On the Walsh-Fourier analysis of Boolean functions

Michel Mitton
SGDN/DCSSI/SDS/Crypto. Lab.
51 boulevard de la Tour-Maubourg
75700 Paris-07 SP, France
e-mail: michel.mitton@sgdn.pm.gouv.fr

January 18, 2006

Abstract

From the representation of Boolean functions based on the Cayley graph adjacency matrix, we evaluate, for each Boolean function, the product of all the values of his Walsh spectrum. An application to the extremal balanced Boolean functions is given.

Keywords

Boolean functions, covering radius, balanced covering radius, Walsh and Fourier transforms, non-linearity, Cayley graph.

1 Introduction

This paper investigates the harmonic analysis of Boolean functions, more precisely a new property of the Walsh-Fourier spectrum of these functions.

For each Boolean function, our problem is to evaluate the product of all the Walsh-Fourier spectrum values because the parity of this product is linked to the weight of the function, and so, perhaps could gives us some new information on the weight parities of the maximally nonlinear Boolean functions.

This calculus uses the adjacency matrix of the Cayley graph of the Boolean function. With this tool, the Walsh-Fourier spectrum of a Boolean function can be viewed as the set of the eigenvalues of the adjacency matrix of his Cayley graph, and this property facilitates the solution of our problem.

2 Preliminaries: basic définitions and notation

In this paper, the finite field $(\mathbf{Z}/2\mathbf{Z}, \oplus, .)$ with its additive and multiplicative laws will be denoted by $\mathbf{F}_2$ and the $\mathbf{F}_2-$algebra of Boolean functions in n variables will be denoted by $\mathcal{F} = \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$.

The additive law $\oplus$ on $\mathbf{F}_2$ is extended from componants to define the additive law $\oplus$ on $\mathbf{F}_2^n$ by $x \oplus y = (x_0 \oplus y_0, ..., x_{n-1} \oplus y_{n-1})$ with $x, y \in \mathbf{F}_2^n$.

For $f \in \mathcal{F}$ and $a \in \mathbf{F}_2$, recall that $f^{-1}(a)$ is the set defined by $f^{-1}(a) = \{u \in \mathbf{F}_2^n |\ f(u) = a\}$.

We will use $\#E$ to denote the number of elements of the set E. The weight $wt(f)$ of $f \in \mathcal{F}$ is defined by $wt(f) = \#f^{-1}(1)$.

A function $f \in \mathcal{F}$ is called *balanced* if $\#f^{-1}(0) = \#f^{-1}(1) = 2^{n-1}$.

The Hamming distance between f and g defined by $\#\left(f \oplus g\right)^{-1}(1)$ will be denoted by $d(f, g)$.

$W_f(a)$ is the Walsh spectrum of $f \in \mathcal{F}$ to a point
$a = (a_0, ..., a_{n-1}) \in \mathbf{F}_2^n$ defined by

$$W_f(a) = \sum_{x \in \mathbf{F}_2^n} f(x)(-1)^{<a,x>}. \tag{1}$$

In this formula, the sum on the right is calculated in $\mathbf{Z}$, and $< a, x >= a_0x_0 \oplus ... \oplus a_{n-1}x_{n-1}$ is the scalar product on $\mathbf{F}_2^n$.

In the sequel, δ_a^b is the Kronecker's symbol, and we will use the notation

$$W_f^*(a) = 2^{n-1}\delta_0^a - W_f(a). \tag{2}$$

Between Walsh and Fourier transforms, we have the relation $2W_f^* = \hat{f}$ with $\hat{f}(a) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+<a,x>}$.

Each $f \in \mathcal{F}$ verifies the important Parseval's relation

$$\sum_{a \in \mathbf{F}_2^n} (W_f^*(a))^2 = 2^{2(n-1)}. \tag{3}$$

Let K be a field. If $X = (x_0, ..., x_{n-1}) \in K^n$ is an arbitrary vector, we denote $(X)_i = x_{i-1}$ the i th componant of X for each $i \in [1, n]$.

In [1][2], the Walsh-Fourier analysis is viewed as a Cayley graph adjacency matrix eigenvalue problem.

