Advances in Mathematics of Communications
Volume 2, No. 4, 2008, 421–431
doi:10.3934/amc.2008.2.421

ON THE CONSTRUCTION OF BENT FUNCTIONS OF $n+2$ VARIABLES FROM BENT FUNCTIONS OF n VARIABLES

Joan-Josep Climent

Institut Universitari d'Investigació Informàtica
Departament de Ciència de la Computació i Intel·ligència Artificial
Universitat d'Alacant, Ap. correus 99, E-03080 Alacant, Spain

Francisco J. García

Departament de Fonaments de l'Anàlisi Econòmica
Universitat d'Alacant, Ap. correus 99, E-03080 Alacant, Spain

Verónica Requena

Departament de Ciència de la Computació i Intel·ligència Artificial
Universitat d'Alacant, Ap. correus 99, E-03080 Alacant, Spain

(Communicated by Joachim Rosenthal)

Abstract. In this paper we present a method to construct iteratively new bent functions of $n+2$ variables from bent functions of n variables using minterms of n variables and minterms of two variables. Also, we provide the number of bent functions of $n+2$ variables that we can obtain with the method here presented.

1. Introduction

At the present time, S-boxes are an essential component in block ciphers. The implementation of an S-box needs nonlinear Boolean functions to guarantee the cryptographic effectiveness in order to resist powerful methods of attack such as the differential cryptanalysis. For an even number of inputs, Boolean functions of maximum nonlinearity are bent functions. Although may bent functions have been found, their properties, their classification, ad their number are not totally known yet.

There are two families of methods for the construction of good S-boxes for cryptographic applications. The simplest method is the direct construction of truth tables. For that purpose, Boolean functions that satisfy the strict avalanche criterion are used [17]. Nevertheless, we are still very far from having an exhaustive general method for their construction. Alternatively, there is a method consisting in obtaining nonlinear functions by random generation [6]. However multidimensional functions with the highest nonlinearity are not frequent, so it becomes difficult to find them randomly. Millan, Clark, and Dawson [12] use genetic algorithms to

2000 *Mathematics Subject Classification:* Primary: 06E30; Secondary: 94A60.

Key words and phrases: Boolean function, bent function, linear function, balanced function, nonlinearity, truth table, Hamming weight, minterm.

This work was partially supported by Spanish grant MTM2005-05759. The work of the third author was also supported by a grant for research students from the Vicerectorat d'Investigació, Desenvolupament i Innovació of the Universitat d'Alacant.

obtain Boolean functions with highly nonlinearity that are only effective in some particular cases.

It is well-known how to construct one-to-one S-boxes such that any linear combination of the output functions is balanced. It is also well-known with the process by which such linear combinations become bent. What is still unknown is the means for constructing all the S-boxes which satisfy those properties. It is for this reason that the study of the properties of bent functions and the methods to construct them have received a very high attention in the last decades.

The origin of bent functions goes back to a theoretical article of McFarland [11] on sets of finite differences in finite groups. One year after, Dillon [5] in his doctoral thesis systematized and extended the ideas of McFarland, proving a great quantity of properties. For example, all bent functions of $n > 2$ variables has degree at most $n/2$, there are bent functions with degree equal to $n/2$, and the only symmetrical bent functions are the quadratic ones, existing exactly four of those functions for each n. The name *bent* for these functions is due to Rothaus [14].

From the truth tables of bent functions and linear functions, it is possible to construct bent functions with a greater number of variables. But not all the bent functions in 6 variables can be obtained from bent functions and linear functions with a smaller number of variables, as proved Chang [3]. This does not mean that it is not interesting to construct bent functions from functions with a fewer number of variables, but it is not possible to generate *all* of them in this way. In fact, thanks to Canteaut and Charpin [1] we know two infinite families of bent functions in n variables that cannot be obtained from bent functions of smaller number of variables. In that paper, the authors also describe how to obtain Boolean functions of $n-1$ and $n-2$ variables with a very high nonlinearity from a bent function of n variables.

Following a different strategy, Hou and Langevin [10] described how, from a well-known bent function, new bent functions can be obtained with the same number of variables.

Another way to analyze bent functions consists in exploring the properties of the algebraic structures on $\mathrm{GF}(2^n)$ (see, for example, [2, 8, 9]). By this procedure some authors have been able to determine all the cubic bent functions in 8 variables from the cubic bent functions in 6 variables (see [7]), to find some homogeneous bent functions of degree 3 and with 8 or 10 variables (see [4]), or to characterize the homogeneous functions of 6 variables and degree 3 that are bent and those that are balanced (see [13]). Qu, Seberry, and Pieprzyk [13] also discuss why the homogeneous functions could be very useful to design hash functions.

The mentioned literature makes an intensive use of the representation of Boolean functions in polynomial form, in matrix form and in sequential form. Nevertheless, the classical concept of minterm, which is, by the way, directly related to the implementation of logic circuits and its complexity, has not been frequently used.

This paper addresses the practical purposes involved in the generation of bent functions using the representation of Boolean functions as a sum of minterms. We will use this concept to obtain, from bent functions of n variables, new bent functions of $n+2$ variables.

The rest of the paper is organized as follows. Firstly, in Section 2 we introduce some basic definitions and notations that are used. In Section 3, we present a general method to construct bent functions of $n+2$ variables from a bent function of n variables. Finally, in Section 4 we prove some results that allow us to verify that all bent functions obtained following the method introduced in Section 3 are all different; then we count the number of bent functions we can construct with that method. Also, we construct a bent function which is not a Maiorana-McFarland function.

