order } 2^n + 1,$$

between $L \oplus L$ and $L(\theta) = GF(2^{2n})$ allows us to interpret the difference set D' in $L \oplus L$ as the set $D'' = \theta L \bigcup_{a \in S} (1 + a\theta)L^*$ in $K = GF(2^{2n})$. The complement of D'' is $D''' = \bigcup (b^{-1} + \theta)L^*$, this union being over all b in L such that $T_{L/F}\{b\} = 1$. Thus, D''' is a cyclotomic difference set of FAMILY IVC. In fact, it may be shown [8] that D''' is given by

$$D''' = \bigcup_{t=1}^{2^{n-1}} (\theta^t + \theta^{-t} + \theta)\, L^*.$$

Alternatively we may observe directly from (*) that D' is the union of $2^{n-1} + 1$ lines through the origin in the 2-dimensional Euclidean geometry $L \oplus L$. It follows from the definition of S that the complement of D' is precisely the set of nonzero points of $L \oplus L$ which lie on a line through the origin whose "slope" has trace 1 with respect to the field extension L/F. Thus, Turyn's "2nd bent function" is contained in FAMILY III and FAMILY IV. qed.

The final "family" we present here, sometimes called "Rothaus' 2nd class," is actually a characterization of bent functions having a certain restricted polynomial form. In his beautiful paper [24] of 1966 Rothaus included the

FAMILY VII(R). *If $A(x)$, $B(x)$, $C(x)$, and $A(x) + B(x) + C(x)$ are all bent functions on V_{2n}, 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_{2n+2}.

At the end of his paper [24] Rothaus stated without proof the

Remark 5.15: The bent function given in FAMILY VII(R) *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 VII(R) and Remark 5.15.

FAMILY VII. *$f(x, y, z) = R(x) + S(x)y + T(x)z + yz$ is bent on V_{2n+2} if and only if $R(x) + S(x)T(x)$, $R(x) + S(x)\overline{T}(x)$, $R(x) + \overline{S}(x)T(x)$, and $R(x) + \overline{S}(x)\overline{T}(x)$* are all bent on V_{2n}.

Proof: We regard V_{2n+2} as the direct sum $V_{2n} \oplus V_2$ and use the "Box Theorem" (Theorem 3.4) of Section 3. Letting $f^{*\square}$ (respectively $\hat{f}^{\square}$) denote the $2^{2n} \times 4$ matrix whose rows and columns are

indexed by the lexicographically ordered vectors in V_{2^n} and V_{2^r} and whose (u, v)th entry is $f^*(u, v)$ (respectively $\hat{f}(u, v)$), we may write

$$\hat{f}^{\square} = H_{2^n}^{-1} f^{*\square} H_{2^r}^{-1}. \qquad (*)$$

The columns of $f^{*\square}$ correspond to the functions

$$f_{00}(x) = f(x, 0, 0) = R(x)$$
$$f_{01}(x) = f(x, 0, 1) = R(x) + T(x)$$
$$f_{10}(x) = f(x, 1, 0) = R(x) + S(x)$$

and

$$f_{11}(x) = f(x, 1, 1) = R(x) + S(x) + T(x) + 1,$$

so that the columns of $H_{2^n}^{-1} f^{*\square}$ are simply the Fourier transforms of the columns of $f^{*\square}$; i.e.,

$$H_{2^n}^{-1} f^{*\square} = [\hat{f}_{00}(x), \hat{f}_{01}(x), \hat{f}_{10}(x), \hat{f}_{11}(x)].$$

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 (e.g., [5]) that if $S_2(x_1, x_2\ x_3)$ denotes $x_1x_2 + x_1x_3 + x_2x_3$ and A, B, C are arbitrary Boolean functions on V_m, then the composite function $S_2(A, B, C)$ has Fourier transform

$$\widehat{S_2(A, B, C)} = \tfrac{1}{2}\{\hat{A} + \hat{B} + \hat{C} - (\widehat{A + B + C})\}.$$

Thus, we have

$$\hat{f}^{\square} = \tfrac{1}{2}[\widehat{S_2(f_{00}, f_{01}, f_{10})}, \widehat{S_2(f_{00}, \overline{f}_{01}, f_{10})}, \widehat{S_2(f_{00}, f_{01}, \overline{f}_{10})}, -\widehat{S_2(f_{00}, f_{01}, f_{10})}]$$

which may be written in terms of R, S, and T as

$$\hat{f}^{\square} = \tfrac{1}{2}[\widehat{R + ST}, \widehat{R + S\overline{T}}, \widehat{R + \overline{S}T}, \widehat{R + \overline{ST}}].$$

The assertion of the theorem is now obvious. qed.

