This is a previous version of the article published by Springer in SeMA Journal. 2015, 72(1): 13-36. doi:10.1007/s40324-015-0042-0

On the construction of new bent functions from the max-weight and min-weight functions of old bent functions

Joan-Josep Climent[1] Francisco J. García[2]
Verónica Requena[3]
[1] Departament de Matemàtiques,
Universitat d'Alacant
[2] Departament de Mètodes Quantitatius i Teoria Econòmica,
Universitat d'Alacant
[3] Departamento de Estadística, Matemáticas e Informática,
Universidad Miguel Hernández de Elche

July 9, 2015

Abstract

Given a bent function $f(\boldsymbol{x})$ of n variables, its max-weight and min-weight functions are introduced as the Boolean functions $f^+(\boldsymbol{x})$ and $f^-(\boldsymbol{x})$ whose supports are the sets $\{\boldsymbol{a} \in \mathbb{F}_2^n \mid w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n}{2}-1}\}$ and $\{\boldsymbol{a} \in \mathbb{F}_2^n \mid w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} - 2^{\frac{n}{2}-1}\}$ respectively, where $w(f \oplus l_{\boldsymbol{a}})$ denotes the Hamming weight of the Boolean function $f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$ and $l_{\boldsymbol{a}}(\boldsymbol{x})$ is the linear function defined by $\boldsymbol{a} \in \mathbb{F}_2^n$. $f^+(\boldsymbol{x})$ and $f^-(\boldsymbol{x})$ are proved to be bent functions. Furthermore, combining the 4 minterms of 2 variables with the max-weight or min-weight functions of a 4-tuple $(f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), f_3(\boldsymbol{x}))$ of bent functions of n variables such that $f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}) \oplus f_2(\boldsymbol{x}) \oplus f_3(\boldsymbol{x}) = 1$, a bent function of $n+2$ variables is obtained. A family of 4-tuples of bent functions satisfying the above condition is introduced, and finally, the number of bent functions we can construct using the method introduced in this paper are obtained. Also, our construction is compared with other constructions of bent functions.

Keywords: Boolean function, linear function, bent function, support, minterm, max-weight function,

AMS subject classifications: 06E30, 94A60

1 Introduction

Boolean functions are components of S-boxes used in different types of cryptographic applications such as block ciphers, stream ciphers and hash functions [3, 5, 22] as well as in coding theory [1, 17], among others.

A fundamental condition for these functions is to render high resistance to differential and linear cryptanalyses, which are the main attacks on block ciphers. A variety of criteria for choosing Boolean functions are determined by its portability in the sense that they can be needed in different applications. The functions achieving the maximal possible nonlinearity possess the best resistance to the

linear attack and they are called bent functions [28, 30]. Bent functions have been the subject of some interest in coding theory [19, 20], in logic synthesis [32] and in cryptography [22].

Bent functions constitute a fascinating issue in cryptography (as evidenced by the abundant literature, see for example [6, 9, 14, 15, 16, 22, 29, 33] and the references included), but unfortunately there is a mist hovering over their properties, their classification and their actual number. A general method for generating all bent functions is not known to exist yet, except for some particular cases; for $n = 2$ there are only 8 bent functions, for $n = 4$ there are 896 bent functions and for $n = 6$, Preneel [26] and Chang [10] proved that the number of bent functions is 5 425 430 528. Langevin and Leander [18] proved recently that the number of bent functions is 99 270 589 265 934 370 305 785 861 242 880 $\approx 2^{106}$. Nevertheless, the classification and the number of bent functions for $n \geq 10$ is still an open problem.

The origin of bent functions goes back to a theoretical article of McFarland [21] on sets of finite differences in finite non-cyclic groups. One year after, Dillon [13] in his doctoral thesis systematized and extended the ideas of McFarland, proving a great quantity of properties. The name *bent* for these functions is due to Rothaus [27].

Our main effort has been made in designing a method to construct a great number of new bent functions. There are different methods to obtain bent functions, most of them are based on the algebraic normal form (ANF) of a Boolean function and the Fourier (or Walsh) transformation; see, for example, [8, 30]. Nevertheless, we use the classical representation of Boolean functions by minterms to construct bent functions of $n+2$ variables from some bent functions of n variables (with n a positive even integer). Moreover, given a bent function of n variables and using the linear functions, we generate two new bent functions of n variables, introducing their properties.

The use of the ANF or the truth table (equivalently, the expression as a sum of minterms), both have its advantages and disadvantages. For example, the ANF of a Boolean function $f(\boldsymbol{x})$ of n variables provides directly its degree and, if it is greather than $n/2$ we can state that $f(\boldsymbol{x})$ is not a bent function (see [27]); nevertheless we do not know the cardinality of its support (that is, the number of its minterms). On the other hand, if we know the truth table of $f(\boldsymbol{x})$, we know if its support has the necessary number of minterms to be a bent function, though we do not know its degree.

The rest of the paper is organized as follows. Firstly, in Section 2 we introduce some basic definitions and notations that are used here after. In Section 3, we define two new bent functions of n variables constructed from a bent function of n variables and using linear functions, and then, we derive some properties, along with other relevant results that are necessary to prove the main theorems. Furthermore, we present a general method to construct bent functions of $n + 2$ variables from bent functions of n variables. In section 4, we introduce the necessary results to count the number of bent functions we can construct according to the method introduced in Section 3. In Section 5, we show, with some examples, that our construction generate bent functions which are not Rothaus, Maiorana-McFarland or Carlet type (see, for example [7, 16, 27]).

2 Preliminaries

We denote by $\mathbb{F}_2$ the Galois field of two elements, 0 and 1, with the addition (denoted by $\oplus$) and the multiplication (denoted by juxtaposition). For any positive integer n, it is well-known that $\mathbb{F}_2^n$ is a linear space over $\mathbb{F}_2$ with the addition (denoted also by $\oplus$) 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 $\mathbb{F}_2^n$; 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 $\boldsymbol{b}$.

For each $\boldsymbol{a} = (a_1, a_2, \ldots, a_{n-1}, a_n) \in \mathbb{F}_2^n$ we consider the nonnegative integer

$$a = a_1 2^{n-1} + a_2 2^{n-2} + \cdots + a_{n-1} 2^1 + a_n 2^0 \in \mathbb{Z}_{2^n}.$$

We call $\boldsymbol{a}$ the **binary expansion** of n digits of a. With this representation, we have that $\mathbb{F}_2^n = \{\boldsymbol{a} \mid a \in \mathbb{Z}_{2^n}\}$.

A **Boolean function** of n variables is a map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. The set $\mathcal{B}_n$ of all Boolean functions of n variables is a linear space over $\mathbb{F}_2$ with the usual addition of functions given by

$$(f \oplus g)(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus g(\boldsymbol{x}), \quad \text{for } f, g \in \mathcal{B}_n.$$

If $f \in \mathcal{B}_n$, we call **truth table** of f (see, for example, [23, 24]) the binary sequence of length 2^n given by

$$\boldsymbol{\xi}_f = (f(\mathbf{0}),\ f(\mathbf{1}),\ \ldots,\ f(\mathbf{2^n - 1}))$$

that is, the i-th component of $\boldsymbol{\xi}_f$ is equal to $f(\boldsymbol{i})$ for $\boldsymbol{i} = \mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \mathbf{2^n - 1}$. 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

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

For practical reasons, we write $m_{\boldsymbol{u}}(\boldsymbol{x})$ or $m_u(\boldsymbol{x})$, as appropriate, where $\boldsymbol{u} \in \mathbb{F}_2^n$ is the binary expansion of $u \in \mathbb{Z}_{2^n}$.

For $i = 0, 1, 2, \ldots, 2^n - 1$, it is obvious that $m_i(\boldsymbol{x}) = 1$ if and only if $\boldsymbol{x} = \boldsymbol{i}$. So, the truth table

$$(m_i(\mathbf{0}),\ m_i(\mathbf{1}),\ \ldots,\ m_i(\mathbf{2^n - 1}))$$

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

$$\bigoplus_{i=0}^{2^n-1} m_i(\boldsymbol{x}) = 1, \quad \text{for all } \boldsymbol{x} \in \mathbb{F}_2^n. \tag{1}$$

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

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

We call the **support** of f, denoted by $\mathrm{Supp}\,(f)$, the set of vectors of $\mathbb{F}_2^n$ whose image by f is 1; that is,

$$\mathrm{Supp}\,(f) = \{\boldsymbol{a} \in \mathbb{F}_2^n \mid f(\boldsymbol{a}) = 1\}.$$

Therefore, according to expression (2), $\mathrm{Supp}\,(f)$ is the set of the indices corresponding to the minterms of $f(\boldsymbol{x})$.

The **Hamming weight** of a binary sequence $\boldsymbol{\alpha}$, denoted by $w(\boldsymbol{\alpha})$, is the number of 1s in $\boldsymbol{\alpha}$. The **Hamming weight** of a Boolean function $f(\boldsymbol{x})$, denoted by $w(f)$, is the Hamming weight of its truth

table $\boldsymbol{\xi}_f$; that is, $w(f) = w(\boldsymbol{\xi}_f)$, and consequently, $w(f)$ is the number of minterms in the expression of $f(\boldsymbol{x})$ taken as a sum of minterms. In this paper, we consider 0 and 1 as elements of $\mathbb{F}_2$ or $\mathbb{Z}$, indistinctly, therefore

$$w(f) = \sum_{\boldsymbol{x} \in \mathbb{F}_2^n} f(\boldsymbol{x}).$$

If $f \in \mathcal{B}_n$, the **complementary function** of f is the function $g \in \mathcal{B}_n$ given by $g(\boldsymbol{x}) = 1 \oplus f(\boldsymbol{x})$ for all $\boldsymbol{x} \in \mathbb{F}_2^n$. We write $g = 1 \oplus f$. It is easy to see that

$$\mathrm{Supp}\,(1 \oplus f) = \mathbb{F}_2^n \setminus \mathrm{Supp}\,(f)$$

and therefore, $w(1 \oplus f) = 2^n - w(f)$.