For $f \in \mathcal{F}$, we consider the set $f^{-1}(1)$ and the following graph G_f where the vertex set is $\mathbf{F}_2^n$, and the edge set is defined by

$$\left\{(a, b) \in \mathbf{F}_2^n \times \mathbf{F}_2^n | a \oplus b \in f^{-1}(1)\right\}.$$

This definition implies that $G_f = G(\mathbf{F}_2^n, f^{-1}(1))$ is the Cayley graph of $\mathbf{F}_2^n$ with respect to the Cayley set $f^{-1}(1)$, and the symmetric matrix $M_f = (m_{i,j})_{i,j \in [0,2^n-1] \times [0,2^n-1]}$ with $m_{i,j} = f(i \oplus j)$ is the adjacency matrix of G_f, where we identify $[0, 2^n - 1]$ with $\mathbf{F}_2^n$.

For a detailed study on this topic, see [1] and [2].

We denote $Sym(E)$ the group of permutations on the set E, and for each $\sigma \in Sym(E)$, $\varepsilon(\sigma)$ the parity $+1$ or -1 of σ.

We denote $m|n$ if the integer m divides the integer n. $|x|$ is the absolute value of the real number x.

The affine function defined by $f(x) =< \alpha, x > \oplus\lambda$, with $\alpha, x \in \mathbf{F}_2^n$ and $\lambda \in \mathbf{F}_2$, will be denoted by $l_\alpha \oplus \lambda$.

The semi-norm on $\mathcal{F}$ defined by $\min_{\alpha\in\mathbf{F}_2^n,\ \lambda\in\mathbf{F}_2} d(f, l_\alpha \oplus \lambda)$, will be denoted by $\delta(f)$.

It is easy to prove that $\delta(f) = 2^{n-1} - \max_{a\in\mathbf{F}_2^n} |W_f^*(a)|$.

The integer $\max_{f\in\mathcal{F}} \delta(f)$ will be denoted by $\rho(n)$. In the theory of error-correcting codes [4], $\rho(n)$ is called the covering radius of the first order Reed-Muller code $R(1, n)$ of length 2^n.

The integer $\max_{f\ balanced} \delta(f)$ will be denoted by $\rho_B(n)$ and will be called the balanced covering radius in dimension n. Of course, we have $\rho_B(n) \leq \rho(n)$.

A function $f \in \mathcal{F}$ will be called *maximally nonlinear* (resp. *extremal balanced)* if $\delta(f) = \rho(n)$ (resp. $\delta(f) = \rho_B(n)$). When n is even, *bent functions* [3][4][5] are defined as Boolean functions f having uniform Walsh spectrum $|W_f^*(a)| = 2^{\frac{n}{2}-1}$ for each $a \in \mathbf{F}_2^n$. For even n, it is easy to prove that f is maximally nonlinear if and only if f is bent.

The subset of $\mathcal{F}$ containing all the maximally nonlinear (resp. extremal balanced) functions will be denoted by $C(n)$ (resp. $E(n)$).

For a study on related topics, see [6].

3 Evaluation of the Walsh spectra product

Our problem is the evaluation of the product

$$\prod_{a\in\mathbf{F}_2^n} W_f(a) \tag{4}$$

considered as a tool for the study of the parity of f.

In fact, we prove a more general result. Namely we obtain the polynomial expression of

$$P(X) = \prod_{a\in\mathbf{F}_2^n} (X - W_f(a)).$$

So, we obtain (4) as corollary.

We have the following result:

Theorem 1 *For each $f \in \mathcal{F}$, each $j \in [1, 2^n]$ and each $i_1, ..., i_j$ verifying $0 \leq i_1 < ... < i_j \leq 2^n - 1$, if we denote*

$$S(i_1,...,i_j) = \left\{ \begin{array}{c} \sigma \in Sym(\mathbf{F}_2^n) | \forall i \notin \{i_1,...,i_j\}, \sigma(i) \neq i \text{ and } f(i \oplus \sigma(i)) = 1, \\ \text{and } \forall i \in \{i_1,...,i_j\} \ \sigma(i) = i \end{array} \right\} \tag{5}$$

and

$$S_0 = \{\sigma \in Sym(\mathbf{F}_2^n) | \forall i \in [0, 2^n - 1] \ \sigma(i) \neq i \text{ and } f(i \oplus \sigma(i)) = 1\}, \tag{6}$$

we have

$$\prod_{a \in \mathbf{F}_2^n} (X - W_f(a)) = \sum_{j=1}^{2^n} \left[\sum_{0 \leq i_1 < ... < i_j \leq 2^n - 1} \left(\sum_{\sigma \in S(i_1,...,i_j)} \varepsilon(\sigma) \right) \right] (f(0) - X)^j + \sum_{\sigma \in S_0} \varepsilon(\sigma). \tag{7}$$

