Two New Classes of Bent Functions

Claude Carlet

INRIA Rocquencourt, Domaine de Voluceau,
Bat 10, BP 105, 78153 Le Chesnay Cedex France
and
LAMIFA, Université de Picardie, France.

Abstract. We introduce a new class of bent functions on $(GF(2))^n$ (n even). We prove that this class is not included in one of the known classes of bent functions, and that, when n equals 6, it covers the whole set of bent functions of degree 3. This class is obtained by using a result from J.F. Dillon. We generalize this result and deduce a second new class of bent functions which we checked was not included in one of the preceding ones.

1. Introduction

Let $n = 2p$ ($p \in \mathbf{N}^*$) be an even positive integer.

The bent functions on $(GF(2))^n = \{0, 1\}^n$ are those boolean functions whose Hamming distance to the set of all affine functions on $(GF(2))^n$ (viewed as a vector space over the field GF(2)) is maximum. They play an important role in cryptography (in stream ciphers, for instance), as well as in error correcting coding (where they are used to define optimum codes such as the Kerdock codes and the Delsarte-Goethals codes). They have been studied by J. F. Dillon [5], [4] (in the wider framework of difference sets) and O. S. Rothaus [9] in the seventies. Since then, generalizations have been studied by several authors (cf. for instance [6], [8], and in another direction [3], see also the papers dealing with the covering radius of the Reed-Muller code of order 1 or with bent sequences), but very few papers lead to new results on the bent functions themselves (cf. [2]). In fact, no paper introducing new classes of bent functions has been published since 1975.

All quadratic bent functions are known (we say that a function is quadratic if the global degree of its algebraic normal form, cf. def. below, is at most 2, cf. [7] ch. 15). If n is at least 4, then any bent function has degree at most n/2 (cf [9]). Therefore, all bent functions on $(GF(2))^2$ and $(GF(2))^4$ are quadratic. Excepted these values, the only (even) value of n for which all bent functions are known is n = 6. In [9], O. S. Rothaus

T. Helleseth (Ed.): Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 77-101, 1994.
© Springer-Verlag Berlin Heidelberg 1994

exhibits three classes of bent functions of degree 3 on $(GF(2))^6$ (the elements of a same class are equivalent each other up to an affine nonsingular transformation on the variable). But the problem of finding a simple characterization of the bent functions of degree 3 on $(GF(2))^6$ is still open.

Using a result from J.F. Dillon [4], we introduce (cf. corollary 1 and the definition which follows it) a new class of bent functions of degree $\frac{n}{2}$ on $(GF(2))^n$. The algebraic normal forms of the elements of this class are deduced from those of some of the elements of Maiorana-Mc Farland's class (whose definition will be recalled below) by adding a function whose support is an $\frac{n}{2}$ - dimensional subspace of G. We call $\mathcal{D}$ the new class of bent functions. We check that it is not included in the completed versions of Maiorana-Mc Farland's class and Partial Spread class (cf. def. below). The size of class $\mathcal{D}$ has approximately same order as that of Maiorana-Mc Farland's class.

We prove that the bent functions of degree 3 on $(GF(2))^6$ all belong to class $\mathcal{D}$. That gives a simple characterization of these functions.

Generalizing Dillon's result, we obtain a theorem which characterizes the conditions under which, a bent function f and a flat E being chosen, the function $f + \phi_E$ is bent (where ϕ_E is the charateristic function of E). We deduce a second class of bent functions that we denote by $\mathcal{C}$. We check that this class is not included in the preceding ones.

We recount now with more details the definitions and known properties about bent functions.

Let F denote the Galois field GF(2), and G the F-space F^n (whose zero (0,...,0) will be simply denoted by 0). We denote by G' the space F^p. Clearly, G may be identified with G'^2.

The *dot product* on G is defined for any elements $x = (x_1, \ldots, x_n)$ and $s = (s_1, \ldots, s_n)$ of G by : $x \cdot s = x_1 s_1 + \ldots + x_n s_n \in F$ (where the operation + is in F). We will use the same notation to denote the dot product on G'.

A well-known property which will often be used in this paper is the following :
if E is any F-linear subspace of G and a, b are any elements of G, the sum $\sum_{x \in b+E} (-1)^{a \cdot x}$ is equal to $|E|\,(-1)^{a \cdot b}$ (where |E| denotes the size of E) if a belongs to the dual of E (that is the linear space : $E^{\perp} = \{y \in G / \forall\, x \in E,\ x \cdot y = 0\}$), and to 0 otherwise.

We will call this property the character-sum property (it extends to more general character sums) and denote it by (1).

Let f be a boolean function on G. We denote by $\hat{F}$ the Walsh (or Hadamard or discrete Fourier) transform of the real-valued function $(-1)^{f(x)}$:

$$\hat{F}(s) = \sum_{x \in G} (-1)^{f(x) + x \cdot s} \quad .$$

It satisfies *Parseval's formula* (cf [7], p.416, corollary 3) : $\sum_{s \in G} (\hat{F}(s))^2 = 2^{2n}$.

The boolean function f is called *bent* if (cf. [4], [5], [9]) for any element s of G, $\hat{F}(s)$ is equal to: $\pm 2^p$. According to Parseval's formula and since $\hat{F}(s)$ is related to the Hamming distance between f and the *affine function* $h_s : x \rightarrow s \cdot x + \varepsilon$ ($\varepsilon \in F$) by the relation : $(-1)^{\varepsilon} \hat{F}(s) = 2^n - 2\, d(f, h_s)$, that is equivalent with the fact that f is at maximum distance from the set of all affine functions. Another equivalent definition is (cf. [4], [7]) : for any non-zero element s of G, the function on G: $x \rightarrow f(x) + f(x+s)$ is *balanced* (a boolean function g on G is called balanced if its support $\{x \in G / g(x) = 1\}$ has size 2^{n-1}, or equivalently if the sum $\sum_{x \in G} (-1)^{g(x)}$ equals 0).

The notion of bent function is invariant under any affine nonsingular transformation on the variable (or in other words under any linear nonsingular mapping, and any translation). If f is bent, then for any affine function g, the function f + g is bent. We shall say that a class of bent functions is *complete* if it is globally invariant under the addition of any affine function and the composition (on the right) with any nonsingular affine transformation.

If a boolean function f on G is bent, then the boolean function $\tilde{f}$ defined by :

$$\hat{F}(s) = 2^p (-1)^{\tilde{f}(s)}$$

is bent itself. Following Dillon, we shall call it the *"Fourier" transform* of f. Its properties are (cf. [1] p. 55-59, [4]) :

- the mapping $f \rightarrow \tilde{f}$ is an isometry (i.e. the Hamming distance between two bent functions is equal to that of their "Fourier" transforms)
- if b is any element of G and ε any element of F, let g be the boolean function defined by : $g(x) = f(x) + b \cdot x + \varepsilon$ (respectively $g(x) = f(x+b) + \varepsilon$)

then $\tilde{g}(x)$ is equal to : $\tilde{f}(x+b) + \varepsilon$ (respectively $\tilde{f}(x) + b \cdot x + \varepsilon$). (2)

Any boolean function on G admits an algebraic normal form, that is a polynomial expression by means of the coordinates $x_1, \ldots, x_n$, each coordinate appearing in any monomial with the degree 0 or 1 (cf [7], ch.13). If n is at least 4 and f is a bent function, then the (global) degree of its algebraic normal form is at most p (cf [9]).