The following result, which proof can be found in [11], provides four minterms of $n+2$ variables from one minterm of n variables.

Lemma 1 (Lemma 1 of [11]): *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*

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

The previous lemma tells us that the four minterms of $n+2$ variables, which can be obtained from the minterm $m_a(\boldsymbol{x})$ of n variables, are

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

Note that if we use the vector representation for the indices of the minterms, the four minterms of $n+2$ variables obtained from the minterm $m_{\boldsymbol{a}}(\boldsymbol{x})$ of n variables, are

$$m_{(0,0,\boldsymbol{a})}(\boldsymbol{y}, \boldsymbol{x}), \quad m_{(0,1,\boldsymbol{a})}(\boldsymbol{y}, \boldsymbol{x}), \quad m_{(1,0,\boldsymbol{a})}(\boldsymbol{y}, \boldsymbol{x}), \quad \text{and} \quad m_{(1,1,\boldsymbol{a})}(\boldsymbol{y}, \boldsymbol{x}).$$

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

$$f(\boldsymbol{x}) = l_{\boldsymbol{a}}(\boldsymbol{x}) \oplus b$$

where $\boldsymbol{a} \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$, and $l_{\boldsymbol{a}}(\boldsymbol{x}) = \langle \boldsymbol{a}, \boldsymbol{x} \rangle$. If $b = 0$, f is called a **linear function**.

The **nonlinearity** of a Boolean function f of n variables is defined as (see [25])

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

where $\mathcal{A}_n$ is the set of all affine functions and $d(f, \varphi) = w(f \oplus \varphi)$ is the Hamming distance between f and φ. The nonlinearity of f is upper bounded (see [30]) 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 [30]). As a consequence, bent functions only exist for n even.

The following result (see [30]), that we quote for further references, gives us a characterization of bent functions.

Theorem 1: *Let $f(\boldsymbol{x})$ be a Boolean function of n variables. $f(\boldsymbol{x})$ is a bent function if and only if the number of 1s in the truth table of the Boolean function $f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$ is $2^{n-1} \pm 2^{\frac{n}{2}-1}$ for all $\boldsymbol{a} \in \mathbb{F}_2^n$.*

Given this, and as a consequence of the previous theorem, if $f(\boldsymbol{x})$ is a bent function, then the number of 1s in its truth table is $2^{n-1} \pm 2^{\frac{n}{2}-1}$, or equivalently, $f(\boldsymbol{x})$ is expressed as sum of $2^{n-1} \pm 2^{\frac{n}{2}-1}$ minterms. Also, $1 \oplus f(\boldsymbol{x})$ and $f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$ are bent functions.

As we mentioned in Section 1, there is no known any method that provides all bent functions of n variables for any even positive integer n. However, there are different methods that allow us to obtain bent functions of $n+2$ variables from bent functions of n variables, or bent functions of n variables from functions (not necessarily bent) of $n/2$ variables.

Next we discuss briefly the constructions of Rothaus, Maiorana-McFarland and Carlet. We can consider such constructions as classical constructions of bent functions, and we will compare these constructions with the construction introduced in Section 3.

Rothaus construction [27]: *Assume that n is even. Let $A(\boldsymbol{x})$, $B(\boldsymbol{x})$ and $C(\boldsymbol{x})$ be bent functions of n variables such that $A(\boldsymbol{x}) \oplus B(\boldsymbol{x}) \oplus C(\boldsymbol{x})$ is also a bent function. Then*

$$\begin{aligned} R(\boldsymbol{x}, x_{n+1}, x_{n+2}) = {} & A(\boldsymbol{x})\, B(\boldsymbol{x}) \oplus B(\boldsymbol{x})\, C(\boldsymbol{x}) \oplus C(\boldsymbol{x})\, A(\boldsymbol{x}) \\ & \oplus (A(\boldsymbol{x}) \oplus B(\boldsymbol{x}))\, x_{n+1} \oplus (A(\boldsymbol{x}) \oplus C(\boldsymbol{x}))\, x_{n+2} \oplus x_{n+1}\, x_{n+2} \end{aligned}$$

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

The main difficulty of this construction lies in the impossibility of determining the triples $(A(\boldsymbol{x}), B(\boldsymbol{x}), C(\boldsymbol{x}))$ of bent functions of n variables such that $A(\boldsymbol{x}) \oplus B(\boldsymbol{x}) \oplus C(\boldsymbol{x})$ is also a bent function of n variables (see [27]), so it is impossible to determine, for the different values of n, how many bent functions of this type exist.

Note that in the construction of Rothaus appears the monomial $x_{n+1}x_{n+2}$, that is, the product of the two variables that we added to the n variables that we had initially. Therefore, the Boolean functions that do not contain this monomial are not of Rothaus type.

Maiorana-McFarland construction (see for example [13, 16]): *Assume that $n = 2k$. If $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^k$, π is any permutation of $\mathbb{F}_2^k$, and f is a Boolean function of k variables, then*

$$M(\boldsymbol{x}, \boldsymbol{y}) = \langle \boldsymbol{x}, \pi(\boldsymbol{y}) \rangle \oplus f(\boldsymbol{y})$$

is a bent function of n variables.

It is easy to check that the number of bent functions of $2k$ variables of the Maiorana-McFarland type is $(2^k)!\, 2^{2^k}$.

Carlet contruction [7]: *If $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ are bent functions of n variables and $g_0(\boldsymbol{y})$ and $g_1(\boldsymbol{y})$ are bent functions of m variables, then*

$$C(\boldsymbol{y}, \boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus g_0(\boldsymbol{y}) \oplus (f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}))\, (g_0(\boldsymbol{y}) \oplus g_1(\boldsymbol{y}))$$

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

Unlike what happens with the Maiorana-McFarland construction, we can not count how many bent functions we can construct using the Carlet construction. This is because using two different 4-tuples of bent functions,

$$(f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), g_0(\boldsymbol{y}), g_1(\boldsymbol{y})) \quad \text{and} \quad (f_0'(\boldsymbol{x}), f_1'(\boldsymbol{x}), g_0'(\boldsymbol{y}), g_1'(\boldsymbol{y})),$$

we can obtain the same bent function, that is,

$$\begin{aligned} C(\boldsymbol{y},\boldsymbol{x}) &= f_0(\boldsymbol{x}) \oplus g_0(\boldsymbol{y}) \oplus (f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}))\,(g_0(\boldsymbol{y}) \oplus g_1(\boldsymbol{y})) \\ &= f'_0(\boldsymbol{x}) \oplus g'_0(\boldsymbol{y}) \oplus \left(f'_0(\boldsymbol{x}) \oplus f'_1(\boldsymbol{x})\right)\left(g'_0(\boldsymbol{y}) \oplus g'_1(\boldsymbol{y})\right) = C'(\boldsymbol{y},\boldsymbol{x}) \end{aligned}$$

as we can see in the following example.

Example 1: Consider the 4-tuple of bent functions of 2 variables

$$(f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), g_0(\boldsymbol{y}), g_1(\boldsymbol{y})) = (m_0(\boldsymbol{x}), m_3(\boldsymbol{x}), m_0(\boldsymbol{y}), m_1(\boldsymbol{y}) \oplus m_2(\boldsymbol{y}) \oplus m_3(\boldsymbol{y}))\,.$$

Then, using Lemma 1 and expression (1), we have that

$$\begin{aligned} C(\boldsymbol{y},\boldsymbol{x}) &= m_0(\boldsymbol{x}) \oplus m_0(\boldsymbol{y}) \oplus (m_0(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}))\,(m_0(\boldsymbol{y}) \oplus m_1(\boldsymbol{y}) \oplus m_2(\boldsymbol{y}) \oplus m_3(\boldsymbol{y})) \\ &= m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_1(\boldsymbol{y},\boldsymbol{x}) \oplus m_2(\boldsymbol{y},\boldsymbol{x}) \oplus m_7(\boldsymbol{y},\boldsymbol{x}) \oplus m_{11}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{15}(\boldsymbol{y},\boldsymbol{x}). \end{aligned}$$

Consider now the 4-tuple of bent functions of 2 variables

$$(f'_0(\boldsymbol{x}), f'_1(\boldsymbol{x}), g'_0(\boldsymbol{y}), g'_1(\boldsymbol{y})) = (m_1(\boldsymbol{x}), m_3(\boldsymbol{x}), m_0(\boldsymbol{y}), m_1(\boldsymbol{y}) \oplus m_2(\boldsymbol{y}) \oplus m_3(\boldsymbol{y}))\,.$$

Proceeding as before, we have that

$$\begin{aligned} C'(\boldsymbol{y},\boldsymbol{x}) &= m_1(\boldsymbol{x}) \oplus m_0(\boldsymbol{y}) \oplus (m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}))\,(m_0(\boldsymbol{y}) \oplus m_1(\boldsymbol{y}) \oplus m_2(\boldsymbol{y}) \oplus m_3(\boldsymbol{y})) \\ &= m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_1(\boldsymbol{y},\boldsymbol{x}) \oplus m_2(\boldsymbol{y},\boldsymbol{x}) \oplus m_7(\boldsymbol{y},\boldsymbol{x}) \oplus m_{11}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{15}(\boldsymbol{y},\boldsymbol{x}). \end{aligned}$$

Therefore, using two different 4-tuples of bent functions, we can get the same bent function of Carlet type. ■

Before moving on to the next section, remember that two Boolean functions $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ are called **affine equivalent** if there exists an $n \times n$ invertible matrix A, two vectors $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$ and a bit $c \in \mathbb{F}_2$ such that $g(\boldsymbol{x}) = f(\boldsymbol{x}A \oplus \boldsymbol{a}) \oplus l_{\boldsymbol{b}}(\boldsymbol{x}) \oplus c$. It is know (see for example [2]) that affine equivalent functions are both bent or both not bent. So, many authors work in the problem of *finding the number and representatives of affine equivalent classes of bent functions.* Nevertheless, we are interested in the problem *find how many different bent functions there exists or we can construct*, because not all affine equivalent bent functions are different as we can see in the following example.

