Partially-bent functions

C. Carlet[1]
INRIA, Domaine de Voluceau, Rocquencourt,
Bat 10, BP 105, 78153 Le Chesnay Cedex, FRANCE

Abstract

We study a conjecture stated in [6] about the numbers of non-zeros of, respectively, the auto-correlation function and the Walsh transform of the function $(-1)^{f(x)}$, where $f(x)$ is any boolean function on $\{0,1\}^n$. The result that we obtain leads us to introduce the class of partially-bent functions. We study within these functions the propagation criterion. We characterize those partially-bent functions which are balanced and prove a relation between their number (which is unknown) and the number of non-balanced partially-bent functions on $\{0,1\}^{n-1}$. Eventually, we study their correlation immunity .

1 Introduction

The study of the properties of the substitution transformations of DES has resulted in nonlinearity criteria for boolean functions. Perfect nonlinear boolean functions, also called *bent functions*, are defined to be at maximum Hamming distance from affine functions. Those functions, of great importance in cryptography, seem to be rare, and very few are known. They are neither balanced nor correlation-immune. So, it seems useful to define a larger class of boolean functions, containing balanced functions, and preserving a high level of nonlinearity. That is what this paper obtains through the proof of a conjecture stated in [6]. The class of functions that we obtain is also a superclass of the class of quadratic functions. It shares with this class all its nice properties relative to the propagation criterion, the balancedness and the correlation immunity.

n is a positive integer, $G = \{0,1\}^n$.
The dot product on G is defined by :

$$\forall x = (x_1, \ldots, x_n), s = (s_1, \ldots, s_n) \in G \quad x \cdot s = x_1 s_1 + \ldots + x_n s_n \in \{0,1\}$$

where the operations on $\{0,1\}$ are the usual operations on $GF(2)$.

[1] Université de Picardie, France

E.F. Brickell (Ed.): Advances in Cryptology - CRYPTO '92, LNCS 740, pp. 280-291, 1993.

Let f be a real-valued function on G. The Walsh (or Hadamard) transform of $f(x)$ is the function on G :

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

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

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

It satisfies the Parseval's relation (cf.[5], p.416, corollary 3 or the lemma below) :

$$\sum_{s \in G} (\hat{F}(s))^2 = 2^{2n}.$$

f is kth-order correlation-immune if (cf.[1], [9]) :
$\hat{F}(s) = 0 \quad 1 \leq w(s) \leq k$ (where $w(s)$ denotes the Hamming weight of s).
The auto-correlation function of F is defined by :

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

f satisfies the propagation criterion $PC(k)$ of degree $k \quad (1 \leq k \leq n)$ if :

$$\hat{r}(s) = 0 \quad 1 \leq w(s) \leq k.$$

There exists functions satisfying $PC(n)$ if and only if n is even (cf.[4]). In that case, any boolean function f satisfies $PC(n)$ if and only if, for any element s of G, the number $\hat{F}(s)$ is equal to : $\pm 2^{n/2}$ (cf.[4] or the lemma below). Such functions are called bent. According to Parseval's relation, the bent functions are those functions which are at maximum Hamming distance from affine functions.

The definition of bent functions is invariant under any linear isomorphism, and we may define the bent functions on any $GF(2)$-space E of even dimension as the functions satisfying :

$\sum_{x \in E} (-1)^{f(x)+f(x+s)} = 0, \forall s \in E, s \neq 0$ or equivalently :

$$\sum_{x \in E} (-1)^{f(x)+x \cdot s} = \pm\sqrt{|E|} \quad \forall s \in E.$$

In [6], the authors conjecture that the numbers of zeros $N_{\hat{r}}$ and $N_{\hat{F}}$ of the functions $\hat{r}$ and $\hat{F}$ associated with any boolean function satisfy :

$$(2^n - N_{\hat{r}})(2^n - N_{\hat{F}}) \geq 2^n$$

and that equality holds only for functions of order 2 (that are functions whose algebraic normal forms have degrees at most 2 : we will call them quadratic) or satisfying $PC(n)$ or $PC(n-1)$. At Las Vegas Conference on Finite Fields, they changed the second part of their conjecture in : "equality holds only for functions of order 2 or satisfying $PC(n)$ (n even) or such that $N_{\hat{r}} = 2^n - 2$ (n odd)".