2. Preliminaries

Consider the binary field $\mathbb{Z}_2$ with the addition modulo 2 (denoted by $\oplus$) and the multiplication modulo 2. For any positive integer n, it is well-known that $\mathbb{Z}_2^n$ is a linear space over $\mathbb{Z}_2$ with the addition $\oplus$ given by

$$\boldsymbol{a} \oplus \boldsymbol{b} = (a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_n \oplus b_n)$$

for $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ and $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)$ in $\mathbb{Z}_2^n$. Also, we consider the inner product

$$\langle \boldsymbol{a}, \boldsymbol{b} \rangle = a_1 b_1 \oplus a_2 b_2 \oplus \cdots \oplus a_n b_n$$

of $\boldsymbol{a}$ and $\boldsymbol{b}$. Furthermore, we say that $\boldsymbol{a} < \boldsymbol{b}$ if there exists k (with $1 \le k \le n$) such that

$$a_1 = b_1,\ a_2 = b_2,\ \ldots,\ a_{k-1} = b_{k-1} \quad \text{but} \quad a_k = 0 \text{ and } b_k = 1.$$

So we can order the elements $\boldsymbol{e}_0, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_{2^n-1}$ of $\mathbb{Z}_2^n$ such that

$$\boldsymbol{e}_0 < \boldsymbol{e}_1 < \cdots < \boldsymbol{e}_{2^n-1}.$$

Finally, if $\boldsymbol{e}_i = (e_1^{(i)}, e_2^{(i)}, \ldots, e_{n-1}^{(i)}, e_n^{(i)}) \in \mathbb{Z}_2^n$, then

$$e_1^{(i)} 2^{n-1} + e_2^{(i)} 2^{n-2} + \cdots + e_{n-1}^{(i)} 2^1 + e_n^{(i)} 2^0 = i$$

and we call $\boldsymbol{e}_i$ the binary expansion of i. With this representation, we can identify the vector $\boldsymbol{e}_i$ with the integer i, and consequently, we can identify $\mathbb{Z}_2^n$ with $\mathbb{Z}_{2^n}$.

A Boolean function of n variables is a mapping $f : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$. We denote by $\mathcal{B}_n$ the set of Boolean functions of n variables. $\mathcal{B}_n$ is also a linear space over $\mathbb{Z}_2$ with the addition $\oplus$ given by

$$(f \oplus g)(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus g(\boldsymbol{x})$$

for $f, g \in \mathcal{B}_n$.

For a function f of $\mathcal{B}_n$, the $(0,1)$-sequence of length 2^n

$$\boldsymbol{\xi}_f = (f(\boldsymbol{e}_0), f(\boldsymbol{e}_1), \ldots, f(\boldsymbol{e}_{2^n-1}))$$

is called the **truth table** of f. The truth table of a Boolean function can be obtained by its minterms. A **minterm** on n variables $x_1, x_2, \ldots, x_n$ is an expression of the form

$$m_{(u_1,u_2,\ldots,u_n)}(x_1, x_2, \ldots, x_n) = (1 \oplus u_1 \oplus x_1)(1 \oplus u_2 \oplus x_2) \cdots (1 \oplus u_n \oplus x_n)$$

where $(u_1, u_2, \ldots, u_n) \in \mathbb{Z}_2^n$.

Now, for $i = 0, 1, 2, \ldots, 2^n - 1$, it is clear that $m_{\boldsymbol{e}_i}(\boldsymbol{x}) = 1$ if and only if $\boldsymbol{x} = \boldsymbol{e}_i$. We will write $m_i(\boldsymbol{x})$ instead of $m_{\boldsymbol{e}_i}(\boldsymbol{x})$. So, the truth table

$$(m_i(\boldsymbol{e}_0), m_i(\boldsymbol{e}_1), \ldots, m_i(\boldsymbol{e}_{2^n-1}))$$

of $m_i(\boldsymbol{x})$ has a 1 in the ith position and 0 elsewhere. Consequently,

$$\bigoplus_{i=0}^{2^n-1} m_i(\boldsymbol{x}) = 1. \tag{1}$$

Also, since $m_i(\boldsymbol{x}) = m_j(\boldsymbol{x})$ if and only if $i = j$, we can identify the minterm $m_i(\boldsymbol{x})$ with the integer i (or with the vector $\boldsymbol{e}_i$).

Now, for all $f \in \mathcal{B}_n$ it is well-known that

$$f(\boldsymbol{x}) = \bigoplus_{i=0}^{2^n-1} f(\boldsymbol{e}_i)\ m_i(\boldsymbol{x}) \tag{2}$$

and since the identity

$$\bigoplus_{i=0}^{2^n-1} a_i\ m_i(\boldsymbol{x}) = 0$$

implies $a_i = 0$ for $i = 0, 1, \ldots, 2^n - 1$, we can state that the set $\{m_0, m_1, \ldots, m_{2^n-1}\}$ is a basis of $\mathcal{B}_n$.

We call the **support** of f the set

$$M = \{\boldsymbol{a} \in \mathbb{Z}_2^n \mid f(\boldsymbol{a}) = 1\} \quad \text{or} \quad M = \{i \in \mathbb{Z}_{2^n} \mid f(\boldsymbol{e}_i) = 1\}$$

according to the expression (2) and the identification of $\mathbb{Z}_2^n$ with $\mathbb{Z}_{2^n}$. So, we can identify M as the set of minterms of $f(\boldsymbol{x})$. Therefore, we can rewrite expression (2) as

$$f(\boldsymbol{x}) = \bigoplus_{i \in M} m_i(\boldsymbol{x}).$$

where $M \subseteq \mathbb{Z}_2^n$ or $M \subseteq \mathbb{Z}_{2^n}$ as best suited.