Any quadratic function $f(x) = \sum_{1 \le i < j \le n} a_{i,j}\, x_i\, x_j + h(x)$ (h affine, $a_{i,j} \in F$) is bent if and only if one of the following equivalent properties is satisfied (cf [7], ch 15) :

- its associated *symplectic form* :

$$\varphi_f : (x, y) \rightarrow f(0) + f(x) + f(y) + f(x+y)$$

is non-degenerate

- the skew-symmetric matrix $(m_{i,j})_{i,j \in \{1,\ldots,n\}}$ over F , defined by : $m_{i,j} = a_{i,j}$ if $i<j$, $m_{i,j} = 0$ if $i=j$, and $m_{i,j} = a_{j,i}$ if $i>j$, is regular

- f(x) is equivalent, up to an affine nonsingular transformation of the variables, to the function on G:

$$x_1\, x_2 + x_3\, x_4 + \ldots + x_{n-1}\, x_n + \varepsilon \quad (\varepsilon \in F) \qquad (3)$$

A first general class of bent functions is the so-called Maiorana-Mc Farland's class (cf. [4] p. 90, [5]) denoted by $\mathcal{M}$:

we use the identification between G and G'^2, a general element of G being denoted by (x,y) (where x and y belong to G'), and we denote by "$\cdot$" the dot product on G'; the elements of class $\mathcal{M}$ are all the functions of the form :

$$f(x,y) = x \cdot \pi(y) + h(y)$$

where π is any permutation on G' and h any boolean function on G' . Notice that function (3) corresponds to the case $\pi = id$, $h = \varepsilon$ modulo a permutation of the coordinates.

The "Fourier" transform $\tilde{f}(x,y)$ is then equal to :

$$y \cdot \pi^{-1}(x) + h(\pi^{-1}(x))$$

where π^{-1} denotes the inverse permutation of π.

Class $\mathcal{M}$ is not complete. We denote by $\mathcal{M}^{\#}$ its completed version.

A second important class of bent functions is that of Partial Spreads, denoted by $\mathcal{PS}$ (cf. [4] p. 95, [5]) :

$\mathcal{PS}$ is the disjoint union of two classes $\mathcal{PS}^-$ and $\mathcal{PS}^+$:

- the elements of $\mathcal{PS}^-$ are those functions whose supports are the unions of 2^{p-1} "disjoint" p-dimensional subspaces of G , less the point 0, "disjoint" meaning that any two of these spaces admit 0 as only common element, and therefore that their sum is direct and equal to G. In other words, they are the sums of 2^{p-1} characteristic functions of "disjoint" p-dimensional subspaces.

- the elements of $\mathcal{PS}^+$ are those functions whose supports are the unions of $2^{p-1}+1$ "disjoint" p-dimensional subspaces of G. They are the sums of $2^{p-1}+1$ characteristic functions of "disjoint" p-dimensional subspaces.

The "Fourier" transform of any function of $\mathcal{PS}$ is (very simply) deduced from the function itself by replacing the spaces by their duals.

This class is not complete. We obtain the completed version, that we denote by $\mathcal{PS}^\#$, by changing the subspaces into flats, two of them having a single (fixed) point in common, and by adding affine functions.

Classes $\mathcal{M}^\#$ and $\mathcal{PS}^\#$ are the only "effective" known classes of bent functions : there exist other classes of bent functions, but their definitions involve non-obvious conditions, so that none of them leads to an explicit description of bent functions. In fact, class $\mathcal{PS}$ is not really effective (the condition on the spaces which are involved in the definition is not simple, contrary to the condition on π which stands in the definition of class $\mathcal{M}$), but class $\mathcal{PS}$ contains subclasses (cf [4] p. 97...) which are more effective.

The generalized bent functions are defined as follows (cf [6], [8]) :

let n and q be any integers greater than 1. Let J_q and G be respectively the ring $\mathbf{Z}/q\mathbf{Z}$ of all integers modulo q, and the J_q-module $(J_q)^n$. Let $w = e^{2\pi i/q}$, then a function f from G to J_q is called bent if it satisfies one of the following equivalent properties :

1) for any element s of G, the sum $\sum_{x \in G} w^{f(x) - s \cdot x}$ (where "$\cdot$" denotes the usual dot product on G) has modulus $q^{n/2}$ (f is called regular if there exists a function $\tilde{f}$ from G to J_q such that, for any s, this sum is equal to $q^{n/2} w^{\tilde{f}(s)}$)

2) for any element s of G\{0}, the sum $\sum_{x \in G} w^{f(x+s) - f(x)}$ is zero (ie the value of the autocorrelation function of f is zero on any nonzero element).

Class $\mathcal{M}$ generalizes to any q : if n is even and π is any permutation on $G'=(J_q)^{n/2}$, the function on $G = G'^2 : (x,y) \rightarrow x \cdot \pi(y)$ is regular-bent.

2. A New Class of Bent Functions

The idea which is the starting point of this work is the following : if we want to obtain new bent functions, a simple way would be to use known ones and to alter them without losing their property.

J.F. Dillon gives in [4, remark 6.2.15 p.82] a result which may be used in this sense. It may be stated as follows : *let f be a bent function on G; suppose its support contains a p-dimensional linear subspace E of G. Then, denoting by ϕ_E the boolean function of support E, the function $f + \phi_E$ is bent.*

Notice that, more generally, the condition : *E is contained in the support of f* may be replaced by: *the restriction of f to E is affine* . Indeed, if this restriction is equal to $a \cdot x + \varepsilon$, then E is included in the support of the (bent) function $f(x) + a \cdot x + \varepsilon + 1$, on which Dillon's remark may be applied.

We will see (cf. Corollary 1) that this result leads to new bent functions if we apply it to the elements of Maiorana-Mc Farland's class (it does not do so if we try to apply it to the elements of $\mathcal{PS}$). We also wish to determine the "Fourier" transforms of the bent functions that we obtain. It would be possible to deduce them from the proof given by Dillon, but it will be almost as simple and more convenient to give a direct proof of the whole result. To achieve it, a lemma will be useful, which is a slight generalization of [4, theorem 6.2.11 p.79]:

Lemma 1 *Let E be any linear subspace of G, f any bent function on G, and $\tilde{f}$ its "Fourier" transform. Then for any elements a and b of G, we have :*

$$\sum_{x \in a+E} (-1)^{f(x) + b \cdot x} = 2^{\dim E - p} (-1)^{a \cdot b} \sum_{x \in b+E^{\perp}} (-1)^{\tilde{f}(x) + a \cdot x} .$$

If E has dimension p and if the restriction of f(x) to E is 0 (respectively 1) then the restriction of $\tilde{f}$ to $E^{\perp}$ is 0 (respectively 1).

Proof:

According to the definition of the "Fourier" transform, we have :

$$\sum_{x\in b+E^{\perp}} (-1)^{\tilde{f}(x)+a\cdot x} = 2^{-p} \sum_{x\in b+E^{\perp}} \sum_{y\in G} (-1)^{f(y)+y\cdot x+a\cdot x} =$$

$$2^{-p} \sum_{y\in G} (-1)^{f(y)} \Big(\sum_{x\in b+E^{\perp}} (-1)^{(y+a)\cdot x} \Big).$$

According to the character-sum property (1), the sum $\Big(\sum_{x\in b+E^{\perp}} (-1)^{(y+a)\cdot x} \Big)$ is equal to $|E^{\perp}|\,(-1)^{(y+a)\cdot b}$ if y + a belongs to E, and to 0 otherwise. Therefore, we have :

$$\sum_{x\in b+E^{\perp}} (-1)^{\tilde{f}(x)+a\cdot x} = |E^{\perp}|\, 2^{-p} \sum_{y\in a+E} (-1)^{f(y)+(y+a)\cdot b}$$ and the first part of the lemma holds, since $|E^{\perp}|$ is equal to $2^{2p-\dim E}$.