In section 2, we prove that the first part of that conjecture : $(2^n - N_{\hat{r}})(2^n - N_{\hat{F}}) \geq 2^n$ is true. We characterize those functions for which equality holds. We call these functions partially-bent for they are related to bent functions (cf. the theorem below). Any quadratic function is partially-bent.

In section 3, we study those partially-bent functions which satisfy $PC(k)$, those which are balanced, kth-order correlation-immune (we deduce that both versions of the second part of the conjecture are false). We prove that the number of partially-bent balanced functions on G is equal to the number of partially-bent non-balanced functions on $\{0,1\}^{n-1}$, times $(2^n - 1)$. All the results of that section hold for quadratic functions, and we deduce that there are more balanced quadratic functions than non-balanced quadratic functions on G if and only if n is odd.

2 Partially-bent functions

Let f be any boolean function on G, let us recall that the functions $\hat{r}$ and $\hat{F}$ defined in section 1 are related to each other the following way :

Lemma 2.1 *The Walsh transform of the function $\hat{r}$ is equal to the function $\hat{F}^2$:*

$$\forall t \in G, \sum_{s \in G} \hat{r}(s)(-1)^{s \cdot t} = (\hat{F}(t))^2.$$

Proof: According to the definition of the autocorrelation function, we have :

$$\forall t \in G, \sum_{s \in G} \hat{r}(s)(-1)^{t \cdot s} = \sum_{s \in G} \left(\sum_{x \in G} (-1)^{f(x)+f(x+s)+t \cdot s} \right) = \sum_{x \in G} \left(\sum_{s \in G} (-1)^{f(x)+f(x+s)+t \cdot s} \right).$$

Since G is invariant under any translation, we may replace s by $x+s$ in the second sum. We obtain :

$$\sum_{s\in G}\hat{r}(s)(-1)^{t\cdot s}=\sum_{x\in G}\left(\sum_{s\in G}(-1)^{f(x)+f(s)+t\cdot(x+s))}\right)=\left(\sum_{x\in G}(-1)^{f(x)+t\cdot x}\right)\left(\sum_{s\in G}(-1)^{f(s)+t\cdot s}\right)$$

$$=\left(\sum_{x\in G}(-1)^{f(x)+t\cdot x}\right)^2=(\hat{F}(t))^2. \qquad \square$$

We now prove the first part of the conjecture stated in [6] and characterize those functions for which equality holds :

Theorem 2.1 *Any boolean function f on G satisfies $(2^n-N_{\hat{r}})(2^n-N_{\hat{F}})\geq 2^n$. Equality holds if and only if :*

(i) there exists an element t in G such that for any s in G, $\hat{r}(s)$ is equal to 0 or to $(-1)^{t\cdot s}2^n$ that is if and only if :

(ii) there exists a linear form $x\to t\cdot x$ on G, two subspaces E and E' in G (E' of even dimension), such that :

- *G is the direct sum of E and E'*
- *the restriction of f to E' is bent*
- *for all x in E, and all y in E', $f(x+y)$ is equal to : $f(y)+t\cdot x$.*

Proof: - Since the values of the function $\hat{r}$ all are at most equal to 2^n, we have :

$$2^n-N_{\hat{r}}\geq 2^{-n}\sum_{s\in G}\hat{r}(s)=2^{-n}(\hat{F}(0))^2.$$

The number $N_{\hat{r}}$ clearly does not change when we replace the function $f(x)$ by any of the functions $f(x)+x\cdot t$ ($t\in G$). Replacing $f(x)$ by $f(x)+x\cdot t$, we change $\hat{F}(0)$ in $\hat{F}(t)$. Thus :

$$2^n-N_{\hat{r}}\geq 2^{-n}(\hat{F}(t))^2 \quad \forall t\in G \tag{1}$$

We also have :

$$2^n-N_{\hat{F}}\geq\frac{\sum_{s\in G}(\hat{F}(t))^2}{\sup(\hat{F}(t))^2}=\frac{2^{2n}}{\sup(\hat{F}(t))^2} \tag{2}$$

Multiplying these two inequalities, we obtain :

$$(2^n-N_{\hat{r}})(2^n-N_{\hat{F}})\geq 2^n.$$

We now shall prove that if equality holds then (i) is true, if (i) is satisfied then so is (ii) and if (ii) is true then equality holds.