The **Hamming weight** of a $(0,1)$-sequence $\boldsymbol{\alpha}$, denoted by $w(\boldsymbol{\alpha})$, is the number of 1s in $\boldsymbol{\alpha}$. The **Hamming distance** between two $(0,1)$-sequences $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, denoted by $d(\boldsymbol{\alpha}, \boldsymbol{\beta})$, is the number of positions where the two sequences differ. It is well-know that $d(\boldsymbol{\alpha}, \boldsymbol{\beta}) = w(\boldsymbol{\alpha} \oplus \boldsymbol{\beta})$.

Let f be a Boolean function and $\boldsymbol{\xi}_f$ its truth table. The **Hamming weight** of f, denoted by $w(f)$, is the Hamming weight of $\boldsymbol{\xi}_f$; that is $w(f) = w(\boldsymbol{\xi}_f)$, and therefore, $w(f)$ is the number of minterms in the expression of $f(\boldsymbol{x})$ as a sum of minterms.

Let f and g be two functions of $\mathcal{B}_n$ and $\boldsymbol{\xi}_f$ and $\boldsymbol{\xi}_g$ be the corresponding truth tables. The **Hamming distance** between f and g, denoted by $d(f, g)$, is the Hamming distance between $\boldsymbol{\xi}_f$ and $\boldsymbol{\xi}_g$; that is, $d(f, g) = d(\boldsymbol{\xi}_f, \boldsymbol{\xi}_g)$.

A $(0,1)$-sequence is **balanced** if it contains an equal number of 0s and 1s, so a function f in $\mathcal{B}_n$ is **balanced** if its truth table is balanced.

We say that f in $\mathcal{B}_n$ is an **affine function** if it takes the form

$$f(\boldsymbol{x}) = \langle \boldsymbol{a}, \boldsymbol{x} \rangle \oplus b$$

where $\boldsymbol{a} \in \mathbb{Z}_2^n$ and $b \in \mathbb{Z}_2$. If $b = 0$, f is called a **linear function**. The set of affine functions is denoted by $\mathcal{A}_n$.

The **nonlinearity** of a function f in $\mathcal{B}_n$ is defined as

$$\mathrm{NL}(f) = \min\{d(f, \varphi) \mid \varphi \in \mathcal{A}_n\}$$

which is upper bounded (see [16]) by

$$\mathrm{NL}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

The Boolean functions that achieve the maximum nonlinearity are called **bent functions** (see [16]). As a consequence, bent functions only exist for n even.

The following result (see [15, 16]), that we quote for further references, gives us a characterization of a bent function.

Theorem 1. *Let $f(\boldsymbol{x})$ be a function in $\mathcal{B}_n$. The following statements are equivalent.*

1. *$f(\boldsymbol{x})$ is a bent function.*
2. *For any $\boldsymbol{a} \in \mathbb{Z}_2^n \backslash \{\boldsymbol{0}\}$ the Boolean function $g_{\boldsymbol{a}}(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus f(\boldsymbol{a} \oplus \boldsymbol{x})$ is balanced.*

3. *For any $\boldsymbol{a} \in \mathbb{Z}_2^n$ the number of 1s in the truth table of the Boolean function $h_{\boldsymbol{a}}(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus \langle \boldsymbol{a}, \boldsymbol{x} \rangle$ is $2^{n-1} \pm 2^{\frac{n}{2}-1}$.*

As a consequence of the previous theorem, the number of 1s in the truth table of a bent function $f(\boldsymbol{x})$ of n variables is $2^{n-1} \pm 2^{\frac{n}{2}-1}$; so that $f(\boldsymbol{x})$ is not balanced. Equivalently, the number of minterms in the expression of $f(\boldsymbol{x})$ as a sum of minterms is $2^{n-1} \pm 2^{\frac{n}{2}-1}$.

Furthermore, it is well-known that for any bent function $f(\boldsymbol{x})$ of n variables, the function $1 \oplus f(\boldsymbol{x})$ is a bent function of n variables too.

3. Main results

In the rest of the paper, we consider that $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ is a vector of $\mathbb{Z}_2^n$ and that $\boldsymbol{y} = (y_1, y_2)$ is a vector of $\mathbb{Z}_2^2$.

Firstly, we introduce two important properties of the minterms which allow us to construct functions of $n+2$ variables from functions of n variables. In fact, for each minterm of n variables, we can obtain four different minterms of $n+2$ variables.

Lemma 1. *Suppose that $a \in \mathbb{Z}_{2^n}$ and $b \in \mathbb{Z}_{2^2}$. If $m_a(\boldsymbol{x})$ is a minterm of n variables and $m_b(\boldsymbol{y})$ is a minterm of 2 variables, then $m_c(\boldsymbol{y}, \boldsymbol{x}) = m_b(\boldsymbol{y}) m_a(\boldsymbol{x})$ is a minterm of $n+2$ variables where*

$$c = b_1 2^{n+1} + b_2 2^n + a \quad \textit{and} \quad b = b_1 2 + b_2.$$

Proof. Assume that $(a_1, a_2, \ldots, a_n)$ is the binary expansion of the integer a; that is $a = a_1 2^{n-1} + a_2 2^{n-2} + \cdots + a_{n-1} 2 + a_n$. Since (b_1, b_2) is the binary expansion of b, we have that

$$\begin{aligned} m_b(\boldsymbol{y})\ m_a(\boldsymbol{x}) &= m_{(b_1,b_2)}(\boldsymbol{y})\ m_{(a_1,a_2,\ldots,a_n)}(\boldsymbol{x}) \\ &= (1 \oplus b_1 \oplus y_1)(1 \oplus b_2 \oplus y_2)(1 \oplus a_1 \oplus x_1) \\ &\quad\ (1 \oplus a_2 \oplus x_2) \cdots (1 \oplus a_n \oplus x_n) \\ &= m_{(b_1,b_2,a_1,a_2,\ldots,a_n)}(\boldsymbol{y}, \boldsymbol{x}) = m_c(\boldsymbol{y}, \boldsymbol{x}), \end{aligned}$$

because $(b_1, b_2, a_1, a_2, \ldots, a_n)$ is the binary expansion of c. □

The proof of the previous lemma tells us that for each minterm of n variables we can obtain the following four minterms of $n+2$ variables

$$m_a(\boldsymbol{y}, \boldsymbol{x}), \quad m_{2^n+a}(\boldsymbol{y}, \boldsymbol{x}), \quad m_{2^{n+1}+a}(\boldsymbol{y}, \boldsymbol{x}), \quad \text{and} \quad m_{2^n+2^{n+1}+a}(\boldsymbol{y}, \boldsymbol{x}).$$

