Normal and Non Normal Bent Functions

Anne Canteaut[1], Magnus Daum[2], Hans Dobbertin[2], Gregor Leander[2]

[1]INRIA-Projet CODES, BP 105, 78153 Le Chesnay Cedex, France
anne.canteaut@inria.fr

[2]Ruhr-Universität Bochum, Postfach 102148, 44780 Bochum, Germany
{daum,dobbertin,leander}@itsc.rub.de

Abstract

The question if there exist non normal bent functions was an open question for several years, as for most of the standard constructions for bent functions it is obvious that they are normal. In this paper we give the first non normal bent function and even an example for a non weakly-normal bent function. These examples belong to a class of bent functions found in [8], namely the Kasami functions. The non-normality of these functions was verified by using a computer algorithm. We furthermore give a construction which extends these examples to higher dimensions. With this extension we have an infinite set of non normal and non weakly-normal bent functions. In the third section we prove the normality of some bent functions derived by modifications of the Maiorana-McFarland type.

Keywords: Boolean function, bent function, normal function

1 Introduction

The main *complexity characteristics* for Boolean functions on $\mathbb{F}_2^n$ which are relevant to cryptography are the algebraic degree and the nonlinearity. But other criteria have also been studied. One of them is the question if there exists a space of dimension $\frac{n}{2}$ such that the restriction of a given function is constant (resp. affine) on this space. We call the functions for which such a space exists normal (resp. weakly-normal). The notion of normality has been introduced for the first time by Hans Dobbertin in [9]. He used this notion to construct balanced functions with high nonlinearities: it is shown in [3] that if a bent function f is constant on an $\frac{n}{2}$-dimensional flat E, then f is balanced on each of the other cosets of the flat. H. Dobbertin used this idea to construct balanced functions with high nonlinearities. Since that time the question if there exist non normal bent functions was open. For arbitrary Boolean functions, it was shown in [9], that for increasing dimension nearly all functions are non normal. Furthermore, there exist Boolean functions on $\mathbb{F}_2^n$ whose restrictions to any k-dimensional flat are non-affine if $k \geq \alpha \log_2(n)$ with $\alpha > 1$ [4].

Let $n = 2m$ be an even number. We recall some definitions:

Definition 1 *Given a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, the function*

$$a \in \mathbb{F}_2^n \mapsto f^w(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\langle a,x \rangle}$$

is called the Walsh transform of f. Moreover, the $f^w(a), a \in \mathbb{F}_2^n$ are called the Walsh coefficients of f.

Definition 2 *A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called* bent *if for all $a \in \mathbb{F}_2^n$ with $a \neq 0$*

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+a)} = 0.$$

This property is equivalent to the fact that all the Walsh-Coefficients are $\pm 2^m$.

Definition 3 *The dual function $\tilde{f}$ of a bent function f is defined by the property*

$$f^w(a) = (-1)^{\tilde{f}(a)} 2^m.$$

The dual of a bent function is also bent.

Definition 4 *A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called* normal *if there exists a flat of dimension m such that f is constant on this flat.*

As bentness is invariant under addition of affine functions it is natural to consider a generalization of Definition 4.

Definition 5 *A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called* weakly-normal *if there exists a flat of dimension m such that the restriction of f to this flat is affine.*

A function f is weakly-normal if and only if there exists an element $a \in \mathbb{F}_2^n$ such that $f(x) + \langle a, x \rangle$ is normal.

The Hamming Weight of a bent function f is $\sum_{x \in \mathbb{F}_2^n} f(x) = 2^{n-1} - (-1)^{\tilde{f}(0)} 2^{m-1}$. It is known that if a bent function is normal with respect to a flat U then it is balanced on all cosets of U. This implies that, if f is constant on a flat of dimension m, the value of the corresponding constant is $\tilde{f}(0)$.

An easy counting argument shows that there must exist non normal functions of n variables for $n \geq 10$, but the question if there exist non normal bent functions was an open problem for several years. In Section 2 we present the first non normal bent function and even a non weakly-normal bent function. In Section 3 we prove the normality of some modified Maiorana-McFarland bent functions.