Proof. Consider the adjacency matrix M_f of the Cayley graph G_f of $f \in \mathcal{F}$. For $a \in F_2^n$, if we denote $\chi_a = {}^t\left((-1)^{<a,0>}, (-1)^{<a,1>}, ..., (-1)^{<a,2^n-1>}\right)$, it is easy to see that the vector χ_a is, for M_f , an eigenvector associated to the eigenvalue $W_f(a)$ since, for each $i \in [0, 2^n - 1]$,

$(M_f \chi_a)_{i+1} = \sum_{0 \leq j \leq 2^n - 1} f(i \oplus j)(-1)^{<a,j>}$

$= \left(\sum_{0 \leq u \leq 2^n - 1} f(u)(-1)^{<a,u>} \right) (-1)^{<a,i>}$.

Therefore $M_f \chi_a = W_f(a)\chi_a$. So, if we consider M_f as element of $M_{2^n}(\mathbf{R})$, we can consider its characteristic polynomial

$P(X) = \det_{\mathbf{R}}(M_f - XI_{2^n}) = \prod_{a \in \mathbf{F}_2^n} (X - W_f(a))$.

But, if K is an arbitrary field and if $M = (m_{i,j})_{i,j \in [1,r]}$ with $m_{i,j} \in K$, we have $\det_{\mathbf{R}}(M) = \sum_{\sigma \in Sym([1,r])} \varepsilon(\sigma) \prod_{i=1}^{r} m_{i,\sigma(i)}$. In the case $M = M_f - XI_{2^n} = (f(i \oplus j) - \delta_i^j X)_{i+1,j+1}$, we obtain

$$P(X) = \sum_{\sigma \in Sym(\mathbf{F}_2^n)} \varepsilon(\sigma) \prod_{i=0}^{2^n-1} \left[f(i \oplus \sigma(i)) - \delta_i^{\sigma(i)} X \right].$$

If we denote $\Omega_F = \{\sigma \in Sym(\mathbf{F}_2^n) | \exists i \in [0, 2^n - 1], \sigma(i) = i\}$

and $\Omega_{\overline{F}} = Sym(\mathbf{F}_2^n) - \Omega_F$, we can write

$$P(X) = \sum_{\sigma \in \Omega_F} \varepsilon(\sigma) \prod_{i=0}^{2^n-1} \left[f(i \oplus \sigma(i)) - \delta_i^{\sigma(i)} X \right] + \sum_{\sigma \in \Omega_{\overline{F}}} \varepsilon(\sigma) \prod_{i=0}^{2^n-1} \left[f(i \oplus \sigma(i)) - \delta_i^{\sigma(i)} X \right]. \tag{8}$$

When $\sigma \in \Omega_{\overline{F}}$, we have $\delta_i^{\sigma(i)} = 0$ for each i, therefore

$$P(X) = \sum_{\sigma \in \Omega_F} \varepsilon(\sigma) \prod_{i=0}^{2^n-1} \left[f(i \oplus \sigma(i)) - \delta_i^{\sigma(i)} X \right] + \sum_{\sigma \in \Omega_{\overline{F}}} \varepsilon(\sigma) \prod_{i=0}^{2^n-1} f(i \oplus \sigma(i)).$$