The following theorem is the main result of this paper. Here, we describe an iterative method to construct bent functions of $n+2$ variables, from two bent functions of n variables.

Theorem 2. *Let $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ be bent functions of n variables and assume that (i_0, i_1, i_2, i_3) is any permutation of $(0, 1, 2, 3)$. Then*

$$B(\boldsymbol{y}, \boldsymbol{x}) = (m_{i_0}(\boldsymbol{y}) \oplus m_{i_1}(\boldsymbol{y}))\, f_0(\boldsymbol{x}) \oplus m_{i_2}(\boldsymbol{y}) f_1(\boldsymbol{x}) \oplus m_{i_3}(\boldsymbol{y})(1 \oplus f_1(\boldsymbol{x}))$$

is a bent function of $n+2$ variables.

Proof. According to Theorem 1 we must prove that the number of 1s of the truth table (that is, the number of minterms) of the Boolean function

$$B_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y}, \boldsymbol{x}) = B(\boldsymbol{y}, \boldsymbol{x}) \oplus \langle (\boldsymbol{b}, \boldsymbol{a}), (\boldsymbol{y}, \boldsymbol{x}) \rangle$$

is $2^{n+1} \pm 2^{\frac{n}{2}}$ for all $(\boldsymbol{b}, \boldsymbol{a}) \in \mathbb{Z}_2^2 \times \mathbb{Z}_2^n$.

y_1	y_2	$\boldsymbol{x}$	$m_0(\boldsymbol{y})$	$m_1(\boldsymbol{y})$	$m_2(\boldsymbol{y})$	$m_3(\boldsymbol{y})$	$B_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$
$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\tau}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\mathbf{0}$	$\mathbf{1}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\xi}_0 \oplus b_2\mathbf{1} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\mathbf{1}$	$\mathbf{0}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0}$	$\boldsymbol{\xi}_1 \oplus b_1\mathbf{1} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\mathbf{1}$	$\mathbf{1}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1} \oplus \boldsymbol{\xi}_1 \oplus b_1\mathbf{1} \oplus b_2\mathbf{1} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$

Table 1. Truth table of $B_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$

$b_1 = 0 \quad b_2 = 0$	$b_1 = 0 \quad b_2 = 1$	$b_1 = 1 \quad b_2 = 0$	$b_1 = 1 \quad b_2 = 1$
$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \mathbf{1} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \mathbf{1} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus \mathbf{1} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus \mathbf{1} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\mathbf{1} \oplus \boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\mathbf{1} \oplus \boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$

Table 2. Truth table of $B_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ for the different values of $\boldsymbol{b} = (b_1, b_2)$

Let us assume that $(i_0, i_1, i_2, i_3) = (0, 1, 2, 3)$. Then

$$\begin{aligned} B_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}) = {} & (m_0(\boldsymbol{y}) \oplus m_1(\boldsymbol{y}))\, f_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) f_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})(1 \oplus f_1(\boldsymbol{x})) \\ & \oplus b_1 y_1 \oplus b_2 y_2 \oplus \langle \boldsymbol{a}, \boldsymbol{x} \rangle \end{aligned}$$

where $\boldsymbol{b} = (b_1, b_2)$.

So, if $\mathbf{0}$ and $\mathbf{1}$ are the $2^n \times 1$ arrays with all entries equal to 0 and 1 respectively; $\boldsymbol{\tau}$ is the $2^n \times n$ array whose ith row is $\boldsymbol{e}_i$; $\boldsymbol{\xi}_0$ and $\boldsymbol{\xi}_1$ are the truth table of $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ respectively; and $\boldsymbol{\Lambda}_{\boldsymbol{a}}$ is the truth table of the linear function $\langle \boldsymbol{a}, \boldsymbol{x} \rangle$, then the last column of Table 1 shows the truth table of $B_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$. Now, each column of Table 2 represents the four blocks of the truth table of $B_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ for the different values of $\boldsymbol{b}$.

Since $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ are bent functions, from Theorem 1, we have that, for $j = 0, 1$, the number of 1s of $\boldsymbol{\xi}_j \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$ is $2^{n-1} \pm 2^{\frac{n}{2}-1}$, and therefore, the number of 1s of $\boldsymbol{\xi}_j \oplus \mathbf{1} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$ is $2^{n-1} \mp 2^{\frac{n}{2}-1}$. So, in any case, we have three blocks in which the number of 1s is $2^{n-1} + 2^{\frac{n}{2}-1}$ and one block in which the number of 1s is $2^{n-1} - 2^{\frac{n}{2}-1}$, or three blocks in which the number of 1s is $2^{n-1} - 2^{\frac{n}{2}-1}$ and one block in which the number of 1s is $2^{n-1} + 2^{\frac{n}{2}-1}$. Consequently, the number of minterms of $B_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ is always $2^{n+1} + 2^{\frac{n}{2}}$ or $2^{n+1} - 2^{\frac{n}{2}}$.