2 Non Normal Bent Functions

The functions that turned out to be non normal are Kasami functions. This class of bent functions was found by Dobbertin and Dillon in [8] and some of the functions in this class seemed to be good candidates for non normal bent functions.

The Kasami functions are defined as follows:

Definition 6 *Let $d = 2^{2k} - 2^k + 1$ with $(k, n) = 1$ and $\alpha \in \mathbb{F}_{2^n}$. Then we call*

$$f_{\alpha,k} : \mathbb{F}_{2^n} \to \mathbb{F}_2$$

with

$$f_{\alpha,k}(x) = \mathrm{Tr}(\alpha x^d)$$

a Kasami function.

Under some conditions these functions are bent.

Theorem 7 *Let k and $f_{\alpha,k}$ be as in Definition 6.*
If n is not divisible by 3 and $\alpha \notin \{x^3 | x \in \mathbb{F}_{2^n}\}$ then $f_{\alpha,k}$ is bent

Proof. The proof can be found in [8]. □

For some values of n it is possible to show, that the Kasami functions are always normal.

Lemma 8 *Let $n = 2m$ with m even. The Kasami power functions*

$$\begin{array}{rccc} f: & \mathbb{F}_{2^n} & \rightarrow & \mathbb{F}_2 \\ & x & \mapsto & \mathrm{Tr}(\alpha x^d) \end{array}$$

are normal.

Proof. First note that $\gcd(d, 2^n - 1) = 3$, i.e.

$$U = \{x^d \mid x \in \mathbb{F}_{2^n}^*\} = \{x^3 \mid x \in \mathbb{F}_{2^n}^*\}$$

and there exist $\lambda_1, \lambda_2 \notin U$ such that

$$\mathbb{F}_{2^n}^* = U \cup \lambda_1 U \cup \lambda_2 U.$$

In the case where $4|n$ we will show, that λ_1, λ_2 can be chosen in $\mathbb{F}_{2^m}$. It is sufficient to show that there exists $x \in \mathbb{F}_{2^m}$ such that $x \notin U$. Let g be a generator of $\mathbb{F}_{2^m}$. g is in U if and only if $g^{\frac{2^n-1}{3}} = 1$. But,

$$\begin{aligned} g^{\frac{2^n-1}{3}} &= g^{\frac{(2^m-1)(2^m+1)}{3}} \\ &= g^{(2^m+1)\frac{2^m-1}{3}} \neq 1 \end{aligned}$$

as $2^m + 1$ is not divisible by 3 if m is even. So we can choose $\lambda_1 = g$ and $\lambda_2 = g^2$. Note that if $\alpha' = \alpha c^d$ for some $c \in \mathbb{F}_{2^n}^*$ then $f_{\alpha,k}(cx) = f_{\alpha',k}(x)$ for all $x \in \mathbb{F}_{2^n}$. Thus we can assume that α is in $\{1, g, g^2\} \subset \mathbb{F}_{2^m}$. So for $x \in \mathbb{F}_{2^m}$ we get

$$\begin{aligned} f_{\alpha,k} &= \mathrm{Tr}(\alpha x^d) \\ &= \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^m}}(\alpha x^d)) \\ &= \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\alpha x^d \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^m}}(1)) \\ &= 0\ . \end{aligned}$$

This proves the lemma. □

So we can only hope to get non normal Kasami functions for m odd. Furthermore, as all quadratic bent functions are normal, only the case $k \neq 1$ is interesting. As it is known that all bent functions on $\mathbb{F}_2^6$ are normal, the first possibility for a Kasami function to be non normal is $n = 10$.

We found out that for $n = 10$ all the Kasami functions are normal but by addition of a linear function they can be modified into non normal functions.

Fact 1 *Let $\alpha \in \mathbb{F}_4 \backslash \mathbb{F}_2 \subset \mathbb{F}_{2^{10}}$. Then there exists $\beta \in \mathbb{F}_{2^{10}}$ such that the function*

$$f : \mathbb{F}_{2^{10}} \rightarrow \mathbb{F}_2$$

with

$$f(x) = \mathrm{Tr}(\alpha x^{57} + \beta x)$$

is non normal.

