On maximally nonlinear and extremal balanced Boolean functions

Michel Mitton
DCSSI/SDS/Crypto.Lab.
18, rue du docteur Zamenhof
92131 Issy-les-Moulineaux cedex, France
e-mail: michelmitton@compuserve.com

Abstract. We prove a new sufficient condition for a Boolean function to be extremal balanced or maximally nonlinear, in odd or even dimension. Under this condition, we deduce the balanced covering radius $\rho_B(n)$ and the covering radius $\rho(n)$. We prove some general properties about maximally nonlinear or extremal balanced functions. Finally, an application to even weights Boolean functions is given.

Keywords: Boolean functions, extremal balanced functions, maximally nonlinear functions, bent functions, covering radius, balanced covering radius, Walsh and Fourier transforms.

1 Introduction

This paper investigates the covering radius and the balanced covering radius for Boolean functions. From Rothaus [8], the covering radius is known in even dimension. The exact value of balanced covering radius is unknown in both even or odd dimension except a finite number of small dimensions, but it has been previously studied by Dobbertin [3] and Seberry, Zhang, Zheng [9] where a lower bound, which is the best achieved so far, was derived.

This problem is known to be difficult, and any new approach to it potentially brings the problem closer to its solution. In this respect, we present a new condition for the study of maximally nonlinear Boolean functions. The condition takes two forms (P) and (Q) depending on whether the functions are balanced or not, respectively. In particular, in even dimension this condition gives a new characterization of bent functions.

However, for the balanced functions in even dimension and for the maximally nonlinear functions in odd dimension, the condition is generally only sufficient and we prove that it is only verified in low dimensions. Under this condition, we compute the values of the covering and balanced covering radii. We finish with an application to even weights Boolean functions in which we link the distance to the affine functions set with the degree of the algebraic normal form of these functions.

Our approach is based on the study of the kernel of the Walsh spectrum. In Carlet [1], the size of this kernel was previously shown to be relevant in the context of partially-bent functions. It is interesting to see that it comes up again in the context of our paper.

2 Basic Definitions and Notation

In this document, the finite field $(\mathbf{Z}/2\mathbf{Z},+,.)$ with his addititive 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 $\mathcal{F}(\mathbf{F}_2^n,\mathbf{F}_2)$.

For $f\in\mathcal{F}(\mathbf{F}_2^n,\mathbf{F}_2)$ and $a\in\mathbf{F}_2$, recall that the set $f^{-1}(a)$ is 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. A function $f\in\mathcal{F}(\mathbf{F}_2^n,\mathbf{F}_2)$ is said *balanced* if $\#f^{-1}(0)=\#f^{-1}(1)=2^{n-1}$. The Hamming distance between f and $g\in\mathcal{F}(\mathbf{F}_2^n,\mathbf{F}_2)$ defined by $\#(f+g)^{-1}(1)$ will be denoted by $d(f,g)$.

$W_f(a)$ is the Walsh spectrum of $f\in\mathcal{F}(\mathbf{F}_2^n,\mathbf{F}_2)$ to a point

$$a=(a_0,...,a_{n-1})\in\mathbf{F}_2^n \text{ defined by } W_f(a)=\sum_{x\in\mathbf{F}_2^n}f(x)(-1)^{<a,x>}. \tag{1}$$

In this formula, the sum is calculated in $\mathbf{Z}$, and

$$<a,x>=a_0x_0+...+a_{n-1}x_{n-1}$$

is the scalar product on $\mathbf{F}_2^n$. The knowledge of the spectrum $(W_f(a))_{a\in\mathbf{F}_2^n}$ is equivalent to the knowledge of f by the following inversion theorem valid for each $x\in\mathbf{F}_2^n$

$$f(x)=2^{-n}\sum_{a\in\mathbf{F}_2^n}W_f(a)(-1)^{<a,x>}. \tag{2}$$

Walsh and Fourier spectrums are equivalent since we have the following passage formula

$$2\left(2^{n-1}\delta_0^a-W_f(a)\right)=\hat{f}(a) \tag{3}$$

valid for each $a\in\mathbf{F}_2^n$, in which δ_a^b is the Kronecker's symbol.

In the sequel, we will use the notation $W_f^*(a)=2^{n-1}\delta_0^a-W_f(a)$.

Each $f\in\mathcal{F}(\mathbf{F}_2^n,\mathbf{F}_2)$ verifies the Parseval's relation $\sum\limits_{a\in\mathbf{F}_2^n}(W_f^*(a))^2=2^{2(n-1)}$.

$|x|$ denotes the absolute value of the real number x, and $\lceil x\rceil$ the integer $\min\{n\in\mathbf{N}|\ n\geq x\}$ for x positive real number.

For each integer $i\in[0,\,2^{n-1}]$, we will have to consider the sets $|W_f^*|^{-1}(i)$ defined by $|W_f^*|^{-1}(i)=\{a\in\mathbf{F}_2^n|\ |W_f^*(a)|=i\}$.

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

The distance defined by $\min\limits_{\alpha \in \mathbf{F}_2^n, \lambda \in \mathbf{F}_2} d(f, l_\alpha + \lambda)$ between $f \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ and the affine functions set, will be denoted by $\delta(f)$.

It is easy to prove that $\delta(f) = 2^{n-1} - \max\limits_{a \in \mathbf{F}_2^n} |W_f^*(a)|$. Thus when f is balanced $\delta(f) = 2^{n-1} - \max\limits_{a \in \mathbf{F}_2^n - \{0\}} |W_f(a)|$.

The integer $\max\limits_{f \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)} \delta(f)$ will be denoted by $\rho(n)$. In theory of Error-Correcting codes [6], $\rho(n)$ is called the covering radius of the first Reed-Muller code of length 2^n.

A function f will be called *maximally nonlinear* if $\delta(f) = \rho(n)$.

The integer $\max\limits_{f \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2),\, f \ balanced} \delta(f)$ 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 balanced function $f \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ will be called *extremal* if $\delta(f) = \rho_B(n)$. The subset of $\mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ containing all the the maximally nonlinear (resp. extremal balanced) functions will be denoted by $C(n)$ (resp. $E(n)$).

3 A Sufficient Condition for Maximally Nonlinearity and Extremality

3.1 The case of extremal balanced functions

Theorem 1 *Let* $g \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ *be a balanced function such that*

$$\# |W_g^*|^{-1}(2^{n-1} - \delta(g)) \geq 2^n - \max_{f \in E(n)} \# W_f^{*\,-1}(0). \qquad \text{(P)}$$

Then $g \in E(n)$.

Proof. Consider a balanced function $g \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ which verifies the condition (P).

