Boolean functions of n variables and permutations on $\mathbf{F}_2^n$

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

May 29, 2006

Abstract

For each Boolean function in n variables, from the expression of the product of all its Walsh spectrum values derived in a precedent paper, we deduce a new characterization of the parity of its distance from the set of all the affine functions. This characterization uses a subset of permutations on $\mathbf{F}_2^n$, and some new properties on this subset are deduced.

Keywords
Boolean functions, Walsh and Fourier transforms, nonlinearity, permutations.

1 Introduction

In a previous paper [1], we have derived, for each integer $n \geq 1$, the following formula

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

where f is an arbitrary Boolean function, W_f the Walsh spectrum of f, and

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

From this formula, and for each Boolean function f, we obtain firstly a characterization of the parity of its distance to the set of all the $n-$variable affine functions.

This parity condition is linked to the weight parity of f so, our aim is, in a further study, to obtain new informations on the parity of f when this function is maximally nonlinear.

In a second part, some new informations on $\#S(f)$ are derived.

2 Basic definitions 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 $\mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ will be denoted by $\mathcal{F}$.

For $f \in \mathcal{F}$ and $a \in \mathbf{F}_2$, recall that $f^{-1}(a) = \{u \in \mathbf{F}_2^n | f(u) = a\}$ and $\overline{a} = a \oplus 1$.

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

The Hamming distance between f and g, defined by $\#(f \oplus g)^{-1}(1)$, 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 $< a, x >= a_0x_0 \oplus ... \oplus a_{n-1}x_{n-1}$ represents 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 $\hat{f}(a) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+<a,x>}$.

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.

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 [3], $\rho(n)$ is called the covering radius of the first Reed-Muller code $R(1, n)$ of length 2^n.

A function $f \in \mathcal{F}$ will be called *maximally nonlinear* if $\delta(f) = \rho(n)$. $C(n)$ denotes the set of maximally nonlinear functions of $\mathcal{F}$. When n is even, *Bent functions*[2][3][4] are defined as Boolean functions 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.

3 Parity of $\delta(f)$

For each $f \in \mathcal{F}$, we give a necessary and sufficient condition in order that $\delta(f)$ to be odd or even.

Theorem 1 *For each $f \in \mathcal{F}$ and each integer $n \geq 1$, if we denote*

$$S(f) = \{\sigma \in Sym(\mathbf{F}_2^n) | \forall a \in \mathbf{F}_2^n, f(a \oplus \sigma(a)) = 1\}, \tag{3}$$

$\delta(f)$ is an even (resp. odd) integer if and only if $\#S(f)$ is even (resp. odd).

Proof. We suppose $\delta(f)$ even and we denote $P = \prod_{a \in \mathbf{F}_2^n} W_f(a)$.

We have proved in [1], Corollary 2, that $\prod_{a \in \mathbf{F}_2^n} W_f(a) = \sum_{\sigma \in S(f)} \varepsilon(\sigma)$ with $S(f) = \{\sigma \in Sym(\mathbf{F}_2^n) | \forall a \in \mathbf{F}_2^n, f(a \oplus \sigma(a)) = 1\}$. Furthermore, we have remarked that $wt(f) \leq \#S(f)$.

Then, if $\#S(f) = 0$ we have necessarily $f = 0$, so we can suppose $\#S(f) \neq 0$.

In this case, if we denote $S(f) = (\sigma_i)_{1 \leq i \leq \#S(f)}$, by the formula $\prod_{a \in \mathbf{F}_2^n} W_f(a) = \sum_{\sigma \in S(f)} \varepsilon(\sigma)$ we deduce that

$$\begin{aligned} P^2 = \left(\sum_{\sigma \in S(f)} \varepsilon(\sigma) \right)^2 &= \sum_{\sigma \in S(f)} (\varepsilon(\sigma))^2 + 2(\sum_{1 \leq i < j \leq \#S(f)} \varepsilon(\sigma_i)\varepsilon(\sigma_j)) \\ &= \#S(f) + 2(\sum_{1 \leq i < j \leq \#S(f)} \varepsilon(\sigma_i)\varepsilon(\sigma_j)). \end{aligned}$$

So, we obtain P^2 even if and only if $\#S(f)$ is even.