If E has dimension p, the restriction of f(x) to E is 0 (respectively 1) if and only if $\sum_{x\in E} (-1)^{f(x)}$ is equal to 2^p (respectively - 2^p), and the conclusion holds, applying the preceding equality with a = b = 0. □

Proposition 1 *Let E be a p-dimensional linear subspace of G and ϕ_E its characteristic function. Let f be a bent function on G whose restriction to E is affine. Then the function on G :*

$$f(x) + \phi_E(x)$$

is bent, and its "Fourier" transform is :

$$\tilde{f}(x) + \phi_{E^{\perp}}(x + a),$$

where a is any element of G such that the restriction to E of f(x) is equal to $a \cdot x + \varepsilon$ ($\varepsilon \in F$).

Proof:

Replacing f(x) by $f(x) + a \cdot x + \varepsilon$, and using property (2) (of section 1), we may without loss of generality assume : a=0, ε=0.

For any λ in G, we have :

$$\sum_{x\in G} (-1)^{f(x)+\phi_E(x) + \lambda\cdot x} =$$

$$\sum_{x\in G} (-1)^{f(x) + \lambda\cdot x} - 2 \sum_{x\in E} (-1)^{f(x) + \lambda\cdot x} .$$

The sum : $\sum_{x\in G} (-1)^{f(x) + \lambda\cdot x}$ is equal to : $2^p (-1)^{\tilde{f}(\lambda)}$, and the sum : $\sum_{x\in E} (-1)^{f(x) + \lambda\cdot x} = \sum_{x\in E} (-1)^{\lambda\cdot x}$ is equal to : $2^p \phi_E\perp(\lambda)$, according to the character-sum property (1).

So, if λ does not belong to $E^\perp$, then the sum : $\sum_{x\in G} (-1)^{f(x)+\phi_E(x)+\lambda\cdot x}$ is equal to $2^p (-1)^{\tilde{f}(\lambda)}$, and if λ belongs to $E^\perp$, it is equal to $2^p (-1)^{\tilde{f}(\lambda)} - 2^{p+1}$ which is equal to $-2^p = 2^p (-1)^{\tilde{f}(\lambda)+1}$, since according to lemma 1, $\tilde{f}(\lambda)$ is equal to 0.

So, f is bent and $\sum_{x\in G} (-1)^{f(x)+\phi_E(x) + \lambda\cdot x}$ is equal to : $2^p (-1)^{\tilde{f}(\lambda) + \phi_E\perp(\lambda)}$. □

In next corollary, we identify G with G'^2, so that we denote by (x,y) any element of G ($x,y \in G'$).

Corollary 1 *Let E be a p-dimensional linear subspace of G and π a permutation on G' such that, for any (x, y) in E, the number : $x \cdot \pi(y)$ equals 0. Then the function defined on G as :*

$$x \cdot \pi(y) + \phi_E(x, y)$$

is bent, and its "Fourier" transform is the function:

$$y \cdot \pi^{-1}(x) + \phi_E\perp(x, y).$$

Proof :

π being a permutation, the function f defined by :

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

belongs to Maiorana-Mc Farland's class, and so is bent. Its "Fourier" transform is the function :

$$\tilde{f}(x,y) = y \cdot \pi^{-1}(x).$$

So, the result follows directly from proposition 1 with $a = 0$ and $\varepsilon = 0$. □

Remark

1) The class of bent functions that we obtain cannot be considered as an effective one since there is no simple description of all the subspaces and permutations satisfying the condition of Corollary 1. But there is a simple subcase : when E is equal to the cartesian product of two subspaces E_1 and E_2 of G' such that dim E_1 + dim E_2 = p and $\pi(E_2) = E_1^{\perp}$. This will lead to our first new class of bent functions (whose definition is below).

When E_1 is equal to the trivial space {0}, (and therefore E_2 = G'), the condition $\pi(E_2) = E_1^{\perp}$ is obviously satisfied. This special case leads to a subclass.

Of course, when E_1 = G' (and E_2 = {0}), the condition on π is empty too, but in that case, the function that we deduce belongs to Maiorana-Mc Farland's class, and we so obtain no new bent function.

2) Corollary 1 may be extended to some non-binary cases : let q be any positive even integer, let J_q, G' and G be respectively $\mathbf{Z}/q\mathbf{Z}$, $(J_q)^p$ and $(J_q)^n = G'^2$ (n =2p). Let E be any subgroup of order q^p of G and π any permutation on $(J_q)^p$. Suppose that, for any (x,y) in E : $x \cdot \pi(y) = 0$. Then the function :

$$(x,y) \rightarrow x \cdot \pi(y) + \frac{q}{2}\phi_E(x,y)$$

is bent :

let $w = e^{2\pi i/q}$, we have (since $w^{q/2} = -1$) :

$$\sum_{(x,y)\in G} w^{x\cdot\pi(y)+(q/2)\phi_E(x,y) - \lambda\cdot x - \mu\cdot y} =$$

$$\sum_{(x,y)\in G} w^{x\cdot\pi(y) - \lambda\cdot x - \mu\cdot y} - 2 \sum_{(x,y)\in E} w^{x\cdot\pi(y) - \lambda\cdot x - \mu\cdot y}.$$

The sum : $\sum_{(x,y)\in G} w^{x\cdot\pi(y) - \lambda\cdot x - \mu\cdot y}$ is equal to : $q^p\, w^{\mu\cdot\pi^{-1}(\lambda)}$ (cf.[6], p.100)

and the sum : $\sum_{(x,y)\in E} w^{- \lambda\cdot x - \mu\cdot y}$ is equal to : $q^p\, \phi_{E^{\perp}}(\lambda,\mu)$, (Lemma 1 generalizes).

That completes this sketch of proof.

Definition 1 *We call $\mathcal{D}$ the class of all the boolean functions of the form :*

$$(x, y) \in G \rightarrow \phi_E(x, y) + x \cdot \pi(y)$$

where E is a subspace of G equal to $E_1 \times E_2$, E_1 and E_2 are subspaces of G' such that dim E_1 + dim E_2 = p, and π is any permutation on G' such that $\pi(E_2) = E_1^{\perp}$.
We call $\mathfrak{D}_o$ the subclass of all the functions of the form :

$$(x, y) \to \prod_{i=1}^{p} (x_i + 1) + x \cdot \pi(y) .$$

$\mathfrak{D}_0$ corresponds to the case : E = {0} x G'.

Example :

Assume $\pi(0) = 0$. Let z be any nonzero element of G'. Let E_1 be the linear hyperplane $\pi(z)^{\perp}$ and E_2 the line {0,z}. The function:

$$x \cdot \pi(y) + \phi_{E_1}(x)\, \phi_{E_2}(y) = x \cdot \pi(y) + (x \cdot \pi(z) + 1) \left(\prod_{i=1}^{p} (y_i+1) + \prod_{i=1}^{p} (y_i+z_i+1) \right)$$

belongs to class $\mathfrak{D}$.