Our proof actually has shown the

Corollary: If $f(x, y, z)$ is bent on $V_{2^{n+2}}$ and $f_{00}(x), f_{01}(x), f_{10}(x), f_{11}(x)$ are the restrictions of f to the affine subspaces $(y, z) = (0, 0), (0, 1), (1, 0)$ and $(1, 1)$, then for each v in V_{2^n} we have (up to permutation of coordinates)

$$2^n(\hat{f}_{00}(v), \hat{f}_{01}(v), \hat{f}_{10}(v), \hat{f}_{11}(v)) = \begin{cases} \pm(-1, 1, 1, 1) \\ \text{or} \\ \pm(2, 0, 0, 0) \end{cases}.$$

Proof: Let $f(x, y, z)$ be the Boolean function defined by the Fourier transform of $f(x, y, z)$; i.e.,

$$\hat{f}(x, y, z) = \frac{1}{2^{n+1}} f^*(x, y, z).$$

Then the fundamental equation (*) may be rewritten as

$$2^{n-1} H_{2^n}^{-1} f^{*\square} = f^{*\square} H_{2^r}^{-1}$$

which is the same as

$$2^{n-1}(\hat{f}_{00}(x), \hat{f}_{01}(x), \hat{f}_{10}(x), \hat{f}_{11}(x)) = f^{*\square} H_{2^r}^{-1}.$$

Since each row of the matrix on the right is the Fourier transform of a Boolean function on V_2 (whose spectrum must be one of $\pm\{1, 0, 0, 0\}$ or $\pm\{-\tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}\}$, depending on whether the function has an even number or an odd number of zeros), the assertion follows. qed.

We incorporate several immediate corollaries in the

Remark 5.16: Let $f(x, y, z) = f_{00}(x)\overline{y}\overline{z} + f_{01}(x)\overline{y}z + f_{10}(x)y\overline{z} + f_{11}(x)yz$ be bent on $V_{2^{n+2}}$. Then the functions $f_{yz}(x)$ on V_{2^n} must satisfy the following:

a) *Each f_{yz} has its Fourier coefficients in the set* $\left\{0, \pm\frac{1}{2^n}, \pm\frac{1}{2^{n-1}}\right\}$.

b) *If any one of the f_{ys}'s is bent they are all bent and*

$$f_{11}(x) = f_{00}(x) + f_{01}(x) + f_{10}(x) + 1,$$

where $f_{ys}(x)$ denotes the "Fourier transform" of $f_{ys}(x)$.

c) *If the linear function $a \cdot x$ is uncorrelated with one $f_{ys}(x)$, it is uncorrelated with exactly three of the $f_{ys}(x)$.*

We now observe a curious property of Boolean functions.

Remark 5.17: Let a, b, c be arbitrary Boolean functions on V_m. Then there exist unique functions A, B, C such that

$$\begin{aligned} a &= \overline{A}B + \overline{A}C + BC \\ b &= A\overline{B} + AC + \overline{B}C \\ c &= AB + A\overline{C} + B\overline{C}. \end{aligned}$$

Indeed, the functions A, B, C are given by

$$\begin{aligned} &A + \overline{a}b + \overline{a}c + \overline{b}c \\ &B + a\overline{b} + ac + \overline{b}c \\ &C + ab + a\overline{c} + b\overline{c}. \end{aligned}$$

Proof. Taking Fourier transforms, we need

$$\begin{bmatrix} \hat{a} \\ \hat{b} \\ \hat{c} \\ \overbrace{a+b+c} \end{bmatrix} = H \begin{bmatrix} \hat{A} \\ \hat{B} \\ \hat{C} \\ \overbrace{A+B+C} \end{bmatrix},$$

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 this is equivalent to

$$\begin{bmatrix} \hat{A} \\ \hat{B} \\ \hat{C} \\ \overbrace{A+B+C} \end{bmatrix} = H \begin{bmatrix} \hat{a} \\ \hat{b} \\ \hat{c} \\ \overbrace{a+b+c} \end{bmatrix}. \quad \textit{qed.}$$