But P^2 is even if and only if P is also even because we can write $P = 2q + r$ with $r = 0$ or $r = 1$. Then $P^2 = 4q(q + r) + r^2$, so P^2 is even if and only if $r^2 = 0$, i.e. $P = 2q$ is even. So, we have P even if and only if $\#S(f)$ even.

But, we know that if $2|mn$ then $2|m$ or $2|n$, so if P is even, there exists $a \in \mathbf{F}_2^n$ at least such that $W_f(a)$ is even. On the other hand, we have seen in [1], lemma 3, that if there exists $a \in \mathbf{F}_2^n$ such that $W_f(a)$ is even, all the values $W_f(a)$, for each $a \in \mathbf{F}_2^n$, are also even.

Finally, we have $\delta(f) = 2^{n-1} - \max_{a \in \mathbf{F}_2^n} |W_f^*(a)|$ with $W_f^*(a) = 2^{n-1}\delta_0^a - W_f(a)$, therefore $\delta(f)$ is even if and only if, for each $a \in \mathbf{F}_2^n$, $W_f^*(a)$ is even and then also $W_f(a)$. Therefore, the hypothesis $\delta(f)$ even integer is equivalent to the property P even, and consequently to the property $\#S(f)$ even, and the theorem is proved. ■

Corollary 2 *For each $f \in \mathcal{F}$ and each $n \geq 1$, $wt(f)$ is even if and only if $\#S(f)$ is even.*

If $n \geq 2$ is even and for each $f \in C(n)$, $\#S(f)$ is even.

Proof. Obvious because if $wt(f) = W_f(0)$ is even, from [1] Lemma 3, $W_f(a)$ is even for each $a \in \mathbf{F}_2^n$ and, equivalently, $\delta(f)$ is also even. Using Theorem 1, we obtain finally the first result.

Now, supppose n even and $f \in C(n)$. In this case we know that $wt(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$, so $wt(f)$ is even when $n \geq 2$, and we have proved the second result. ■

We continue with a result which clarifies the inequality $\prod_{a \in \mathbf{F}_2^n} |W_f(a)| \leq \#S(f)$ proved in [1].

Proposition 3 *For each non-null $f \in \mathcal{F}$ and each $n \geq 1$, if we denote $S(f) = (\sigma_i)_{1 \leq i \leq \#S(f)}$ and $A(f) = \sum_{1 \leq i < j \leq \#S(f)} \varepsilon(\sigma_i \sigma_j)$, we have the two following cases:*

- *$A(f) \geq 0$ if and only if $(\#S(f))^{\frac{1}{2}} \leq \prod_{a \in \mathbf{F}_2^n} |W_f(a)| \leq \#S(f)$,*
- *$A(f) \leq -1$ if and only if $\prod_{a \in \mathbf{F}_2^n} |W_f(a)| \leq (\#S(f) - 2)^{\frac{1}{2}}$.*

Proof. With the notations of this proposition, we have seen in the proof of Theorem 1 that $\prod_{a \in \mathbf{F}_2^n} W_f^2(a) = \#S(f) + 2A(f)$.

If $\#S(f) = 1$, from the definition of $A(f)$ we deduce $A(f) = 0$, so we have $\prod_{a \in \mathbf{F}_2^n} W_f^2(a) = 1$ and then $|W_f(a)| = 1$ for each $a \in \mathbf{F}_2^n$. In particular we must have $W_f(0) = 1$, i.e. $wt(f) = 1$, so there exists $\lambda \in \mathbf{F}_2^n$ such that $f = \delta_\lambda$ (for each $a \in \mathbf{F}_2^n$ $\delta_\lambda(a) = 1$ if $a = \lambda$ and $\delta_\lambda(a) = 0$ if $a \neq \lambda$). It is easy to see that $S(\delta_\lambda) = \{\sigma_\lambda\}$ where σ_λ is the permutation on $\mathbf{F}_2^n$ defined by $\sigma_\lambda(a) = a \oplus \lambda$ and we obtain finally $\prod_{a \in \mathbf{F}_2^n} |W_f(a)| \in [(\#S(f))^{\frac{1}{2}}, \#S(f)] = \{1\}$.