Example 2: Consider the bent function

$$f(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_8(\boldsymbol{x}) \oplus m_{15}(\boldsymbol{x})$$

of 4 variables, the invertible matrix

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

the vectors $\boldsymbol{a} = (0,0,0,1)$ and $\boldsymbol{b} = (0,0,0,0)$ and the bit $c = 0$. It is easy to check that both functions $f(\boldsymbol{x}A \oplus \boldsymbol{a}) \oplus l_{\boldsymbol{b}}(\boldsymbol{x}) \oplus c$ and $f(\boldsymbol{x})$ have the same truth table and, consequently, that are the same Boolean bent function. ■

3 Main results

Suppose that $f(\boldsymbol{x})$ is a bent function of n variables, then, according to Theorem 1, we know that $w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$ for all $\boldsymbol{a} \in \mathbb{F}_2^n$. This fact motivates the following definition.

Definition 1: Let $f(\boldsymbol{x})$ be a bent function of n variables. We call the **max-weight function** associated to $f(\boldsymbol{x})$ the Boolean function of n variables $f^+(\boldsymbol{x})$ such that

$$\text{Supp}\left(f^+\right) = \{\boldsymbol{a} \in \mathbb{F}_2^n \mid w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n}{2}-1}\}.$$

Analogously, we call the **min-weight function** associated to $f(\boldsymbol{x})$ the Boolean function of n variables $f^-(\boldsymbol{x})$ such that

$$\text{Supp}\left(f^-\right) = \{\boldsymbol{a} \in \mathbb{F}_2^n \mid w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} - 2^{\frac{n}{2}-1}\}.$$

Note that, since $f(\boldsymbol{x})$ is a bent function, by Theorem 1 we have that

$$\mathbb{F}_2^n \setminus \text{Supp}\left(f^+\right) = \text{Supp}\left(f^-\right)$$

and by expression (1), we have that

$$1 \oplus f^+(\boldsymbol{x}) = \bigoplus_{\boldsymbol{a} \in \mathbb{F}_2^n} m_{\boldsymbol{a}}(\boldsymbol{x}) \oplus \bigoplus_{\boldsymbol{a} \in \text{Supp}(f^+)} m_{\boldsymbol{a}}(\boldsymbol{x}) = \bigoplus_{\boldsymbol{a} \in \text{Supp}(f^-)} m_{\boldsymbol{a}}(\boldsymbol{x}) = f^-(\boldsymbol{x}) \tag{3}$$

that is, the min-weight function of $f(\boldsymbol{x})$ is the complementary function of the max-weight function of $f(\boldsymbol{x})$.

Our first goal consists in proving that $f^+(\boldsymbol{x})$ and $f^-(\boldsymbol{x})$ are also bent functions. But, as a consequence of expression (3) and the comment after Theorem 1, it is sufficient to prove that $f^+(\boldsymbol{x})$ is a bent function. However, we need beforehand some technical lemmas which will simplify the proof of the above mentioned result.

Lemma 2: *Let $f(\boldsymbol{x})$ be a bent function of n variables and consider its associated max-weight function $f^+(\boldsymbol{x})$. For $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$ consider the Boolean function of n variables*

$$g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}). \tag{4}$$

Then $f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = 1$ if and only if $w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{n-1} + 2^{\frac{n}{2}-1}$.

Proof: Firstly, assume that $f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = 1$, then $f^+(\boldsymbol{a}) = 1$ and $l_{\boldsymbol{a}}(\boldsymbol{b}) = 0$, or $f^+(\boldsymbol{a}) = 0$ and $l_{\boldsymbol{a}}(\boldsymbol{b}) = 1$. In the first case, $\boldsymbol{a} \in \text{Supp}\left(f^+\right)$ and from expression (4) we obtain

$$w(g_{\boldsymbol{a},\boldsymbol{b}}) = w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n}{2}-1}.$$

In the second case, $\boldsymbol{a} \notin \text{Supp}\left(f^+\right)$ and, again from expression (4), we have that

$$w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^n - w(f \oplus l_{\boldsymbol{a}}) = 2^n - (2^{n-1} - 2^{\frac{n}{2}-1}) = 2^{n-1} + 2^{\frac{n}{2}-1}.$$

Reciprocally, assume now that $w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{n-1} + 2^{\frac{n}{2}-1}$. If $l_{\boldsymbol{a}}(\boldsymbol{b}) = 0$, from expression (4) we obtain

$$g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x});$$

so, $w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n}{2}-1}$ and, consequently, $\boldsymbol{a} \in \text{Supp}\left(f^+\right)$, that is, $f^+(\boldsymbol{a}) = 1$. If $l_{\boldsymbol{a}}(\boldsymbol{b}) = 1$, from expression (4) we obtain

$$g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}) \oplus 1$$

and so, $w(f \oplus l_{\boldsymbol{a}}) = 2^n - w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{n-1} - 2^{\frac{n}{2}-1}$, therefore, $\boldsymbol{a} \notin \text{Supp}\left(f^+\right)$, that is, $f^+(\boldsymbol{a}) = 0$. In any case, $f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = 1$. □

Note that, with the notation of the previous lemma, we also get that

$$f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = 0 \quad \text{if and only if} \quad w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Therefore, we can state that $w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$. But this fact does not guarantee that $g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x})$ is a bent function. It only ensures that $g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x})$ has the number of minterms required so that it can be.

Now, as an immediate consequence of the previous lemma we have the following result that establishes the relationship between the weight of the Boolean function $g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x})$ and the value of $f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b})$.

Lemma 3: *Let $f(\boldsymbol{x})$ be a bent function of n variables and consider its max-weight function $f^+(\boldsymbol{x})$. For $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$ consider the Boolean function $g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x})$ defined by expression (4). Then*

$$f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = \frac{w(g_{\boldsymbol{a},\boldsymbol{b}}) - (2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}}.$$

Next we introduce the latest technical lemma needed to prove that the max-weight function associated to a bent function is also a bent function.

Lemma 4: *Let $f(\boldsymbol{x})$ be a bent function of n variables. Then*

$$\sum_{\boldsymbol{a} \in \mathbb{F}_2^n} w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{2n-1} \pm 2^{n-1} \quad \textit{for all} \quad \boldsymbol{b} \in \mathbb{F}_2^n$$

where $g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x})$ is the Boolean function defined by expression (4).

Proof: From expression (4) we obtain

$$\begin{aligned} \sum_{\boldsymbol{a} \in \mathbb{F}_2^n} w(g_{\boldsymbol{a},\boldsymbol{b}}) &= \sum_{\boldsymbol{a} \in \mathbb{F}_2^n} \left(\sum_{\boldsymbol{x} \in \mathbb{F}_2^n} (f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b})) \right) \\ &= \sum_{\boldsymbol{a} \in \mathbb{F}_2^n} f(\boldsymbol{b}) + \sum_{\substack{\boldsymbol{x} \in \mathbb{F}_2^n \\ \boldsymbol{x} \neq \boldsymbol{b}}} \left(\sum_{\boldsymbol{a} \in \mathbb{F}_2^n} (f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x} \oplus \boldsymbol{b})) \right) \end{aligned} \tag{5}$$

because $l_{\boldsymbol{a}}(\boldsymbol{b}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = 0$ and $l_{\boldsymbol{a}}(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = l_{\boldsymbol{a}}(\boldsymbol{x} \oplus \boldsymbol{b})$.

Furthermore, considered as a function in the variable $\boldsymbol{a}$,

$$f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x} \oplus \boldsymbol{b}) = f(\boldsymbol{x}) \oplus l_{\boldsymbol{x} \oplus \boldsymbol{b}}(\boldsymbol{a}), \quad \text{for} \quad \boldsymbol{x} \neq \boldsymbol{b},$$

is an affine function; therefore

$$\sum_{\boldsymbol{a} \in \mathbb{F}_2^n} (f(\boldsymbol{x}) \oplus l_{\boldsymbol{x} \oplus \boldsymbol{b}}(\boldsymbol{a})) = 2^{n-1}$$

and replacing it in expression (5) we get

$$\sum_{\boldsymbol{a} \in \mathbb{F}_2^n} w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^n f(\boldsymbol{b}) + (2^n - 1)2^{n-1} = \begin{cases} 2^{2n-1} + 2^{n-1}, & \text{if } f(\boldsymbol{b}) = 1, \\ 2^{2n-1} - 2^{n-1}, & \text{if } f(\boldsymbol{b}) = 0. \end{cases}$$

□

Now, we have the necessary conditions to prove that the max-weight function of a bent function is also a bent function.