Finally, if (i_0, i_1, i_2, i_3) is a permutation of $(0, 1, 2, 3)$ other than $(0, 1, 2, 3)$, then the four blocks of the truth table of $B_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ given in Table 2 are permuted according to (i_0, i_1, i_2, i_3) and therefore, the same result follows. □

Note that as a consequence of Lemma 1 and Theorem 2 if M_0 and M_1 are the set of minterms of $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$, respectively, and if (b_0, b_1, b_2, b_3) is a permutation of $(0, 2^n, 2^{n+1}, 2^n + 2^{n+1})$, then the set of minterms of the bent function $B(\boldsymbol{y}, \boldsymbol{x})$ constructed in Theorem 2 is

$$\begin{aligned} M = {} & \{b_0 + b \mid b \in M_0\} \cup \{b_1 + b \mid b \in M_0\} \\ & \cup \{b_2 + b \mid b \in M_1\} \cup \left\{b_3 + b \mid b \in \bar{M}_1\right\} \end{aligned} \tag{3}$$

where $\bar{M}_1 = \mathbb{Z}_{2^n} \setminus M_1$ is the set of minterms of $1 \oplus f_1(\boldsymbol{x})$. The sets of the second hand of expression (3) are pairwise disjoints by Lemma 1.

4. Counting bent functions

In this section we introduce some results in order to compute the number of bent functions that we can construct using Theorem 2.

Firstly we consider two particular cases (see Corollaries 1 and 2 bellow) that we can derive directly from Theorem 2. The first one corresponds to the case

$$f_1(\boldsymbol{x}) = f_0(\boldsymbol{x}) \quad \text{or} \quad f_1(\boldsymbol{x}) = 1 \oplus f_0(\boldsymbol{x})$$

and it is based on the fact that (see expression (1))

$$m_0(\boldsymbol{y}) \oplus m_1(\boldsymbol{y}) \oplus m_2(\boldsymbol{y}) \oplus m_3(\boldsymbol{y}) = 1.$$

The second one coresponds to the case

$$f_1(\boldsymbol{x}) \neq f_0(\boldsymbol{x}) \quad \text{and} \quad f_1(\boldsymbol{x}) \neq 1 \oplus f_0(\boldsymbol{x}).$$

Corollary 1. *If $f(\boldsymbol{x})$ is a bent function of n variables and if $i \in \{0,1,2,3\}$, then*

$$F_f(\boldsymbol{y},\boldsymbol{x}) = f(\boldsymbol{x}) \oplus m_i(\boldsymbol{y})$$

is a bent function of $n+2$ variables.

Corollary 2. *Let $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ be bent functions of n variables such that*

$$f_1(\boldsymbol{x}) \neq f_0(\boldsymbol{x}) \qquad \text{and} \qquad f_1(\boldsymbol{x}) \neq 1 \oplus f_0(\boldsymbol{x}). \tag{4}$$

If (i_0,i_1,i_2,i_3) is any permutation of $(0,1,2,3)$, then

$$G_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x}) = (m_{i_0}(\boldsymbol{y}) \oplus m_{i_1}(\boldsymbol{y}))\, f_0(\boldsymbol{x}) \oplus m_{i_2}(\boldsymbol{y}) f_1(\boldsymbol{x}) \oplus m_{i_3}(\boldsymbol{y})\,(1 \oplus f_1(\boldsymbol{x}))$$

is a bent function of $n+2$ variables.

The next result establishes that the bent functions constructed in Corollary 1 are all different.

Lemma 2. *Let $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ be different bent functions of n variables. If $F_f(\boldsymbol{y},\boldsymbol{x})$ and $F_g(\boldsymbol{y},\boldsymbol{x})$ are the bent functions constructed in Corollary 1 using $f(\boldsymbol{x})$ and $i \in \{0,1,2,3\}$, and $g(\boldsymbol{x})$ and $j \in \{0,1,2,3\}$, respectively, then*

$$F_f(\boldsymbol{y},\boldsymbol{x}) \neq F_g(\boldsymbol{y},\boldsymbol{x}).$$

Proof. If $\boldsymbol{\xi}$ and $\boldsymbol{\eta}$ are the truth tables of $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ respectively, then the truth table of $F_f(\boldsymbol{y},\boldsymbol{x})$ and $F_g(\boldsymbol{y},\boldsymbol{x})$ have four blocks (not necessarily in that order and not the same order for all):

$$\begin{array}{lcccc} F_f: & \boldsymbol{\xi} & \boldsymbol{\xi} & \boldsymbol{\xi} & \boldsymbol{1} \oplus \boldsymbol{\xi}, \\ F_g: & \boldsymbol{\eta} & \boldsymbol{\eta} & \boldsymbol{\eta} & \boldsymbol{1} \oplus \boldsymbol{\eta}. \end{array}$$

Since $f(\boldsymbol{x}) \neq g(\boldsymbol{x})$, we know that $\boldsymbol{\xi} \neq \boldsymbol{\eta}$. Therefore, if $F_f(\boldsymbol{y},\boldsymbol{x}) = F_g(\boldsymbol{y},\boldsymbol{x})$, necessarily $\boldsymbol{\xi} = \boldsymbol{1} \oplus \boldsymbol{\eta}$ and $\boldsymbol{\xi} = \boldsymbol{\eta}$ which is a contradiction.

So, $F_f(\boldsymbol{y},\boldsymbol{x}) \neq F_g(\boldsymbol{y},\boldsymbol{x})$. □

The next result establishes that the bent functions constructed in Corollary 2 are all different.