If $a \in |W_g^*|^{-1}(2^{n-1} - \delta(g))$,we have $|W_g^*(a)| = 2^{n-1} - \delta(g) \neq 0$, and thus $|W_g^*|^{-1}(2^{n-1} - \delta(g)) \subseteq \mathbf{F}_2^n - W_g^{*\,-1}(0)$. This implies the inequality

$$2^n - \# W_g^{*\,-1}(0) \geq \# |W_g^*|^{-1}(2^{n-1} - \delta(g)) \qquad (4)$$

On the other hand, the Parseval's identity implies for each f, $g \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$

$$2^{2(n-1)} = \sum_{a \notin W_g^{*\,-1}(0)} (W_g^*(a))^2 = \sum_{b \notin W_f^{*\,-1}(0)} (W_f^*(b))^2.$$

Now, we choose $f \in E(n)$ such that

$$\# W_f^{*\,-1}(0) = \max_{h \in E(n)} \# W_h^{*\,-1}(0) \qquad (5)$$

If we denote $p = 2^n - \#{W_g^*}^{-1}(0)$ and $q = 2^n - \#{W_f^*}^{-1}(0)$, (P), (4) and (5) imply $q \leq p$. Therefore for each indexation of p elements of $\mathbf{F}_2^n - {W_g^*}^{-1}(0)$ and q elements of $\mathbf{F}_2^n - {W_f^*}^{-1}(0)$, we have from Parseval's relation

$$\sum_{k=1}^{p} (W_g^*(a_k))^2 = \sum_{k=1}^{q} (W_f^*(b_k))^2$$

which implies successively

$$\sum_{k=1}^{q} [(W_g^*(a_k))^2 - (W_f^*(b_k))^2] + \sum_{k=q+1}^{p} (W_g^*(a_k))^2 = 0$$

$$\sum_{k=1}^{q} [(W_f^*(b_k))^2 - (W_g^*(a_k))^2] = \sum_{k=q+1}^{p} (W_g^*(a_k))^2 \geq 0 \qquad (6)$$

(when $p = q$, $\sum_{k=1}^{q} [(W_f^*(b_k))^2 - (W_g^*(a_k))^2] = 0$). We also remark that the choice of f verifying (5), together with the inequality (P), implies the following property:

$$\#|W_g^*|^{-1}(2^{n-1} - \delta(g)) \geq q \qquad (7)$$

Now, we choose the indexation of p elements of $\mathbf{F}_2^n - {W_g^*}^{-1}(0)$ by decreasing values of $|W_g^*(a_k)|$. So from (6) we have at least one integer $k^* \in [1, q]$ such that $(W_f^*(b_{k^*}))^2 - (W_g^*(a_{k^*}))^2 \geq 0$.

Then it follows from (7) that for any $k \in [1, q]$, $|W_g^*(a_k)| = 2^{n-1} - \delta(g)$. For $k = k^*$, $|W_f^*(b_{k^*})| \geq |W_g^*(a_{k^*})| = 2^{n-1} - \delta(g)$ and we obtain the following three properties:

$$\begin{aligned}
2^{n-1} - \max_{b \in \mathbf{F}_2^n} |W_f^*(b)| &\leq 2^{n-1} - |W_f^*(b_{k^*})| \\
2^{n-1} - |W_f^*(b_{k^*})| &\leq \delta(g) \\
2^{n-1} - \max_{b \in \mathbf{F}_2^n} |W_f^*(b)| &= \delta(f) = \rho_B(n) \text{ since } f \text{ is extremal balanced}
\end{aligned}$$

These properties imply $\rho_B(n) \leq \delta(g)$, and thus since g is balanced,

$\rho_B(n) = \delta(g)$. Finally g is balanced with $\delta(g) = \rho_B(n)$, therefore $g \in E(n)$. ■

At section 3, we will see that there exists functions verifying (P). From Theorem 1, we can deduce the following Corollary:

Corollary 2 *If there exists a balanced function g verifying (P), then*

$$\#|W_g^*|^{-1}(2^{n-1} - \rho_B(n)) \geq 2^n - \max_{f \in E(n)} \#{W_f^*}^{-1}(0).$$

Proof. Obvious. ■

3.2 The case of maximally nonlinear functions

Now, consider a function $g \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ which verifies the new condition

$$\#|W_g^*|^{-1}(2^{n-1} - \delta(g)) \geq 2^n - \max_{f \in C(n)} \#{W_f^*}^{-1}(0)$$

Then we observe that the proof of Theorem 1, suitably adjusted, is valid when replacing $E(n)$ by $C(n)$. We get:

Theorem 3 *Let $g \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ be a function such that*

$$\#|W_g^*|^{-1}(2^{n-1} - \delta(g)) \geq 2^n - \max_{f \in C(n)} \#{W_f^*}^{-1}(0). \tag{Q}$$

Then $g \in C(n)$.

Proof. The same as Theorem 1. ■

As seen previously at Corollary 2, we have the following result:

Corollary 4 *If there exists a function g verifying (Q), then*

$$\#|W_g^*|^{-1}(2^{n-1} - \rho(n)) \geq 2^n - \max_{f \in C(n)} \#{W_f^*}^{-1}(0).$$

Proof. Obvious. ■

Remark that these results are independant of the hypothesis on n to be odd or even.

We also have the following result:

Corollary 5 *If there exists a function $g \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ such that*

$$2^n - 1 \geq \#|W_g^*|^{-1}(2^{n-1} - \delta(g)) \geq 2^n - \max_{f \in C(n)} \#{W_f^*}^{-1}(0),$$

then $\rho(n) = \rho_B(n)$.

Proof. We know that g verifies (Q) and therefore we have $\max_{f \in C(n)} \#{W_f^*}^{-1}(0) \geq 2^n - \#|W_g^*|^{-1}(2^{n-1} - \delta(g))$.

But g also verifies the condition $2^n - \#|W_g^*|^{-1}(2^{n-1} - \delta(g)) \geq 1$, then $\max_{f \in C(n)} \#{W_f^*}^{-1}(0) \geq 1$. Thus there exists one function $f \in C(n)$ at least such that ${W_f^*}^{-1}(0) \neq \varnothing$.

Therefore, let a be an element in $\mathbf{F}_2^n$ such that $W_f^*(a) = 0$. Then it is easy to prove that the function $f + l_a$ is balanced and such that $\delta(f + l_a) = \delta(f) = \rho(n)$. Thus this function is balanced and maximally nonlinear and we have proved the result. ■

Our aim is now to use these results to compute $\rho_B(n)$ and $\rho(n)$ under (P) and (Q) hypothesis, respectively. But before, we give some examples of functions which verify these (P) and (Q) conditions.

3.3 Some examples of functions

3.3.1 For even n :

When n is even, bent functions [6, 8] are defined as boolean functions f having uniform Walsh spectrum $|W_f^*(a)| = 2^{\frac{n}{2}-1}$ for each $a \in \mathbf{F}_2^n$. Then it is easy to see that f is bent if and only if f is maximally nonlinear.

We have seen, from Theorem 3, that if a function verifies (Q), this function is maximally nonlinear. We have the following converse result:

Corollary 6 *If* $n \geq 2$ *is even,* $g \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ *is bent if and only if* g *verifies (Q).*

Proof. From Theorem 3, when g verifies (Q) g is maximally nonlinear (for even or odd n) and in particular bent for even n.

Now, let g be a bent function. In this case, we know that his Walsh spectrum is such that $|W_g^*(a)| = 2^{\frac{n}{2}-1}$for each $a \in \mathbf{F}_2^n$. So we have $\delta(g) = 2^{n-1} - 2^{\frac{n}{2}-1}$ and $\#|W_g^*|^{-1}(2^{n-1} - \delta(f)) = \#|W_g^*|^{-1}(2^{\frac{n}{2}-1}) = 2^n$.