- If equality holds then, according to (1) and (2) :

$$2^n - N_{\hat{r}} = 2^{-n}\sup(\hat{F}(t))^2 \quad (\text{and} \quad 2^n - N_{\hat{F}} = \frac{2^{2n}}{\sup(\hat{F}(t))^2}).$$

Let $\tilde{r}$ be the auto-correlation function associated with the function $f(x) + x \cdot t$ where $(\hat{F}(t))^2$ is maximal. By applying the previous lemma to the function $f(x) + x \cdot t$, we obtain :
$\sum_{s\in G} \tilde{r}(s) = (\hat{F}(t))^2$ and therefore : $\sum_{s\in G} \tilde{r}(s) = 2^n(2^n - N_{\hat{r}}) = \sum_{s\in G/\tilde{r}(s)\neq 0} 2^n$.
Thus : $\forall s \in G, \tilde{r}(s) = 0$ or 2^n. We have : $\forall s \in G, \tilde{r}(s) = (-1)^{t\cdot s}\hat{r}(s)$, and (i) is true.

- If (i) is true, then let E be the set of all the elements x of G such that :
$\hat{r}(x) = (-1)^{t\cdot x}2^n$ that is $\forall s \in G, f(x+s) = f(s) + x \cdot t$.
E is clearly a subspace of G. Let E' be any subspace of G such that G is the direct sum of E and E'. Then :

$\forall v \in E', v \neq 0 \Rightarrow v \notin E \Rightarrow \hat{r}(v) = 0 \Rightarrow$

$$\sum_{x\in E}\sum_{y\in E'}(-1)^{f(y)+f(y+v)} = |E|\sum_{y\in E'}(-1)^{f(y)+f(y+v)} = 0.$$

Thus (ii) is satisfied.

- Suppose (ii) is true. We may without loss of generality suppose that $t = 0$ since changing the value of t does not change $N_{\hat{r}}$ or $N_{\hat{F}}$. Then, the value of $f(x+y)$ $(x \in E, y \in E')$ does not depend on x, and we have :

$$\forall s = u + v, u \in E, v \in E', \hat{r}(s) = |E|\sum_{y\in E'}(-1)^{f(y)+f(y+v)} = \begin{cases} 0 \quad \text{if } s \notin E \quad (v \neq o) \\ |E||E'| = 2^n \text{ otherwise} \end{cases}$$

$$2^n - N_{\hat{r}} = |E| \text{ and } \forall s \in G, \hat{F}^2(s) = \sum_{x\in G}\hat{r}(x)(-1)^{s\cdot x} = \sum_{x\in E} 2^n(-1)^{s\cdot x} = \begin{cases} 0 \text{ if } s \notin E^\perp \\ 2^n|E| \text{ otherwise} \end{cases}$$

where $E^\perp = \{s \in G/\forall x \in E, s \cdot x = 0\}$.
So, $2^n - N_{\hat{F}} = |E^\perp|$ and $(2^n - N_{\hat{r}})(2^n - N_{\hat{F}}) = 2^n$. □

REMARK :
1) We have in fact : $\forall x \in E, \forall y \in G, f(x+y) = f(y) + t \cdot x$

2) We have proved :

$$\frac{2^n - N_{\hat{f}}}{2^n} \geq \sup_t \left(\frac{\hat{F}(t)}{2^n}\right)^2 \geq \frac{1}{2^n - N_{\hat{F}}},$$

which shows the trade-offs between the highest correlation to linear functions (in the middle), a certain measure of correlation immunity (on the right) and the non-vanishing of the auto-correlation function.