Remark

1) Both classes $\mathcal{M}^{\#}$ and $\mathcal{PS}^{\#}$ are invariant under the "Fourier" transform $f \to \tilde{f}$. According to Corollary 1, that is still the case of classes $\mathfrak{D}_o^{\#}$ and $\mathfrak{D}^{\#}$ (the completed classes of $\mathfrak{D}_o$ and $\mathfrak{D}$) .

2) The sizes of $\mathfrak{D}$ and $\mathcal{M}$ have approximately same order since the number 2^{2^p} of boolean functions on F^p is small, compared with the number of permutations on the same space : $(2^p)!$.

We check now that class $\mathfrak{D}$ is not included in class $\mathcal{M}^{\#}$. We shall obtain this result as a corollary of next proposition.

Proposition 2 *If $p \geq 4$ and if the restriction of permutation π to any linear hyperplane of G' is not affine, then the following function does not belong to class $\mathcal{M}^{\#}$:*

$$(x,y) \to \prod_{i=1}^{p} x_i + (x + 1) \cdot \pi(y)$$

(where 1 denotes the all-one word).

Proof :

We know that if a function f belongs to $\mathcal{M}^{\#}$, then there exists a p-dimensional subspace E of G, such that, for any elements (a,a') and (b,b') of E, the function :

$$x \to f(x,y) + f(x+a,y+a') + f(x+b,y+b') + f(x+a+b,y+a'+b')$$

is equal to 0 . Indeed, if f(x,y) is equal to $x \cdot \pi'(y) + h(y)$, where π' is a permutation, we may take E = G' x {0}, and any element of $\mathcal{M}^{\#}$ is equivalent to such a function, up to a nonsingular affine transformation on the variable .

Suppose that, two elements (a,a') and (b,b') being chosen in G, the function :

$$f(x,y) = \prod_{i=1}^{p} x_i + (x+1) \cdot \pi(y)$$

satisfies the condition :

$$\forall (x,y) \in G,\ f(x,y) + f(x+a,y+a') + f(x+b,y+b') + f(x+a+b,y+a'+b') = 0.$$

That implies that the degree of the function :

$$\prod_{i=1}^{p} x_i + \prod_{i=1}^{p} (x_i+a_i) + \prod_{i=1}^{p} (x_i+b_i) + \prod_{i=1}^{p} (x_i+a_i+b_i)$$

is at most 1 (since the degree relative to x of : $(x+1) \cdot \pi(y) + (x+a+1) \cdot \pi(y+a') + (x+b+1) \cdot \pi(y+b') + (x+a+b+1) \cdot \pi(y+a'+b')$ is at most 1).

For any pair {i,j} of indices, the coefficient of $\prod_{k \neq i,j} x_k$ in that expression is :

$$a_ia_j + b_ib_j + (a_i+a_j)(b_i+b_j) = a_ib_j + a_jb_i$$

and must be equal to 0, since $p \geq 4$. So, any two elements (a,a') and (b,b') of E are such that a and b are linearly dependent (ie one of them is 0, or they are equal each other).We deduce that E is either equal to {0} x G' or to the direct sum of a line {0,α} (where α is a nonzero element of G') and of an hyperplane H of G'. In any case, there exists at least a linear hyperplane H of G' such that {0} x H is included in E. This hyperplane satisfies that for any elements a' and b' of H, and any elements x and y of G', we have :

$$(x+1) \cdot (\pi(y) + \pi(y+a') + \pi(y+b') + \pi(y+a'+b')) = 0.$$

Since the restriction to H of at least one of the coordinate functions of π is not affine, we arrive to a contradiction. □

Corollary 2 *Classes $\mathcal{D}_0$ and $\mathcal{D}$ are in general not included in class $\mathcal{M}^{\#}$.*

Proof :

The function $\prod_{i=1}^{p} x_i + (x+1)\cdot\pi(y)$ is equivalent to the function $\prod_{i=1}^{p} (x_i+1) + x\cdot\pi(y)$ which belongs to class $\mathcal{D}_0$. So, all we need to prove is that there does exist in general a permutation π whose restriction to any linear hyperplane is not affine.

Let us identify G' with the Galois field of order 2^p. Let i be any integer prime to $2^p - 1$. The mapping on G' : $x \rightarrow x^i$ is a permutation on G'. Its retriction to a linear hyperplane $\{x \in G' / tr(ax) = 0\}$ (where tr is the trace function from G' to F and a is any nonzero element of G') is affine if and only if its restriction to the linear hyperplane $H_0 = \{x \in G' / tr(x) = 0\}$ is affine (since $\pi(ax) = a^i \pi(x)$).

H_0 being equal to the image of the linear mapping : $x \rightarrow x^2 + x$, that is true if and only if the mapping : $x \rightarrow (x^2 + x)^i$ is affine.

It is a simple matter to show that there exists in general i such that this last mapping is not affine. Take for instance $i = 1 + 2^j$. Suppose 2j is prime to p (and so, p is odd), then i is prime to 2^p-1. Suppose $2^{j+1}+2 < 2^p$. Then $(x^2 + x)^i$, equal to $:x^{2^{j+1}+2} + x^{2^{j+1}+1} + x^{2^j+2} + x^{2^j+1}$ cannot be affine since it is a non-affine polynomial of degree at most 2^p-1 (cf [7] p. 402). □

We now wish to prove that class $\mathcal{D}$ is not included in class $\mathcal{PS}^{\#}$. That is much more difficult since there does not seem to exist simple necessary conditions for a function to belong to $\mathcal{PS}^{\#}$. That is perhaps why it has never been proved until now that class $\mathcal{M}$ is not included in class $\mathcal{PS}^{\#}$ (J.F.Dillon has only proved in his thesis [4 p.53] that class $\mathcal{M}$ is not included in class $\mathcal{PS}$).

Proposition 3 *If p is any odd integer at least equal to 5, the function:*

$$(x,y) \in G \rightarrow \prod_{i=1}^{p} x_i + (x+1)\cdot y$$

does not belong to class $\mathcal{PS}^{\#}$.

Proof:

We have to prove that, for any affine function g on G, the function : $f(x,y) = \prod_{i=1}^{p} x_i + (x+1) \cdot y + g(x,y)$ is not equivalent, up to a nonsingular affine transformation, to a function of $\mathcal{PS}$.

Suppose first that it is equivalent to a function of $\mathcal{PS}^-$. There exist $k=2^{p-1}$ flats $H_1,\ldots, H_k$ of G such that any two of them intersect in a single (fixed) point (a,b), and that the support of f is their union less the point (a,b).

Let i be any element of $\{1,\ldots,k\}$. The intersection between H_i and the support of f is $H_i \setminus \{(a,b)\}$ and so has an odd number of elements. Therefore, denoting by h_i the boolean function of support H_i, the function f h_i (whose value in x is $f(x)h_i(x)$) has an odd weight, and so has degree 2p. Consequently, since $\prod_{i=1}^{p} x_i$ is the only monomial in the algebraic normal form of f (x,y) whose degree is p, and since h_i has degree p, the product of the function h_i with any function $\prod_{i=1}^{p} (x_i+\lambda_i)$ has degree 2p. Applying this result to $\lambda_i = a_i + 1$ (i=1...p), we deduce that the flat {a}xG' has an odd number of elements in commun with H_i. That means that it has the point (a,b) only in commun with H_i.