On the other hand, we also have $\max\limits_{f \in C(n)} \#W_f^{*\,-1}(0) = 0$ since for even $n \geq 2$, $|W_f^*(a)| = 2^{\frac{n}{2}-1} \neq 0$ for each $a \in \mathbf{F}_2^n$ and each $f \in C(n)$. Then we obtain $\#|W_g^*|^{-1}(2^{n-1} - \delta(g)) = 2^n = 2^n - \max\limits_{f \in C(n)} \#W_f^{*\,-1}(0)$ which proves that g verifies (Q). ■

3.3.2 For odd n :

Using classical constuctions of bent functions in even dimension, for instance Maiorana-MacFarland functions [2, 5], we are able to construct two bent functions

$g_1,\, g_2 \in \mathcal{F}(\mathbf{F}_2^{n-1}, \mathbf{F}_2)$ such that $W_{g_1}^*(0) = -W_{g_2}^*(0) = 2^{\frac{n-1}{2}-1}$. Let us consider the new function $g \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ defined by

$g(x_1, ..., x_n) = x_n g_1(x_1, ..., x_{n-1}) + (x_n + 1) g_2(x_1, ..., x_{n-1})$. Then we have the following properties for g:

g is balanced, $|W_g^*(a)| = 0$ or $2^{\frac{n-1}{2}}$for each $a \in \mathbf{F}_2^n$, $\#W_g^{*\,-1}(0) = 2^{n-1}$,

$\delta(g) = 2^{n-1} - 2^{\frac{n-1}{2}}$, $\#|W_g^*|^{-1}(2^{n-1} - \delta(g)) = 2^{n-1}$. Moreover, it is known from [5] that $\rho(3) = 2 = 2^{3-1} - 2^{\frac{3-1}{2}}$, $\rho(5) = 12 = 2^{5-1} - 2^{\frac{5-1}{2}}$,

$\rho(7) = 56 = 2^{7-1} - 2^{\frac{7-1}{2}}$, and thus the functions g for $n = 3, 5, 7$ are extremal balanced.

For these three values of n, since $g \in E(n)$ we have

$\max\limits_{f \in E(n)} \#W_f^{*\,-1}(0) \geq \#W_g^{*\,-1}(0) = 2^{n-1}$ and finally

$2^n - \max\limits_{f \in E(n)} \#W_f^{*\,-1}(0) \leq \#|W_g^*|^{-1}(2^{n-1} - \delta(g)) = 2^{n-1}$.

Therefore, when $n = 3, 5, 7$ these functions g verify (P).

4 $\rho(n)$ and $\rho_B(n)$ Computations

Theorem 7 *If there exists a balanced (resp. any) function $g \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ verifying (P) (resp. (Q)), we have*

$$\rho_B(n) \;=\; 2^{n-1} - \frac{2^{n-1}}{(2^n - \underset{f\in E(n)}{max} \# {W_f^*}^{-1}(0))^{\frac{1}{2}}}. \tag{8}$$

$$(resp.\ \rho(n) \;=\; 2^{n-1} - \frac{2^{n-1}}{(2^n - \underset{f\in C(n)}{max} \# {W_f^*}^{-1}(0))^{\frac{1}{2}}}.) \tag{9}$$

Proof. Let f be a function in $\mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$. The Parseval's relation $\sum\limits_{a \notin {W_f^*}^{-1}(0)} (W_f^*(a))^2 = 2^{2(n-1)}$ implies the existence of $a \notin {W_f^*}^{-1}(0)$ such that $(W_f^*(a))^2 \geq \frac{2^{2(n-1)}}{2^n - \# {W_f^*}^{-1}(0)}$, so $|W_f^*(a)| \geq \frac{2^{n-1}}{(2^n - \# {W_f^*}^{-1}(0))^{\frac{1}{2}}}$.
We have $\delta(f) = 2^{n-1} - \max\limits_{a \notin {W_f^*}^{-1}(0)} |W_f^*(a)| \leq 2^{n-1} - \frac{2^{n-1}}{(2^n - \# {W_f^*}^{-1}(0))^{\frac{1}{2}}}$.
If we choose $f \in E(n)$ (resp. $f \in C(n)$), we see that
$\rho_B(n) \leq 2^{n-1} - \frac{2^{n-1}}{(2^n - \# {W_f^*}^{-1}(0))^{\frac{1}{2}}}$ for each $f \in E(n)$
(resp. $\rho(n) \leq 2^{n-1} - \frac{2^{n-1}}{(2^n - \# {W_f^*}^{-1}(0))^{\frac{1}{2}}}$ for each $f \in C(n)$).
From this, one can deduce the first inequality

$$\begin{aligned} \rho_B(n) &\leq \min_{f\in E(n)} \left(2^{n-1} - \frac{2^{n-1}}{(2^n - \# {W_f^*}^{-1}(0))^{\frac{1}{2}}} \right) \\ &= 2^{n-1} - \frac{2^{n-1}}{(2^n - \max\limits_{f\in E(n)} \# {W_f^*}^{-1}(0))^{\frac{1}{2}}}. \end{aligned} \tag{10}$$

$$\begin{aligned} (\text{resp. } \rho(n) &\leq \min_{f\in C(n)} \left(2^{n-1} - \frac{2^{n-1}}{(2^n - \# {W_f^*}^{-1}(0))^{\frac{1}{2}}} \right) \\ &= 2^{n-1} - \frac{2^{n-1}}{(2^n - \max\limits_{f\in C(n)} \# {W_f^*}^{-1}(0))^{\frac{1}{2}}}). \end{aligned} \tag{11}$$

We now suppose the existence of $g \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$, balanced (resp. any) function verifying (P):

$$\# |W_g^*|^{-1}(2^{n-1} - \delta(g)) \geq 2^n - \max_{f\in E(n)} \# {W_f^*}^{-1}(0).$$

(resp. (Q): $\# |W_g^*|^{-1}(2^{n-1} - \delta(g)) \geq 2^n - \max\limits_{f\in C(n)} \# {W_f^*}^{-1}(0)$)

This function g satisfies

$$\begin{aligned} 2^{2(n-1)} = \sum_{a\in\mathbf{F}_2^n} (W_g^*(a))^2 &= \sum_{i=1}^{2^{n-1}-\delta(g)} \# |W_g^*|^{-1}(i)\, i^2 \\ &\geq (2^{n-1} - \delta(g))^2 \, \# |W_g^*|^{-1}(2^{n-1} - \delta(g)) \end{aligned} \tag{12}$$

and from theorem 1(resp. theorem 3), g is such that $\delta(g) = \rho_B(n)$ (resp. $\delta(g) = \rho(n)$). So we obtain $2^{2(n-1)} \geq (2^{n-1} - \rho_B(n))^2 \, \#|W_g^*|^{-1}(2^{n-1} - \rho_B(n))$ (resp. $2^{2(n-1)} \geq (2^{n-1} - \rho(n))^2 \, \#|W_g^*|^{-1}(2^{n-1} - \rho(n))$).