Definition 2.1 *A function f which satisfies the equality $(2^n - N_{\hat{f}})(2^n - N_{\hat{F}}) = 2^n$ is called partially-bent.*

Let f be a partially-bent function, E and E' two linear subspaces of G such that G is the direct sum of E and E', f is bent on E' and $f(x+y) = f(y) + t.x$, $x \in E, y \in E'$.
Let φ_f be the function defined on $G \times G$ by : $\varphi_f(u,v) = f(0) + f(u) + f(v) + f(u+v)$.
Then : $\forall x, x' \in E, \forall y, y' \in E', \varphi_f(x+y, x'+y') = \varphi_f(y, y')$. Since $f\,|_{E'}$ is bent , the restriction of φ_f to $E' \times E'$ is non-degenerate, and :

$$(\varphi_f(x+y, v) = 0 \quad \forall v \in G) \Leftrightarrow (y = 0).$$

E is the set of all the elements u of G such that $\varphi_f(u,v) = 0 \quad \forall v \in G$.
Thus E is unique.
Clearly, E' is not.
If E has dimension $n - 2h$, then t may take 2^{2h} values since the values of the linear form $x \to t \cdot x$ are fixed only on E.

Definition 2.2 *Let f be a partially-bent function, φ_f be the function defined on $G \times G$ by :*

$$\varphi_f(u,v) = f(0) + f(u) + f(v) + f(u+v).$$

The linear space $E = \{u \in G / \varphi_f(u,v) = 0 \quad \forall v \in G\}$ is called the kernel associated with f.

Any quadratic function is partially-bent (cf [6]) and the kernel associated with f is the kernel of its associated symplectic form φ_f.

REMARK :
1) The definition and the linearity of the set E are valid for any boolean function
2) Since the degree of any bent function on a linear space of dimension $2p$ is at most p, the degree of a partially-bent function is at most the half of the codimension of its kernel.

3) the set of partially-bent functions on G is not a linear space : for instance, if $n = 6$, the non-quadratic partially-bent functions are the non-quadratic bent functions which all are known (cf [7]) and it is easy to find two bent functions whose sum is neither bent nor quadratic.
4) The number of partially-bent functions seems to be difficult to obtain : it depends on the number of bent functions which is unknown (except for small values of n).
5) Let f be a boolean quadratic function on G and 1 an affine boolean function on the same space, then the following boolean function on $\{0,1\}^{n+1}$:

$$(x_1, \ldots, x_n, x_{n+1}) \in \{0,1\}^{n+1} \rightarrow f(x_1, \ldots, x_n) + x_{n+1} 1(x_1, \ldots, x_n)$$

is quadratic and any quadratic function on $\{0,1\}^{n+1}$ is of that type (thus, the number of quadratic functions on $\{0,1\}^{n+1}$ equals the number of quadratic functions on $\{0,1\}^n$, times 2^{n+1}). *That is no more true if we replace "quadratic" by "partially-bent".*

3 Properties of partially-bent functions

Since the authors conjecture in [6] that, if n is even, the non-quadratic partially-bent functions satisfy $PC(n)$, let us begin with the propagation criterion :

Proposition 3.1 *A partially-bent function f on G satisfies $PC(k)$ $(k = 1, ..., n)$ if and only if its associated kernel E only contains elements of Hamming weight $> k$, or equal to 0.*

Proof: The proof is straightforward : $\hat{r}(x) = 0$ if and only if $x \notin E$. □

Thus, the second parts of the conjectures stated by B. Preneel in [6] and at Las Vegas Conference on Finite Fields (which characterize the functions for which equality holds) are false :
if n is even, suppose that E contains an element of weight 1, then f does not satisfy $PC(1)$,
if n is odd, $2^n - N_f = |E|$ may be any odd power of 2, and if the codimension of E is at least 6, then f may be non-quadratic.

REMARK :
The number of partially-bent functions satisfying $PC(k)$ seems to be even more difficult to obtain than that of the partially-bent functions : it depends on the number of linear spaces of minimum weights greater than k, which is unknown except for small values of n.

The weight of a boolean function on G is the size of its support. A function $f(x)$ is called balanced if its weight is 2^{n-1}, that is if $\hat{F}(0) = 0$.

Proposition 3.2 *A partially-bent function f on G is balanced if and only if its restriction to its associated kernel is non-constant, that is if and only if there exists an element u in G such that :*

$$\forall x \in G, f(x+u) = f(x) + 1.$$

Otherwise, its weight is equal to $2^{n-1} \pm 2^{n-1-h} (h \in \mathbb{N}, h \leq n/2)$.