Verification. This can be verified using the algorithm described in [6]. □

Furthermore we found that for $n = 14$ and $k = 3$ the corresponding Kasami functions are non weakly-normal.

Fact 2 *Let $\alpha \in \mathbb{F}_4 \backslash \mathbb{F}_2 \subset \mathbb{F}_{2^{14}}$. The function*

$$f : \mathbb{F}_{2^{14}} \rightarrow \mathbb{F}_2$$

with

$$f(x) = \mathrm{Tr}(\alpha x^{57})$$

is non weakly-normal.

Verification. By using the algorithm described in [6]. □

These results are verified with a computer algorithm, proving these results theoretically is still an open problem. We state the following conjecture.

Conjecture 9 *All non quadratic Kasami functions on $\mathbb{F}_{2^{2m}}$ with m not divisible by 2 and $m \geq 7$ are non weakly-normal.*

The following lemma is a generalization of Theorem 4.5 of [10].

Lemma 10 *Let $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be a Boolean function. The following properties are equivalent:*

1. *f is (weakly) normal*
2. *The function*

$$\begin{array}{rcl} g : \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2 & \rightarrow & \mathbb{F}_2 \\ (x, y, z) & \mapsto & f(x) + yz \end{array}$$

is (weakly) normal

Proof. 1.) $\Rightarrow$ 2.) : We assume that f is normal, i.e. there exists a $\frac{n}{2}$ dimensional flat E, such that $f|_E$ is constant. We define:

$$E' = (E \times \{0\} \times \{0\}) \cup (E \times \{1\} \times \{0\})$$

which is a $\frac{n+2}{2}$ dimensional flat. It is easy to see that $g|_{E'} = c$ i.e. g is normal. Furthermore if f is linear on E then g is linear on E'.

1.) $\Leftarrow$ 2.) : We now assume that g is weakly-normal, i.e there exists a $\frac{n+2}{2}$ dimensional flat E, $\gamma \in \mathbb{F}_2^n$ and $\alpha, \beta \in \mathbb{F}_2$ such that

$$h(x,y,z) = g(x,y,z) + \alpha y + \beta z + \langle \gamma, x \rangle$$

takes the same value, c, on E. We claim that $f(x) + \langle \gamma, x \rangle$ is normal.

For $a, b \in \mathbb{F}_2$ we define

$$E_{ab} = \{x \in \mathbb{F}_2^n | (x, a, b) \in E\}.$$

Then, $f(x) + \langle \gamma, x \rangle$ is constant on all flats $E_{a,b}$ since for all $x \in E_{ab}$,

$$f(x) + \langle \gamma, x \rangle = h(x, a, b) + ab + \alpha a + \beta b = c + ab + \alpha a + \beta b \ . \tag{1}$$

If one of the flats E_{ab} has dimension $\geq \frac{n}{2}$ we are done.

If this is not true, all the flats E_{ab} have dimension $\frac{n}{2} - 1$. Furthermore, since the union of all E_{ab} is a flat, all E_{ab} are cosets of the same subspace U: $E_{ab} = U + x_{ab}$. Moreover, $x_{\alpha\bar{\beta}} \neq x_{\bar{\alpha}\beta}$. Otherwise, for any element $(x, \bar{\alpha}, \beta)$ in E, $(x, \alpha, \bar{\beta})$ belongs to E. Then, if we consider two elements $(x, \bar{\alpha}, \beta)$ and (x', α, β) in E, we obtain that

$$(x, \bar{\alpha}, \beta) + (x, \alpha, \bar{\beta}) + (x', \alpha, \beta) = (x', \bar{\alpha}, \bar{\beta})$$

belongs to E. Thus, both (x', α, β) and $(x', \bar{\alpha}, \bar{\beta})$ lie in E, implying that $h(x', \alpha, \beta) = h(x', \bar{\alpha}, \bar{\beta})$. But,

$$h(x', \alpha, \beta) = f(x') + \alpha\beta + \alpha + \beta + \langle \gamma, x' \rangle$$