As (P) (resp. (Q)) is verified, the Corollary 2 (resp. Corollary 4) applied to the above inequality implies

$$2^{2(n-1)} \geq (2^{n-1} - \rho_B(n))^2 \, (2^n - \max_{f \in E(n)} \#W_f^{*\,-1}(0))$$

$$(\text{resp. } 2^{2(n-1)} \geq (2^{n-1} - \rho(n))^2 \, (2^n - \max_{f \in C(n)} \#W_f^{*\,-1}(0)\,).$$

Thus we get

$$2^{n-1} \geq (2^{n-1} - \rho_B(n)) \, (2^n - \max_{f \in E(n)} \#W_f^{*\,-1}(0))^{\frac{1}{2}}$$

$$(\text{resp. } 2^{n-1} \geq (2^{n-1} - \rho(n)) \, (2^n - \max_{f \in C(n)} \#W_f^{*\,-1}(0))^{\frac{1}{2}}\,)$$

and finally

$$\rho_B(n) \geq 2^{n-1} - \frac{2^{n-1}}{(2^n - \max_{f \in E(n)} \#W_f^{*\,-1}(0))^{\frac{1}{2}}} \tag{13}$$

$$(\text{resp. } \rho(n) \geq 2^{n-1} - \frac{2^{n-1}}{(2^n - \max_{f \in C(n)} \#W_f^{*\,-1}(0))^{\frac{1}{2}}}\,). \tag{14}$$

Combining the inequalities (10) and (13) (resp. (11) and (14)), we have proved the theorem. ■

Remark 8 *When n is even, from corollary 6, we recover the well-known value $\rho(n) = 2^{n-1} - 2^{\frac{n}{2}-1}$ because $\#W_f^{*\,-1}(0) = 0$ for any $f \in C(n)$.*

5 Consequences for Balanced and Maximally Nonlinear Functions

Proposition 9 *For any odd integer $n \geq 1$, we have*

$$\max_{g \in E(n)} \#W_g^{*\,-1}(0) \leq 2^{n-1} \text{ and } \max_{g \in C(n)} \#W_g^{*\,-1}(0) \leq 2^{n-1}. \tag{15}$$

Proof. Suppose there exists a balanced function $f \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ such that the absolute value of his Walsh spectrum is constant on his support:

$\exists\, c \in \mathbf{N}-\{0\}, \forall a \notin W_f^{*\,-1}(0),\ \ |W_f^*(a)| = c.$

Then any function $g \in E(n)$ is such that $\delta(g) \geq \delta(f) = 2^{n-1} - c,$and thus $\max_{a \notin W_g^{*\,-1}(0)} |W_g^*(a)| \leq c.$

By the Parseval's relation we also have

$$2^{2(n-1)} = \sum_{a \notin W_g^{*\,-1}(0)} \left(W_g^*(a)\right)^2 \leq \left(2^n - \#W_g^{*\,-1}(0)\right)\, c^2,$$

then $c^2 \geq \frac{2^{2(n-1)}}{2^n - \#W_g^{*\,-1}(0)}$.

On the other hand, the same Parseval's relation on f implies the existence of $a^* \notin W_f^{*\,-1}(0)$ such that $\left(W_f^*(a^*)\right)^2 \leq \frac{2^{2(n-1)}}{2^n - \#W_f^{*\,-1}(0)}$, and the hypothesis on f implies $\left(W_f^*(a^*)\right)^2 = c^2$.

These properties give us the inequalities $\frac{2^{2(n-1)}}{2^n - \#W_g^{*\,-1}(0)} \leq c^2 \leq \frac{2^{2(n-1)}}{2^n - \#W_f^{*\,-1}(0)}$ that imply $\#W_g^{*\,-1}(0) \leq \#W_f^{*\,-1}(0)$ for any $g \in E(n)$.

If we denote
$A(n) = \{f \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2) |\, f$ balanced and
$\exists\, c \in \mathbf{N}-\{0\}, \forall a \notin W_f^{*\,-1}(0),\ |W_f^*(a)| = c\}$,
the above result implies $\#W_g^{*\,-1}(0) \leq \min_{f \in A(n)} \#W_f^{*\,-1}(0)$ for each $g \in E(n)$, and thus

$$\max_{g \in E(n)} \#W_g^{*\,-1}(0) \leq \min_{f \in A(n)} \#W_f^{*\,-1}(0) \tag{16}$$

Therefore, if $A(n) \neq \varnothing$, each $f \in A(n)$ verifies
$\left(2^n - \#W_f^{*\,-1}(0)\right) c^2 = 2^{2(n-1)}$. In that case, there exists an integer i which verifies the following two conditions

$$c^2 = 2^i \tag{17}$$
$$2^n - \#W_f^{*\,-1}(0) = 2^{2(n-1)-i}. \tag{18}$$

It follows from (17) that i is even, and from (18) that
$\#W_f^{*\,-1}(0) = 2^n - 2^{2(n-1)-i} > 0$ since $0 \in W_f^{*\,-1}(0)$ (f is balanced). Thus we have $i \geq n-1$ and, if there exists a function $f \in A(n)$ such that $c = 2^{\frac{n-1}{2}}$, we see that $\min_{f \in A(n)} \#W_f^{*\,-1}(0)$ equals $\#W_f^{*\,-1}(0) = 2^n - 2^{2(n-1)-i}$ calculated for $i = n-1$. So n is necessarily odd.

But as seen at § 2.3.2, we are able to construct such functions $f \in A(n)$ when n is odd: the functions $f(x_1, ..., x_n) = x_n f_1(x_1, ..., x_{n-1}) + (x_n+1) f_2(x_1, ..., x_{n-1})$, with $f_1, f_2 \in \mathcal{F}(\mathbf{F}_2^{n-1}, \mathbf{F}_2)$ bent functions and $W_{f_1}^*(0) = -W_{f_2}^*(0) = 2^{\frac{n-1}{2}-1}$, are elements of $A(n)$ with $c = 2^{\frac{n-1}{2}}$, so $A(n) \neq \varnothing$ when n is odd.

We deduce from this that $\min_{f \in A(n)} \#W_f^{*\,-1}(0) = [2^n - 2^{2(n-1)-i}]_{i=n-1} = 2^{n-1}$ for odd n. It implies from (16) the first inequality proof

$$\max_{g \in E(n)} \#W_g^{*\,-1}(0) \leq 2^{n-1}. \tag{19}$$

Now, considerer the set
$B(n) = \{f \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2) |\, \exists\, c \in \mathbf{N}-\{0\}, \forall a \notin W_f^{*\,-1}(0), |W_f^*(a)| = c\}$.

$B(n)$ is never empty since, if n even $C(n) \subseteq B(n)$, and if n odd $A(n) \subseteq B(n)$. So let's $f \in B(n)$.

For any function $g \in C(n)$ we have $\delta(g) \geq \delta(f) = 2^{n-1} - c$ and thus $\max\limits_{a \notin W_g^{*\,-1}(0)} |W_g^*(a)| \leq c$. Therefore, we have

$2^{2(n-1)} = \sum\limits_{a \notin W_g^{*\,-1}(0)} \left(W_g^*(a)\right)^2 \leq \left(2^n - \#W_g^{*\,-1}(0)\right) c^2,$

so $c^2 \geq \frac{2^{2(n-1)}}{2^n - \#W_g^{*\,-1}(0)}$.