Proof: Let f be a partially-bent function, E its associated kernel, and E' a subspace such that G is the direct sum of E and E'.
$\hat{F}(0)$ is equal to : $\sum_{u \in G} (-1)^{f(u)} = \sum_{x \in E} (-1)^{t \cdot x} \sum_{y \in E'} (-1)^{f(y)}$ and these two last sums satisfy :
$\sum_{y \in E'} (-1)^{f(y)} = \pm\sqrt{|E'|} \neq 0$ since $f|_{E'}$ is bent, and : $\sum_{x \in E} (-1)^{t \cdot x} = \begin{cases} 0 \text{ if } t \notin E^{\perp} \\ |E| \quad \text{otherwise.} \end{cases}$
Thus, f is balanced if and only if t does not belong to $E^{\perp}$, that is if and only if f is non-constant on E.
In that case, let u be any element in $E \backslash t^{\perp}$, where $t^{\perp} = \{x \in G / x \cdot t = 0\}$. We have :

$$\forall x \in G, f(x+u) = f(x) + t.u = f(x) + 1.$$

Conversely, if u satisfies that property, then f is non-constant on E.

If f is non-balanced, suppose E has dimension $n - 2h$, then the sum $\sum_{u \in G} (-1)^{f(u)}$, which is equal to $2^n - 2w(f)$, is also equal to : $\pm|E|\sqrt{|E'|} = \pm 2^{n-2h} 2^h = \pm 2^{n-h}$.
So, $w(f) = 2^{n-1} \pm 2^{n-h-1}$. □

Proposition 3.3 *The number λ_n of partially-bent balanced functions on $G = \{0,1\}^n$ is equal to $(2^n - 1)$ times the number λ'_{n-1} of partially-bent non-balanced functions on $\{0,1\}^{n-1}$ $(n \geq 2)$.*

Proof: Let f be a partially-bent balanced function on G and E its associated kernel (since f is balanced, E is not the trivial space $\{0\}$).
Let E' be a subspace of G such that G is the direct sum of E and E', t any element of G such that $f(x+y) = f(y) + t.x$, $x \in E$, $y \in E'$ ($t \neq 0$ since f is balanced) and H the linear hyperplane $t^{\perp} = \{x \in G / x \cdot t = 0\}$.
Let $\phi : \{0,1\}^{n-1} \to H$ be a linear isomorphism. Then the boolean function $g = f \circ \phi$

is clearly partially-bent of associated kernel $\phi^{-1}(E)$. According to proposition 3.2, it is non-balanced since :

$$\forall x \in \phi^{-1}(E), \forall y \in \phi^{-1}(E'), g(x+y) = g(y).$$

Let us now calculate the number of (H, ϕ, g) so associated with f :
suppose E has dimension $n-2h (2h < n)$, then the set of all the possible values of t is an affine set of direction $E^{\perp}$, so its size (which is the number of possible H) is 2^{2h}.
H being chosen, there exists (cf [5]) $(2^{n-1}-1)(2^{n-1}-2)\ldots(2^{n-1}-2^{n-2})$ isomorphisms ϕ from $\{0,1\}^{n-1}$ to H, and if H and ϕ are chosen, then g is unique. So the number of (H, ϕ, g) associated with f is $2^{2h}(2^{n-1}-1)\ldots(2^{n-1}-2^{n-2})$.
Notice that the dimension of the associated kernel $\phi^{-1}(E)$ of g is $n-1-2h \geq 0$.

