Theoretical Upper Bounds on the Covering Radii of Boolean Functions

Michel Mitton
DCSSI/SDS/Crypto. Lab.
18, rue du docteur Zamenhof
92131 Issy-les-Moulineaux cedex, France
e-mail: michel.mitton@sgdn.pm.gouv.fr

November 26, 2004

Abstract

We prove new upper bounds for the covering radii $\rho(n)$ and $\rho_B(n)$ of the first order Reed-Muller code $R(1,n)$. Although these bounds be actually theoretical, they improve the classical Helleseth-Kløve-Mykkeltveit (H.K.M.) bound $2^{n-1} - 2^{\frac{n}{2}-1}$.

Keywords

Boolean functions, covering radius, balanced covering radius, Walsh and Fourier transforms, non-linearity, Reed-Muller codes.

1 Introduction

This paper investigates the covering radius $\rho(n)$ and the balanced covering radius $\rho_B(n)$ for Boolean functions in dimension n. From Rothaus [1], the covering radius is known for even dimension n, contrary to the balanced covering radius which is unknown for $n \geq 8$. In odd dimension, the exact values of both $\rho(n)$ and $\rho_B(n)$ are unknown, except a finite number of small dimensions $n = 3, 5, 7$ where $\rho(n) = \rho_B(n) = 2^{n-1} - 2^{\frac{n-1}{2}}$. From H.K.M. [2], for odd or even n, we know that

$$\rho(n) \leq 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{1}$$

We prove new theoretical bounds $b(n)$ and $b_B(n)$ such that for even n, $\rho_B(n) \leq b_B(n) \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2$, and for odd n, $\rho(n) \leq b(n) \leq \lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \rfloor, \rho_B(n) \leq b_B(n) \leq \lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \rfloor$.

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 $\mathcal{F} = \mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$.

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.

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

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

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

$$W_f^*(a) = 2^{n-1}\delta_0^a - W_f(a). \tag{3}$$

Between Walsh and Fourier transforms we have the relation $2W_f^* = \hat{f}$.

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

$$\sum_{a \in \mathbf{F}_2^n} (W_f^*(a))^2 = 2^{2(n-1)}. \tag{4}$$

$|x|$ denotes the absolute value of the real number x, and $\lfloor x \rfloor$ the integer $\max\{n \in \mathbf{N} | n \leq x\}$.

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

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

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

The integer $\max\limits_{f \in \mathcal{F}} \delta(f)$ will be denoted by $\rho(n)$. In the theory of error-correcting codes [3], $\rho(n)$ is called the covering radius of the first order Reed-Muller code $R(1, n)$ of length 2^n.

The integer $\max\limits_{f\ balanced} \delta(f)$ 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*

[1], [3], [4] are defined as boolean functions f having uniform Walsh spectrum $|W_f^*(a)| = 2^{\frac{n}{2}-1}$ for each $a \in \mathbf{F}_2^{\mathrm{n}}$. 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 [5].

3 Theoretical Results

Proposition 1

$$\begin{aligned}
\rho(n) &\leq 2^{n-1} - \max_{f\in A}\left(\frac{2^{2(n-1)} - \sum_{q=1}^{k} i_q^2 \#|W_f^*|^{-1}(i_q)}{2^n - \sum_{q=1}^{k}\#|W_f^*|^{-1}(i_q)}\right)^{\frac{1}{2}} \\
\textit{with } A &= \{f \in C(n) | \exists (i_1, ..., i_k) \in [0, 2^{n-1}]^k, \\
i_1 &< ... < i_k, \mathop{\overset{\circ}{\cup}}_{1\leq q\leq k} |W_f^*|^{-1}(i_q) \subsetneq \mathbf{F}_2^n\} \qquad (5)
\end{aligned}$$