The same Parseval's relation on f implies the existence of $a^* \notin W_f^{*\,-1}(0)$ such that $\Big(W_f^*(a^*)\Big)^2 \leq \frac{2^{2(n-1)}}{2^n - \#W_f^{*\,-1}(0)}$, and from the hypothesis on f,

$\Big(W_f^*(a^*)\Big)^2 = c^2$. Then $c^2 \leq \frac{2^{2(n-1)}}{2^n - \#W_f^{*\,-1}(0)}$ and therefore

$\frac{2^{2(n-1)}}{2^n - \#W_g^{*\,-1}(0)} \leq c^2 \leq \frac{2^{2(n-1)}}{2^n - \#W_f^{*\,-1}(0)}$ which implies

$\#W_g^{*\,-1}(0) \leq \#W_f^{*\,-1}(0)$ for any $g \in C(n)$. so we have

$$\max_{g \in C(n)} \#W_g^{*\,-1}(0) \leq \min_{f \in B(n)} \#W_f^{*\,-1}(0) \tag{20}$$

But, for each $f \in B(n)$, we have $\Big(2^n - \#W_f^{*\,-1}(0)\Big)\, c^2 = 2^{2(n-1)}$ which implies the existence of an integer i such that

$$c^2 = 2^i \tag{21}$$

$$2^n - \#W_f^{*\,-1}(0) = 2^{2(n-1)-i}. \tag{22}$$

It follows from (21) that i is even, and from (22) that

$\#W_f^{*\,-1}(0) = 2^n - 2^{2(n-1)-i} \geq 0$. This implies $i \geq n-2$.

The three conditions n is odd, i is even and $i \geq n-2$, imply $i \geq n-1$, and $A(n) \subseteq B(n)$ with $A(n) \neq \varnothing$ implies also $i = n-1$.

Therefore, from (20) we obtain

$\max\limits_{g \in C(n)} \#W_g^{*\,-1}(0) \leq [2^n - 2^{2(n-1)-i}]_{i=n-1} = 2^{n-1}$ and the second inequality is proved. ■

Corollary 10 *For odd n≥ 1,*

if (P) true for $g \in E(n)$, *then* $\#|W_g^*|^{-1}(2^{n-1} - \rho_B(n)) \geq 2^{n-1}$.

If (P) false, we have $\max\limits_{f \in E(n)} \#W_f^{*\,-1}(0) < 2^{n-1}$.

If (Q) true for $g \in C(n)$, *then* $\#|W_g^*|^{-1}(2^{n-1} - \rho(n))| \geq 2^{n-1}$.

If (Q) false, we have $\max\limits_{f \in C(n)} \#W_f^{*\,-1}(0) < 2^{n-1}$.

Proof. From Corollary 2 (resp. Corollary 4), if (P) (resp. (Q)) true for g balanced, we have $\#|W_g^*|^{-1}(2^{n-1} - \rho_B(n)) \geq 2^n - \max\limits_{f \in E(n)} \#W_f^{*\,-1}(0)$

(resp. $\#|W_g^*|^{-1}(2^{n-1} - \rho(n)) \geq 2^n - \max\limits_{f \in C(n)} \#W_f^{*\,-1}(0)$). On the other hand, since n is odd, from Proposition 9 we have $\max\limits_{f \in E(n)} \#W_f^{*\,-1}(0) \leq 2^{n-1}$

(resp. $\max_{f\in C(n)} \#W_f^{*\ -1}(0) \ \leq\ 2^{n-1}$) and the results are proved when (P) (respectively (Q)) is true. Now, if (P) (resp. (Q)) is false, there exists no balanced function g (resp. no function g) such that

$|W_g^*|^{-1}(2^{n-1} - \delta(g)) \geq 2^n - \max_{f\in E(n)} \#W_f^{*\ -1}(0)$

(resp. $\#|W_g^*|^{-1}(2^{n-1} - \delta(g)) \geq 2^n - \max_{f\in C(n)} \#W_f^{*\ -1}(0)$).

So for any balanced function g (resp. any function g) we have

$\#|W_g^*|^{-1}(2^{n-1} - \delta(g)) < 2^n - \max_{f\in E(n)} \#W_f^{*\ -1}(0)$

(resp. $|W_g^*|^{-1}(2^{n-1} - \delta(g)) < 2^n - \max_{f\in C(n)} \#W_f^{*\ -1}(0)$). In particular when n is odd, we can use g balanced such that $\delta(g) = 2^{n-1} - 2^{\frac{n-1}{2}}$ and

$\#|W_g^*|^{-1}(2^{\frac{n-1}{2}}) = 2^{n-1}$ (generalized functions of $A(n)$). Therefore

$|W_g^*|^{-1}(2^{n-1} - \delta(g)) = \#|W_g^*|^{-1}(2^{\frac{n-1}{2}}) = 2^{n-1} < 2^n - \max_{f\in E(n)} \#W_f^{*\ -1}(0)$

(resp. $\#|W_g^*|^{-1}(2^{n-1}-\delta(g)) = \#|W_g^*|^{-1}(2^{\frac{n-1}{2}}) = 2^{n-1} < 2^n - \max_{f\in C(n)} \#W_f^{*\ -1}(0)$) and the corollary is proved. ■

Corollary 11 *If there exists a balanced function $g\in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ verifying (P), we have*

for even n, $\rho_B(n) = 2^{n-1} - 2^{\frac{n}{2}}$ and $\max_{f\in E(n)} \#W_f^{*\ -1}(0) = 2^{n-1} + 2^{n-2}$,

for odd n, $\rho_B(n) = 2^{n-1} - 2^{\frac{n-1}{2}}$ and $\max_{f\in E(n)} \#W_f^{*\ -1}(0) = 2^{n-1}$.

Proof. Consider g balanced verifying (P). From Theorems 1 and 7 we have $\delta(g) = \rho_B(n) = 2^{n-1} - \frac{2^{n-1}}{(2^n - \max_{f\in E(n)} \#W_f^{*\ -1}(0))^{\frac{1}{2}}}$, and thus

$2^{2(n-1)} = \left(2^n - \max_{f\in E(n)} \#W_f^{*\ -1}(0)\right)(2^{n-1} - \rho_B(n))^2$. Therefore, there exists an integer j such that

$$(2^{n-1} - \rho_B(n))^2 = 2^j$$
$$2^n - \max_{f\in E(n)} \#W_f^{*\ -1}(0) = 2^{2(n-1)-j}$$

Then j is even and $\max_{f\in E(n)} \#W_f^{*\ -1}(0) = 2^n - 2^{2(n-1)-j} \in\ ]0, 2^n[$ since the balancedness of each $f \in E(n)$ implies $0 \in W_f^{*\ -1}(0)$ and f not everywhere equal to zero. So we have $j \in]n-2, 2(n-1)]$, and finally $j \in [n-1, 2(n-1)]$. Therefore, $\rho_B(n) = 2^{n-1} - 2^{\frac{j}{2}}$ for an even integer $j \in [n-1, 2(n-1)]$.We have the following two cases:

If n is odd, the Proposition 9 implies $\max_{f\in E(n)} \#W_f^{*\ -1}(0) \leq 2^{n-1}$ and, since $\max_{f\in E(n)} \#W_f^{*\ -1}(0) = 2^n - 2^{2(n-1)-j}$ for j even, $j \geq n-1$, we also obtain $j \leq n-1$ and finally $j = n-1$. Thus $\max_{f\in E(n)} \#W_f^{*\ -1}(0) = 2^{n-1}$ and $\rho_B(n) = 2^{n-1} - 2^{\frac{n-1}{2}}$.