Let now g be any partially-bent non-balanced function on $\{0,1\}^{n-1}$, suppose its associated kernel E'' has dimension $n-1-2h$, and let H be a linear hyperplane of $\{0,1\}^n$ and ϕ an isomorphism from $\{0,1\}^{n-1}$ onto H. Let us calculate the number of partially-bent balanced functions f on G such that $g = f \circ \phi$.
The associated kernel E of f necessarily contains $\phi(E'')$, has dimension $n-2h$, and is not contained in H. So, it is equal to a linear space of the type : $\{u+v, u \in \phi(E''), v \in \{0,s\}\}$ where s is any element outside H. The number of such E is equal to the number of such elements s in $\{0,1\}^n \backslash H$, divided by the size of $\phi(E'')$, since two elements s and s' define the same set E if and only if $s+s'$ belongs to $\phi(E'')$. The number of kernels E is therefore 2^{2h}.
E being chosen, f is unique since the value of f on $E \backslash \phi(E'')$ must be equal to $f(0)+1$.
So the number of partially-bent balanced functions f on G corresponding to (H, ϕ, g) is 2^{2h} and the number λ_n of partially-bent balanced functions on G equals the number of ordered pairs (H, g) where H is any linear hyperplane and g any partially-bent non-balanced function on $\{0,1\}^{n-1}$. The number of linear hyperplanes being 2^n-1, we have $\lambda_n = (2^n-1)\lambda'_{n-1}$. □

REMARK :
1) The previous proof is valid when we restrict ourselves to the quadratic functions since f is quadratic if and only if g is quadratic.
Therefore, the number μ_n of balanced quadratic functions on G is equal to (2^n-1) times the number μ'_{n-1} of non-balanced quadratic functions on $\{0,1\}^{n-1}$ $(n \geq 2)$.
This result can be recovered by another way : the number mn is known (cf[5]) :

$$\mu_n = 2^{\binom{n}{2}+n+1} - 2 - 2\sum_{h=1}^{\left[\frac{n}{2}\right]} 2^{h(h+1)} \frac{(2^n-1)\ldots(2^{n-2h+1}-1)}{(2^{2h}-1)(2^{2h-2}-1)\ldots(2^2-1)}$$

(where [ ] denotes the integer part), and therefore equality $\mu_n = (2^n - 1)\mu'_{n-1}$ is equivalent with :

$$2^{\binom{n}{2}+n+1} - 2 - 2\sum_{h=1}^{\left[\frac{n}{2}\right]} 2^{h(h+1)} \frac{(2^n-1)\dots(2^{n-2h+1}-1)}{(2^{2h}-1)(2^{2h-2}-1)\dots(2^2-1)} =$$

$$(2^n-1)\left(2 + 2\sum_{h=1}^{\left[\frac{n-1}{2}\right]} 2^{h(h+1)} \frac{(2^{n-1}-1)\dots(2^{n-2h}-1)}{(2^{2h}-1)\dots(2^2-1)}\right).$$

That last equality is checked in [2].

2) Proposition 3 would give us a chance to evaluate the number of partially-bent balanced functions if the number of partially-bent functions was known.

That is not the case, but we have :

Proposition 3.4 *The number of balanced quadratic functions on G is greater than that of the quadratic non-balanced functions when n is odd and smaller when n is even.*

Proof: Let μ_n (respectively μ'_n) be the number of quadratic balanced (respectively non-balanced) functions on G.

Since the number of quadratic functions is $2^{\binom{n+1}{2}+1}$ (cf [5]),we have :

$$\forall n \geq 2, \mu'_n = 2^{\binom{n+1}{2}+1} - (2^n - 1)\mu'_{n-1}.$$

Let us prove by induction on n that :

$\mu_n < \mu'_n$, that is $\mu'_n > 2^{\binom{n+1}{2}}$ if n is even, $n \geq 2$

$\mu_n > \mu'_n$, that is $\mu'_n < 2^{\binom{n+1}{2}}$ if n is odd, $n \geq 3$.

That is true for $n = 2, 3$ since $\mu_2 = 6$, $\mu'_n = 10$, $\mu_3 = 70$, $\mu'_3 = 58$.