Consequently we can suppose $\#S(f) \geq 2$. Now if $A(f) \geq 0$, the equality $\prod_{a \in \mathbf{F}_2^n} W_f^2(a) = \#S(f) + 2A(f)$ implies $\prod_{a \in \mathbf{F}_2^n} W_f^2(a) \geq \#S(f)$, so we firstly obtain

$$(\#S(f))^{\frac{1}{2}} \leq \prod_{a \in \mathbf{F}_2^n} |W_f(a)| \leq \#S(f).$$

If $A(f) < 0$, i.e. $A(f) \leq -1$, we have $\prod_{a \in \mathbf{F}_2^n} W_f^2(a) = \#S(f) + 2A(f) \leq \#S(f) - 2$ and we secondly obtain $\prod_{a \in \mathbf{F}_2^n} |W_f(a)| \leq (\#S(f) - 2)^{\frac{1}{2}}$ which proves the proposition. ■

Remark that $f \neq 0$ jointly with $\#S(f) \geq wt(f)$ implies that, in the first case, we have $0 \notin [(\#S(f))^{\frac{1}{2}}, \#S(f)]$.

The proof of the precedent proposition implies that, in the second case, $\#S(f) \geq 2$.

We deduce from this proposition the following result.

Corollary 4 *For each non-null $f \in \mathcal{F}$ and each $n \geq 1$, if $\prod_{a \in \mathbf{F}_2^n} W_f(a) = 0$, then $A(f) \leq -1$.*

Proof. When $A(f) \geq 0$, the proposition 3 implies $\prod_{a \in \mathbf{F}_2^n} |W_f(a)| \in [(\#S(f))^{\frac{1}{2}}, \#S(f)]$ and $0 \notin [(\#S(f))^{\frac{1}{2}}, \#S(f)]$ if $f \neq 0$. ■

We obtain the following general upper bound on $\#S(f)$.

Proposition 5 *For each $f \in \mathcal{F}$ and each $n \geq 1$,*

- If $f(0) = 0, \#S(f) \leq \min(wt(f)^{2^n}, 2^n! \sum_{q=0}^{2^n} \frac{(-1)^q}{q!})$

- If $f(0) = 1, \#S(f) \leq \min(wt(f)^{2^n}, 2^n!)$.

Furthermore, if $wt(f)$ verifies $wt(f)^{2^n} = 2^n!$ or $wt(f)^{2^n} = 2^n! e^{-1}$, we have $wt(f) \sim 2^n e^{-1}$ for $n \to +\infty$.

Proof. Firstly, from Definition (3) of $S(f)$ and if we suppose $f(0) = 0$ (resp. $f(0) = 1$), it is clear that if $\sigma \in S(f)$, necessarily $\sigma(a) \neq a$ for each $a \in \mathbf{F}_2^n$ so σ is a derangement of $Sym(\mathbf{F}_2^n)$ as defined in [5], §4.2, p. 180 (resp. $S(f) \subset Sym(\mathbf{F}_2^n)$). In this case, Theorem A of [5], p. 180, gives us a first result

$$\#S(f) \leq 2^n! \sum_{q=0}^{2^n} \frac{(-1)^q}{q!} \text{ (resp. } \#S(f) \leq 2^n!). \tag{4}$$

Secondly, independently of the value $f(0)$, we can write

$$S(f) = \left\{ \sigma \in Sym(\mathbf{F}_2^n) | \forall a \in \mathbf{F}_2^n, (\sigma \oplus Id)(a) \in f^{-1}(1) \right\}.$$

So, we can consider the application $\Phi : S(f) \to \mathcal{F}(\mathbf{F}_2^n, f^{-1}(1))$ such that $\Phi(\sigma) = \sigma \oplus Id$, and the injectivity of Φ implies the second result

$$\#S(f) \leq wt(f)^{2^n}. \tag{5}$$

Finally, combining (4) and (5), we obtain the two upper bounds on $\#S(f)$ of the proposition.