If n is even, since the integer $j \geq n-1$ such that $\rho_B(n) = 2^{n-1} - 2^{\frac{j}{2}}$ will be also even, we have necessarily $j \neq n-1$, and then $j \in [n, 2(n-1)]$. Thus we obtain $\rho_B(n) \leq 2^{n-1} - 2^{\frac{n}{2}}$. But, as seen at § 2.3.2, for even n we are able to construct balanced functions f such that $|W_f^*(a)| = 2^{\frac{n}{2}}$ for $a \notin {W_f^*}^{-1}(0)$. Thus $A(n) \neq \varnothing$.

The Parseval's relation applied to functions $f \in A(n)$ give us the equality $\left(2^n - \#{W_f^*}^{-1}(0)\right)\left(2^{\frac{n}{2}}\right)^2 = 2^{2(n-1)}$, which implies $\#{W_f^*}^{-1}(0) = 2^{n-1} + 2^{n-2}$. From this we deduce $\min\limits_{f \in A(n)} \#{W_f^*}^{-1}(0) \leq 2^{n-1} + 2^{n-2}$ and from (16) we also obtain $\max\limits_{g \in E(n)} \#{W_g^*}^{-1}(0) \leq 2^{n-1} + 2^{n-2}$. Then $2^n - 2^{2(n-1)-j} \leq 2^{n-1} + 2^{n-2}$, and therefore $j \leq n$. Finally $j = n$ and we see that $\rho_B(n) = 2^{n-1} - 2^{\frac{n}{2}}$ and $\max\limits_{f \in E(n)} \#{W_f^*}^{-1}(0) = 2^n - 2^{2(n-1)-j} = 2^n - 2^{n-2} = 2^{n-1} + 2^{n-2}$. ■

Corollary 12 *If $n \geq 1$ is odd, and if there exists a function $g \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ verifying (Q), we have*
$\rho(n) = \rho_B(n) = 2^{n-1} - 2^{\frac{n-1}{2}}$ *and* $\max\limits_{f \in E(n)} \#{W_f^*}^{-1}(0) = 2^{n-1}$.

Proof. For this function g, Theorems 3 and 7 imply
$\delta(g) = \rho(n) = 2^{n-1} - \frac{2^{n-1}}{(2^n - \max\limits_{f \in C(n)} \#{W_f^*}^{-1}(0))^{\frac{1}{2}}}$,

so $2^{2(n-1)} = \left(2^n - \max\limits_{f \in C(n)} \#{W_f^*}^{-1}(0)\right)\left(2^{n-1} - \rho(n)\right)^2$ and thus we have an integer j such that

$$\begin{aligned} (2^{n-1} - \rho(n))^2 &= 2^j \\ 2^n - \max_{f \in C(n)} \#{W_f^*}^{-1}(0) &= 2^{2(n-1)-j} \end{aligned}$$

Therefore j is even, $\max\limits_{f \in C(n)} \#{W_f^*}^{-1}(0) = 2^n - 2^{2(n-1)-j} \geq 0$ implies $j \geq n-2$, and $\rho(n) = 2^{n-1} - 2^{\frac{j}{2}}$. As n is odd, the two conditions j even and $j \geq n-2$ imply $j \geq n-1$. So $\rho(n) = 2^{n-1} - 2^{\frac{j}{2}} \leq 2^{n-1} - 2^{\frac{n-1}{2}}$. But for odd n, we have construct balanced functions f such that $\delta(f) = 2^{n-1} - 2^{\frac{n-1}{2}}$ and thus $\rho_B(n) \geq 2^{n-1} - 2^{\frac{n-1}{2}}$. Combining these properties, we obtain
$2^{n-1} - 2^{\frac{n-1}{2}} \leq \rho_B(n) \leq \rho(n) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$ so $\rho_B(n) = \rho(n) = 2^{n-1} - 2^{\frac{n-1}{2}}$, $j = n-1$ and finally $\max\limits_{f \in C(n)} \#{W_f^*}^{-1}(0) = 2^{n-1}$. ■

We conclude this section by the two following results:

Corollary 13 *For any even integer n, $n \geq 6$, and for any balanced function $g \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ we have*

$$\#|W_g^*|^{-1}(2^{n-1} - \delta(g)) < 2^n - \max_{f \in E(n)} \#{W_f^*}^{-1}(0).$$

In particular, for any $g \in E(n)$

$$\#|W_g^*|^{-1}(2^{n-1} - \rho_B(n)) < 2^n - \max_{f \in E(n)} \#{W_f^*}^{-1}(0).$$

Proof. From Corollary 11 for even n, we have $\rho_B(n) = 2^{n-1} - 2^{\frac{n}{2}}$ if there exists a balanced function g verifying (P). From [3, 9], if we write $n = 2^s t$ for $s \geq 1$ and $t \geq 1$ odd, we know that

$$\rho_B(n) \geq 2^{n-1} - (\sum_{i=1}^{s} 2^{\frac{n}{2^i}-1}) - 2^{\frac{1}{2}(\frac{n}{2^s}-1)}$$

Therefore if g verifies (P) we will have

$$2^{\frac{n}{2}} \leq (\sum_{i=1}^{s} 2^{\frac{n}{2^i}-1}) + 2^{\frac{1}{2}(\frac{n}{2^s}-1)}$$

As this inequality is not verified for $n \geq 6$, we obtain the result. ■

Therefore, for even $n \geq 6$, there exists no balanced functions verifying (P). When n is odd, we have the following similar result:

Corollary 14 *For any odd integer n, n≥ 15, and for any function g∈* $\mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ *we have*

$$\#|W_g^*|^{-1}(2^{n-1} - \delta(g)) < 2^n - \max_{f \in C(n)} \#W_f^{*\,-1}(0).$$

In particular, for any $g \in C(n)$

$$\#|W_g^*|^{-1}(2^{n-1} - \rho(n)) < 2^n - \max_{f \in C(n)} \#W_f^{*\,-1}(0).$$

Proof. From Corollary 12 for odd n, if there exists g function verifying (Q), we have $\rho(n) = 2^{n-1} - 2^{\frac{n-1}{2}}$. On the other hand, Patterson-Wiedemann [7] have proved that $\rho(n) \geq 2^{n-1} - 108.2^{\frac{n-1}{2}-7}$ for any odd $n \geq 15$. So for odd $n \geq 15$, if there exists a function g verifying (Q), we must have $2^{\frac{n-1}{2}} \leq 108.2^{\frac{n-1}{2}-7}$, and we see that this is false. So (Q) is false for odd $n \geq 15$, and the corollary is proved. ■

Because (Q) false for odd $n \geq 15$, note that the result of the Corollary 10 is verified.