Suppose it is true for odd $n > 2$, then :

$$\begin{aligned}
\mu'_n < 2^{\binom{n+1}{2}} \Rightarrow \mu'_{n+1} &> 2^{\binom{n+2}{2}+1} - (2^{n+1}-1)2^{\binom{n+1}{2}} \\
&= 2^{\binom{n+2}{2}} + 2^{\binom{n+1}{2}} \\
\Rightarrow \mu'_{n+2} &< 2^{\binom{n+3}{2}+1} - (2^{n+2}-1)\left(2^{\binom{n+2}{2}} + 2^{\binom{n+1}{2}}\right) \\
&= 2^{\binom{n+3}{2}} - 2^{\binom{n+2}{2}} + 2^{\binom{n+1}{2}} \\
&< 2^{\binom{n+3}{2}}.
\end{aligned}$$

And the proof is complete. □

Proposition 3.5 *A partially-bent function defined by* : $\forall x \in E, \forall y \in E', f(x+y) = f(y) + t.x$ *is kth-order correlation-immune (respectively kth-order correlation-immune and balanced) if and only if* $t + E^{\perp}$ *only contains elements of Hamming weight greater than* k *or equal to 0 (respectively greater than* k*).*

Proof: We have :

$$\hat{F}(s) = \sum_{x \in E, y \in E'} (-1)^{x.t+x.s+f(y)+y.s} = \sum_{x \in E} (-1)^{x.(t+s)} \sum_{y \in E'} (-1)^{f(y)+y.s}.$$

Since f is bent on E', the sum $\sum_{y \in E'} (-1)^{f(y)+y.s}$ is different from 0.

Therefore : $\hat{F}(s) \neq 0 \Leftrightarrow s + t \in E^{\perp}$. □

REMARK :

If f is non-balanced, then we may take $t = 0$ and the condition becomes :
$E^{\perp} \backslash \{0\}$ only contains elements of Hamming weight greater than k.
According to the singleton bound (cf [5]), we then have : $\dim E^{\perp} \leq n - k$ and since the degree of the restriction of f to a subspace E' of G is bounded by $\dim E'/2$ (cf [4]), the degree of f is bounded by $(n-k)/2$.
So, there does not exist any function which would be partially-bent and kth-order correlation immune of maximal degree : the maximal degree of the kth-order correlation immune functions is $n - k$ (cf [9]).
On the contrary, there does exist partially-bent balanced k-th order correlation-immune functions of maximal degree (that degree is $n-k-1$) : see [1] or [2] for the case $k = n-3$.

4 Conclusion

The main interest of the class of quadratic functions is in its nice properties : we know the weights of the functions and we can characterize the functions which satisfy $PC(k)$, those which are balanced, kth-order correlation-immune. But the quadratic functions are of a poor interest from a cryptographic point of view since they are too simple.

The class of partially-bent functions shares the same qualities since all the properties of the quadratic functions can be generalized to the partially-bent functions (with three exceptions : it is not a linear space, we are not able to calculate its size or to give the general algebraic normal form of these functions).

The interest of this class of functions is greater from a cryptographic point of view because the partially-bent functions involve bent functions whose complexity may be great

(clearly, a partially-bent function will have a high level of nonlinearity if its associated kernel is small).

Acknowledgement

The author is grateful to Kaisa Nyberg who made an interesting remark on what the theorem proves (see the remark which follows it).

References

[1] P. CAMION, C. CARLET, P. CHARPIN AND N. SENDRIER *On correlation-immune functions*, Crypto'91, Advances in Cryptology, Lecture Notes on Computer Science, Springer Verlag n° 576.

[2] C. CARLET *Codes de Reed-Muller, codes de Kerdock et de Preparata, thèse*, publication du LITP, Institut Blaise Pascal, Université Paris 6, n° 90.59 (1990).

[3] 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 (1991).

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

[5] F. J. MAC WILLIAMS & N. J. A. SLOANE *The theory of error correcting codes*, North Holland 1977.

[6] B. PRENEEL, R. GOVAERTS AND J. VANDEWALLE *Boolean Functions Satisfying Higher Order Propagation Critereia* Eurocrypt'91, Lecture Notes in Computer Science 547 p 141-152 also presented at Las Vegas Int. Conf. on Finite Fields and Adv. in Com. and Comp. 1991.

[7] O. S. ROTHAUS *On bent functions*, J. Comb. Theory, 20A (1976) 300- 305.

[8] T. SIEGENTHALER *Correlation-immunity of nonlinear combining functions for cryptographic applications*, IEEE on Inf. Theory, vol IT-30, n° 5, Sept. 84.

[9] G.-Z. XIAO & J. L. MASSEY *A spectral characterization of correlation-immune combining functions*, IEEE, Vol 34, n° 3, May 88.