We deduce:

$\forall y \in G'$, $f(a,y) = 0$,

$\forall\, y,\ \prod_{i=1}^{p} a_i + (a+1) \cdot y + g\,(x,y) = 0$.

So, replacing g(x,y) by its value, we obtain :

$$f\,(x,y) = \prod_{i=1}^{p} x_i + \prod_{i=1}^{p} a_i + (x+a) \cdot y\,.$$

The translation $(x,y) \rightarrow (x+a,y+b)$ translates the point (a,b) in (0,0) and changes f (x,y) in:

$$\prod_{i=1}^{p} (x_i+a_i) + \prod_{i=1}^{p} a_i + x \cdot (y+b)\,.$$

The subspace $E = \{0\}xG'$ is disjoint from the support of f and so is "disjoint" from any of the H_i. Using an idea from J. F. Dillon [4, p.53], we may deduce that there exist linear mappings ϕ_i on G' such that, for any i, H_i is equal to the set : $\{(x,\phi_i(x)), x \in G'\}$. Since for any i, the set $H_i \setminus \{(0,0)\}$ is included in the support of f, we deduce :

$\forall\, i,j\ \forall\, x \in G'$, $f(x,\phi_i(x)) = f(x,\phi_j(x))$, and therefore :

$\forall\, i,j\ \forall\, x \in G'$, $x \cdot (\phi_i(x)+\phi_j(x)) = 0$.

That implies that the matrix of the linear mapping $\phi_i+\phi_j$ is skew-symmetric. If $i \neq j$, H_i and H_j admit 0 as only commun element. So, this matrix is regular. The dimension p being odd, that is impossible.

Suppose now that the function :

$$f : (x,y) \rightarrow \prod_{i=1}^{p} x_i + (x+1) \cdot y + g\ (x,y)$$

is equivalent to a function of $\mathcal{PS}^+$. Its support is the union of $2^{p-1}+1$ p-dimensional flats, any two of them intersecting in a single fixed point (a,b).

We may suppose without loss of generality that g depends only on y (if $g(x,y) = u \cdot x + v \cdot y + \varepsilon$, change y in $y + u$). The restriction of f to the flat $H = \{(a,y), y \in G'\}$ is the function :

$$y \rightarrow \prod_{i=1}^{p} a_i + (a+1) \cdot y + g\ (y)\ .$$

This function is affine. Suppose it is not the constant function 1, then its weight is at most 2^{p-1}, and at least two spaces H_i have (a,b) as only commun point with H. We can apply the translation of vector (a,b) and complete the proof as previously.

Otherwise, f(x,y) is equal to : $\prod_{i=1}^{p} x_i + (x+a) \cdot y + \prod_{i=1}^{p} a_i + 1$. Let us apply again the translation of vector (a,b), so that f(x,y) becomes : $\prod_{i=1}^{p} (x_i+a_i) + x \cdot (y+b) + \prod_{i=1}^{p} a_i + 1$.

Let α be an element of G' such that : $\prod_{i=1}^{p} (\alpha_i+a_i) + \alpha \cdot b + \prod_{i=1}^{p} a_i = 1$ (such an element exists since the function $\prod_{i=1}^{p} (x_i+a_i) + x \cdot b + \prod_{i=1}^{p} a_i$ is not the zero function).

Let E denote the linear hyperplane of G' : $\{x \in G' / \alpha \cdot x = 0\} = \alpha^{\perp}$.

The restriction of f to the space : $\{0,\alpha\} \times E$ is balanced since it is equal to 1 on $\{0\} \times E$ and to 0 on $\{\alpha\} \times E$. Therefore, there exist at least two spaces H_i (say H_1 and H_2) which are "disjoint" from the space $\{0,\alpha\} \times E$.

We shall now compose f on the right by an automorphism ψ of G which maps $\{0\} \times G'$ onto $\{0,\alpha\} \times E$, so that we can apply on $f \circ \psi$ the same technique as the one we applied previously on f. Let β be an element of G' such that $\alpha \cdot \beta = 1$, and $E' = \beta^{\perp}$.

We have : $G = (\{0,\alpha\} \oplus E') \times (\{0,\beta\} \oplus E)$.

Let ψ be the involutive isomorphism of G defined by :

$\forall \varepsilon, \eta \in F, \forall u \in E, \forall v \in E', \psi(\varepsilon \alpha + v, \eta \beta + u) = (\eta \alpha + v, \varepsilon \beta + u)$.

ψ maps $\{0\} \times G'$ onto $\{0,\alpha\} \times E$.

The function $\left(\prod_{i=1}^{p} (x_i+a_i) \right) \circ \psi$ has support : $\psi(\{a+1\} \times G')$, since $\prod_{i=1}^{p} (x_i+a_i)$ has support $\{a+1\} \times G'$ and $\psi^{-1} = \psi$. If γ and w are the elements of F and E' (respectively) such that a+1 is equal to : $\gamma \alpha + w$, this support is the set : $\{(\varepsilon \alpha + w, \gamma \beta + u), \varepsilon \in F, u \in E\}$.

Remember that f(x,y) is equal to $\prod_{i=1}^{p} (x_i+a_i) + x \cdot (y+b) + \prod_{i=1}^{p} a_i + 1$. We deduce : $\forall \varepsilon, \eta \in F, \forall u \in E, \forall v \in E'$,

$$f \circ \psi (\varepsilon \alpha + v, \eta \beta + u) = (\eta+\gamma+1) \chi_w(v) + \eta \varepsilon + v \cdot u + (\eta \alpha + v) \cdot b + \prod_{i=1}^{p} a_i + 1$$

where $\chi_w(v) = \begin{cases} 1 \text{ if } v = w \\ 0 \text{ otherwise} \end{cases}$.

We know that there exist (at least) two linear subspaces $\psi(H_1)$ and $\psi(H_2)$ (since $\psi^{-1} = \psi$) of G which are "disjoint" from each other and "disjoint" from the space $\{0\} \times G'$ and which are included in the support of $f \circ \psi$. We deduce that there exist two linear mappings ϕ_1 and ϕ_2 from G' to itself such that :

$\forall \varepsilon \in F, \forall v \in E', f \circ \psi (\varepsilon \alpha + v, \phi_1(\varepsilon \alpha + v)) = f \circ \psi (\varepsilon \alpha + v, \phi_2(\varepsilon \alpha + v))$.

Let l_i and L_i (i=1, 2) be respectively the boolean function on G' and the linear mapping from G' onto E such that : $\phi_i(\varepsilon\alpha + v) = l_i(\varepsilon\alpha + v)\beta + L_i(\varepsilon\alpha + v)$. We have :

$\forall \varepsilon \in F, \forall v \in E'$,

$(l_1 + l_2)(\varepsilon\alpha + v)\ \chi_w(v) + ((l_1 + l_2)(\varepsilon\alpha + v))\ \varepsilon + v \cdot [(L_1 + L_2)(\varepsilon\alpha + v)] +$

$[(l_1 + l_2)(\varepsilon\alpha + v)]\ [\alpha \cdot b] = 0.$

We shall prove that this is impossible.

If v is different from w, then for any ε, we have :

$((l_1 + l_2)(\varepsilon\alpha + v))\ \varepsilon + v \cdot [(L_1 + L_2)(\varepsilon\alpha + v)] + [(l_1 + l_2)(\varepsilon\alpha + v)]\ [\alpha \cdot b] = 0.$

That means that the function of the variable (ε,v) which is equal to the LHS of that equality has weight at most 2. But, this function is quadratic, and we know (cf. [7] ch 15) that if a function is quadratic, then either its weight is at least 2^{p-2} (ans so is at least 8) or it is the zero function. We deduce that it is the zero function. But this function is equal to : $x \cdot (\phi_1(x) + \phi_2(x))$, where $x = \varepsilon\alpha + v$.