Proof. Consider $f \in \mathcal{F}$ and k integers $i_1, ..., i_k$ such that $0 \leq i_1 < ... < i_k \leq 2^{n-1}$. We denote $B = \mathop{\overset{\circ}{\cup}}_{1\leq q\leq k} |W_f^*|^{-1}(i_q)$.
Rewriting Parseval's relation (4), we have
$2^{2(n-1)} = \sum_{a\in B} (W_f^*(a))^2 + \sum_{a\notin B} (W_f^*(a))^2$ and finally
$2^{2(n-1)} - \sum_{q=1}^{k} \#|W_f^*|^{-1}(i_q) = \sum_{a\notin B} (W_f^*(a))^2$.
On the other hand, $\mathbf{F}_2^n = \mathop{\overset{\circ}{\cup}}_{0\leq i\leq 2^{n-1}} \#|W_f^*|^{-1}(i)$, so
$2^n - \sum_{q=1}^{k} \#|W_f^*|^{-1}(i_q) = \sum_{i\notin\{i_1,...,i_k\}} \#|W_f^*|^{-1}(i)$.
If $2^n - \sum_{q=1}^{k} \#|W_f^*|^{-1}(i_q) \neq 0$, i.e. $B \subsetneq \mathbf{F}_2^n$, there exists $b \notin B$ such that
$(W_f^*(b))^2 \geq \frac{2^{2(n-1)} - \sum_{q=1}^{k} \#|W_f^*|^{-1}(i_q)}{2^n - \sum_{q=1}^{k} \#|W_f^*|^{-1}(i_q)}$. Since $\delta(f) \leq 2^{n-1} - |W_f^*(b)|$, we obtain
$\delta(f) \leq 2^{n-1} - \left(\frac{2^{2(n-1)} - \sum_{q=1}^{k} \#|W_f^*|^{-1}(i_q)}{2^n - \sum_{q=1}^{k} \#|W_f^*|^{-1}(i_q)}\right)^{\frac{1}{2}}$, with this inequality in particular true for each $f \in A$. This proves the Proposition. ■

Observe that this proof, suitably adjusted, is valid when replacing $C(n)$ by $E(n)$. Therefore, we have also the below result:

Proposition 2

$$\begin{aligned}\rho_B(n) &\leq 2^{n-1} - \max_{f\in B}\left(\frac{2^{2(n-1)} - \sum_{q=1}^{k} i_q^2 \#|W_f^*|^{-1}(i_q)}{2^n - \sum_{q=1}^{k}\#|W_f^*|^{-1}(i_q)}\right)^{\frac{1}{2}} \\ \text{with } B &= \{f \in E(n) | \exists (i_1,...,i_k) \in [0,2^{n-1}]^k, \\ i_1 &< ... < i_k, \overset{\circ}{\bigcup_{1\leq q\leq k}} |W_f^*|^{-1}(i_q) \subsetneq \mathbf{F}_2^n\} \end{aligned} \tag{6}$$

Proof. The same as Proposition 1. ■

Since $\rho(n) = 2^{n-1} - 2^{\frac{n}{2}-1}$ for even n, the only unknown values of $\rho(n)$ are these for odd n. So, in the sequel, we can suppose n odd, although generally Proposition 1 implies the following result:

Corollary 3 *Let us consider the set I defined by $I = [0, 2^{n-1}] - \{2^{\frac{n}{2}-1}\}$ for even n, and $I = [0, 2^{n-1}]$ for odd n. We have the following inequalities*

$$\begin{aligned}\rho(n) &\leq 2^{n-1} - \max_{f\in C(n), i\in I}\left(\frac{2^{2(n-1)} - i^2\#|W_f^*|^{-1}(i)}{2^n - \#|W_f^*|^{-1}(i)}\right)^{\frac{1}{2}} \\ &\leq 2^{n-1} - \frac{2^{n-1}}{(2^n - \max_{f\in C(n)} \#W_f^{*-1}(0))^{\frac{1}{2}}}\end{aligned} \tag{7}$$

Proof. Consider $i \in I$, and $f \in C(n)$. If $|W_f^*|^{-1}(i) = \mathbf{F}_2^n$, we must have $|W_f^*|(a) = i$ for each $a \in \mathbf{F}_2^n$, and by Parseval's relation (4) we must have also $2^n i^2 = 2^{2(n-1)}$. So, $i^2 = 2^{n-2}$ and this contradicts the hypothesis $i \in I$.

Consequently, $|W_f^*|^{-1}(i) \subsetneq \mathbf{F}_2^n$ and the first inequality results of the Proposition 1 applied for $k = 1$ and $i_1 = i$.