Now, if $wt(f)^{2^n} = 2^n!$ (resp. $wt(f)^{2^n} = 2^n! e^{-1}$), using the Stirling formula for $n \to +\infty$ we obtain

$wt(f) = (2^n!)^{\frac{1}{2^n}} \sim [2^{n2^n} e^{-2^n} (2\pi 2^n)^{\frac{1}{2}}]^{\frac{1}{2^n}} = 2^n e^{-1} (2^{n+1}\pi)^{\frac{1}{2^n}} \sim 2^n e^{-1}$ (resp. $wt(f) = (2^n!)^{\frac{1}{2^n}} e^{-\frac{1}{2^n}} \sim 2^n e^{-1}$). ■

Remark 6 *Obviously, $\sum_{q=0}^{2^n} \frac{(-1)^q}{q!} \sim e^{-1}$ for $n \to +\infty$.*

The propositions 3 and 5 give us the possibility to clarify and improve the lower bound on $\#S(f)$ of the proposition 4 of [1] where we have proved that $\#S(f) \geq 2^{2^n}$ when jointly, $wt(f)$ is even and $\prod_{a \in \mathbf{F}_2^n} W_f(a) \neq 0$.

Proposition 7 *For* $n \geq 1$ *and for each* $f \in \mathcal{F}$ *such that* $wt(f)$ *even and* $\prod_{a\in\mathbf{F}_2^n} W_f(a) \neq 0$*, if we denote* $\lambda_n = (\sum_{q=0}^{2^n} \frac{(-1)^q}{q!})\overline{f(0)} + f(0)$*, we have the two following cases:*

$$\begin{aligned}
\text{- If } A(f) &\geq 0, \min(wt(f)^{2^n}, 2^n!\lambda_n) \geq \#S(f) \geq 2^{2^n-1}wt(f), &(6)\\
\text{- If } A(f) &\leq -1, \min(wt(f)^{2^n}, 2^n!\lambda_n) \geq \#S(f) \geq \left(2^{2^n-1}wt(f)\right)^2 + 2 &(7)
\end{aligned}$$

Proof. As $wt(f)$ is even and $\prod_{a\in\mathbf{F}_2^n} W_f(a) \neq 0$, from [1], Lemma 3, we have necessarily $|W_f(a)| \geq 2$ for each $a \in \mathbf{F}_2^n$, which implies

$$\prod_{a\in\mathbf{F}_2^n} |W_f(a)| \geq 2^{2^n-1}wt(f). \tag{8}$$

Moreover, it is clear that $f \neq 0$, so we are under the hypothesis of the proposition 3, and consequently we have two cases $A(f) \geq 0$ or $A(f) \leq -1$.

If $A(f) \geq 0$, the propositions 3 and 5 give us $\prod_{a\in\mathbf{F}_2^n} |W_f(a)| \leq \#S(f) \leq \min(wt(f)^{2^n}, 2^n!\lambda_n)$, and combining this first inequality with $\prod_{a\in\mathbf{F}_2^n} |W_f(a)| \geq 2^{2^n-1}wt(f)$, we obtain the first result.

Now, if we are in the case $A(f) \leq -1$, then $\prod_{a\in\mathbf{F}_2^n} |W_f(a)| \leq (\#S(f) - 2)^{\frac{1}{2}}$ and, from the above inequality (8), we obtain finally $(\#S(f) - 2)^{\frac{1}{2}} \geq 2^{2^n-1}wt(f)$ which, combined with Proposition 5, proves the result. ■

Corollary 8 *For each* $f \in \mathcal{F}$ *balanced such that* $\prod_{a\in\mathbf{F}_2^n} W_f(a) \neq 0$*, we have for* $n \geq 2$ *and* n *enough large,* $\min(wt(f)^{2^n}, 2^n!\lambda_n) = 2^n!\lambda_n$ *and*

$$\begin{aligned}
\text{- If } A(f) &\geq 0, \ 2^n!\lambda_n \geq \#S(f) \geq 2^{2^n+n-2}, &(9)\\
\text{- If } A(f) &\leq -1, \ 2^n!\lambda_n \geq \#S(f) \geq 2^{2(2^n+n-2)} + 2. &(10)
\end{aligned}$$

Proof. If $n \geq 2$, $wt(f) = 2^{n-1}$ is even, so we are under the hypothesis of Proposition 7. Consequently we obtain firstly $\min(wt(f)^{2^n}, 2^n!\lambda_n) \geq \#S(f)$ for each $n \geq 2$.