and

$$\begin{aligned} h(x', \bar{\alpha}, \bar{\beta}) &= f(x') + \bar{\alpha}\bar{\beta} + \alpha\bar{\alpha} + \beta\bar{\beta} + \langle \gamma, x' \rangle \\ &= f(x') + \alpha\beta + \alpha + \beta + 1 + \langle \gamma, x' \rangle \\ &= h(x', \alpha, \beta) + 1 \ , \end{aligned}$$

which leads to a contradiction. Therefore, since $x_{\alpha\bar{\beta}} \neq x_{\bar{\alpha}\beta}$, the set $E_{\alpha\bar{\beta}} \cup E_{\bar{\alpha}\beta}$ is a flat of dimension $\frac{n}{2}$. Moreover, we deduce from (1) that

$$\forall x \in E_{\alpha\bar{\beta}}, \quad f(x) + \langle \gamma, x \rangle = c + \alpha\bar{\beta} + \alpha + \beta\bar{\beta} = c + \alpha\beta$$

and

$$\forall x \in E_{\bar{\alpha}\beta}, \quad f(x) + \langle \gamma, x \rangle = c + \bar{\alpha}\beta + \alpha\bar{\alpha} + \beta = c + \alpha\beta \ ,$$

implying that $f(x) + \langle \gamma, x \rangle$ is constant on $E_{\alpha\bar{\beta}} \cup E_{\bar{\alpha}\beta}$. The special case $\gamma = 0$ and $\alpha = \beta = 0$ shows that if g is normal then f is normal as well. □

According to Lemma 10 (applied recursively), if f is a Boolean function on $\mathbb{F}_2^n$ and if f' is a quadratic bent function on $\mathbb{F}_2^{n'}$, then f is (weakly) normal iff $g(x,y) = f(x) + f'(y)$ is (weakly) normal. The question if this is true for any normal bent function f' is still open. The important observation from our point of view is, that if the function f in the above lemma is bent, then g is also bent.

With Fact 1 and Fact 2 we get:

Fact 3 *There exist non normal bent functions of n variables for all even $n \geq 10$ and non weakly-normal bent functions for all even $n \geq 14$.*

3 Modified Maiorana-McFarland Bent Functions

We consider functions derived from the Maiorana-McFarland family by adding an indicator function of a flat E. In particular we are interested in functions described in [3] and below. These functions are all of the following form:

$$f : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$$

$$f(x, y) = \langle x, \pi(y) \rangle + h(x) + \Phi_E(x, y)$$

where $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is a permutation, $h : \mathbb{F}_2^m \to \mathbb{F}_2$ is an arbitrary function and Φ_E is the characteristic function of E:

$$\Phi_E(x, y) : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2\,,$$

$$\Phi_E(x, y) = 1 \quad \text{iff} \quad (x, y) \in E.$$

For some of these functions we shall show that they are normal, or at least weakly-normal.

Carlet's construction

Carlet considers only the special situation, where E is of the form $\tilde{E} \times \mathbb{F}_2^m$ for a subspace $\tilde{E}$ of $\mathbb{F}_2^m$. We denote the characteristic function $\Phi_{\tilde{E} \times \mathbb{F}_2^m}(x, y)$ simply by $\phi_{\tilde{E}}(x)$ to simplify the notation.

The bent functions constructed in [3] are described in the following theorem.

Theorem 11 *[3] Let E be any linear subspace of $\mathbb{F}_2^m$, and π be a permutation on $\mathbb{F}_2^m$ such that for any element λ of $\mathbb{F}_2^m$, the set $\pi^{-1}(\lambda + E^\perp)$ is a flat. Then the function*

$$f(x, y) = \langle x, \pi(y) \rangle + \phi_E(x)$$

is bent.

It is obvious that these functions are normal, because f restricted to $\{0\} \times \mathbb{F}_2^m$ equals 1. Therefore, in order to find non normal bent functions in a similar way, we consider a small appropriate generalization which can be proven in the same way as Carlet's original result and which involves also a function h as the general form of the MM-construction requires.