The second inequality results of

$$\max_{f\in C(n), i\in I}\left(\frac{2^{2(n-1)} - i^2\#|W_f^*|^{-1}(i)}{2^n - \#|W_f^*|^{-1}(i)}\right)^{\frac{1}{2}} \geq \max_{f\in C(n), i=0}\left(\frac{2^{2(n-1)} - i^2\#|W_f^*|^{-1}(i)}{2^n - \#|W_f^*|^{-1}(i)}\right)^{\frac{1}{2}}$$

$$= \max_{f\in C(n)}\left(\frac{2^{2(n-1)}}{2^n - \#|W_f^*|^{-1}(0)}\right)^{\frac{1}{2}} = \left(\frac{2^{2(n-1)}}{2^n - \max_{f\in C(n)} \#W_f^{*-1}(0)}\right)^{\frac{1}{2}} \quad ■$$

It is easy to deduce of Proposition 2 the following properties:

Corollary 4 *Let us consider the set I defined by $I = [0, 2^{n-1}] - \{2^{\frac{n}{2}-1}\}$ if n*

even, and $I = [0, 2^{n-1}]$ *if* n *odd. We have the inequalities*

$$\begin{aligned} \rho_B(n) &\leq 2^{n-1} - \max_{f \in E(n), i \in I} \left(\frac{2^{2(n-1)} - i^2 \# |W_f^*|^{-1}(i)}{2^n - \ \# |W_f^*|^{-1}(i)} \right)^{\frac{1}{2}} \\ &\leq 2^{n-1} - \frac{2^{n-1}}{(2^n - \max\limits_{f \in E(n)} \# W_f^{*-1}(0))^{\frac{1}{2}}} \end{aligned} \tag{8}$$

Proof. The same as Corollary 3. ∎

Remark 5 *Since* $\frac{2^{n-1}}{(2^n - \max\limits_{f \in C(n)} \# W_f^{*-1}(0))^{\frac{1}{2}}} \geq 2^{\frac{n}{2}-1}$ *and*
$\frac{2^{n-1}}{(2^n - \max\limits_{f \in E(n)} \# W_f^{*-1}(0))^{\frac{1}{2}}} \geq \frac{2^{n-1}}{(2^n - 1)^{\frac{1}{2}}}$, *we have*
$2^{n-1} - \frac{2^{n-1}}{(2^n - \max\limits_{f \in C(n)} \# W_f^{*-1}(0))^{\frac{1}{2}}} \leq 2^{n-1} - 2^{\frac{n}{2}-1}$ *and*
$2^{n-1} - \frac{2^{n-1}}{(2^n - \max\limits_{f \in E(n)} \# W_f^{*-1}(0))^{\frac{1}{2}}} \leq 2^{n-1} - \frac{2^{n-1}}{(2^n - 1)^{\frac{1}{2}}}$.

4 Upper bounds for $\rho(n)$ and $\rho_B(n)$

Theoretical upper bounds on $\rho(n)$ and $\rho_B(n)$ have been obtained. These bounds on $\rho(n)$ are better than the well-known value $2^{n-1} - 2^{\frac{n}{2}-1}$ but very theoretical and nonconstructive. Using some additional properties, we can prove now new upper bounds on $\rho(n)$ and $\rho_B(n)$ that we hope more usable.

As seen previously, the new bounds of corollaries 3 and 4 are formally identical for $C(n)$ and $E(n)$. So, in the sequel, we denote $A(n)$ the set $C(n)$ (respectively $E(n)$), and $\rho_A(n)$ the integer $\rho(n)$ (respectively $\rho_B(n)$) when $A(n) = C(n)$ (respectively $A(n) = E(n)$).

Recall that $I = [0, 2^{n-1}] - \{2^{\frac{n}{2}-1}\}$ for even n, and $I = [0, 2^{n-1}]$ for odd n.

From $\overset{\circ}{\bigcup\limits_{0 \leq i \leq 2^{n-1}}} |W_f^*|^{-1}(i) = \mathbf{F}_2^n$ and from Parseval's relation (4), we have, for each $i \in I - \{0\}$ and for each $f \in A(n)$, $\# |W_f^*|^{-1}(i) < 2^n$.