6 Application to Boolean Functions of Degree at most $n-1$

6.1 Structure of $\delta(f)$

Let us consider $f \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ as an element of $\mathbf{F}_2[x_1, ..., x_n]$ and suppose that $d^\circ(f) \leq n-1$. Let $l_\alpha + \lambda$ be one of its nearest affine functions. We have (see section 2) $\delta(f) = d(f, l_\alpha + \lambda) = 2^{n-1} - |W_f^*(\alpha)|$ with $|W_f^*(\alpha)| = \max_{a \in \mathbf{F}_2^n} |W_f^*(a)|$. Let us consider the functions family $(f_\Omega)_{\Omega \in \mathbf{F}_2^n}$ defined by

$f_\Omega = f + l_{\Omega+\alpha}$. We will use the following technical lemma:

Lemma 15 *$W_f^*(\Omega+\alpha) = 2^{n-1} - W_{f_\Omega}(0)$ for any $\Omega \in \mathbf{F}_2^n - \{0\}$.*

Proof. For $\alpha \in \mathbf{F}_2^n$ and $\lambda \in \mathbf{F}_2$, let us consider $g = f + l_\alpha + \lambda$. If we denote $p = \# g^{-1}(1)$ the weight of g, we have $g^{-1}(1) = \{x_1, ..., x_p\}$ for p elements $x_i \in \mathbf{F}_2^n$. Then if we introduce the functions δ_x defined by $\delta_x(y) = \delta_x^y$, we can write $g = \delta_{x_1} + ... + \delta_{x_p}$. So $f = l_\alpha + \lambda + \delta_{x_1} + ... + \delta_{x_p}$.

Moreover, for all $a \in \mathbf{F}_2^n$, a direct calculation proves the formula

$$W_f(a) = \left(\delta_0^a + (-1)^{\lambda+1}\delta_\alpha^a\right) 2^{n-1} + (-1)^\lambda \sum_{k=1}^{p} (-1)^{<\alpha+a, x_k>}. \tag{23}$$

Since $\delta(f) = d(f,\, l_\alpha + \lambda) = d(g + l_\alpha + \lambda, l_\alpha + \lambda)$, we also have
$\delta(f) = p$ and if $a = 0$,

$$W_f(0) = \left(1 + (-1)^{\lambda+1}\delta_\alpha^0\right) 2^{n-1} + (-1)^\lambda \sum_{k=1}^{p} (-1)^{<\alpha, x_k>}. \tag{24}$$

Then $f_\Omega = f + l_{\Omega+\alpha} = f + l_\Omega + l_\alpha = l_\Omega + \lambda + \delta_{x_1} + ... + \delta_{x_p}$.
For each $\Omega \neq 0$, we observe that (24) implies
$W_{f_\Omega}(0) = [W_f(0)]_{\alpha=\Omega} = 2^{n-1} + (-1)^\lambda \ \left[(-1)^{<\Omega,x_1>} + ... + (-1)^{<\Omega,x_p>}\right]$.
Thus using (23) with $\Omega = a + \alpha \neq 0$, we finally obtain
$W_{f_\Omega}(0) - 2^{n-1} = (-1)^\lambda \ \left[(-1)^{<\Omega,x_1>} + ... + (-1)^{<\Omega,x_p>}\right]$
$\qquad = W_f(\Omega+\alpha) - 2^{n-1}\delta_0^{\Omega+\alpha} = -W_f^*(\Omega+\alpha)$. ■

Theorem 16 *Let $f \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ be a nonaffine function such that $d^\circ(f) \leq n-1$ for $n \geq 3$. There exists an integer m_f verifying*
$0 < m_f \leq \left(2^{2\left(n - \lceil \frac{n}{d^\circ(f)} \rceil\right)} - 2^n + \# W_f^{*\,-1}(0) + 1\right)^{\frac{1}{2}}$ *such that*

$$\delta(f) = 2^{n-1} - 2^{\lceil \frac{n}{d^\circ(f)} \rceil - 1} m_f. \tag{25}$$

Proof. Consider again the family $(f_\Omega)_{\Omega \in \mathbf{F}_2^n}$ with $f_\Omega = f + l_{\Omega+\alpha}$. Since f is nonaffine we have $d^\circ(f_\Omega) = d^\circ(f)$, and functions f_Ω verify $2 \leq d^\circ(f_\Omega) \leq n-1$. As $d^\circ(f_\Omega) \leq n-1$, the theorem of Ax-Katz ([10] pp. 51-52, or [4] pp. 319) applied to f_Ω implies

$$2^b \mid \# f_\Omega^{-1}(0) \text{ with } b = \left\lceil \frac{n}{d^\circ(f_\Omega)} \right\rceil - 1, \text{ for any } \Omega \in \mathbf{F}_2^n \tag{26}$$

For $n \geq 3$, we have $b \leq \left\lceil \frac{n}{2} \right\rceil - 1 < n - 1$.
As $\# f_\Omega^{-1}(0) = 2^n - W_{f_\Omega}(0)$, (26) implies $2^b \mid W_{f_\Omega}(0)$.
So when $W_{f_\Omega}(0) \neq 2^{n-1}$, $W_{f_\Omega}(0) - 2^{n-1}$ will be divisible by 2^b. Thus if we denote $\Omega = a + \alpha \neq 0$, the Lemma 15 implies

$$2^b \mid W_f^*(a) \text{ for any } a \neq \alpha \text{ such that } W_f^*(a) \neq 0. \tag{27}$$

The Parseval's identity $\sum\limits_a \left(W_f^*(a)\right)^2 = 2^{2(n-1)}$ together with the equality $\max\limits_{a\in\mathbf{F}_2^n} |W_f^*(a)| = |W_f^*(\alpha)|$ implies $|W_f^*(\alpha)| \neq 0$, and we also have

$$2^{2(n-1)} - \left(W_f^*(\alpha)\right)^2 = 2^{2(n-1)} - \left(2^{n-1} - \delta(f)\right)^2 = \sum_{\{a\notin W_f^{*\,-1}(0)|a\neq\alpha\}} (W_f^*(a))^2.$$

Using property (27) for any $a \neq \alpha$ such that $W_f^*(a) \neq 0$, there exists $q_a \in \mathbf{Z}-\{0\}$ such that $W_f^*(a) = 2^b q_a$. Thus if we denote

$$q_f = \sum_{\{a\notin W_f^{*\,-1}(0)|a\neq\alpha\}} q_a^2 \tag{28}$$

we obtain the following equation for $\delta(f)$:

$$2^{2(n-1)} - \left(2^{n-1} - \delta(f)\right)^2 = 2^{2b} q_f$$

Since f is nonaffine, we have $\delta(f) > 0,$ and therefore

$|2^{n-1} - \delta(f)| = \left(2^{2(n-1)} - 2^{2b} q_f\right)^{\frac{1}{2}}$ with $q_f < 2^{2\left(n-\lceil\frac{n}{d^\circ(f)}\rceil\right)}$ which finally implies

$$\begin{aligned}\delta(f) &= 2^{n-1} - \left(2^{2(n-1)} - 2^{2b} q_f\right)^{\frac{1}{2}} \\ &= 2^{n-1} - 2^{\left\lceil\frac{n}{d^\circ(f)}\right\rceil-1}\left(2^{2\left(n-\left\lceil\frac{n}{d^\circ(f)}\right\rceil\right)} - q_f\right)^{\frac{1}{2}}\end{aligned} \tag{29}$$