Theorem 2: *If $f(\boldsymbol{x})$ is a bent function of n variables, then its max-weight function $f^+(\boldsymbol{x})$ is also a bent function of n variables.*

Proof: If $\boldsymbol{b} \in \mathbb{F}_2^n$, from Lemmas 3 and 4 and the identity $l_{\boldsymbol{b}}(\boldsymbol{a}) = l_{\boldsymbol{a}}(\boldsymbol{b})$ we get that

$$\begin{aligned} w(f^+ \oplus l_{\boldsymbol{b}}) &= \sum_{\boldsymbol{a}\in\mathbb{F}_2^n} \left(f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{b}}(\boldsymbol{a})\right) = \sum_{\boldsymbol{a}\in\mathbb{F}_2^n} \frac{w(g_{\boldsymbol{a},\boldsymbol{b}}) - (2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}} \\ &= \frac{2^{2n-1} \pm 2^{n-1} - 2^n(2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}} = 2^{n-1} \pm 2^{\frac{n}{2}-1} \end{aligned}$$

and $f^+(\boldsymbol{x})$ is a bent function by Theorem 1. □

Now, as an immediate consequence of the previous theorem we have the following results which establish some properties of the max-weight and min-weight functions associated with a bent function.

Firstly, we establish that the max-weight of the complementary function of a bent function is the complementary of the max-weight of the bent function.

Corollary 1: *Let $f(\boldsymbol{x})$ be a bent function of n variables. If $g(\boldsymbol{x}) = 1 \oplus f(\boldsymbol{x})$, then $g^+(\boldsymbol{x}) = 1 \oplus f^+(\boldsymbol{x})$.*

Proof: From Definition 1, we have that

$$\begin{aligned} \mathrm{Supp}\left(f^-\right) &= \left\{\boldsymbol{a} \in \mathbb{F}_2^n \mid w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} - 2^{\frac{n}{2}-1}\right\}, \\ \mathrm{Supp}\left(g^+\right) &= \left\{\boldsymbol{a} \in \mathbb{F}_2^n \mid w(g \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n}{2}-1}\right\}. \end{aligned}$$

If $\boldsymbol{a} \in \mathrm{Supp}\,(g^+)$, then

$$2^{n-1} + 2^{\frac{n}{2}-1} = w(g \oplus l_{\boldsymbol{a}}) = w(1 \oplus f \oplus l_{\boldsymbol{a}}) = 2^n - w(f \oplus l_{\boldsymbol{a}})$$

therefore, $w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} - 2^{\frac{n}{2}-1}$, that is, $\boldsymbol{a} \in \mathrm{Supp}\,(f^-)$ and so $\mathrm{Supp}\,(g^+) \subseteq \mathrm{Supp}\,(f^-)$.

Now, assume that $\boldsymbol{a} \in \mathrm{Supp}\,(f^-)$, then $w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} - 2^{\frac{n}{2}-1}$, and therefore

$$w(g \oplus l_{\boldsymbol{a}}) = w(1 \oplus f \oplus l_{\boldsymbol{a}}) = 2^n - w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n}{2}-1},$$

that is, $\boldsymbol{a} \in \mathrm{Supp}\,(g^+)$ and then $\mathrm{Supp}\,(f^-) \subseteq \mathrm{Supp}\,(g^+)$.

So, we can conclude that $\mathrm{Supp}\,(g^+) = \mathrm{Supp}\,(f^-)$ and, therefore, $g^+(\boldsymbol{x}) = f^-(\boldsymbol{x})$.

Finally, from expression (3), we have that $g^+(\boldsymbol{x}) = 1 \oplus f^+(\boldsymbol{x})$. □

The following result establishes that the max-weight function associated to the max-weight function associated to a bent function is the same bent function.

Corollary 2: *If $f(\boldsymbol{x})$ is a bent function of n variables, then $f^{+^+}(\boldsymbol{x}) = f(\boldsymbol{x})$.*

Proof: We will prove that $\mathrm{Supp}\left(f^{+^+}\right) = \mathrm{Supp}\,(f)$.

If $\boldsymbol{b} \in \mathrm{Supp}\left(f^{+^+}\right)$, then, according to Definition 1, $w(f^+ \oplus l_{\boldsymbol{b}}) = 2^{n-1} + 2^{\frac{n}{2}-1}$. Now, from Lemma 2,

$$w(f^+ \oplus l_{\boldsymbol{b}}) = \sum_{\boldsymbol{a}\in\mathbb{F}_2^n} \left(f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{b}}(\boldsymbol{a})\right) = \sum_{\boldsymbol{a}\in\mathbb{F}_2^n} \frac{w(g_{\boldsymbol{a},\boldsymbol{b}}) - (2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}}$$

$$= \frac{\sum_{\boldsymbol{a}\in\mathbb{F}_2^n} w(g_{\boldsymbol{a},\boldsymbol{b}}) - 2^n(2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}},$$

where $g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x})$ is the function defined by expression (4); therefore

$$\sum_{\boldsymbol{a}\in\mathbb{F}_2^n} w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{\frac{n}{2}}(2^{n-1} + 2^{\frac{n}{2}-1}) + 2^n(2^{n-1} - 2^{\frac{n}{2}-1}) = 2^{2n-1} + 2^{n-1}.$$

But then, according to the proof of Lemma 4, $f(\boldsymbol{b}) = 1$; that is, $\boldsymbol{b} \in \mathrm{Supp}\,(f)$. So, we have proved that $\mathrm{Supp}\left(f^{+^+}\right) \subseteq \mathrm{Supp}\,(f)$.

Now assume that $\boldsymbol{b} \in \mathrm{Supp}\,(f)$. Then $f(\boldsymbol{b}) = 1$ and, from the proof of Lemma 4,

$$\sum_{\boldsymbol{a}\in\mathbb{F}_2^n} w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{2n-1} + 2^{n-1},$$

but then, proceeding as in the proof of Theorem 2, we obtain

$$\begin{aligned} w(f^+ \oplus l_{\boldsymbol{b}}) &= \sum_{\boldsymbol{a}\in\mathbb{F}_2^n} \left(f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{b}}(\boldsymbol{a})\right) = \sum_{\boldsymbol{a}\in\mathbb{F}_2^n} \frac{w(g_{\boldsymbol{a},\boldsymbol{b}}) - (2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}} \\ &= \frac{2^{2n-1} + 2^{n-1} - 2^n(2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}} = 2^{n-1} + 2^{\frac{n}{2}-1} \end{aligned}$$

and, from Definition 1, $\boldsymbol{b} \in \mathrm{Supp}\left(f^{+^+}\right)$. Therefore, $\mathrm{Supp}\,(f) \subseteq \mathrm{Supp}\left(f^{+^+}\right)$.

So, we can conclude that $\mathrm{Supp}\left(f^{+^+}\right) = \mathrm{Supp}\,(f)$. □

Next result establishes that the max-weight functions associated with different bent functions are also different.

Corollary 3: *Let $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ be bent functions of n variables. If $f(\boldsymbol{x}) \neq g(\boldsymbol{x})$, then $f^+(\boldsymbol{x}) \neq g^+(\boldsymbol{x})$.*

Proof: If $f^+(\boldsymbol{x}) = g^+(\boldsymbol{x})$, then by Corollary 2, we have that

$$f(\boldsymbol{x}) = f^{+^+}(\boldsymbol{x}) = g^{+^+}(\boldsymbol{x}) = g(\boldsymbol{x})$$

which is a contradiction. So $f^+(\boldsymbol{x}) \neq g^+(\boldsymbol{x})$. □

Note that, as a consequence of expression (3) and the comment after Theorem 1, we have that Theorem 2 and Corollaries 1, 2, and 3 are also valid for min-weight functions.

Note also that, in general,

$$f^+ \neq f \neq f^-, \quad w(f^+) \neq 2^{n-1} + 2^{\frac{n}{2}-1} \quad \text{and} \quad w(f^-) \neq 2^{n-1} - 2^{\frac{n}{2}-1}$$

as we can see in Table 1 which shows the relationship between f, f^+ and f^- when f runs the eight bent functions of 2 variables.