On the other hand, for $j \in [1, 2^n]$ and $0 \leq i_1 < ... < i_j \leq 2^n - 1$, if we denote

$$\Omega(i_1, ..., i_j) = \{\sigma \in Sym(\mathbf{F}_2^n) | \forall k \in [1, j]\ \sigma(i_k) = i_k, \text{and } \sigma(l) \neq l\ \forall l \notin [i_1, ..., i_j]\},$$

we have

$$\Omega_F = \overset{\circ}{\bigcup_{1 \leq j \leq 2^n}} \left(\overset{\circ}{\bigcup_{0 \leq i_1 < ... < i_j \leq 2^n - 1}} \Omega(i_1, ..., i_j) \right)$$

so we can write

$$\sum_{\sigma \in \Omega_F} \varepsilon(\sigma) \prod_{i=0}^{2^n-1} \left[f(i \oplus \sigma(i)) - \delta_i^{\sigma(i)} X \right] =$$

$$\sum_{j=1}^{2^n} \left[\sum_{0 \leq i_1 < ... < i_j \leq 2^n - 1} \left(\sum_{\sigma \in \Omega(i_1, ..., i_j)} \varepsilon(\sigma) \prod_{i=0}^{2^n-1} \left[f(i \oplus \sigma(i)) - \delta_i^{\sigma(i)} X \right] \right) \right].$$

For each $\sigma \in \Omega(i_1, ..., i_j)$, we have $\prod_{i=0}^{2^n-1} \left[f(i \oplus \sigma(i)) - \delta_i^{\sigma(i)} X \right] =$

$\left(\prod_{k=1}^{j} \left[f(i_k \oplus \sigma(i_k)) - \delta_{i_k}^{\sigma(i_k)} X \right] \right) \left(\prod_{i \notin \{i_1, ..., i_j\}} \left[f(i \oplus \sigma(i)) - \delta_i^{\sigma(i)} X \right] \right)$ and,

since $\sigma(i_k) = i_k$ for $k \in [1, j]$, and $\sigma(i) \neq i$ for $i \notin \{i_1, ..., i_j\}$,

$\prod_{i=0}^{2^n-1} \left[f(i \oplus \sigma(i)) - \delta_i^{\sigma(i)} X \right] = (f(0) - X)^j \left(\prod_{i \notin \{i_1, ..., i_j\}} f(i \oplus \sigma(i)) \right)$.

From (8), if we denote for $j \in [1, 2^n]$

$$\Omega^*(i_1, ..., i_j) = \{\sigma \in \Omega(i_1, ..., i_j) | \forall l \notin [i_1, ..., i_j]\ f(l \oplus \sigma(l)) = 1\ \},$$

and $\Omega_0^* = \left\{ \sigma \in \Omega_{\bar{F}} | \forall i \in [0, 2^n - 1], f(i \oplus \sigma(i)) = 1 \right\}$, we obtain finally

$$\begin{aligned} P(X) &= \sum_{j=1}^{2^n} \left[\sum_{0 \leq i_1 < ... < i_j \leq 2^n - 1} \left(\sum_{\sigma \in \Omega^*(i_1, ..., i_j)} \varepsilon(\sigma) \right) \right] (f(0) - X)^j + \\ &\quad \sum_{\sigma \in \Omega_0^*} \varepsilon(\sigma) \end{aligned}$$

which proves the theorem. ■

From this result, we deduce immediately the value of the searched product (4):

Corollary 2 *For each $f \in \mathcal{F}$, if we denote*

$$S(f) = \{\sigma \in Sym(\mathbf{F}_2^n) | \forall a \in \mathbf{F}_2^n,\ f(a \oplus \sigma(a)) = 1\} \tag{9}$$

we have

$$\prod_{a \in \mathbf{F}_2^n} W_f(a) = \sum_{\sigma \in S(f)} \varepsilon(\sigma). \tag{10}$$

In particular

$$\prod_{a\in\mathbf{F}_2^n} |W_f(a)| \leq \#S(f). \tag{11}$$

Proof. Firstly, remark that we have $S_0 \subset S(f)$.

From Theorem 1 and from the property $f(0)^j = f(0)$ for each $j \geq 1$, we deduce

$$P(0) = \prod_{a\in\mathbf{F}_2^n} W_f(a) = f(0)\left\{\sum_{j=1}^{2^n}\left[\sum_{0\leq i_1<\ldots<i_j\leq 2^n-1}\left(\sum_{\sigma\in S(i_1,\ldots,i_j)}\varepsilon(\sigma)\right)\right]\right\} + \sum_{\sigma\in S_0}\varepsilon(\sigma).$$

When $f(0) = 0$, we obtain $\prod_{a\in\mathbf{F}_2^n} W_f(a) = \sum_{\sigma\in S_0}\varepsilon(\sigma)$. But as $f(0) = 0$, each $\sigma \in S(f)$ is such that, for each $a \in \mathbf{F}_2^n$, $\sigma(a) \neq a$.