Lemma 12 *Let E and π be as in Theorem 11, and h be a Boolean function on $\mathbb{F}_2^m$, such that for any element λ of $\mathbb{F}_2^m$, the function h is affine on $\pi^{-1}(\lambda + E^\perp)$. Then*

$$f(x, y) = \langle x, \pi(y) \rangle + h(y) + \phi_E(x)$$

is bent.

Lemma 13 *All bent functions f defined in Lemma 12 are normal.*

Proof. We assume w.l.o.g that $\pi(0) = 0$ and $h(0) = 0$. We first consider the case that h is not constant on $\pi^{-1}(E^\perp)$. Then, we find an element $y_0 \in \pi^{-1}(E^\perp)$, with $h(y_0) = 1$. Define the hyperplane

$$S = \{x \in \mathbb{F}_2^m : \langle x, \pi(y_0)\rangle = 1\},$$

then it is clear that $S \cap E = \emptyset$ since $\pi(y_0) \in E^\perp$. Therefore, the restriction of f to the m-dimensional flat

$$(S \times \{0\}) \cup (S \times \{y_0\})$$

is constant and equal to 0.

If h is constant on the flat $\pi^{-1}(E^\perp)$ then $f(x, y)$ is constant and equal to $1 + h(y)$ on the n-dimensional flat $E \times \pi^{-1}(E^\perp)$. □

Note that the first part of the above proof shows that actually *every* function derived from the Maiorana-McFarland family by adding an indicator function of the form $\Phi_{E \times \mathbb{F}_2^m}$ is weakly-normal.

Canteaut's construction

Another class of bent functions can be derived from the Maiorana-McFarland functions by adding an indicator function of a linear subspace E of $\mathbb{F}_2^m \times \mathbb{F}_2^m$ with codimension 2. This construction is based on some properties of the derivatives of the dual function. Recall that the derivative of a Boolean function on $\mathbb{F}_2^n$, f, with respect to any direction $a \in \mathbb{F}_2^n$ is the Boolean function $D_a f : x \mapsto f(x + a) + f(x)$.

Proposition 14 *[1, 2] Let f be a bent function of $2m$ variables, $m \geq 2$. Let a and b be two distinct nonzero elements of $\mathbb{F}_2^{2m}$ and $E = \langle a, b\rangle^\perp$. Then, the function $f + \Phi_E$ is bent if and only if the dual function, $\widetilde{f}$, satisfies $D_a D_b \widetilde{f} = 0$.*

Note that this result can also be derived from [3, p. 94]. The previous proposition enables us to derive some new bent functions from the Maiorana-McFarland family. From now on, we use an explicit description of the scalar product via the trace mapping: $\mathbb{F}_2^m$ is identified with the finite field of order 2^m, $\mathbb{F}_{2^m}$, and the linear functions are the mappings $y \mapsto \mathrm{Tr}(by)$ on $\mathbb{F}_{2^m}$, where b describes $\mathbb{F}_{2^m}$ and Tr is the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. The scalar product of two elements x and y then corresponds to $\mathrm{Tr}(xy)$. As an example, the following corollary exhibits a bent function obtained from the MM-family by the construction described in Proposition 14.

Corollary 15 *Let $m = gk$ where g is odd and $k > 1$. Let*

$$s = 1 + \sum_{i=0}^{\frac{g-1}{2}-1} (2^k - 1)2^{(2i+1)k}.$$

Let α,β and λ be three nonzero elements in $\mathbb{F}_{2^m}$ such that α has order $(2^k - 1)$, $\mathrm{Tr}(\beta^2(\alpha^2 + \alpha)) = 0$ and $\mathrm{Tr}(\lambda(\alpha^2 + \alpha)) = 0$. Then, the $2m$-variable function

$$g(x, y) = \mathrm{Tr}(xy^s) + \mathrm{Tr}(\lambda y^{3s}) + \mathrm{Tr}(x + \beta y)\mathrm{Tr}(\alpha x + \alpha^{2^{k-1}}\beta y)$$

is bent and does not belong to the completed version of the Maiorana-McFarland family.