We may use this result to establish Rothaus' Remark 5.15. According to FAMILY VII 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

$$\begin{aligned} A &= f_{00}f_{01} + f_{00}f_{10} + f_{01}f_{10}, \\ B &= f_{00}\overline{f}_{01} + f_{00}f_{10} + \overline{f}_{01}f_{10}, \\ C &= f_{00}f_{01} + f_{00}\overline{f}_{10} + f_{01}\overline{f}_{10}, \end{aligned}$$

and

$$A+B+C = \overline{f}_{00}f_{01} + \overline{f}_{00}f_{10} + f_{01}f_{10},$$

are all bent, where

$$\begin{aligned} f_{00} &= R \\ f_{01} &= R + T \\ f_{10} &= R + S. \end{aligned}$$

and

But by Remark 5.17 we have

$$\begin{aligned} f_{00} &= AB + AC + BC \\ f_{01} &= A\overline{B} + AC + \overline{B}C = f_{00} + A + C \\ f_{10} &= AB + A\overline{C} + B\overline{C} = f_{00} + A + B \end{aligned}$$

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 $f(x, y, z) = R(x) + S(x)y + T(x)z + yz$ is given by $f(x, y, z) = A(x)B(x) + A(x)C(x) + B(x)C(x) + (A(x) + B(x))y + (A(x) + C(x))z + yz$ where $A(x)$, $B(x)$, $C(x)$, and $A(x) + B(x) + C(x)$ are all bent. qed.

Note that if A, B, C and $A+B+C$ are all bent on V_{2n} we have immediately that

$$[g^*] = 2^n(\hat{A}, \hat{B}, \hat{C}, \overbrace{(A + B + C + 1)})$$

represents a bent function on V_{2n+2}. Indeed, transforming the columns of $[g^*]$ yields $(A^*, B^*, C^*, (A+B+C+1)^*)$ every row of which represents a bent function on V_2. Of course, this bent function is precisely the "Fourier transform" of the bent function of Rothaus' "2nd Class." We thus have

FAMILY VII'. *If A, B, C, and $A+B+C$ are bent on V_{2n}, then*

$$g(x, y, z) = a(x)\overline{y}\,\overline{z} + b(x)\overline{y}\,z + c(x)y\,\overline{z} + d(x)y\,z$$

is bent on V_{2n+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 VII).

Question 5: For which FAMILY VII *bent functions is the "Fourier transform" also in* FAMILY VII?

We have shown above that Rothaus' FAMILY VII is precisely the class of bent functions of the form

$$f(x, y, z) = R(x) + S(x)y + T(x)z + yz.$$

Thus, a bent function in $2n$ variables is in FAMILY VII if and only if it has two variables which occur together only in a quadratic term. Clearly any quadratic bent function is of this type. We now establish the

Remark 5.18: Every cubic bent function is equivalent to a bent function in FAMILY VII.

Proof: If $f(x)$ is a cubic bent function in $2n$ variables $x_1, x_2, \ldots, x_{2n}$ we may assume (by permuting variables if necessary) that $f(x)$ is of the form

$$f(x) = g(x)\,x_{2n} + h(x),$$

where $g(x)$ and $h(x)$ are independent of x_{2n} and $g(x)$ has degree two. Since $g(x)$, being a derivative of $f(x)$, is balanced, we may apply an affine linear transformation of the variables $x_1, x_2, \ldots, x_{2n-1}$ so that g(x) takes the form

$$x_1x_2 + x_3x_4 + \ldots + x_{2r-1}x_{2r} + x_{2r+1} + c$$

(this follows from Dickson's Theorem; see proof of Remark 5.5). Then variables x_{2r+1} and x_{2n} appear together in $f(x)$ only in a quadratic term. qed.

The same proof establishes the more general

Remark 5.19: The bent function $f(x)$ is equivalent to a bent function in FAMILY VII *if some variable x_i appears in no term of degree greater than three.*

A similar result is the

Remark 5.20: The Maiorana (FAMILY III) *bent function*

$$f(x, y) = p_1(x)y_1 + p_2(x)y_2 + \ldots + p_n(x)y_n + g(x)$$

is equivalent to a FAMILY VII *bent function if some* $\Sigma\, e_i p_i(x)$, $e \neq 0$, *has degree less than three.*

Corollary: Rothaus' FAMILY II *is contained in Rothaus'* FAMILY VII.