with $2^{2\left(n-\lceil\frac{n}{d^\circ(f)}\rceil\right)} > q_f > 0.$

Moreover, définition (28) also implies

$$q_f \geq 2^n - \#W_f^{*\,-1}(0) - 1 \tag{30}$$

Now, since $2^{n-1}(-1)^{f(x)} = \sum\limits_{a\notin W_f^{*\,-1}(0)} W_f^*(a)(-1)^{<a,x>}$ and $\alpha \notin W_f^{*\,-1}(0)$, we may write at the point $x = 0, 2^{n-1}(-1)^{f(0)} = \quad 2^b \ (\sum\limits_{a\notin W_f^{*\,-1}(0),\, a\neq\alpha} q_a \quad) + W_f^*(\alpha)$ so,

$$\begin{aligned}|W_f^*(\alpha)| = 2^{n-1} - \delta(f) &= |2^{n-1}(-1)^{f(0)} - \quad 2^b(\sum_{a\notin W_f^{*\,-1}(0),\, a\neq\alpha} q_a \quad)\,| \\ &= 2^b|2^{n-b-1}(-1)^{f(0)} - \sum_{a\notin W_f^{*\,-1}(0),\, a\neq\alpha} q_a \quad |.\end{aligned}$$

On the other hand, it follows from (29) that

$2^{n-1} - \delta(f) = 2^b\left(2^{2(n-\left\lceil\frac{n}{d^\circ(f)}\right\rceil)} - q_f\right)^{\frac{1}{2}}$, and finally

$$\left(2^{2(n-\left\lceil\frac{n}{d^\circ(f)}\right\rceil)} - q_f\right)^{\frac{1}{2}} = |(-1)^{f(0)}2^{n-\left\lceil\frac{n}{d^\circ(f)}\right\rceil} - \sum_{a\notin W_f^{*\,-1}(0),\, a\neq\alpha} q_a \quad | \in \mathbf{N}.$$

Therefore, if we denote

$$m_f = \left(2^{2(n-\lceil \frac{n}{d^\circ(f)} \rceil)} - q_f\right)^{\frac{1}{2}} = |(-1)^{f(0)} 2^{n-\lceil \frac{n}{d^\circ(f)} \rceil} - \sum_{a \notin W_f^{*\,-1}(0),\, a \neq \alpha} q_a \quad |,$$

and if we use the inequality on q_f together with (30), we obtain $2^{2\left(n-\lceil \frac{n}{d^\circ(f)} \rceil\right)} - 2^n + \# W_f^{*\,-1}(0) + 1 \geq m_f^2 > 0$ and we have proved the Theorem. ■

Corollary 17 *For* $n \geq 3$, *let* $f \in \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ *be a nonaffine function of even weight* $\# f^{-1}(1)$. *Then* $\delta(f)$ *verifies (25).*

Proof. If we consider $f(x_1, ..., x_n) = \sum_{i_1 \in \{0,1\}, ..., i_n \in \{0,1\}} a_{i_1 ... i_n} x_1^{i_1} ... x_n^{i_n}$ as element of $\mathbf{F}_2[x_1, ..., x_n]$, we have

$$a_{i_1 ... i_n} = \left(\sum_{0 \leq x_1 \leq i_1, ..., 0 \leq x_n \leq i_n} f(x_1, ..., x_n) \right) \bmod 2. \text{ Thus}$$

$$a_{1...1} = \left(\sum_{x_1 \in \mathbf{F}_2, ..., x_n \in \mathbf{F}_2} f(x_1, ..., x_n) \right) \bmod 2 = \# f^{-1}(1) \bmod 2.$$

Then $\# f^{-1}(1)$ is even if and only if $a_{1...1} = 0,$ idem $d^\circ(f) \leq n-1$, and the Corollary results of Theorem 16. ■

6.2 Application to balanced functions

Since $\# f^{-1}(1) = 2^{n-1},$ all the balanced functions f are of even weights, and we finish with the following result:

Corollary 18 *For odd* n, $n \geq 3$, *if there exists an extremal balanced function of degree 2, then* $\rho_B(n) = 2^{n-1} - 2^{\frac{n-1}{2}}$.

Proof. Since n is odd, the Proposition 9 implies $\max_{f \in E(n)} \# W_f^{*\,-1}(0) \leq 2^{n-1}$. For any $f \in E(n)$, it follows from Theorem 16 that

$$0 < m_f \leq \left(2^{2\left(n - \lceil \frac{n}{d^\circ(f)} \rceil\right)} - 2^n + \# W_f^{*\,-1}(0) + 1 \right)^{\frac{1}{2}}$$
$$\leq \left(2^{2\left(n - \lceil \frac{n}{d^\circ(f)} \rceil\right)} - 2^{n-1} + 1 \right)^{\frac{1}{2}}.$$

If there exists $f \in E(n)$ with $d^\circ(f) = 2$, we obtain for this function $\lceil \frac{n}{d^\circ(f)} \rceil = \frac{n+1}{2}$ and then $2^{2\left(n - \lceil \frac{n}{d^\circ(f)} \rceil\right)} - 2^{n-1} + 1 = 1$. Thus $m_f = 1$ and the $\rho_B(n)$ value results of (25). ■

7 Conclusion

We have studied a new sufficient condition for maximal nonlinear and extremal balanced Boolean functions. For even n, this condition characterizes the bent functions. For even or odd n, under forms (P) and (Q) of the condition we have computed $\rho_B(n)$ and $\rho(n)$, respectively. Later, these values are proved only valid in low dimensions, so in a subsequent study one may ask how to generalize (P) and (Q). In high odd or even dimensions, we have deduced some new inequalities on the size of the Walsh spectrum's kernel of functions in $E(n)$ and $C(n)$. In a second part, for even weights functions f, a general form for $\delta(f)$ including $d^\circ(f)$ is given.

Acknowledgements. We would like to thank P. Camion, A. and F. Le Leslé, for their constructive comments which greatly improved the presentation of the paper.

8 References

1. Carlet, C.: Partially-bent functions. Designs, Codes and Cryptography, 3, 135-145, (1993)

2. Dillon, J.F.: Elementary Hadamard difference sets. PhD thesis, University of Maryland, 1974

3. Dobbertin, H.: Construction of maximally nonlinear functions and balanced boolean functions with high nonlinearity. In Proc. Fast Software Encryption, 61-74, Berlin Heidelberg New-York: Springer 1994

4. Lidl, R., Niederreiter, H.: Finite fields. Cambridge University Press 1987

5. Mc Farland, R.L.: A family of noncyclic difference sets. J. Comb. Th. (Series A) 15, 1-10 (1973)

6. Mc Williams, F.J., Sloane, N.J.A.: The theory of Error-Correcting codes. Amsterdam: North-Holland 1977

7. Patterson, N.J., Wiedemann, D.H.: The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. IEEE Trans. Inform. Theory, IT-29, 354-356 (1983).

8. Rothaus, O.S.: On "bent" functions. J. Comb. Th. (Series A) 20, 300-305 (1976)

9. Seberry, J., Zhang, M., Zheng, Y.: Nonlinearly balanced boolean functions and their propagation characteristics. In Proc. CRYPTO'93, 49-60, Berlin Heidelberg New-York: Springer 1993

10. Small, C.: Arithmetic of finite fields. Marcel Dekker 1991