Therefore, in this case we have also $S(f) \subset S_0$, so $S(f) = S_0$ and the corollary is proved in this first case.

Suppose now $f(0) = 1$. In this case we obtain

$$\prod_{a\in\mathbf{F}_2^n} W_f(a) = \sum_{j=1}^{2^n}\left[\sum_{0\leq i_1<\ldots<i_j\leq 2^n-1}\left(\sum_{\sigma\in S(i_1,\ldots,i_j)}\varepsilon(\sigma)\right)\right] + \sum_{\sigma\in S_0}\varepsilon(\sigma).$$

But we have $S(f) = \{\sigma|\forall i \in \mathbf{F}_2^n, \sigma(i) \neq i \text{ and } f(i\oplus\sigma(i)) = 1\} \overset{\circ}{\bigcup}_{1\leq j\leq 2^n} [\overset{\circ}{\bigcup}_{1\leq i_1<\ldots<i_j\leq 2^n-1}$
$\{\sigma|\forall k \in [1,j]\sigma(i_k) = i_k, \text{ and }, \forall i \notin [i_1,\ldots,i_j]\sigma(i) \neq i \text{ and } f(i\oplus\sigma(i)) = 1\}]$
$= S_0 \overset{\circ}{\bigcup}_{1\leq j\leq 2^n} [\overset{\circ}{\bigcup}_{1\leq i_1<\ldots<i_j\leq 2^n-1} S(i_1,\ldots,i_j)]$
so we obtain
$\prod_{a\in\mathbf{F}_2^n} W_f(a) = \sum_{\sigma\in S(f)}\varepsilon(\sigma)$, and the first part of the corollary is also proved when $f(0) = 1$.

From this, we deduce $\prod_{a\in\mathbf{F}_2^n} |W_f(a)| = \left|\prod_{a\in\mathbf{F}_2^n} W_f(a)\right| = \left|\sum_{\sigma\in S(f)}\varepsilon(\sigma)\right| \leq$
$\sum_{\sigma\in S(f)} |\varepsilon(\sigma)| = \#S(f)$. ■

For each $f \in \mathcal{F}$, remark that we have $\#f^{-1}(1) \leq \#S(f)$:
this inequality is firstly verified for $f = 0$ and secondly, when $f \neq 0$ and for each $\lambda \in f^{-1}(1)$, the function $a \longmapsto \sigma_\lambda(a) = a \oplus \lambda \in Sym(\mathbf{F}_2^n)$ and verifies $f(a\oplus\sigma_\lambda(a)) = 1$ for each $a \in \mathbf{F}_2^n$. Therefore $\sigma_\lambda \in S(f)$ and, finally, the function $\Lambda : f^{-1}(1) \longrightarrow S(f)$ defined by $\Lambda(\lambda) = \sigma_\lambda$ is injective.

We deduce from Theorem 1, another proposition which uses the following lemma:

Lemma 3 *For each $f \in \mathcal{F}$,*
$(\exists b \in \mathbf{F}_2^n,\ W_f(b)$ *is even*$) \Longleftrightarrow (\forall a \in \mathbf{F}_2^n, W_f(a)$ *is even*$)$

Proof. Suppose that $W_f(b)$ is even for $b \in \mathbf{F}_2^{\mathrm{n}}$. From the definition (1) and using the formula $(-1)^u = 1 - 2u$ when $u \in \mathbf{F}_2$, we obtain for each $a \in \mathbf{F}_2^{\mathrm{n}}$,

$$\begin{aligned} W_f(a) &= \sum_{x \in \mathbf{F}_2^{\mathrm{n}}} f(x)(-1)^{<b,x>}(-1)^{<a \oplus b,x>} \\ &= \sum_{x \in \mathbf{F}_2^{\mathrm{n}}} f(x)(-1)^{<b,x>}(1 - 2 < a \oplus b, x >) \\ &= W_f(b) - 2\sum_{x \in \mathbf{F}_2^{\mathrm{n}}} f(x)(-1)^{<b,x>} < a \oplus b, x > \end{aligned}$$

therefore we have $W_f(a)$ even and the lemma is proved. ■

Using this lemma, we obtain

Proposition 4 *For each $f \in \mathcal{F}$, $wt(f)$ is even if and only if*

$$\sum_{\sigma \in S(f)} \varepsilon(\sigma) = 0 \text{ or } 2^{2^n} \mid \sum_{\sigma \in S(f)} \varepsilon(\sigma). \tag{12}$$

In particular, if $wt(f)$ is even and $\sum_{\sigma \in S(f)} \varepsilon(\sigma) \neq 0$, then $\#S(f) \geq 2^{2^n}$.