Finally, for $f \in \mathcal{F}$, we denote J_f the set defined by

$$J_f = \{ i \in I - \{0\} | \# |W_f^*|^{-1}(i) < 4i^2 \} \tag{9}$$

Proposition 6 *Let us consider* $f \in A(n)$ *for* $n \geq 3$. *If* $J_f \subsetneq I - \{0\}$, *there exists at least one integer* $i \in I - J_f, i \neq 0$, *such that*

$$\frac{2^n - 2i(\# |W_f^*|^{-1}(i))^{\frac{1}{2}}}{2^n - \# |W_f^*|^{-1}(i)} \geq 1 \tag{10}$$

Proof. If this result was false, there would exist at least one fonction $f \in A(n)$ such that for each $i \in I - J_f, i \neq 0$, we should have $\frac{2^n - 2i(\#|W_f^*|^{-1}(i))^{\frac{1}{2}}}{2^n - \#|W_f^*|^{-1}(i)} < 1$. This last inequality implies $\#|W_f^*|^{-1}(i) < 4i^2$ so $i \in J_f$ and we see that $I - J_f \subseteq J_f$. Then we obtain $\emptyset = (I - J_f) \cap J_f \supseteq (I - J_f) \cap (I - J_f) = I - J_f$ and finally $I - J_f = \emptyset$ which proves the assertion. ■

Remark 7 *For $f \in A(n)$, consider an integer $i \in I - J_f, i \neq 0$. The definition (9) of J_f implies $2^n > \#|W_f^*|^{-1}(i) \geq 4i^2$ and consequently $0 < i < 2^{\frac{n}{2}-1}$.*

Consider the case $A(n) = C(n)$ for even n. For $i \in I - \{0\}$ and $f \in A(n)$, we have $|W_f^*|^{-1}(i) = \varnothing$ ($|W_f^*(a)| = 2^{\frac{n}{2}-1}$ for each $a \in \mathbf{F}_2^n$) and then $\#|W_f^*|^{-1}(i) = 0 < 4i^2$, so $i \in J_f$ and finally $J_f = I - \{0\}$.

Consequently, we see that the hypothesis of the Proposition 6, in the case $A(n) = C(n)$ with n even, is not satisfied. Is it also true for $A(n) = E(n)$ or when n is odd ? We give below two functions for $n = 6$ and $A(n) = E(n)$ where the two possible cases are realised. The tables below represent the elements

$$f(0).......f(31)$$
$$f(32).....f(63)$$

Case $J_f \subsetneq I - \{0\}$:
The balanced function $f \in E(6)$ defined by

00001001011101111011010111000101
11011100011011011000100000011001

is such that $W_f^{*-1}(0) = \{0, 13, 18, 31, 36, 41, 54, 59\}$ and $\#W_f^{*-1}(0) = 8$, $\#|W_f^*|^{-1}(2) = 16$, $\#|W_f^*|^{-1}(4) = 24$, $\#|W_f^*|^{-1}(6) = 16$, so $2 \notin J_f$ because $\#|W_f^*|^{-1}(2) \geq 4 \times 2^2$.

Case $J_f = I - \{0\}$:
The balanced function $f \in E(6)$ defined by

01100001011101111000111101011001
11100111101000110110010000000001

is such that
$W_f^{*-1}(0) = \{0, 12, 14, 15, 23, 26, 34, 47, 53, 57, 58, 59\}$ and $\#W_f^{*-1}(0) = 12$, $\#|W_f^*|^{-1}(2) = 14$, $\#|W_f^*|^{-1}(4) = 20$, $\#|W_f^*|^{-1}(6) = 18$.

From this, we can suppose that generally, except for n even and $A(n) = C(n)$, the two cases $J_f \subsetneq I - \{0\}$ and $J_f = I - \{0\}$ are possible for certain functions $f \in A(n)$.

Now, we have all the necessery elements to prove our principal result.

Theorem 8 *Let us consider $f \in A(n)$ for $n \geq 3$.*

If $J_f \subsetneq I - \{0\}$, there exists at least one integer $i \in I - J_f$ verifying $0 < i < 2^{\frac{n}{2}-1}$ and $\#|W_f^*|^{-1}(i) \geq 4i^2$, such that

$$\rho_A(n) \leq 2^{n-1} - \left[2^{n-2} + \frac{i}{2}\left(\#|W_f^*|^{-1}(i)\right)^{\frac{1}{2}}\right]^{\frac{1}{2}} \tag{11}$$

If $J_f = I - \{0\}$, we have

$$\rho_A(n) \leq 2^{n-1} - \max_{0 \leq i < 2^{\frac{n}{2}-1}} \left(\frac{2^{2(n-1)} - 4i^4}{2^n - \#|W_f^*|^{-1}(i)}\right)^{\frac{1}{2}} \tag{12}$$