We shall show in the next section that every bent function in fewer than eight variables is equivalent to a Maiorana bent function of FAMILY III. Thus, each of our Remarks 5.18, 5.19, and 5.20 implies that every bent function in fewer than eight variables is also equivalent to a Rothaus bent function of FAMILY VII; however, not every Maiorana bent function need satisfy the condition of Remark 5.20. Indeed, the eight-dimensional Maiorana bent function

$$f(x, y) = (x_1x_2x_4 + x_3x_4 + x_1)y_1 + (x_1x_2x_3 + x_1x_4 + x_2)y_2 + (x_2x_3x_4 + x_1x_2 + x_3)y_3 + (x_1x_3x_4 + x_2x_3 + x_4)y_4$$

has the property that no $\Sigma\, e_i p_i(x)$ is equivalent to a function having an independent linear term.

Question 6: Is every bent function equivalent to one in FAMILY VII?

Question 7: Must every bent function contain a quadratic term?

6. BENT FUNCTIONS OF DIMENSION LESS THAT EIGHT.

The bent function in two variables and the bent function in four variables are both unique up to affine equivalence and complementation of functions. We may take the bent function in two variables x and y to be $f(x, y) = xy$, which is the characteristic function of a "trivial" (4, 1, 0, 1)-difference set in V_2. We showed directly in Remark 2.9 that the (16, 6, 2, 4)-difference set in V_4 was unique; the bent function corresponding to the difference set produced there is the (complement of the) elementary symmetric function of degree two in four variables, i.e.,

$$f(x_1, x_2, x_3, x_4,) = 1 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4.$$

A simpler representative of the bent functions in four variables is the "dot product" $f(x_1, x_2, y_1, y_2) = x_1y_1 + x_2y_2$. Of course, as P.J. Chase has pointed out (Remark 5.5), there is always a unique (up to affine equivalence and complementation) quadratic bent function in $2n$ variables.

For functions in six variables the problem of determining the distinct (up to equivalence and complementation) bent functions is considerably more complicated. In his 1966 paper [24] O.S. Rothaus presented three cubic "bent" functions in six variables and stated without proof [Note: the result had been verified by a computer program written by [redacted]] that any cubic bent function could be obtained from one of these by an affine transformation of coordinates followed by the addition of linear terms. Rothaus' representative cubics, found on page 8 of [24], were

1) $x_1x_2x_3 + x_1x_4 + x_2x_5 + x_3x_6$
3) $x_1x_2x_3 + x_2x_4x_5 + x_1x_2 + x_1x_4 + x_2x_6 + x_3x_5$
4) $x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_1x_4 + x_2x_6 + x_3x_4 + x_3x_5 + x_3x_6 + x_4x_5 + x_4x_6.$

We note here that the second cubic given above is *not a bent function*. (To see this, use the theorem of FAMILY VII with $y = x_3$ and $z = x_5$.) Addition of the term x_4x_5, however, does render it bent; so it seems likely that this term was inadvertently dropped. Only this year by a veritable tour de force [redacted] demonstrated that every cubic bent function in six

variables is equivalent (via affine transformation of coordinates and complementation of functions) to (exactly) one of

K1. $x_1x_2x_3 + x_1x_4 + x_2x_5 + x_3x_6$,
K2. $x_1x_2x_3 + x_1x_4x_5 + x_1x_6 + x_2x_4 + x_2x_5 + x_3x_5 + x_4x_5$,
K3. $x_1x_2x_3 + x_1x_4x_5 + x_3x_4x_6 + x_1x_6 + x_2x_4 + x_3x_5 + x_3x_6 + x_4x_5 + x_4x_6$.

Thus, there are essentially only four bent functions in six variables—one quadratic and three cubics.

It is a remarkable stroke of good fortune that [redacted] representative cubics K1, K2 and K3 turn out to be Maiorana bent functions (FAMILY III). This fact permits a simple proof of the

(b) (3)-P.L. 86-36

Theorem: Every six-dimensional bent function is equivalent to a Maiorana bent function.

Proof: We already know that every quadratic bent function is equivalent to the "dot product" which is in FAMILIES I, II, and III. According to [redacted] result, every cubic six-dimensional bent function is equivalent (up to complementation) to one of K1, K2 or K3.