Now we are ready to establish the main result of this paper that allow us to construct two bent functions of $n+2$ variables from 4 bent functions of n variables.

f	f^+	f^-
m_0	$m_1 \oplus m_2 \oplus m_3$	m_0
m_1	m_2	$m_0 \oplus m_1 \oplus m_3$
m_2	m_1	$m_0 \oplus m_2 \oplus m_3$
m_3	m_3	$m_0 \oplus m_1 \oplus m_2$
$m_0 \oplus m_1 \oplus m_2$	$m_0 \oplus m_1 \oplus m_2$	m_3
$m_0 \oplus m_1 \oplus m_3$	$m_0 \oplus m_2 \oplus m_3$	m_1
$m_0 \oplus m_2 \oplus m_3$	$m_0 \oplus m_1 \oplus m_3$	m_2
$m_1 \oplus m_2 \oplus m_3$	m_0	$m_1 \oplus m_2 \oplus m_3$

Table 1: Max-weight and min-weight functions of the 8 bent functions of 2 variables

y_1	y_2	$\boldsymbol{x}$	$m_0(\boldsymbol{y})$	$m_1(\boldsymbol{y})$	$m_2(\boldsymbol{y})$	$m_3(\boldsymbol{y})$	$F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$
$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\tau}$	$\boldsymbol{I}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\xi}_0^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\mathbf{0}$	$\boldsymbol{I}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\boldsymbol{I}$	$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\xi}_1^+ \oplus b_2\boldsymbol{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{I}$	$\mathbf{0}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{I}$	$\mathbf{0}$	$\boldsymbol{\xi}_2^+ \oplus b_1\boldsymbol{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{I}$	$\boldsymbol{I}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{I}$	$\boldsymbol{\xi}_3^+ \oplus b_1\boldsymbol{I} \oplus b_2\boldsymbol{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$

Table 2: Truth table of $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$

Theorem 3: *Let $f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x})$, $f_2(\boldsymbol{x})$, and $f_3(\boldsymbol{x})$ be four bent functions of n variables such that*

$$f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}) \oplus f_2(\boldsymbol{x}) \oplus f_3(\boldsymbol{x}) = 1. \tag{6}$$

If σ is a permutation of $\{0,1,2,3\}$ and $\boldsymbol{y} = (y_1, y_2)$ is a vector of two variables, then

$$F(\boldsymbol{y},\boldsymbol{x}) = m_{\sigma(0)}(\boldsymbol{y})\, f_0^+(\boldsymbol{x}) \oplus m_{\sigma(1)}(\boldsymbol{y})\, f_1^+(\boldsymbol{x}) \oplus m_{\sigma(2)}(\boldsymbol{y})\, f_2^+(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y})\, f_3^+(\boldsymbol{x})$$

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

Proof: It is sufficient to prove, according to Theorem 1, that the number of 1s in the truth table (that is, the number of minterms) of the Boolean function

$$F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}) = F(\boldsymbol{y},\boldsymbol{x}) \oplus l_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$$

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

Firstly, assume that σ is the identity permutation. If $\boldsymbol{b} = (b_1, b_2)$, then

$$\begin{aligned} F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}) = {} & m_0(\boldsymbol{y})\, f_0^+(\boldsymbol{x}) \oplus m_1(\boldsymbol{y})\, f_1^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})\, f_2^+(\boldsymbol{x}) \\ & \oplus m_3(\boldsymbol{y})\, f_3^+(\boldsymbol{x}) \oplus b_1 y_1 \oplus b_2 y_2 \oplus l_{\boldsymbol{a}}(\boldsymbol{x}). \end{aligned}$$

If $\mathbf{0}$ and $\boldsymbol{I}$ are the columns of length 2^n with all the entries equal to 0 and 1 respectively; $\boldsymbol{\tau}$ is the $2^n \times n$ array whose ith row is $\boldsymbol{i}$; $\boldsymbol{\xi}_j^+$ is the truth table of $f_j^+(\boldsymbol{x})$, for $j = 0,1,2,3$; and $\boldsymbol{\Lambda}_{\boldsymbol{a}}$ is the truth table of the linear function $l_{\boldsymbol{a}}(\boldsymbol{x})$, then the last column of Table 2 is the truth table of $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$, where $b_t\,\boldsymbol{I}$, for $t = 0,1$, is the column of length 2^n with all the elements equal to b_t. Therefore, each

$b_1=0 \quad b_2=0$	$b_1=0 \quad b_2=1$	$b_1=1 \quad b_2=0$	$b_1=1 \quad b_2=1$
$\boldsymbol{\xi}_0^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{\xi}_1^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1^+ \oplus \boldsymbol{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1^+ \oplus \boldsymbol{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{\xi}_2^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_2^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_2^+ \oplus \boldsymbol{1} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_2^+ \oplus \boldsymbol{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{\xi}_3^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_3^+ \oplus \boldsymbol{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_3^+ \oplus \boldsymbol{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_3^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$

Table 3: Truth table of $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ for the different values of $\boldsymbol{b}=(b_1,b_2)$

column of Table 3 represents the four blocks of the truth table of $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ for the different values of $\boldsymbol{b}$.

Now, if for some $j \in \{0,1,2,3\}$ is $f_j(\boldsymbol{a})=1$, then, by Corollary 2, also $f_j^{++}(\boldsymbol{a})=1$ and, according to Definition 1, we get that $w(f_j^+ \oplus l_{\boldsymbol{a}}) = 2^{n-1}+2^{\frac{n}{2}-1}$; that is, the number of 1s in the block $\boldsymbol{\xi}_j^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$ is $2^{n-1}+2^{\frac{n}{2}-1}$; nevertheless, if $f_j(\boldsymbol{a})=0$, using the same argument, we get that the number of 1s in the block $\boldsymbol{\xi}_j^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$ is $2^{n-1}-2^{\frac{n}{2}-1}$. Since from expression (6) we have that in $(f_0(\boldsymbol{a}), f_1(\boldsymbol{a}), f_2(\boldsymbol{a}), f_3(\boldsymbol{a}))$ there are a 1 and three 0s or a 0 and three 1s, we conclude that the number of 1s of each column of Table 3 is

$$2^{n-1}+2^{\frac{n}{2}-1}+3(2^{n-1}-2^{\frac{n}{2}-1}) = 2^{n+1}-2^{\frac{n}{2}} \quad \text{or} \quad 3(2^{n-1}+2^{\frac{n}{2}-1})+2^{n-1}-2^{\frac{n}{2}-1} = 2^{n+1}+2^{\frac{n}{2}}.$$

Finally, if σ is a permutation of $\{0,1,2,3\}$ different of the identity, then the four blocks of the truth table of $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ given in Table 3 are permuted according to σ and, therefore, we obtain the same result. □

Note that as a consequence of Lemma 1 we can identify the permutation σ with the permutation $\begin{pmatrix} 0 & 2^n & 2^{n+1} & 2^n+2^{n+1} \\ a_0 & a_1 & a_2 & a_3 \end{pmatrix}$ of the set $\{0, 2^n, 2^{n+1}, 2^n+2^{n+1}\}$; so, according to Theorem 3, we have that

$$\begin{aligned} \text{Supp}\,(F) = &\{a_0+a \mid a \in \text{Supp}\,(f_0^+)\} \cup \{a_1+a \mid a \in \text{Supp}\,(f_1^+)\} \\ &\cup \{a_2+a \mid a \in \text{Supp}\,(f_2^+)\} \cup \{a_3+a \mid a \in \text{Supp}\,(f_3^+)\} \end{aligned} \tag{7}$$

if we use the decimal notation for the indices of the minterms. Nevertheless, if we use the vector notation for the indices of the minterms, then

$$\begin{aligned} \text{Supp}\,(F) = &\{(\boldsymbol{a}_0,\boldsymbol{a}) \mid \boldsymbol{a} \in \text{Supp}\,(f_0^+)\} \cup \{(\boldsymbol{a}_1,\boldsymbol{a}) \mid \boldsymbol{a} \in \text{Supp}\,(f_1^+)\} \\ &\cup \{(\boldsymbol{a}_2,\boldsymbol{a}) \mid \boldsymbol{a} \in \text{Supp}\,(f_2^+)\} \cup \{(\boldsymbol{a}_3,\boldsymbol{a}) \mid \boldsymbol{a} \in \text{Supp}\,(f_3^+)\} \end{aligned} \tag{8}$$

where $\begin{pmatrix} \boldsymbol{0} & \boldsymbol{1} & \boldsymbol{2} & \boldsymbol{3} \\ \boldsymbol{a}_0 & \boldsymbol{a}_1 & \boldsymbol{a}_2 & \boldsymbol{a}_3 \end{pmatrix}$ is a permutation of the set $\{\boldsymbol{0},\boldsymbol{1},\boldsymbol{2},\boldsymbol{3}\}$. The sets of expression (7) (respectively, expression (8)) are pairwise disjoints by Lemma 1.

The following examples show that all hypotheses of Theorem 3 are necessary. So, if we use the functions $f_j(\boldsymbol{x})$ in Theorem 3, instead of the functions $f_j^+(\boldsymbol{x})$, for $j=0,1,2,3$, then the function $F(\boldsymbol{y},\boldsymbol{x})$ is not necessarily a bent function as we can see in the following example.

Example 3: Consider the bent functions of 4 variables

$$f_0(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_{11}(\boldsymbol{x}) \oplus m_{13}(\boldsymbol{x}),$$

$$f_1(\boldsymbol{x}) = m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_8(\boldsymbol{x}) \oplus m_{12}(\boldsymbol{x}),$$
$$f_2(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_6(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_{10}(\boldsymbol{x}) \oplus m_{15}(\boldsymbol{x}),$$
$$f_3(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_9(\boldsymbol{x}) \oplus m_{14}(\boldsymbol{x}).$$

From expression (1), it is easy to check that

$$f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}) \oplus f_2(\boldsymbol{x}) \oplus f_3(\boldsymbol{x}) = 1.$$

Nevertheless, the function

$$F(\boldsymbol{y}, \boldsymbol{x}) = m_0(\boldsymbol{y}) f_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{y}) f_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) f_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) f_3(\boldsymbol{x})$$

is not a bent function because, according to Lemma 1,

$$\begin{aligned} F(\boldsymbol{y}, \boldsymbol{x}) = {} & m_0(\boldsymbol{y}, \boldsymbol{x}) \oplus m_1(\boldsymbol{y}, \boldsymbol{x}) \oplus m_2(\boldsymbol{y}, \boldsymbol{x}) \oplus m_5(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{11}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{13}(\boldsymbol{y}, \boldsymbol{x}) \\ & \oplus m_{18}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{20}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{21}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{23}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{24}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{28}(\boldsymbol{y}, \boldsymbol{x}) \\ & \oplus m_{33}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{37}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{38}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{39}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{42}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{47}(\boldsymbol{y}, \boldsymbol{x}) \\ & \oplus m_{49}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{50}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{51}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{55}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{57}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{62}(\boldsymbol{y}, \boldsymbol{x}) \end{aligned}$$

has only 24 minterms and the bent functions of 6 variables must have 28 or 36 minterms (see comment after Theorem 1). ■

The condition expressed by equation (6) about the functions $f_j(\boldsymbol{x})$, for $j = 0, 1, 2, 3$, is also necessary as we can see in the following example.