Proof. Let f be the $2m$-variable bent function in the Maiorana-McFarland family defined by

$$f(x,y) = \mathrm{Tr}(xy^s) + \mathrm{Tr}(\lambda y^{3s}) \ .$$

Let $a = (1,\beta)$, $b = (\alpha, 2^{k-1}\beta)$ and $V = \langle a,b\rangle^\perp$. From Prop. 14, we deduce that g is bent if and only if $D_aD_b\widetilde{f} = 0$. Let $x \mapsto x^d$ be the inverse of $x \mapsto x^s$ over $\mathbb{F}_{2^m}$, i.e. $d = 2^{m-1} + 2^{k-1}$. The dual $\widetilde{f}$ of f is given by [7, p. 91]:

$$\widetilde{f}(x,y) = \mathrm{Tr}(x^d y) + \mathrm{Tr}(\lambda (x^d)^{3s}) = \mathrm{Tr}(x^d y) + Tr(\lambda x^3) \ .$$

We obtain after some calculations that, for this choice of α, β and λ, $D_aD_b\widetilde{f} = 0$, implying that g is bent.

Now, g belongs to the completed MM-family if and only if there exists an m-dimensional subspace $U \subset \mathbb{F}_2^{2m}$ such that $D_uD_vg = 0$ for any $u,v \in U$ [7, page 102]. We can prove that $U = \mathbb{F}_2^m \times \{0\}$ does not satisfy this condition. Thus, if g belongs to the completed MM-class, there exist two nonzero distinct elements $u,v \in \mathbb{F}_2^{2m}$ with $u \notin \mathbb{F}_2^m \times \{0\}$ such that $D_uD_vg = D_uD_vf + D_uD_v\Phi_V = 0$. This implies that D_uD_vf is constant on $\mathbb{F}_2^{2m}$. By computing D_uD_vf, we deduce that the function D_uD_vf is constant only if there exist $\mu,\nu \in \mathbb{F}_{2^m}^*$, $\mu \neq \nu$, such that

$$(x+\mu+\nu)^s + (x+\mu)^s + (x+\nu)^s + x^s = 0, \quad \forall x \in \mathbb{F}_{2^m} \ ,$$

or if there exist $\mu,\nu \in \mathbb{F}_{2^m}^*$ such that

$$x \mapsto \mathrm{Tr}(\mu((x+\nu)^s + x^s))$$

is constant on $\mathbb{F}_{2^m}$. Using the expression of s, we can then prove that none of these conditions is satisfied (see e.g. [1]). □

However, we can prove that any function derived from the Maiorana-McFarland family by adding the indicator function of a linear subspace of codimension 2, as described in Proposition 14, is normal.

Lemma 16 *Let π be a permutation on $\mathbb{F}_2^m$ and ξ_i be arbitrary Boolean functions on $\mathbb{F}_2^m$. For any nonzero α and β in $\mathbb{F}_{2^m}$, $\alpha \neq \beta$, the function*

$$g(x,y) = \mathrm{Tr}(x\pi(y)) + \mathrm{Tr}(\alpha x)\mathrm{Tr}(\beta x) + \xi_1(y)\mathrm{Tr}(\alpha x) + \xi_2(y)\mathrm{Tr}(\beta x) + \xi_3(y)$$

is normal.

Proof. Let

$$E = \{x \in \mathbb{F}_{2^m} \ : \ \mathrm{Tr}(x) = \mathrm{Tr}(\alpha x) = 0\} = \langle 1,\alpha\rangle^\perp$$

The function g restricted to $y \in \pi^{-1}(E^\perp)$ can be represented as

$$g(x,y)_{|\mathbb{F}_2^m \times \pi^{-1}(E^\perp)} = \mathrm{Tr}(\alpha x)\mathrm{Tr}(\beta x) + \xi_1(y)\mathrm{Tr}(\alpha x) + \xi_2(y)\mathrm{Tr}(\beta x) + \xi_3(y)$$

by changing the functions ξ_i appropriately.