Class K1 is the classical Rothaus-Maiorana cubic which is in FAMILIES II and III. Class K2 has no term containing two of x_3, x_4, and x_6; so it may be written as

$$(x_1x_2 + x_6)x_3 + (x_1x_5 + x_2 + x_5)x_4 + (x_1)x_6 + (x_2x_5),$$

which is in FAMILY III. Note: The variable permutation $x_2 \to x_3 \to x_5 \to x_2$ transforms this function into

$$(x_1x_2 + x_2 + x_3)x_4 + (x_1x_3 + x_3)x_5 + (x_1)x_6 + (x_2x_3).$$

Class K3 has no term containing two of x_2, x_5, and x_6; so it may be written as

$$(x_1x_3 + x_4)x_2 + (x_1x_4 + x_3 + x_4)x_5 + (x_3x_4 + x_1 + x_3 + x_4)x_6,$$

which is in FAMILY III. Note: The permutation $x_2 \to x_4 \to x_3 \to x_2$ transforms this function into

$$(x_1x_2 + x_3)x_4 + (x_1x_3 + x_2 + x_3)x_5 + (x_2x_3 + x_1 + x_2 + x_3)x_6).$$ qed.

Corollary: Every bent function in fewer than eight variables is equivalent to a Maiorana bent function.

We note that [redacted] representatives K1, K2, and K3 are also in Rothaus' FAMILY VII; i.e., they each contain a quadratic term whose factors appear together in no other term (e.g., for K1 take x_3x_6, for K2 and K3 take x_3x_5). In fact, Rothaus states [24] that his FAMILY VII was suggested by the fact that his representative six-dimensional bent functions were of this type. Indeed, it was in the attempt to fit Rothaus' examples to his Theorem (FAMILY VII) that the error in Rothaus' listing was discovered.

REFERENCES

[1] Leonard D. Baumert, "Cyclic Difference Sets," *Lecture Notes in Mathematics # 182* (Springer-Verlag, New York, 1971).

[2] [redacted] J. F. Dillon, "Geometric Bent Functions," *R41 Technical Paper*, to appear.

[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] [redacted] "Composition of Boolean Functions," *R41 Technical Paper* (September 1970).

[6] [redacted] J. F. Dillon, and K. D. Lerche, "Bent Functions and Difference Sets," *R41 Technical Paper* (April 1971).

[7] J. F. Dillon, "Mobius Inversion and Boolean Functions," *S12 Informal Note # 219* (April 1968).

[8] ———, "Singer Difference Sets and Bent Functions," *R41 Technical Paper* (August 1972).

[9] [redacted] "A Slow Look at Fast Transforms," in this special issue of the *NSA TJ*.

[10] [redacted] "Some Symptoms of Boolean Functions," *R41 Technical Paper* (January 1970).

[11] Marshall Hall, Jr., *Combinatorial Theory* (Ginn-Blaisdell, Waltham, 1967).

[12a] [redacted] "Six-Dimensional Bent Functions," *R41 Technical Paper* (March 1971).

[12b] [redacted] Errata to "Six-Dimensional Bent Functions" (August 1971).

[13] R. J. Lechner, "Harmonic Analysis of Switching Functions," in *Recent Developments in Switching Theory*, edited by Amar Mukhopadhyay (Academic Press, New York, 1971).

[14] [redacted] "Freshman Calculus over GF(2)," *SCAMP W.P. # 13/68.*

[15] J. A. Maiorana, "A Class of Bent Functions," *R41 Technical Paper*, (August 1970).

[16] H. B. Mann, *Addition Theorems* (Interscience, New York, 1965).

[17] ———, and R. L. McFarland, "On Multipliers of Difference Sets," *Canadian Journal of Math.*, 17 (1965), 541–542.

[18] R. L. McFarland, "A Discrete Fourier Theory for Binary Functions," *R41 Technical Paper* (June 1971).

[19] ———, *On Multipliers of Abelian Difference Sets*, (Ohio State University Thesis, 1970).

[20] ———, "A Family of Noncyclic Difference Sets," Submitted to *Journal of Combinatorial Theory*.

[21] ———, "The Multipliers of the Difference Set in the Elementary Abelian Group of Order 16," unpublished (August 1971).

[22] P. Kesava Menon, "Difference Sets in Abelian Groups," *Proceedings of the A.M.S.*, 11 (1960), 368–377.

[23] ———, "On Difference Sets whose Parameters Satisfy a Certain Relation," *Proceedings of the A.M.S.*, 13 (1962), 739–745.

[24] O. S. Rothaus, "On Bent Functions," *IDA-CRD W.P. # 169* (1966).

[25] M. P. Schutzenberger, "A Non-Existence Theorem for an Infinite Family of Symmetrical Block Designs," *Annals of Eugenics*, 14 (1949), 286–287.

[26] R. J. Turyn, "Character Sums and Difference Sets," *Pacific Journal of Math.*, 15 (1965), 319–346.