Example 4: Assume that $n = 2$ and consider the bent functions

$$f_0(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}), \quad f_1(\boldsymbol{x}) = m_1(\boldsymbol{x}), \quad f_2(\boldsymbol{x}) = m_2(\boldsymbol{x}) \quad \text{and} \quad f_3(\boldsymbol{x}) = m_3(\boldsymbol{x}).$$

It is easy to check that

$$f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}) \oplus f_2(\boldsymbol{x}) \oplus f_3(\boldsymbol{x}) = 0$$

and so, these functions do not satisfy equation (6). Now, we get that

$$f_0^+(\boldsymbol{x}) = m_0(\boldsymbol{x}), \quad f_1^+(\boldsymbol{x}) = m_2(\boldsymbol{x}), \quad f_2^+(\boldsymbol{x}) = m_1(\boldsymbol{x}), \quad \text{and} \quad f_3^+(\boldsymbol{x}) = m_3(\boldsymbol{x})$$

but

$$\begin{aligned} F(\boldsymbol{y}, \boldsymbol{x}) &= m_0(\boldsymbol{y}) f_0^+(\boldsymbol{x}) \oplus m_1(\boldsymbol{y}) f_1^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) f_2^+(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) f_3^+(\boldsymbol{x}) \\ &= m_0(\boldsymbol{y}, \boldsymbol{x}) \oplus m_6(\boldsymbol{y}, \boldsymbol{x}) \oplus m_9(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{15}(\boldsymbol{y}, \boldsymbol{x}) \end{aligned}$$

is not a bent function because it has only 4 minterms and the bent functions of 4 variables must have 6 or 10 minterms (see comment after Theorem 1). ■

Finally, note that as a consequence of expression (3) and the comment after Theorem 1, the above results are also valid if we change the max-weight functions for the corresponding min-weight functions. However, this fact does not guarantee that the bent functions obtained using max-weight functions are different from those bent functions obtained from min-weight functions. For example, if $f_i(\boldsymbol{x})$, for $i = 0, 1, 2, 3$, are bent functions and $g_i(\boldsymbol{x}) = 1 \oplus f_i(\boldsymbol{x})$, from Corollary 1 and expression (3), it follows that

$g_i^-(\boldsymbol{x}) = f_i^+(\boldsymbol{x})$. Moreover, if $f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}) \oplus f_2(\boldsymbol{x}) \oplus f_3(\boldsymbol{x}) = 1$, then $g_0(\boldsymbol{x}) \oplus g_1(\boldsymbol{x}) \oplus g_2(\boldsymbol{x}) \oplus g_3(\boldsymbol{x}) = 1$, and therefore

$$\begin{aligned} &m_{\sigma(0)}(\boldsymbol{y})\, f_0^+(\boldsymbol{x}) \oplus m_{\sigma(1)}(\boldsymbol{y})\, f_1^+(\boldsymbol{x}) \oplus m_{\sigma(2)}(\boldsymbol{y})\, f_2^+(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y})\, f_3^+(\boldsymbol{x}) \\ &\quad = m_{\sigma(0)}(\boldsymbol{y})\, g_0^-(\boldsymbol{x}) \oplus m_{\sigma(1)}(\boldsymbol{y})\, g_1^-(\boldsymbol{x}) \oplus m_{\sigma(2)}(\boldsymbol{y})\, g_2^-(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y})\, g_3^-(\boldsymbol{x}). \end{aligned}$$

Consequently, any bent function that we may obtain from Theorem 3 by using max-weight functions, may also be obtained by using min-weight functions.

4 Counting bent functions

In this section we introduce some results in order to compute the number of different bent functions we can construct using Theorem 3. Note that as a consequence of the results in previous sections, all results in this section will be valid for max-weight and min-weight functions, although to simplify the presentation, we only will use max-weight functions.

4.1 The general case

Assume that $f(\boldsymbol{x})$ is a bent function of n variables and consider

$$(f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), f_3(\boldsymbol{x})) = (f(\boldsymbol{x}), f(\boldsymbol{x}), f(\boldsymbol{x}), 1 \oplus f(\boldsymbol{x}))\,. \tag{9}$$

It is evident that equality (6) holds and therefore, by Theorem 3 and Corollary 1, we have the following result.

Theorem 4: *If $f(\boldsymbol{x})$ is a bent function of n variables and $i \in \{0,1,2,3\}$, then*

$$A_{f,i}(\boldsymbol{y}, \boldsymbol{x}) = f^+(\boldsymbol{x}) \oplus m_i(\boldsymbol{y})$$

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

Now, assume that $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ are different bent functions of n variables and consider

$$(f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), f_3(\boldsymbol{x})) = (f(\boldsymbol{x}), f(\boldsymbol{x}), g(\boldsymbol{x}), 1 \oplus g(\boldsymbol{x}))\,. \tag{10}$$

It is also evident that equality (6) holds. So, by Theorem 3 and Corollary 1 we have the following result.

Theorem 5: *Let $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ be two bent functions of n variables such that*

$$g(\boldsymbol{x}) \neq f(\boldsymbol{x}) \quad \text{and} \quad g(\boldsymbol{x}) \neq 1 \oplus f(\boldsymbol{x}).$$

If σ is a permutation of $\{0,1,2,3\}$, then

$$B_{f,g,\sigma}(\boldsymbol{y}, \boldsymbol{x}) = \left(m_{\sigma(0)}(\boldsymbol{y}) \oplus m_{\sigma(1)}(\boldsymbol{y})\right) f^+(\boldsymbol{x}) \oplus m_{\sigma(2)}(\boldsymbol{y}) g^+(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y}) \left(1 \oplus g^+(\boldsymbol{x})\right)$$

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

We can observe that the previous particular cases are the same constructions of bent functions introduced in Corollaries 2 and 3, respectively, of [11] using max-weight functions. Note that starting with a bent function $f(\boldsymbol{x})$ of n variables, Theorem 4 provides a different bent function that Corollary 1 of [11], because, in general, $f^+(\boldsymbol{x}) \neq f(\boldsymbol{x})$; nevertheless, the total number of bent functions provided by both corollaries are the same. The same argument is valid for the bent functions constructed by Corollary 2 of [11] and Theorem 5. So, the construction of bent functions introduced in [11] is a particular case of the construction introduced here.

According to the previous comments, the next theorem establishes the number of bent functions of $n+2$ variables we can construct using Theorems 4 and 5.

Theorem 6 (Theorem 3 of [11]): *If ν_n is the number of bent functions of n variables, then*

$$6\nu_n^2 - 8\nu_n \tag{11}$$

is the number of different bent functions of $n+2$ variables we can construct using Theorems 4 and 5.

Outside the two cases provided by Theorems 4 and 5, it is difficult to count how many different 4-tuples $(f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), f_3(\boldsymbol{x}))$ of bent functions satisfy equation (6). Therefore, if we denote by ω_n the number of 4-tuples of bent functions that satisfy equation (6), excluded the corresponding to Theorems 4 and 5, we can construct $4!\,\omega_n$ bent functions of $n+2$ variables. Consequently, we have the following result.

Theorem 7: *If ν_n is the number of bent functions of n variables and ω_n is the number of 4-tuples of bent functions that satisfy equation (6), excluded the corresponding to Theorems 4 and 5, then*

$$6\nu_n^2 - 8\nu_n + 24\omega_n$$

is the number of bent functions of $n+2$ variables we can construct using Theorem 3.

In the next section we introduce a family of 4-tuples of bent functions that satisfies expression (6) and we establish a lower bound for ω_n.

4.2 A lower bound

Let $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ be bent functions of n variables, assume that $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$, and consider the 4-tuple of bent functions

$$\left(f(\boldsymbol{x}), f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}), g(\boldsymbol{x}) \oplus l_{\boldsymbol{b}}(\boldsymbol{x}), 1 \oplus g(\boldsymbol{x}) \oplus l_{\boldsymbol{a}\oplus\boldsymbol{b}}(\boldsymbol{x})\right). \tag{12}$$

Since $l_{\boldsymbol{a}\oplus\boldsymbol{b}}(\boldsymbol{x}) = l_{\boldsymbol{a}}(\boldsymbol{x}) \oplus l_{\boldsymbol{b}}(\boldsymbol{x})$, it is evident that this 4-tuple satisfy expression (6). Before to continue, note that if we take $\boldsymbol{a} = \boldsymbol{b} = \boldsymbol{0}$, then the 4-tuples (9) and (10) are a particular case of the above 4-tuple for $g(\boldsymbol{x}) = f(\boldsymbol{x})$ and $g(\boldsymbol{x}) \neq f(\boldsymbol{x})$ respectively. So, we only need to consider the following two cases (we will justify this affirmation later).