Proof. From Proposition 6, if $J_f \subsetneq I - \{0\}$ for $f \in A(n)$, $n \geq 3$, there exists at least one integer $i \in I - J_f$, $i \neq 0$ verifying (10). We have seen in the Remark 7 that $0 < i < 2^{\frac{n}{2}-1}$ and $\#|W_f^*|^{-1}(i) \geq 4i^2$. Rewriting the inequalities of Corollaries 3 and 4, we obtain

$$\rho_A(n) \leq 2^{n-1} - \max_{g \in A(n), j \in I} \left(\frac{2^{2(n-1)} - j^2 \#|W_g^*|^{-1}(j)}{2^n - \#|W_g^*|^{-1}(j)}\right)^{\frac{1}{2}}.$$

So, for $g = f$ and $j = i \in I - J_f, i \neq 0$, the above inequality

$$\rho_A(n) \leq 2^{n-1} - \left(\frac{2^{2(n-1)} - i^2 \#|W_f^*|^{-1}(i)}{2^n - \#|W_f^*|^{-1}(i)}\right)^{\frac{1}{2}}$$

is valid. On the other hand, if we denote $B_i = \#|W_f^*|^{-1}(i)$, we have also

$$\begin{aligned} \frac{2^{2(n-1)} - i^2 B_i}{2^n - B_i} &= \frac{1}{4}\frac{2^{2n} - 4i^2 B_i}{2^n - B_i} \\ &= \frac{1}{4}\frac{\left(2^n - 2iB_i^{\frac{1}{2}}\right)\left(2^n + 2iB_i^{\frac{1}{2}}\right)}{2^n - B_i}. \end{aligned}$$

From Proposition (6), the integers i and B_i are such that $\frac{\left(2^n - 2iB_i^{\frac{1}{2}}\right)}{2^n - B_i} \geq 1$, and thus

$$\frac{2^{2(n-1)} - i^2 B_i}{2^n - B_i} \geq \frac{1}{4}\left(2^n + 2iB_i^{\frac{1}{2}}\right) = 2^{n-2} + \frac{i}{2}B_i^{\frac{1}{2}}.$$

Using the inequality $\rho_A(n) \leq 2^{n-1} - \left(\frac{2^{2(n-1)} - i^2 B_i}{2^n - B_i}\right)^{\frac{1}{2}}$ we obtain the first result.

Now, suppose $J_f = I - \{0\}$. From definition (9), we have $B_i < 4i^2$ for each $i \in I - \{0\}$ or equivalently for each $i \in [1, 2^{\frac{n}{2}-1}[$. From Corollaries 3 and 4,

$$\begin{aligned} \rho_A(n) \quad \leq \quad & 2^{n-1} - \max_{i \in I} \left(\frac{2^{2(n-1)} - i^2 B_i}{2^n - B_i} \right)^{\frac{1}{2}} = \\ & 2^{n-1} - \max \{ \max_{i \in I - \{0\}} \left(\frac{2^{2(n-1)} - i^2 B_i}{2^n - B_i} \right)^{\frac{1}{2}}, \\ & \left(\frac{2^{2(n-1)}}{2^n - B_0} \right)^{\frac{1}{2}} \}. \end{aligned}$$

$B_i < 4i^2$ for each $i \in I - \{0\}$ implies $2^{2(n-1)} - i^2 B_i > 2^{2(n-1)} - 4i^4$ and finally

$$\rho_A(n) \leq 2^{n-1} - \max_{0 \leq i < 2^{\frac{n}{2}-1}} \left(\frac{2^{2(n-1)} - 4i^4}{2^n - B_i} \right)^{\frac{1}{2}}$$

for each $n \geq 3$. ■

From this, we deduce immediately a classification of different possible cases.