Lemma 3. *Let $f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x})$, $g_0(\boldsymbol{x})$, and $g_1(\boldsymbol{x})$ be bent functions of n variables such that*

- $f_0(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$,
- $f_1(\boldsymbol{x}) \neq f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x}) \neq 1 \oplus f_0(\boldsymbol{x})$,
- $g_1(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$, $g_1(\boldsymbol{x}) \neq 1 \oplus g_0(\boldsymbol{x})$.

Assume also that (i_0, i_1, i_2, i_3) *and* (j_0, j_1, j_2, j_3) *are permutations of* $(0, 1, 2, 3)$*. If* $G_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x})$ *and* $G_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x})$ *are the bent functions constructed in Corollary 2 using the functions* $f_0(\boldsymbol{x})$ *and* $f_1(\boldsymbol{x})$*, and the permutation* (i_0, i_1, i_2, i_3)*, and the functions* $g_0(\boldsymbol{x})$ *and* $g_1(\boldsymbol{x})$*, and the permutation* (j_0, j_1, j_2, j_3)*, respectively, then*

$$G_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x}) \neq G_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x}).$$

Proof. If $\boldsymbol{\xi}_0$, $\boldsymbol{\xi}_1$, $\boldsymbol{\eta}_0$, and $\boldsymbol{\eta}_1$ are the truth tables of $f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x})$, $g_0(\boldsymbol{x})$, and $g_1(\boldsymbol{x})$, respectively, then the truth tables of $G_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x})$ and $G_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x})$ have four blocks (not necessarily in that order and not in the same order for all):

$$\begin{array}{lllll} G_{f_0,f_1}: & \boldsymbol{\xi}_0 & \boldsymbol{\xi}_0 & \boldsymbol{\xi}_1 & \mathbf{1} \oplus \boldsymbol{\xi}_1, \\ G_{g_0,g_1}: & \boldsymbol{\eta}_0 & \boldsymbol{\eta}_0 & \boldsymbol{\eta}_1 & \mathbf{1} \oplus \boldsymbol{\eta}_1. \end{array}$$

Since $f_0(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$, we know that $\boldsymbol{\xi}_0 \neq \boldsymbol{\eta}_0$. Therefore, if $G_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x}) = G_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x})$ then we have one of the following cases:

- $\boldsymbol{\xi}_0 = \boldsymbol{\eta}_1$, $\boldsymbol{\xi}_0 = \boldsymbol{\eta}_1 \oplus \mathbf{1}$, $\boldsymbol{\xi}_1 = \boldsymbol{\eta}_0$, and $\boldsymbol{\xi}_1 \oplus \mathbf{1} = \boldsymbol{\eta}_0$.
- $\boldsymbol{\xi}_0 = \boldsymbol{\eta}_1 \oplus \mathbf{1}$, $\boldsymbol{\xi}_0 = \boldsymbol{\eta}_1$, $\boldsymbol{\xi}_1 = \boldsymbol{\eta}_0$, and $\boldsymbol{\xi}_1 \oplus \mathbf{1} = \boldsymbol{\eta}_0$.

But, then $f_i(\boldsymbol{x}) = f_i(\boldsymbol{x}) \oplus 1$ and $g_i(\boldsymbol{x}) = g_i(\boldsymbol{x}) \oplus 1$, for $i = 0, 1$, which is a contradiction.

So, $G_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x}) \neq G_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x})$. □

One question that arises at this point is the following: starting with the same bent function $f_0(\boldsymbol{x})$ of n variables, the bent functions $F_{f_0}(\boldsymbol{y}, \boldsymbol{x})$ and $G_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x})$ in $n + 2$ variables (for any bent function $f_1(\boldsymbol{x})$ of n variables), constructed following Corollaries 1 and 2 respectivelly are will they be different? And indeed they are and the following result will prove it.

Lemma 4. *Let* $f_0(\boldsymbol{x})$ *and* $f_1(\boldsymbol{x})$ *be two bent functions of* n *variables such that* $f_1(\boldsymbol{x}) \neq f_0(\boldsymbol{x})$ *and* $f_1(\boldsymbol{x}) \neq 1 \oplus f_0(\boldsymbol{x})$*. Let* (i_0, i_1, i_2, i_3) *and* (j_0, j_1, j_2, j_3) *be permutations of* $(0, 1, 2, 3)$*. Assume that* $F_{f_0}(\boldsymbol{y}, \boldsymbol{x})$ *and* $G_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x})$ *are the bent functions constructed in Corollaries 1 and 2 using permutations* (i_0, i_1, i_2, i_3) *and* (j_0, j_1, j_2, j_3)*, respectively. Then*

$$F_{f_0}(\boldsymbol{y}, \boldsymbol{x}) \neq G_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x}).$$

Proof. According to Corollaries 1 and 2 we have that

$$\begin{aligned} F_{f_0}(\boldsymbol{y}, \boldsymbol{x}) &= f_0(\boldsymbol{x}) \oplus m_{i_3}(\boldsymbol{y}), \\ G_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x}) &= (m_{j_0}(\boldsymbol{y}) \oplus m_{j_1}(\boldsymbol{y}))\, f_0(\boldsymbol{x}) \oplus m_{j_2}(\boldsymbol{y}) f_1(\boldsymbol{x}) \oplus m_{j_3}(\boldsymbol{y})\,(1 \oplus f_1(\boldsymbol{x})). \end{aligned}$$

If $\boldsymbol{\xi}_0$ and $\boldsymbol{\xi}_1$ are the truth tables of $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$, respectively, then the truth table of $F_{f_0}(\boldsymbol{y}, \boldsymbol{x})$ and $G_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x})$ have four blocks (not necessarily in that order and not the same order for all):

$$\begin{array}{lllll} F_{f_0}: & \boldsymbol{\xi}_0 & \boldsymbol{\xi}_0 & \boldsymbol{\xi}_0 & \mathbf{1} \oplus \boldsymbol{\xi}_0, \\ G_{f_0,f_1}: & \boldsymbol{\xi}_0 & \boldsymbol{\xi}_0 & \boldsymbol{\xi}_1 & \mathbf{1} \oplus \boldsymbol{\xi}_1. \end{array}$$