Theorem 8: *Let $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$ with $\boldsymbol{a} \neq \boldsymbol{b}$. If $f(\boldsymbol{x})$ is a bent function of n variables and σ is any permutation of $\{0,1,2,3\}$, then*

$$\begin{aligned} C_{f,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x}) = {} & m_{\sigma(0)}(\boldsymbol{y}) f^+(\boldsymbol{x}) \oplus m_{\sigma(1)}(\boldsymbol{y})(f \oplus l_{\boldsymbol{a}})^+(\boldsymbol{x}) \\ & \oplus m_{\sigma(2)}(\boldsymbol{y})(f \oplus l_{\boldsymbol{b}})^+(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y}) \left(1 \oplus (f \oplus l_{\boldsymbol{a}\oplus\boldsymbol{b}})^+(\boldsymbol{x})\right) \end{aligned}$$

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

Theorem 9: *Let $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ with $\boldsymbol{a} \neq \boldsymbol{b}$. If $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ are bent functions of n variables such that $f(\boldsymbol{x}) \neq g(\boldsymbol{x})$ and σ is a permutation of $\{0,1,2,3\}$, then*

$$D_{f,g,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x}) = m_{\sigma(0)}(\boldsymbol{y})f^+(\boldsymbol{x}) \oplus m_{\sigma(1)}(\boldsymbol{y})(f \oplus l_{\boldsymbol{a}})^+(\boldsymbol{x}) \\ \oplus m_{\sigma(2)}(\boldsymbol{y})(g \oplus l_{\boldsymbol{b}})^+(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y})\left(1 \oplus (g \oplus l_{\boldsymbol{a}\oplus\boldsymbol{b}})^+(\boldsymbol{x})\right)$$

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

The proof of both results is an immediate consequence of Corollary 1 and Theorem 3.

Note that not all the bent functions provided by Theorem 8 are different as we can see in the following example.

Example 5: Assume that $n = 2$, consider the vectors $\boldsymbol{a} = \mathbf{1} = (0,1)$ and $\boldsymbol{b} = \mathbf{2} = (1,0)$, and the bent function of 2 variables $f(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})$. It is easy to check that

$$l_{\mathbf{1}}(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}), \quad l_{\mathbf{2}}(\boldsymbol{x}) = m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}) \quad \text{and} \quad l_{\mathbf{1}\oplus\mathbf{2}}(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}).$$

If we consider the permutation $\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 1 & 3 \end{pmatrix}$, then, according to Theorem 8, Table 1, and expression (1) we have that

$$\begin{aligned} C_{f,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x}) &= m_0(\boldsymbol{y})f^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})(f \oplus l_{\mathbf{1}})^+(\boldsymbol{x}) \oplus m_1(\boldsymbol{y})(f \oplus l_{\mathbf{2}})^+(\boldsymbol{x}) \\ &\quad \oplus m_3(\boldsymbol{y})\left(1 \oplus (f \oplus l_{\mathbf{3}})^+(\boldsymbol{x})\right) \\ &= m_0(\boldsymbol{y})m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})m_2(\boldsymbol{x}) \oplus m_1(\boldsymbol{y})m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})\left(1 \oplus m_3(\boldsymbol{x})\right) \\ &= m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_5(\boldsymbol{y},\boldsymbol{x}) \oplus m_{10}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{12}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{13}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{14}(\boldsymbol{y},\boldsymbol{x}). \end{aligned}$$

On the other hand, if we consider the vectors $\boldsymbol{u} = \mathbf{1} = (0,1)$ and $\boldsymbol{v} = \mathbf{3} = (1,1)$, the bent function $g(\boldsymbol{x}) = m_2(\boldsymbol{x})$ of 2 variables, and the permutation $\tau = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 2 & 3 \end{pmatrix}$, then, proceeding as in the previous case, we have that

$$\begin{aligned} C_{g,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x}) &= m_1(\boldsymbol{y})g^+(\boldsymbol{x}) \oplus m_0(\boldsymbol{y})(g \oplus l_{\mathbf{1}})^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})(g \oplus l_{\mathbf{3}})^+(\boldsymbol{x}) \\ &\quad \oplus m_3(\boldsymbol{y})\left(1 \oplus (g \oplus l_{\mathbf{2}})^+(\boldsymbol{x})\right) \\ &= m_1(\boldsymbol{y})m_1(\boldsymbol{x}) \oplus m_0(\boldsymbol{y})m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})\left(1 \oplus m_3(\boldsymbol{x})\right) \\ &= m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_5(\boldsymbol{y},\boldsymbol{x}) \oplus m_{10}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{12}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{13}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{14}(\boldsymbol{y},\boldsymbol{x}) \end{aligned}$$

which evidently coincides with $C_{f,\boldsymbol{a},\boldsymbol{b},\tau}(\boldsymbol{y},\boldsymbol{x})$. ■

Note that in the previous example $\{\mathbf{1},\mathbf{2}\}$ and $\{\mathbf{1},\mathbf{3}\}$ are bases of the same linear subspace $\{\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3}\}$ of $\mathbb{F}_2^n$. In order to avoid this situation, we will consider only vectors $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$ such that $\{\boldsymbol{a},\boldsymbol{b}\}$ is a Gauss-Jordan basis of $\mathbb{F}_2^n$ of cardinality 2. Recall that the set $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\} \subseteq \mathbb{F}_2^n$ is a **Gauss-Jordan basis** of cardinality k if the matrix whose rows are $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ is in reduced row echelon form (see also [4, 12]).

The following result establishes that the bent functions constructed according to Theorem 8 are different if $\{\boldsymbol{a},\boldsymbol{b}\}$ is a Gauss-Jordan basis of $\mathbb{F}_2^n$ of cardinality 2.

Lemma 5: *Let $f(\boldsymbol{x})$ and $p(\boldsymbol{x})$ be two bent functions of n variables. Assume also that $C_{f,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x})$ is the bent function of $n+2$ variables constructed according to Theorem 8 using $f(\boldsymbol{x})$, the Gauss-Jordan basis $\{\boldsymbol{a},\boldsymbol{b}\}$ of $\mathbb{F}_2^n$ of cardinality 2 and the permutation σ of $\{0,1,2,3\}$. Assume also that $C_{p,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x})$ is the bent function of $n+2$ variables constructed according to Theorem 8 using $p(\boldsymbol{x})$, the Gauss-Jordan basis $\{\boldsymbol{u},\boldsymbol{v}\}$ of $\mathbb{F}_2^n$ cardinality 2 and the permutation τ of $\{0,1,2,3\}$. If $f(\boldsymbol{x}) \neq p(\boldsymbol{x})$, then $C_{f,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x}) \neq C_{p,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x})$.*

Proof: If $\boldsymbol{\xi}$ and $\boldsymbol{\eta}$ are the truth tables of $f(\boldsymbol{x})$ and $p(\boldsymbol{x})$ respectively, then the truth tables of $C_{f,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x})$ and $C_{p,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x})$ have four blocks (not necessarily in that order and not the same order for all):

$$\begin{array}{lcccc} C_{f,\boldsymbol{a},\boldsymbol{b},\sigma}: & \boldsymbol{\xi}^{+} & (\boldsymbol{\xi}\oplus\boldsymbol{\Lambda}_{\boldsymbol{a}})^{+} & (\boldsymbol{\xi}\oplus\boldsymbol{\Lambda}_{\boldsymbol{b}})^{+} & \boldsymbol{I}\oplus(\boldsymbol{\xi}\oplus\boldsymbol{\Lambda}_{\boldsymbol{a}\oplus\boldsymbol{b}})^{+} \\ C_{p,\boldsymbol{u},\boldsymbol{v},\tau}: & \boldsymbol{\eta}^{+} & (\boldsymbol{\eta}\oplus\boldsymbol{\Lambda}_{\boldsymbol{u}})^{+} & (\boldsymbol{\eta}\oplus\boldsymbol{\Lambda}_{\boldsymbol{v}})^{+} & \boldsymbol{I}\oplus(\boldsymbol{\eta}\oplus\boldsymbol{\Lambda}_{\boldsymbol{u}\oplus\boldsymbol{v}})^{+} \end{array}$$

where $\boldsymbol{\Lambda}_{\boldsymbol{a}}$, $\boldsymbol{\Lambda}_{\boldsymbol{b}}$, $\boldsymbol{\Lambda}_{\boldsymbol{a}\oplus\boldsymbol{b}}$, $\boldsymbol{\Lambda}_{\boldsymbol{u}}$, $\boldsymbol{\Lambda}_{\boldsymbol{v}}$, and $\boldsymbol{\Lambda}_{\boldsymbol{u}\oplus\boldsymbol{v}}$ are the truth tables of the linear functions $l_{\boldsymbol{a}}(\boldsymbol{x})$, $l_{\boldsymbol{b}}(\boldsymbol{x})$, $l_{\boldsymbol{a}\oplus\boldsymbol{b}}(\boldsymbol{x})$, $l_{\boldsymbol{u}}(\boldsymbol{x})$, $l_{\boldsymbol{v}}(\boldsymbol{x})$, and $l_{\boldsymbol{u}\oplus\boldsymbol{v}}(\boldsymbol{x})$ respectively, and $\boldsymbol{I}$ is the truth table of the constant function 1.