Corollary 9 *Let us consider $f \in E(n)$ (resp. $C(n)$) for even $n \geq 6$, or odd $n \geq 5$ (resp. odd $n \geq 3$).*

** If $J_f \subsetneq I - \{0\}$, there exists at least one even (resp. arbitrary) integer i verifying $1 \leq i < 2^{\frac{n}{2}-1}$ and $\#|W_f^*|^{-1}(i) \geq 4i^2$, such that $\rho_B(n)$ (resp. $\rho(n)$)*

$$\begin{aligned} & \leq \quad 2^{n-1} - \left[2^{n-2} + \frac{i}{2} \left(\#|W_f^*|^{-1}(i) \right)^{\frac{1}{2}} \right]^{\frac{1}{2}} \\ & \leq \quad 2^{n-1} - (2^{n-2} + i^2)^{\frac{1}{2}} \qquad (13) \end{aligned}$$

** If $J_f = I - \{0\}$, we have the following two cases:*

- If there exits at least one even (resp. arbitrary) integer $j \in [1, 2^{\frac{n}{2}-1}[$ such that

$$\frac{2^n - \#|W_f^*|^{-1}(j)}{2^n - \#W_f^{*-1}(0)} < 1 - \frac{j^4}{2^{2n-4}} \qquad (14)$$

then

$$\begin{aligned} \rho_B(n) \text{ (resp. } \rho(n)) & \leq 2^{n-1} - \left(\frac{2^{2n-2} - 4j^4}{2^n - \#|W_f^*|^{-1}(j)} \right)^{\frac{1}{2}} \\ & < 2^{n-1} - \frac{2^{n-1}}{(2^n - \#W_f^{*-1}(0))^{\frac{1}{2}}} \qquad (15) \end{aligned}$$

- If not,

$$\rho_B(n) \text{ (resp. } \rho(n)) \leq 2^{n-1} - \frac{2^{n-1}}{\left(2^n - \#W_f^{*-1}(0)\right)^{\frac{1}{2}}} \qquad (16)$$

Proof. Let be $f \in E(n), n \geq 6$ even or $n \geq 5$ odd, and suppose $J_f \subsetneq I - \{0\}$. From Theorem 8 with $A(n) = E(n)$, we have

$$\rho_B(n) \leq 2^{n-1} - \left[2^{n-2} + \frac{i}{2}\left(\#|W_f^*|^{-1}(i)\right)^{\frac{1}{2}}\right]^{\frac{1}{2}}$$

for a certain integer i verifying $0 < i < 2^{\frac{n}{2}-1}$ and $\#|W_f^*|^{-1}(i) \geq 4i^2$.This proves the first inequality.

Using now the balancedness of f , we have $W_f^*(0) = 0$, and consequently, it's easy to prove that $W_f^*(a)$ is necessary even for each $a \in \mathbf{F}_2^n$. On the other hand, the integer i is such that $\#|W_f^*|^{-1}(i) \geq 4i^2 > 0$ and therefore i is necessary even because the precedent property implies $\#|W_f^*|^{-1}(j) = 0$ for each odd j.

Let us consider the case $J_f = I - \{0\}$ and suppose verified the condition (14) for an integer $j \in [1, 2^{\frac{n}{2}-1}[$. This condition is equivalent to the inequality

$$\frac{2^{2n-2} - 4j^4}{2^n - \#|W_f^*|^{-1}(j)} > \frac{2^{2n-2}}{2^n - \#W_f^{*-1}(0)}.$$

Therefore,

$$\begin{aligned} \max_{0 \leq i < 2^{\frac{n}{2}-1}} \left(\frac{2^{2(n-1)} - 4i^4}{2^n - \#|W_f^*|^{-1}(i)}\right)^{\frac{1}{2}} &\geq \left(\frac{2^{2n-2} - 4j^4}{2^n - \#|W_f^*|^{-1}(j)}\right)^{\frac{1}{2}} \\ &> \frac{2^{n-1}}{(2^n - \#W_f^{*-1}(0))^{\frac{1}{2}}} \end{aligned}$$

and combining these inequalities with the inequality (12) of Theorem 8, we obtain the result (15).

Now, if we have (14) false for each $j \in [1, 2^{\frac{n}{2}-1}[$, as seen previously this property is equivalent to

$$\frac{2^{2n-2} - 4j^4}{2^n - \#|W_f^*|^{-1}(j)} \leq \frac{2^{2n-2}}{2^n - \#W_f^{*-1}(0)},$$

and (16) is again the consequence of the inequality (12) of Theorem (8).