For $n \to +\infty$, we have seen that $(2^n!)^{\frac{1}{2^n}} \sim 2^n e^{-1}$ and

$\lim_{n\to+\infty} \lambda_n^{\frac{1}{2^n}} = \lim_{n\to+\infty} ((\sum_{q=0}^{2^n} \frac{(-1)^q}{q!})\overline{f(0)} + f(0))^{\frac{1}{2^n}} = (e^{-1}\overline{f(0)} + f(0))^0 = 1$, so we obtain $\lim_{n\to+\infty} \frac{(2^n!)^{\frac{1}{2^n}} \lambda_n^{\frac{1}{2^n}}}{2^{n-1}} = 2e^{-1} < 1$.

Denote $u_n = \frac{(2^n!)^{\frac{1}{2^n}} \lambda_n^{\frac{1}{2^n}}}{2^{n-1}}$ for $n \geq 1$. The properties $\lim_{n\to+\infty} u_n = 2e^{-1}$ and $1 - 2e^{-1} > 0$ implies the existence of an integer $N \geq 1$ such that, for each

$n \geq N$, $|u_n - 2e^{-1}| \leq 1 - 2e^{-1}$. We deduce of this last inequality $u_n \leq 1$, i.e. $\frac{(2^n!)^{\frac{1}{2^n}}\lambda_n^{\frac{1}{2^n}}}{2^{n-1}} \leq \frac{wt(f)}{2^{n-1}}$ and equivalently $(2^n!)\lambda_n \leq wt(f)^{2^n}$ for each $n \geq N$.

So, for $n \geq N$ we have necessarily $\min(wt(f)^{2^n}, 2^n!\lambda_n) = 2^n!\lambda_n$, and the upper bounds on $\#S(f)$ are proved.

Finally, the lower bounds on $\#S(f)$ results dircctly from Proposition 7 with $wt(f) = 2^{n-1}$. ■

For $n \geq 2$, say that there exits f balanced with $\prod_{a \in \mathbf{F}_2^n} W_f(a) \neq 0$ implicetely implies that $n \geq 3$ because, for $n = 2$ it is easy to see that the only existing balanced functions are the non-constant affine functions (we have $\binom{2^n}{2^{n-1}} = \binom{4}{2} = 6$ balanced functions which coincide with the $2(2^2 - 1) = 6$ non-constant affine functions $l_\alpha \oplus \lambda$ with $\lambda \in \mathbf{F}_2$ and $\alpha \in \mathbf{F}_2^n - \{0\}$).

So, if f is balanced and $n = 2$, $\prod_{a \in \mathbf{F}_2^n} W_f(a) = 0$ because, for $f = l_\alpha \oplus \lambda$ with $\alpha \in \mathbf{F}_2^n - \{0\}$ and $\lambda \in \mathbf{F}_2$ we obtain $W_f(\alpha) = \pm 2^{n-1} = \pm 2$, $W_f(0) = 2^{n-1} = 2$ and $W_f(a) = 0$ for each $a \in \mathbf{F}_2^n - \{\alpha, 0\}$.

This remark explains why (9) and (10) are not verified when $n = 2$: there exits no function verifying the hypothesis of the corollary for $n = 2$.

Furthermore, one can verify that the corollary 8 is practically applicable as soon as $n \geq 3$.

Corollary 9 *For each $f \in \mathcal{F}$ such that $wt(f)$ even and* $\prod_{a \in \mathbf{F}_2^n} W_f(a) \neq 0$,

- If $n = 2$, or $wt(f) \leq 5$ for $n = 3$, or $wt(f) \leq 4$ for each $n \geq 4$, then $A(f) \geq 0$.

- For each $n \geq 2$, if $wt(f) = 2$ then $\#S(f) = 2^{2^n}$.

Proof. By Proposition 7, if $A(f) \leq -1$ we have seen that (7) is verified, so we have $wt(f)^{2^n} \geq \left(2^{2^n - 1} wt(f)\right)^2 + 2 > \left(2^{2^n - 1} wt(f)\right)^2$. Consequently we obtain $wt(f)^{2^n - 2} > 2^{2(2^n - 1)}$, i.e. $wt(f) > 4.2^{\frac{1}{2^{n-1}-1}} > 4$ if $n \geq 2$.

If $n = 2$ then $wt(f) > 8$ which is impossible, so in this case we have $A(f) \geq 0$.