Now, since $\boldsymbol{\xi}_1 \neq \boldsymbol{\xi}_0$ and $\boldsymbol{\xi}_1 \neq 1 \oplus \boldsymbol{\xi}_0$, it is evident that $F_{f_0}(\boldsymbol{y}, \boldsymbol{x}) \neq G_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x})$, because $F_{f_0}(\boldsymbol{y}, \boldsymbol{x})$ has three blocks $\boldsymbol{\xi}_0$ and $G_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x})$ only has two blocks $\boldsymbol{\xi}_0$. □

Another question that appears at this point is the following: Let $F_{f_0}(\boldsymbol{y}, \boldsymbol{x})$ and $G_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x})$ be bent functions of $n + 2$ variables, constructed according to Corollaries 1 and 2, but starting with bent functions of n variables $f_0(\boldsymbol{x})$, and $g_0(\boldsymbol{x})$ and $g_1(\boldsymbol{x})$, respectively; if $f_0(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$ is it possible that $F_{f_0}(\boldsymbol{y}, \boldsymbol{x}) = G_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x})$? Next result shows that this situation can not occur.

Lemma 5. *Let $f_0(\boldsymbol{x})$, $g_0(\boldsymbol{x})$, and $g_1(\boldsymbol{x})$ be bent functions of n variables such that:*

- $f_0(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$,
- $g_1(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$, $g_1(\boldsymbol{x}) \neq 1 \oplus g_0(\boldsymbol{x})$.

Assume that (i_0, i_1, i_2, i_3) and (j_0, j_1, j_2, j_3) are permutations of $(0,1,2,3)$. If $F_{f_0}(\boldsymbol{y}, \boldsymbol{x})$ and $G_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x})$ are the bent functions constructed in Corollaries 1 and 2 using the bent functions $f_0(\boldsymbol{x})$ and the permutation (i_0, i_1, i_2, i_3), and the bent functions $g_0(\boldsymbol{x})$ and $g_1(\boldsymbol{x})$, and the permutation (j_0, j_1, j_2, j_3), respectively. Then

$$F_{f_0}(\boldsymbol{y}, \boldsymbol{x}) \neq G_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x}).$$

Proof. According to Corollaries 1 and 2 we have that

$$\begin{aligned} F_{f_0}(\boldsymbol{y}, \boldsymbol{x}) &= f_0(\boldsymbol{x}) \oplus m_{i_3}(\boldsymbol{y}), \\ G_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x}) &= \left(m_{j_0}(\boldsymbol{y}) \oplus m_{j_1}(\boldsymbol{y})\right) g_0(\boldsymbol{x}) \oplus m_{j_2}(\boldsymbol{y}) g_1(\boldsymbol{x}) \oplus m_{j_3}(\boldsymbol{y}) \left(1 \oplus g_1(\boldsymbol{x})\right). \end{aligned}$$

If $\boldsymbol{\xi}_0$, $\boldsymbol{\eta}_0$, and $\boldsymbol{\eta}_1$ are the truth tables of $f_0(\boldsymbol{x})$, $g_0(\boldsymbol{x})$, and $g_1(\boldsymbol{x})$, respectively, then the truth tables of $F_{f_0}(\boldsymbol{y}, \boldsymbol{x})$ and $G_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x})$ have four blocks (not necessarily in that order and not the same order for all):

$$F_{f_0}: \quad \boldsymbol{\xi}_0 \quad \boldsymbol{\xi}_0 \quad \boldsymbol{\xi}_0 \quad \mathbf{1} \oplus \boldsymbol{\xi}_0, \tag{5}$$

$$G_{g_0,g_1}: \quad \boldsymbol{\eta}_0 \quad \boldsymbol{\eta}_0 \quad \boldsymbol{\eta}_1 \quad \mathbf{1} \oplus \boldsymbol{\eta}_1. \tag{6}$$

Since $f_0(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$, we have, without loss of generality, that

$$f_0(\boldsymbol{x}) = m_i(\boldsymbol{x}) \oplus f'(\boldsymbol{x})$$

where $m_i(\boldsymbol{x})$ is a minterm that is not in the expression of $g_0(\boldsymbol{x})$ as a sum of minterms.

So, according to expression (5), in the ith position of each one of the four blocks of the truth table of $F_{f_0}(\boldsymbol{y}, \boldsymbol{x})$ we have

$$1 \quad 1 \quad 1 \quad 0$$

but, according to expression (6), in the ith position of each one of the four blocks of the truth table of $G_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x})$ we have

$$0 \quad 0 \quad ? \quad ?$$

depending on $g_1(\boldsymbol{x})$. In any case, it is evident that both truth tables are different.

So, $F_{f_0}(\boldsymbol{y}, \boldsymbol{x}) \neq G_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x})$. □

Now, as a consequence of the previous lemmas, we can obtain the number of bent functions of $n+2$ variables that we can construct using Corollaries 1 and 2.

Theorem 3. *If ν_n is the number of bent functions of n variables, then the number of bent functions of $n+2$ variables that we can construct using Corollaries 1 and 2 is*

$$4\nu_n + \frac{4!}{2!}\nu_n \frac{\nu_n - 2}{2}.$$

Proof. We can choose $f_0(\boldsymbol{x})$ from ν_n different ways.

Fixed $f_0(\boldsymbol{x})$, Corollary 1 provides $4\nu_n$ different bent functions of $n+2$ variables.