For a fixed $y \in \pi^{-1}(E^\perp)$ we denote $g_y(x) := g(x,y)$. The support of g_y is either a coset of E or the complement of a coset of E. We have

$$E^\perp = \{0, \alpha, \beta, \alpha+\beta\}.$$

Thus, there are four possibility to choose y. At least for two different values y_0 and y_1 the support of g_{y_0} and g_{y_1} has the same size. W.l.o.g we assume that the size of the support of g_{y_0} and g_{y_1} is $\#E$. Now, it follows that $g_{y_0}(x) = g_{y_1}(x) = 0$ for x in the affine hyperplane $(c_0 + E) \cup (c_1 + E)$, where the $c_i + E$, $i = 0, 1$ are different cosets of E. Hence g is constant on the m-dimensional flat

$$\{(c_0 + E) \cup (c_1 + E)\} \times \{y_0, y_1\}.$$

□

Theorem 17 *Let π be a permutation of $\mathbb{F}_2^m$ and h be an arbitrary Boolean function on $\mathbb{F}_2^m$. Let E be a linear subspace of $\mathbb{F}_2^m \times \mathbb{F}_2^m$ of codimension 2 such that*

$$f(x, y) = \mathrm{Tr}(x\pi(y)) + h(y) + \Phi_E(x, y)$$

is bent. Then, f is normal.

Proof. Let $E = \langle(\alpha_1, \alpha_2), (\beta_1, \beta_2)\rangle^\perp$. If $\dim\langle\alpha_1, \beta_1\rangle < 2$, then f belongs to the Maiorana-McFarland class, implying that it is normal. Actually, a bent function f of $2m$ variables belongs to the completed MM-class if and only if there exists an m-dimensional subspace $V \subset \mathbb{F}_2^{2m}$ such that $D_a D_b f = 0$ for any $(a, b) \in V$ [7, page 102]. Here, we obviously have that $D_a D_b f = 0$ for any $a, b \in \mathbb{F}_2^m \times \{0\}$.

Now, if α_1 and β_1 are two nonzero distinct elements of $\mathbb{F}_2^m$, f corresponds to the sum of $\mathrm{Tr}(x\pi(y)) + \mathrm{Tr}(\alpha_1 x)\mathrm{Tr}(\beta_1 x) + \xi_1(y)\mathrm{Tr}(\alpha_1 x) + \xi_2(y)\mathrm{Tr}(\beta_1 x) + \xi_3(y)$ and a linear mapping. From the previous lemma, we deduce that f is normal. □

References

[1] A. Canteaut and P. Charpin. Decomposing bent functions. *IEEE Transactions on Information Theory*, 2003. To appear.

[2] A. Canteaut and P. Charpin. Decomposing bent functions. In *Proceedings 2002 IEEE International Symposium on Information Theory*, page 42, Lausanne, Switzerland, July 2002. IEEE.

[3] C. Carlet. Two new classes of bent functions. In *Advances in Cryptology - EUROCRYPT'93*, number 765 in Lecture Notes in Computer Science, pages 77–101. Springer-Verlag, 1994.

[4] C. Carlet. On cryptographic complexity of boolean functions. In *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas (Proceedings of Fq6)*, pages 53–69. Springer-Verlag, 2002.

[5] P. Charpin. Normal Boolean functions. Preprint, 2003.

[6] M. Daum, H. Dobbertin and G. Leander. An algorithm for checking normality of Boolean functions. In *Proceedings of the 2003 International Workshop on Coding and Cryptography (WCC 2003)*.

[7] J.F. Dillon. *Elementary Hadamard Difference sets.* PhD thesis, University of Maryland, 1974.

[8] J.F. Dillon and H. Dobbertin. New Cyclic Difference Sets with Singer Parameters. In *Finite Fields And Applications*. To appear.

[9] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In *Fast Software Encryption - FSE'94*, number 1008 in Lecture Notes in Computer Science, pages 61–74. Springer-Verlag, 1995.

[10] S. Dubuc-Camus. *Etude des fonctions Booléennes dégénérées et sans corrélation*. PhD thesis, Université de Caen, 1998.

[11] R. L. McFarland. A family of noncyclic difference sets. *J. Combin. Theory Ser. A*, 15:1–10, 1973.