If $n = 3$ then $wt(f) > 4.2^{\frac{1}{3}} = 5.039... > 5$. So, when $wt(f) \leq 5$ the only possibility is $A(f) \geq 0$.

If $n \geq 4$ then $wt(f) > 4$, so we have again $A(f) \geq 0$ when $wt(f) \leq 4$.

Now, if $wt(f) = 2$, using Proposition 7 and the precedent result for each $n \geq 2$, we are necessarily in the case $A(f) \geq 0$ and the inequalities $wt(f)^{2^n} \geq \#S(f) \geq 2^{2^n - 1} wt(f)$ deduced of (6) proves the result. ■

4 Lower bounds on $\rho(n)$

We finish with the following proposition which give us, under the hypothesis $\rho(n) > \rho_B(n)$, lower bounds on the covering radius $\rho(n)$ using $\#S(f)$ for $f \in C(n)$.

Proposition 10 *For each integer $n \geq 2$, if $\rho(n) > \rho_B(n)$, for each $f \in C(n)$ we have the two following cases:*

- If $A(f) \geq 0$ then $\rho(n) \geq 2^{n-1} - \left(|1 - \frac{2^{n-1}}{wt(f)}|\#S(f)\right)^{\frac{1}{\#|W_f^*|^{-1}(2^{n-1}-\rho(n))}}$.

- If $A(f) \leq -1$ then $\rho(n) \geq 2^{n-1} - \left(|1 - \frac{2^{n-1}}{wt(f)}|(\#S(f)-2)^{\frac{1}{2}}\right)^{\frac{1}{\#|W_f^*|^{-1}(2^{n-1}-\rho(n))}}$.

Proof. Firstly, for each $f \neq 0$, we have

$$\prod_{a \in \mathbf{F}_2^n} |W_f^*(a)| = |1 - \frac{2^{n-1}}{wt(f)}| \prod_{a \in \mathbf{F}_2^n} |W_f(a)|$$

so, from Proposition 3, if $A(f) \geq 0$ (respectively $A(f) \leq -1$) we obtain

$$\prod_{a \in \mathbf{F}_2^n} |W_f^*(a)| \leq |1 - \frac{2^{n-1}}{wt(f)}|\#S(f) \tag{11}$$

(resp. $\prod_{a \in \mathbf{F}_2^n} |W_f^*(a)| \leq |1 - \frac{2^{n-1}}{wt(f)}|(\#S(f)-2)^{\frac{1}{2}}$).

On the other hand, if we suppose that $\rho(n) > \rho_B(n)$, each $f \in C(n)$ is such that $W_f^{*-1}(0) = \emptyset$ ([1] Proposition 7) so we have $|W_f^*(a)| \geq 1$ for each $a \in \mathbf{F}_2^n$. Furthermore if $n \geq 2$, for each $f \in C(n)$ we have $\delta(f) = \rho(n) \geq 1$, so $f \neq 0$.

Consequently, we can write

$$\prod_{a \in \mathbf{F}_2^n} |W_f^*(a)| \geq (2^{n-1} - \rho(n))^{\#|W_f^*|^{-1}(2^{n-1}-\rho(n))} \tag{12}$$

and, combining (11) (12), we obtain for each $f \in C(n)$ such that $A(f) \geq 0$ (resp. $A(f) \leq -1$),

$$|1 - \frac{2^{n-1}}{wt(f)}|\#S(f) \quad \geq \quad (2^{n-1} - \rho(n))^{\#|W_f^*|^{-1}(2^{n-1}-\rho(n))}$$

$$\text{(resp. } |1 - \frac{2^{n-1}}{wt(f)}|(\#S(f)-2)^{\frac{1}{2}} \quad \geq \quad (2^{n-1} - \rho(n))^{\#|W_f^*|^{-1}(2^{n-1}-\rho(n))}).$$

We obtain the result in the two cases by resolution of these inequations in $\rho(n)$. ■

5 References

[1] M. Mitton, On the Walsh-Fourier analysis of Boolean functions, *Jour. Discr. Maths. Sciences. & Crypto., (September 2005),* accepted.

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

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

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

[5] L. Comtet, *Advanced Combinatorics,* D. Reidel Publishing Compagny, Dordrecht, 1974.