Proof. If $wt(f)$ is even, since $wt(f) = \#f^{-1}(1) = W_f(0)$, we have also, from the Lemma 3, $W_f(a)$ even for each $a \in \mathbf{F}_2^{\mathrm{n}}$. We deduce from this that, if $\prod_{a \in \mathbf{F}_2^{\mathrm{n}}} W_f(a) \neq 0$ then $2^{2^n} \mid \prod_{a \in \mathbf{F}_2^{\mathrm{n}}} W_f(a)$. Then, (12) results of the formula (10) of the Corollary 2.

Now suppose that we have (12). From (10) we have $\prod_{a \in \mathbf{F}_2^{\mathrm{n}}} W_f(a) = 0$ or $2^{2^n} \mid \prod_{a \in \mathbf{F}_2^{\mathrm{n}}} W_f(a)$. So, there exists $b \in \mathbf{F}_2^{\mathrm{n}}$ such that $W_f(b) = 0$ or $2 | W_f(b)$ (since $2|mn \Longrightarrow 2|m$ or $2|n$) and this assures that we have, as in the first part of the proof, $W_f(a)$ even for each $a \in \mathbf{F}_2^{\mathrm{n}}$, therefore also $W_f(0) = wt(f)$, and the proof of (12) is complete.

Now, if we have $\sum_{\sigma \in S(f)} \varepsilon(\sigma) \neq 0$ and $wt(f)$ even, (12) implies that there exists an integer u such that $\sum_{\sigma \in S(f)} \varepsilon(\sigma) = 2^{2^n} u$, therefore $\sum_{\sigma \in S(f)} |\varepsilon(\sigma)| \geq 2^{2^n} |u|$, with $u \neq 0$, and the result is proved. ■

Proposition 5 *For each $f \in \mathcal{F}$ with $wt(f)$ even,*

$$\text{if } \#S(f) < wt(f)2^{2^n - 1} \text{ then } \sum_{\sigma \in S(f)} \varepsilon(\sigma) = 0.$$

Proof. From the formula (10) of the Corollary 2, $f = 0$ implies $W_f(0) = 0$ and then $\sum_{\sigma \in S(f)} \varepsilon(\sigma) = 0$.

So, we can suppose $f \neq 0$. In this case, we have $W_f(0) = wt(f) \neq 0$. This property, jointly with the inequality (11) of the Corollary 2, implies $\prod_{a \in \mathbf{F}_2^n - \{0\}} |W_f(a)| \leq \frac{\#S(f)}{wt(f)}$, so there exists $b \in \mathbf{F}_2^n - \{0\}$ such that $|W_f(b)| \leq \left(\frac{\#S(f)}{wt(f)}\right)^{\frac{1}{2^n-1}}$.

Using now the hypothesis $\#S(f) < wt(f)2^{2^n-1}$, we obtain $\left(\frac{\#S(f)}{wt(f)}\right)^{\frac{1}{2^n-1}} < 2$ and necessarily $|W_f(b)| < 2$. But $wt(f) = W_f(0)$ is even, therefore from Lemma 3 we must also have $W_f(b)$ even.