Thus, the matrix of the linear mapping $\phi_1 + \phi_2$ is skew-symmetric and regular, a contradiction. □

Corollary 3 *Classes $\mathcal{D}_o$, $\mathcal{D}$ and $\mathcal{M}$ are not included in class $\mathcal{PS}^{\#}$.*

Proof :

It is straightforward, according to Proposition 3, since the function $(x,y) \in G \rightarrow \prod_{i=1}^{p} x_i + (x+1) \cdot y$ of Proposition 3 belongs to classes $\mathcal{D}_o^{\#}$, $\mathcal{D}^{\#}$, and $\mathcal{M}^{\#}$, . □

3. Generalization of Dillon's result

We shall now extend Dillon's result to cases where E is a flat whose dimension is not necessarily equal to p. That will lead us to new bent functions.

Before we state the theorem, we need some preliminary definition and lemmas.

Lemma 2 *Let f be any boolean function on G. Let E be any flat of G and k its dimension. Let ψ be any affine mapping from F^k to G such that $E = \psi(F^k)$. Then the degree of the boolean function $f \circ \psi$ on F^k does not depend on the choice of ψ.*

Proof :

Suppose that ψ_1 and ψ_2 are two affine mappings from FP to G such that $\psi_1(F^k) = \psi_2(F^k) = E$. The boolean functions $f \circ \psi_1$ and $f \circ \psi_2$ are then equivalent and so have same degree (cf [4], p.39, [7] ch.13). □

Definition 2 *Let f be any boolean function on G and E any flat in G. We call degree of the restriction of f to E the degree of the function $f \circ \psi$ on F^k, where k is the dimension of E and ψ is any affine mapping from F^k to G such that $\psi(F^k) = E$.*

Lemma 3 *Let f be any boolean function on G and E any k-dimensional flat in G. If there exists an integer r such that, for any element a of G, the sum :*

$$\sum_{x \in E} (-1)^{f(x) + a \cdot x}$$

is divisible by 2^r, then the degree of the restriction of f to E is at most : $k - r + 1$.

Proof :

We just adapt the proof due to Rothaus [9] on the degrees of the bent functions.

We may suppose that E is equal to F^k (otherwise, we can compose by an appropriate affine nonsingular mapping). Let d be the degree of the restriction of f to E and $\prod_{i \in I} x_i$ one of its monomials of degree d (I is a subset of $\{1,\ldots,k\}$ of size d).

The sum : $\sum_{x \in E / x_i = 0, \forall i \notin I} (-1)^{f(x)}$ is equal to the size 2^d of the linear subspace $\{x \in E / x_i = 0, \forall i \notin I\}$ minus twice the weight of the restriction of f to this subspace, which is odd, since the degree of this function is equal to the dimension of this subspace (cf. [7], ch 13 or [9]) . Therefore, $\sum_{x \in E / x_i = 0, \forall i \notin I} (-1)^{f(x)}$ is divisible by 2 but not by 4 .

For any a in G, let $\lambda_a = \sum_{x \in E} (-1)^{f(x) + a \cdot x}$.

According to the inverse formula of the Walsh transform (cf. [7], p. 127), for any x in E, we have: $(-1)^{f(x)} = 2^{-k} \sum_{a \in E} \lambda_a (-1)^{a \cdot x}$, and therefore :

$$\sum_{x \in E/x_i=0, \forall i \notin I} (-1)^{f(x)} = \sum_{x \in E/x_i=0, \forall i \notin I} 2^{-k} \sum_{a \in E} \lambda_a (-1)^{a \cdot x} =$$

$$2^{-k} \sum_{a \in E} \lambda_a \left(\sum_{x \in E/x_i=0, \forall i \notin I} (-1)^{a \cdot x} \right) = 2^{|I|-k} \sum_{a \in E/a_i=0, \forall i \in I} \lambda_a$$ (according to the character-sum property (1)).

So, the sum $\sum_{x \in E/x_i=0, \forall i \notin I} (-1)^{f(x)}$ is divisible by $2^{|I|-k+r} = 2^{d-k+r}$ and therefore, $d - k + r$ is at most 1. We so have proved : $d \leq k - r + 1$. □

Theorem *Let $E = b + E'$ be any flat in $G = F_2^p$ (E', its direction, is a linear subspace of G). Let ϕ_E be the boolean function whose support is E and f(x) any bent function on G. Then the function $f^* = f + \phi_E$ is bent if and only if one of the following equivalent conditions is satisfied :*

1) for any x in $G \setminus E'$, the function:

$$y \rightarrow f(y) + f(x+y)$$

is balanced on E

2) for any λ in G, the restriction of the function $\widetilde{f}(x) + b \cdot x$ to the flat $\lambda + E'^{\perp}$ is either constant or balanced.

If one of these conditions is satisfied, then E has dimension at least p and the degree of the restriction of f to E is at most dim E - p + 1.

If E has dimension p, then this last condition is also sufficient and the function $\widetilde{f}^*(x)$ is equal to :

$$\widetilde{f}(x) + \phi_{a + E'^{\perp}}(x),$$

where a is any element of G such that for any x in E : $f(x) = a \cdot x + \varepsilon$.

Proof :

1) The function f* is bent if and only if, for any x in $G \setminus \{0\}$, the function $y \rightarrow f^*(y) + f^*(x+y)$ is balanced on G, that is :

$$\sum_{y \in G} (-1)^{f^*(y) + f^*(x+y)} = 0.$$

If x belongs to E', then we have for any y in G : $f^*(y) + f^*(x+y) = f(y) + f(x+y)$ and therefore :

$$\sum_{y \in G} (-1)^{f^*(y) + f^*(x+y)} = \sum_{y \in G} (-1)^{f(y) + f(x+y)} = 0 \text{ (since f is bent).}$$

If x does not belong to E', then the flats E and x+E are disjoint, the function $\phi_E(y) + \phi_E(x+y)$ takes the value 1 on $E \cup (x+E)$ and :

$$\sum_{y \in G} (-1)^{f^*(y) + f^*(x+y)} =$$

$$\sum_{y \in G} (-1)^{f(y) + f(x+y)} - 2 \sum_{y \in E} (-1)^{f(y) + f(x+y)} - 2 \sum_{y \in x+E} (-1)^{f(y) + f(x+y)} =$$

$$- 4 \sum_{y \in E} (-1)^{f(y) + f(x+y)}.$$

We deduce that f^* is bent if and only if, for any element x of $G \setminus E'$, the function $y \to f(y) + f(x+y)$ is balanced on E.

2) We have :

$$\sum_{x \in G} (-1)^{f^*(x) + \lambda \cdot x} = \sum_{x \in G} (-1)^{f(x) + \lambda \cdot x} - 2 \sum_{x \in E} (-1)^{f(x) + \lambda \cdot x}$$

$$= 2^p (-1)^{\tilde{f}(\lambda)} - 2 \sum_{x \in E} (-1)^{f(x) + \lambda \cdot x}.$$

So, f^* is bent if and only if for any λ in G, the sum $\sum_{x \in E} (-1)^{f(x) + \lambda \cdot x}$ is equal either to 0 or to $2^p (-1)^{\tilde{f}(\lambda)}$.