The proof of case $f \in C(n)$ is the same as previously. ■

Corollary 10 *Let be $f \in E(n)$ for $n \geq 5$.*

If $J_f \subsetneq I - \{0\}$ (resp. $J_f = I - \{0\}$) , we denote

$r_n = 2^{n-1} - \left[2^{n-2} + \frac{i}{2}\left(\#|W_f^*|^{-1}(i)\right)^{\frac{1}{2}}\right]^{\frac{1}{2}}$ *(resp. $r_n = 2^{n-1} - \frac{2^{n-1}}{\left(2^n - \#W_f^{*-1}(0)\right)^{\frac{1}{2}}}$).*

For even $n \geq 6$ (resp. odd $n \geq 5$), let be $b_B(n) = \lfloor r_n \rfloor - (\lfloor r_n \rfloor \bmod 2)$. We have $\rho_B(n) \leq b_B(n) \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2$ (resp. $\rho_B(n) \leq b_B(n) \leq \lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \rfloor$).

Proof. Suppose even $n \geq 6$ and $J_f \subsetneq I - \{0\}$ (resp. $J_f = I - \{0\}$). From Corollary 9 there exists an even integer $i \in [1, 2^{\frac{n}{2}-1}[$ (resp. j) with

$\#|W_f^*|^{-1}(i) \geq 4i^2$ such that $\rho_B(n) \leq r_n$. Because $\frac{i}{2}(\#|W_f^*|^{-1}(i))^{\frac{1}{2}} > 0$ (resp. $2^{n-2}\#W_f^{*-1}(0) > 0$ if $n \geqslant 2$), these conditions imply $r(n) < 2^{n-1} - 2^{\frac{n}{2}-1}$ and therefore $\rho_B(n) \leq \lfloor r_n \rfloor \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 1$. But $\rho_B(n)$, as $2^{n-1} - 2^{\frac{n}{2}-1}$ for $n \geq 4$, is always even, so $\rho_B(n) \leq \lfloor r_n \rfloor - (\lfloor r_n \rfloor \bmod 2) \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2$.

For odd $n \geq 5$, we have also $\rho_B(n) \leq r(n) < 2^{n-1} - 2^{\frac{n}{2}-1}$, but here $2^{n-1} - 2^{\frac{n}{2}-1}$ is not integer but just a real positive number. Consequently $\rho_B(n) \leq \lfloor r_n \rfloor \leq \lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \rfloor$ and the Corollary is proved. ■

We have the following similar result for $\rho(n)$.

Corollary 11 *Let be $f \in C(n)$ for odd $n \geq 3$.*
If $J_f \subsetneq I - \{0\}$ (resp. $J_f = I - \{0\}$) , we denote
$$r_n = 2^{n-1} - \left[2^{n-2} + \frac{i}{2}\left(\#|W_f^*|^{-1}(i)\right)^{\frac{1}{2}}\right]^{\frac{1}{2}} \text{ (resp. } r_n = 2^{n-1} - \frac{2^{n-1}}{\left(2^n - \#W_f^{*-1}(0)\right)^{\frac{1}{2}}}\text{)}.$$
Let be $b(n) = \lfloor r_n \rfloor - (\lfloor r_n \rfloor \bmod 2)$. We have $\rho(n) \leq b(n) \leq \lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \rfloor$.

Proof. The same as Corollary 10. ■

5 Conclusion

We have obtained theoretical upper bounds (7),(8) on $\rho(n)$ and $\rho_B(n)$. Except the already known $\rho(n)$ for even n, theses bounds minorate the H.K.M. bound. In the case where exists $f \in C(n)$ or $f \in E(n)$, according to $J_f \subsetneq I - \{0\}$ or $J_f = I - \{0\}$, new upper bounds $b(n), b_B(n)$ deduced from(13), (15) and (16) have been derived. Although $b(n)$ and $b_B(n)$ be actually only theoretical, they improve the H.K.M. bound. So, in a further work, one may ask how to deduce from Corollary 9 more explicit results on these new bounds.

References

[1] O. S. Rothaus, "On 'bent' functions," *J. Comb. Theory,* ser. A, vol.20, pp. 300-305, 1976.

[2] T. Helleseth, T. Kløve, J. Mykkeltveit, "On the covering radius of binary codes," *IEEE Trans. Inform. Theory,* vol. IT-24, pp. 627-628, July 1978.

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

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

[5] M. Mitton, "On maximally non linear and extremal balanced boolean functions", *J. Discr. Math. Sciences & Crypto.*, vol. 5, no. 3, pp. 231-253, December 2002.