This last property, jointly with $|W_f(b)| < 2$, implies $W_f(b) = 0$ and finally, from the formula (10) of Corollary 2, $\sum_{\sigma \in S(f)} \varepsilon(\sigma) = 0$. ■

4 Application to the extremal balanced Boolean functions

We will use the two following results:

Lemma 6 *For each $f \in \mathcal{F}$ and each $a, b \in \mathbf{F}_2^n$, $W^*_{f \oplus l_a}(b) = W^*_f(a \oplus b)$.*

Proof. We have

$2W^*_f(a) = \hat{f}(a) = \sum_x (-1)^{f(x) \oplus <a,x>} = f \hat{\oplus} l_a(0) = 2W^*_{f \oplus l_a}(0)$, so we have $W^*_f(a) = W^*_{f \oplus l_a}(0)$, and therefore also $W^*_f(a \oplus b) = W^*_{f \oplus l_{a \oplus b}}(0) = W^*_{f \oplus l_a \oplus l_b}(0) = W^*_{f \oplus l_a}(b)$. ■

Proposition 7 *For each integer n,*

$$\rho_B(n) < \rho(n) \text{ if and only if, for each } f \in C(n),\ W_f^{*-1}(0) = \emptyset. \qquad (13)$$

Proof. Remark that an equivalent statement is:

$\rho_B(n) = \rho(n)$ if and only if there exists $f \in C(n)$ such that $W_f^{*-1}(0) \neq \emptyset$. So, we can prove the proposition under this last form.

If $\rho_B(n) = \rho(n)$, there exists at least one extremal balanced function f verifying $\delta(f) = \rho_B(n) = \rho(n)$, so $0 \in W_f^{-1}(2^{n-1})$, i.e. $0 \in W_f^{*-1}(0)$.

Conversely, if $W_f^{*-1}(0) \neq \varnothing$ for $f \in C(n)$, there exists $a \in W_f^{*-1}(0)$, so $W^*_f(a) = 0$. As $W^*_f(a) = W^*_{f \oplus l_a}(0)$ (Lemma 6) and $\delta(f \oplus l_a) = \delta(f) = \rho(n)$, the function $f \oplus l_a$ is balanced and maximally nonlinear so we have $\rho(n) = \rho_B(n)$. ■

For $j = \pm 1$ and $f \in \mathcal{F}$, we denote $S_j(f) = \{\sigma \in S(f) | \varepsilon(\sigma) = j\}$. With this notation we obtain finally

Proposition 8 *For each integer n, if $\rho_B(n) < \rho(n)$, we have $\#S_1(f) \neq \#S_{-1}(f)$ for each $f \in C(n)$.*

Proof. Suppose $\rho_B(n) < \rho(n)$ and consider $f \in C(n)$.

We have from Proposition 7 $W_f(a) \neq 0$ if $a \neq 0$, and $W_f(0) \neq 2^{n-1}$. So, if $\prod_{a \in \mathbf{F}_2^n} W_f(a) = W_f(0) \left(\prod_{a \in \mathbf{F}_2^n - \{0\}} W_f(a) \right) = 0$, necessarily $W_f(0) = \#f^{-1}(1) = 0$ and then $f = 0$ which contradicts the hypothesis $f \in C(n)$ and $\rho_B(n) < \rho(n)$.

Therefore, we obtain $\prod_{a \in \mathbf{F}_2^n} W_f(a) \neq 0$ and, using the formula (10) of Corollary 2, also $\sum_{\sigma \in S(f)} \varepsilon(\sigma) \neq 0$.

But $\sum_{\sigma \in S(f)} \varepsilon(\sigma) = \sum_{\sigma \in S_1(f)} \varepsilon(\sigma) + \sum_{\sigma \in S_{-1}(f)} \varepsilon(\sigma) = \#S_1(f) - \#S_{-1}(f)$ and the proof is complete. ■

5 References

[1] A. Bernasconi, *Mathematical techniques for the analysis of Boolean functions,* Ph. D. dissertation TD-2/98, Università di Pisa-Udine, 1998.

[2] A. Bernasconi and B. Codenotti, Spectral Analysis of Boolean Functions as Graph Eigenvalue Problem, *IEEE Trans. on Computers,* Vol 48 (3) (1999), pp. 345-351.

[3] O. S. Rothaus, On "bent" functions, *J. Comb. Th. (SeriesA), Vol. 20, pp. 300-305 (1976).*

[4] F. J. Mac Williams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* Amsterdam North-Holland, 1977.

[5] J. F. Dillon, Elementary Hadamard difference sets, Ph. D. dissertation, University of Maryland, 1974.

[6] M. Mitton, On maximally non linear and extremal balanced Boolean functions, *Jour. Discr. Maths. Sciences & Crypto.,* Vol. 5 (3) (December 2002), pp.231-253.