According to Lemma 1, we have :

$$\sum_{x \in E} (-1)^{f(x) + \lambda \cdot x} = |E| \, 2^{-p} (-1)^{\lambda \cdot b} \sum_{x \in \lambda + E'^{\perp}} (-1)^{\tilde{f}(x) + b \cdot x}.$$

That sum is equal to $2^p (-1)^{\tilde{f}(\lambda)}$ if and only if $\sum_{x \in \lambda + E'^{\perp}} (-1)^{\tilde{f}(x) + b \cdot x}$ is equal to: $\frac{2^{2p}}{|E|} (-1)^{\tilde{f}(\lambda) + \lambda \cdot b}$, that is if and only if $\tilde{f}(x) + b \cdot x$ is constant on $\lambda + E'^{\perp}$, since $\frac{2^{2p}}{|E|}$ is equal to the size of $E'^{\perp}$. This same sum is equal to zero if and only if $\tilde{f}(x) + b \cdot x$ is balanced on $\lambda + E'^{\perp}$. That completes the proof of part 2.

If f and f* are bent, then the degrees of their algebraic normal forms are at most p (cf. [9]), and therefore, ϕ_E has degree at most p. That is equivalent with the fact that the dimension of E is at least p.

For any λ in G, since f and f* are bent and since $\sum_{x\in G} (-1)^{f^*(x) + \lambda\cdot x}$ is equal to : $\sum_{x\in G} (-1)^{f(x) + \lambda\cdot x} - 2\sum_{x\in E} (-1)^{f(x) + \lambda\cdot x}$, the number $2\sum_{x\in E} (-1)^{f(x) + \lambda\cdot x}$ is the difference between two numbers which are both equal to $\pm 2^p$. So, it is divisible by 2^{p+1} and lemma 3 (with r = p) may be applied. Thus the restriction of f to E has degree at most dim E - p + 1.

If E has dimension p, then the restriction of f to E is affine (that is the converse of Dillon's result). There exist a in G and ε in F such that, for any x in E: $f(x) = a \cdot x + \varepsilon$. Proposition 1 and property (2) complete the proof. □

Remark

1) If E is the whole space G, then conditions 1 and 2 in the theorem are obviously satisfied. That corresponds to the fact that for any bent function f, the function f+1 is bent.

If E is an hyperplane, then $\phi_E(x)$ is of the form : $a \cdot x + \varepsilon$ ($a \in G$, $\varepsilon \in F$). So conditions 1 and 2 must be satisfied (since if f(x) is any bent function then $f(x) + a \cdot x + \varepsilon$ is bent). It is a simple matter to check it. Notice that, in that case, $\tilde{f^*}(x)$ is equal to : $\tilde{f}(x+a) + \varepsilon$. We see that the expression of $\tilde{f^*}(x)$ by means of $\tilde{f}(x)$ may be quite different depending on whether E has dimension p or not.

2) The characterization by condition 1 of those bent functions f such that $f + \phi_E$ is bent generalizes to non-binary cases the following way :

let n and q be any integers greater than 1. Let J_q and G be respectively the groups $\mathbf{Z}/q\mathbf{Z}$ and $(J_q)^n$, f a bent function from G to J_q, E' any subgroup of G, b any element of G, E the set b + E' and λ any element of J_q. Then the function $f^* = f + \lambda\,\phi_E$ is bent if and only if, for any x in G \ E', the element of J_q equal to:

$(w^{-\lambda} - 1)\sum_{y\in E} w^{f(x+y) - f(y)} + (w^{\lambda} - 1)\sum_{y\in -x+E} w^{f(x+y) - f(y)}$ is zero. Indeed, let x be any nonzero element of G, the sum :

$$\sum_{y \in G} w^{f^*(x+y) - f^*(y)}$$

is equal to : $\sum_{y \in G} w^{f(x+y) - f(y)} = 0$ if x belongs to E' (since x + E is then equal to E), and to:

$$\sum_{y \in G} w^{f(x+y) - f(y)} + (w^{-\lambda} - 1) \sum_{y \in E} w^{f(x+y) - f(y)} + (w^{\lambda} - 1) \sum_{y \in -x+E} w^{f(x+y) - f(y)}$$

otherwise.

Condition 2 may also be generalized to some non-binary cases, but only for regular-bent functions.

We deduce now the existence of another superclass of $\mathcal{D}_0$ whose elements are bent functions :

Corollary 4 *Let L be any linear subspace of $G' = F_p^n$ and π any permutation on G' such that, for any element λ of G', the set $\pi^{-1}(\lambda + L)$ is a flat. Then the function on G:*

$$x \cdot \pi(y) + \phi_{L^\perp}(x)$$

is bent.

Proof :

Let E be the subspace of G : $L^\perp \times G'$.

The function $f(x,y) = x \cdot \pi(y)$ belongs to Maiorana-Mac Farland's class and so is bent. Its "Fourier" transform is $\tilde{f}(x,y) = y \cdot \pi^{-1}(x)$. Let (λ, μ) be any element of G. The size of the support of the restriction of $\tilde{f}(x,y)$ to the set $(\lambda, \mu) + E^\perp = (\lambda + L) \times \{\mu\}$ is equal to that of the support of the restriction of the function : $x \rightarrow \mu \cdot x$ to the flat $\pi^{-1}(\lambda + L)$, which is either balanced or constant, since this function is affine. So, condition 2 of the theorem is satisfied. □

Definition *We call $\mathcal{C}$ the class of all the functions of the form :*

$$x \cdot \pi(y) + \phi_{L^\perp}(x),$$

where L and π satisfy the conditions of the preceding corollary.

Class $\mathfrak{C}$ contains $\mathfrak{D}_0$ (which corresponds to the case L = G'), and so is not included in classes $\mathfrak{M}^\#$ and $\mathfrak{PS}^\#$.

Notice that class $\mathfrak{C}$ is not included in class $\mathfrak{D}^\#$, since it contains functions of degrees less than p.

4. A simple characterization of the bent functions on F^6

We shall deduce from the theorem a characterization of the bent functions of degree 3 on F^6.

Proposition 4 *Let f be any boolean function of degree 3 on F^6 of the form :*

$f(x_1,\ldots,x_6) = x_1 x_2 x_3 + x_1 h_1(x_4,x_5,x_6) + x_2 h_2(x_4,x_5,x_6) + x_3 h_3(x_4,x_5,x_6) + g(x_4,x_5,x_6)$

where h_1, h_2, and h_3 are three (quadratic) functions on F^3, and g is a boolean function on F^3.

Then f is bent if and only if :

1) the mapping $(x_1,x_2,x_3) \to (h_1(x_1,x_2,x_3), h_2(x_1,x_2,x_3), h_3(x_1,x_2,x_3))$ is a permutation on F^3

2) the function $h_1 + h_2 + h_3 + g$ is affine.

Any bent function of degree 3 on F^6 is equivalent, up to a nonsingular affine transformation on the variables, to such a function .