Fixed $f_0(\boldsymbol{x})$, if we consider $f_1(\boldsymbol{x}) = f_0(\boldsymbol{x})$ or $f_1(\boldsymbol{x}) = 1 \oplus f_0(\boldsymbol{x})$, we obtain the 4 bent functions of the previous case; so, we can choose $f_1(\boldsymbol{x})$ from $\nu_n - 2$ bent functions but, since the choices $f_1(\boldsymbol{x}) = g(\boldsymbol{x})$ and $f_1(\boldsymbol{x}) = 1 \oplus g(\boldsymbol{x})$ provide the same bent function of $n+2$ variables, we only have $\frac{\nu_n - 2}{2}$ bent functions to choose.

Furthermore, since any permutation of (i_0, i_1) provides the same bent function, we have that Corollary 2 provides, according to Lemma 3,

$$\frac{4!}{2!}\nu_n \frac{\nu_n - 2}{2}$$

bent functions of $n+2$ variables.

The result follows now from the fact that Lemmas 4 and 5 guarantee that bent functions constructed according to Corollaries 1 and 2 are different. □

As a particular case, since $\nu_2 = 8$ we can construct

$$4 \cdot 8 + \frac{4!}{2!} 8 \frac{8-2}{2} = 32 + 288 = 320$$

bent functions of 4 variables. Note that $\nu_4 = 896$.

The following example shows that some bent functions constructed according with Theorem 2 are not Maiorana-McFarland functions.

Example 1. Assume that $n = 2$ and consider the bent functions of 2 variables

$$f_0(\boldsymbol{x}) = m_0(\boldsymbol{x}) \quad \text{and} \quad f_1(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}).$$

Now, according to Corollary 2 and Lemma 1, the Boolean function $B(\boldsymbol{y}, \boldsymbol{x})$ of 4 variables given by

$$\begin{aligned} B(\boldsymbol{y}, \boldsymbol{x}) &= (m_0(\boldsymbol{y}) \oplus m_1(\boldsymbol{y}))f_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})f_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})(1 \oplus f_1(\boldsymbol{x})) \\ &= m_0(\boldsymbol{y}, \boldsymbol{x}) \oplus m_4(\boldsymbol{y}, \boldsymbol{x}) \oplus m_8(\boldsymbol{y}, \boldsymbol{x}) \oplus m_9(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{11}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{14}(\boldsymbol{y}, \boldsymbol{x}) \\ &= 1 \oplus x_1 \oplus x_2 \oplus x_1x_2 \oplus y_1x_2 \oplus y_1y_2 \end{aligned}$$

is a bent function which is not a Maiorana-McFarland function.

References

[1] A. Canteaut and P. Charpin, *Decomposing bent functions*, IEEE Trans. Inform. Theory, **49** (2003), 2004–2019.

[2] C. Carlet and P. Guillot, *A characterization of binary bent functions*, J. Combin. Theory Ser. A, **76** (1996), 328–335.

[3] D. K. Chang, *Binary bent sequences of order* 64, Utilitas Math., **52** (1997), 141–151.

[4] C. Charnes, M. Rötteler and T. Beth, *Homogeneous bent functions, invariants, and designs*, Des. Codes Cryptogr., **26** (2002), 139–154.

[5] J. F. Dillon, "Elementary Hadamard Difference Sets," Ph.D thesis, University of Maryland, 1974.

[6] A. Grocholewska-Czuryło, *A study of differences between bent functions constructed using Rothaus method and randomly generated bent functions*, J. Telecommun. Inform. Techno., **4** (2003), 19–24.

[7] X.-D. Hou, *Cubic bent functions*, Discrete Math., **189** (1998), 149–161.

[8] X.-D. Hou, GL$(m, 2)$ *acting on* $R(r, m)/R(r-1, m)$, Discrete Math., **149** (1996), 99–122.

[9] X.-D. Hou, *On the coefficients of binary bent functions*, Proc. Amer. Math. Soc., **128** (2000), 987–996.

[10] X.-D. Hou and P. Langevin, *Results on bent functions*, J. Combin. Theory Ser. A, **80** (1997), 232–246.

[11] R. L. McFarland, *A family of difference sets in non-cyclic groups*, J. Combin. Theory Ser. A, **15** (1973), 1–10.

[12] W. Millan, A. Clark and E. Dawson, *Smart hill climbing finds better Boolean functions*, in "Proceedings of Selected Areas in Cryptology (SAC'97)," Ottowa, Canada, August 11–12 1997.

[13] C. Qu, J. Seberry and J. Pieprzyk, *On the symmetric property of homogeneous Boolean functions*, in "Proceedings of the Australasian Conference on Information Security and Privacy – ACISP'99" (eds. J. Pieprzyk, R. Safavi-Naini and J. Seberry), Springer-Verlag, Berlin, (1999), 26–35.

[14] O. S. Rothaus, *On "bent" functions*, J. Combin. Theory Ser. A, **20** (1976), 300–305.

[15] J. Seberry, X.-M. Zhang and Y. Zheng, *Systematic generation of cryptographically robust S-boxes (extended abstract)*, in "Proceedings of the 1st ACM Conference on Computer and Communications Security," Fairfax, VA, (1993), 171–182.

[16] J. Seberry, X.-M. Zhang and Y. Zheng, *Nonlinearity and propagation characteristics of balanced Boolean functions*, Inform. Comput., **119** (1995), 1–13.

[17] A. F. Webster and S. E. Tavares, *On the design of S-boxes*, in "Advances in Cryptology – CRYPTO'85" (ed. H.C. Williams), Springer-Verlag, Berlin, (1986), 523–534.

Received June 2008; revised October 2008.

E-mail address: jcliment@ua.es
E-mail address: francisco.garcia@ua.es
E-mail address: vrequena@ua.es