Proof :

Suppose f is bent, then the functions on F^6 :

$f(x_1, x_2,\ldots,x_6) + f(x_1+1, x_2,\ldots,x_6) = x_2x_3 + h_1(x_4,x_5,x_6)$

$f(x_1, x_2, x_3,\ldots,x_6) + f(x_1+1, x_2+1, x_3,\ldots, x_6) = (x_1+x_2+1)x_3 + h_1(x_4, x_5, x_6) + h_2(x_4, x_5, x_6)$

$f(x_1, x_2, x_3, x_4, x_5, x_6) + f(x_1+1, x_2+1, x_3+1, x_4, x_5, x_6) =$

$x_1x_2+x_1x_3+x_2x_3+x_1+x_2+x_3+1 + h_1(x_4, x_5, x_6) + h_2(x_4, x_5, x_6) + h_3(x_4, x_5, x_6) =$

$(x_1+x_2+1)(x_1+x_3+1) + h_1(x_4, x_5, x_6) + h_2(x_4, x_5, x_6) + h_3(x_4, x_5, x_6)$

are balanced.

We have (cf [2]) : $\sum_{(x_2,\ldots,x_6)\in F^5} (-1)^{x_2x_3 + h_1(x_4,x_5,x_6)} = 2 \sum_{(x_4,x_5,x_6)\in F^3} (-1)^{h_1(x_4,x_5,x_6)}$

Thus, h_1 is balanced. Similarly, h_2, h_3, $h_1 + h_2$, $h_1 + h_3$, $h_2 + h_3$, and $h_1 + h_2 + h_3$ are balanced.

It is then a simple matter to prove that (h_1, h_2, h_3) is a permutation on F^3 :

let us denote by h the real-valued function on F^3 whose value on any element (a_1,a_2,a_3) of F^3 is equal to the size of the set :

$\{(x_4,x_5,x_6) \in F^3 / (h_1(x_4,x_5,x_6) = a_1, h_2(x_4,x_5,x_6) = a_2 , \text{ and } h_3(x_4,x_5,x_6) = a_3 \}$.

The Walsh transform of h is the function :

$(x_1, x_2, x_3) \rightarrow \sum_{(a_1,a_2,a_3)\in F^3} h(a_1, a_2, a_3) (-1)^{x_1a_1+x_2a_2+x_3a_3} =$

$\sum_{(x_4,x_5,x_6)\in F^3} (-1)^{x_1h_1(x_4,x_5,x_6)+x_2h_2(x_4,x_5,x_6)+x_3h_3(x_4,x_5,x_6)}$.

So, it is equal to 8 if $x_1=x_2=x_3=0$, and to 0 otherwise (since the functions h_1, h_2, h_3, $h_1 + h_2$, $h_1 + h_3$, $h_2 + h_3$, and $h_1 + h_2 + h_3$ are balanced). According to the inverse formula of the Walsh transform (cf.[7]), h is the constant function equal to 1, and the mapping :

$$(x_4,x_5,x_6) \in F^3 \rightarrow (h_1 (x_4,x_5,x_6) , h_2 (x_4,x_5,x_6) , h_3 (x_4,x_5,x_6)) \in F^3$$

is therefore a permutation.

So, the function $x_1 h_1(x_4,x_5,x_6)+ x_2 h_2(x_4,x_5,x_6)+ x_3 h_3(x_4,x_5,x_6)+ g(x_4,x_5,x_6)$ belongs to class $\mathcal{M}$. It is equal to $f(x) + x_1x_2x_3$.

$x_1x_2x_3$ is the algebraic normal form of the 3-dimensional flat of equations $x_1=x_2=x_3=1$. According to the theorem, the restriction of f(x) to this flat must be affine, and so, $h_1 + h_2 + h_3 + g$ is affine. So, 1) and 2) are satisfied.

The converse is straightforward, according to the theorem.

Let f be now any bent function of degree 3 on F^6. We may without loss of generality suppose that its algebraic normal form contains the monomial $x_1x_2x_3$. Let $g_1(x_4,x_5,x_6)$, $g_2(x_4,x_5,x_6)$, and $g_3(x_4,x_5,x_6)$ be the factors in $f(x_1,\ldots,x_6)$ of respectively x_2x_3, x_1x_3, and x_1x_2. Then $f(x_1,\ldots,x_6)$ is equal to :

$x_1x_2x_3 + x_1x_2\, g_3(x_4,x_5,x_6) + x_1x_3\, g_2(x_4,x_5,x_6) + x_2x_3\, g_1(x_4,x_5,x_6)$ plus an expression whose (global) degree relative to x_1, x_2 and x_3 is at most 1. So, there exist boolean functions h_1, h_2, h_3, and g on F^3 such that :

$f(x_1,\ldots,x_6) =$

$(x_1+g_1(x_4,x_5,x_6))\ (x_2+g_2(x_4,x_5,x_6))\ (x_3+g_3(x_4,x_5,x_6)) + (x_1+g_1(x_4,x_5,x_6))$ $h_1(x_4,x_5,x_6)+ (x_2+ g_2(x_4,x_5,x_6))\ h_2(x_4,x_5,x_6)+ (x_3+g_3(x_4,x_5,x_6))\ h_3(x_4,x_5,x_6)+$ $g(x_4,x_5,x_6)$.

Thus, $f(x_1,\ldots,x_6)$ is equivalent to :

$x_1\ x_2\ x_3 + x_1\ h_1(x_4,x_5,x_6)+ x_2\ h_2(x_4,x_5,x_6)+ x_3\ h_3(x_4,x_5,x_6)+ g(x_4,x_5,x_6)$

up to the nonsingular affine transformation :

$(x_1,\ldots,x_6) \rightarrow (x_1+g_1(x_4,x_5,x_6),\ x_2+g_2(x_4,x_5,x_6),\ x_3+g_3(x_4,x_5,x_6),\ x_4,\ x_5,\ x_6)$. □

Corollary 5 *The bent functions of degree 3 on* F^6 *all belong to class* $\mathcal{D}_0^{\#}$.

Conclusion

We have now twice more classes of bent functions than we had before.

We have also obtained new generalized bent functions, but the extension to non-binary cases has only been sketched in this paper. That gives a direction in which a research may be done.

Acknowledgement

We wish to thank J. Wolfmann for having drawn our attention to Dillon's remark.

References

[1] C. Carlet, *Codes de Reed-Muller, codes de Kerdock et de Preparata , thèse* , publication du LITP n° 90.59 (1990), Institut Blaise Pascal, Université Paris 6, 4 place Jussieu, 75005 Paris, France.

[2] C. Carlet, *A transformation on boolean functions, its consequences on some problems related to Reed-Muller codes* , EUROCODE '90, Lecture Notes in Computer Science 514, 42-50 (1991).

[3] C. Carlet, *Partially Bent Functions* , Designs, Codes and Cryptography, 3, 135-145 (1993) , presented at Crypto'92, Santa Barbara, USA.

[4] J. F. Dillon, *Elementary Hadamard Difference Sets*, Ph. D. Thesis, Univ. of Maryland (1974).

[5] J. F. Dillon, *Elementary Hadamard Difference Sets*, in Proc. Sixth S-E Conf. Comb. Graph Theory and Comp., p 237-249, F. Hoffman et al. (Eds), Winnipeg Utilitas Math (1975)

[6] P. V. Kumar, R. A. Scholtz, and L. R. Welch, *Generalized Bent Functions and their Properties*, Journal of Combinatorial Theory, Series A 40, 90-107 (1985)

[7] F. J. Mac Williams & N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland 1977.

[8] Kaisa Nyberg, *Constructions of Bent Functions and Difference Sets*, EUROCRYPT'90, Lecture Notes in Computer Science 473, 151-160 (1991).

[9] O. S. Rothaus, *On Bent Functions* , J. Comb. Theory, 20A, 300- 305 (1976)