If $C_{f,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x}) = C_{p,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x})$, then the four blocks of the second row are a permutation of the four blocks of the first row. But, if we consider the 4! cases corresponding to these permutations we obtain, using Corollaries 2 and 3, that $f(\boldsymbol{x}) = p(\boldsymbol{x})$, or that $l_{\boldsymbol{c}}(\boldsymbol{x}) = 1$ for some $\boldsymbol{c} \in \mathbb{F}_2^n$ which depend on the vectors $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{u}$, and $\boldsymbol{v}$, or that

$$(\boldsymbol{u},\boldsymbol{v}) \in \{(\boldsymbol{a},\boldsymbol{a}\oplus\boldsymbol{b}),(\boldsymbol{b},\boldsymbol{a}\oplus\boldsymbol{b}),(\boldsymbol{a}\oplus\boldsymbol{b},\boldsymbol{a}),(\boldsymbol{a}\oplus\boldsymbol{b},\boldsymbol{b})\}\,. \tag{13}$$

In any case, we have a contradiction, because $f(\boldsymbol{x}) \neq p(\boldsymbol{x})$ by hypothesis, $l_{\boldsymbol{c}}(\boldsymbol{x}) \neq 1$ for all $\boldsymbol{c} \in \mathbb{F}_2^n$, and if the relation (13) holds, then $\{\boldsymbol{a},\boldsymbol{b}\}$ and $\{\boldsymbol{u},\boldsymbol{v}\}$ cannot be simultaneously Gauss-Jordan bases of cardinality 2. Consequently, $C_{f,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x}) \neq C_{p,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x})$. □

Now, as a consequence of the previous lemma, we have the following result which establishes the number of different bent functions of $n+2$ variables that we can construct according to Theorem 8.

Theorem 10: *If ν_n is the number of bent functions of n variables, then*

$$\left(2^{2n+2} - 3\cdot 2^{n+2} + 2^3\right)\nu_n \tag{14}$$

is the number of different bent functions of $n+2$ variables that we can construct according to Theorem 8.

Proof: According to Lemma 5, using Theorem 8, we can construct $4!\,\nu_n\,N(n,2)$ bent functions of $n+2$ variables, where $N(n,2)$ is the number of Gauss-Jordan bases of $\mathbb{F}_2^n$ of cardinality 2. Now, taking into account that each linear subspace of dimension 2 of $\mathbb{F}_2^n$ has a unique Gauss-Jordan basis of cardinality 2, we have that $N(n,2)$ coincides with the number of linear subspaces of $\mathbb{F}_2^n$ of dimension 2; so (see [31, page 46])

$$N(n,2) = \frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)}$$

and therefore,

$$4!\,\nu_n\,N(n,2) = \left(2^{2n+2} - 3\cdot 2^{n+2} + 2^3\right)\nu_n$$

is the number of different bent functions of $n+2$ variables provided by Theorem 8. □

Similarly to Theorem 8, not all the bent functions constructed according to Theorem 9 are different from each other, as we can see in the following example.

Example 6: Assume that $n = 2$, consider the vectors $\boldsymbol{a} = \mathbf{1} = (0,1)$ and $\boldsymbol{b} = \mathbf{2} = (1,0)$, the bent functions $f(\boldsymbol{x}) = m_0(\boldsymbol{x})$ and $g(\boldsymbol{x}) = 1 \oplus m_3(\boldsymbol{x})$, and the permutation $\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 1 & 3 \end{pmatrix}$. According to Theorem 9, Table 1 and expression (1) (see also Example 5 for the functions $l_{\mathbf{1}}(\boldsymbol{x})$, $l_{\mathbf{2}}(\boldsymbol{x})$ and $l_{\mathbf{3}}(\boldsymbol{x})$), we have that

$$\begin{aligned} D_{f,g,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x}) &= m_0(\boldsymbol{y})f^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})(f \oplus l_{\mathbf{1}})^+(\boldsymbol{x}) \\ &\quad \oplus m_1(\boldsymbol{y})(g \oplus l_{\mathbf{2}})^+(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) \left(1 \oplus (g \oplus l_{\mathbf{3}})^+(\boldsymbol{x})\right) \\ &= m_0(\boldsymbol{y}) \left(m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})\right) \\ &\quad \oplus m_2(\boldsymbol{y}) \left(m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})\right) \\ &\quad \oplus m_1(\boldsymbol{y}) \left(m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})\right) \\ &\quad \oplus m_3(\boldsymbol{y}) \left(1 \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})\right) \\ &= m_1(\boldsymbol{y},\boldsymbol{x}) \oplus m_2(\boldsymbol{y},\boldsymbol{x}) \oplus m_3(\boldsymbol{y},\boldsymbol{x}) \oplus m_4(\boldsymbol{y},\boldsymbol{x}) \oplus m_6(\boldsymbol{y},\boldsymbol{x}) \\ &\quad \oplus m_7(\boldsymbol{y},\boldsymbol{x}) \oplus m_8(\boldsymbol{y},\boldsymbol{x}) \oplus m_{10}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{11}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{12}(\boldsymbol{y},\boldsymbol{x}). \end{aligned}$$

On the other hand, if we consider the vectors $\boldsymbol{u} = \mathbf{1} = (0,1)$ and $\boldsymbol{v} = \mathbf{3} = (1,1)$, the bent functions $p(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})$ and $q(\boldsymbol{x}) = m_3(\boldsymbol{x})$, and the permutation $\tau = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}$ then, proceeding as in the previous case, we have that

$$\begin{aligned} D_{p,q,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x}) &= m_1(\boldsymbol{y})p^+(\boldsymbol{x}) \oplus m_0(\boldsymbol{y})(p \oplus l_{\mathbf{1}})^+(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})(q \oplus l_{\mathbf{3}})^+(\boldsymbol{x}) \\ &\quad \oplus m_2(\boldsymbol{y}) \left(1 \oplus (q \oplus l_{\mathbf{2}})^+(\boldsymbol{x})\right) \\ &= m_1(\boldsymbol{y}) \left(m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})\right) \\ &\quad \oplus m_0(\boldsymbol{y}) \left(m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})\right) \\ &\quad \oplus m_3(\boldsymbol{y})m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) \left(1 \oplus m_1(\boldsymbol{x})\right) \\ &= m_1(\boldsymbol{y},\boldsymbol{x}) \oplus m_2(\boldsymbol{y},\boldsymbol{x}) \oplus m_3(\boldsymbol{y},\boldsymbol{x}) \oplus m_4(\boldsymbol{y},\boldsymbol{x}) \oplus m_6(\boldsymbol{y},\boldsymbol{x}) \\ &\quad \oplus m_7(\boldsymbol{y},\boldsymbol{x}) \oplus m_8(\boldsymbol{y},\boldsymbol{x}) \oplus m_{10}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{11}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{12}(\boldsymbol{y},\boldsymbol{x}). \end{aligned}$$

which evidently, coincides with $D_{f,g,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x})$. ■

Note that in the previous example the following equalities are satisfied

$$g(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus l_{\mathbf{3}}(\boldsymbol{x}) \qquad \text{and} \qquad q(\boldsymbol{x}) = p(\boldsymbol{x}) \oplus l_{\mathbf{2}}(\boldsymbol{x}) \oplus 1.$$

Therefore, to avoid these situations, in the construction of the functions $D_{f,g,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x})$ provided by Theorem 9 we always will assume that

$$g(\boldsymbol{x}) \neq f(\boldsymbol{x}) \oplus l_{\boldsymbol{c}}(\boldsymbol{x}) \oplus c, \quad \text{for all } (\boldsymbol{c},c) \in \mathbb{F}_2^n \times \mathbb{F}_2.$$

The following result establishes that the bent functions constructed according to Theorem 9 are all different from each other when the functions $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ satisfy the above inequality.

Lemma 6: *Assume that $f(\boldsymbol{x})$, $g(\boldsymbol{x})$, $p(\boldsymbol{x})$, and $q(\boldsymbol{x})$ are bent functions of n variables such that*

$$g(\boldsymbol{x}) \neq f(\boldsymbol{x}) \oplus l_{\boldsymbol{c}}(\boldsymbol{x}) \oplus c \text{ and } q(\boldsymbol{x}) \neq p(\boldsymbol{x}) \oplus l_{\boldsymbol{c}}(\boldsymbol{x}) \oplus c, \text{ for all } (\boldsymbol{c},c) \in \mathbb{F}_2^n \times \mathbb{F}_2.$$

Assume that $D_{f,g,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x})$ *is the bent function constructed according to Theorem 9 using the bent functions* $f(\boldsymbol{x})$ *and* $g(\boldsymbol{x})$*, the vectors* $\boldsymbol{a}$ *and* $\boldsymbol{b}$ *of* $\mathbb{F}_2^n$ *(with* $\boldsymbol{a} \neq \boldsymbol{b}$*), and the permutation* σ *of* $\{0,1,2,3\}$*. Assume also that* $D_{p,q,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x})$ *is the bent function constructed according to Theorem 9 using the bent functions* $p(\boldsymbol{x})$ *and* $q(\boldsymbol{x})$*, the vectors* $\boldsymbol{u}$ *and* $\boldsymbol{v}$ *of* $\mathbb{F}_2^n$ *(with* $\boldsymbol{u} \neq \boldsymbol{v}$*), and the permutation* τ *of* $\{0,1,2,3\}$*. If*

$$f(\boldsymbol{x}) \neq p(\boldsymbol{x}) \oplus l_{\boldsymbol{c}}(\boldsymbol{x}) \quad \textit{for all } \boldsymbol{c} \in \mathbb{F}_2^n$$

then $D_{f,g,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x}) \neq D_{p,q,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x})$.

Proof: If $\boldsymbol{\xi}_f$, $\boldsymbol{\xi}_{f,\boldsymbol{a}}$, $\boldsymbol{\xi}_{g,\boldsymbol{b}}$, $\boldsymbol{\xi}_{g,\boldsymbol{a}\oplus\boldsymbol{b}}$, $\boldsymbol{\xi}_p$, $\boldsymbol{\xi}_{p,\boldsymbol{u}}$, $\boldsymbol{\xi}_{q,\boldsymbol{v}}$, $\boldsymbol{\xi}_{q,\boldsymbol{u}\oplus\boldsymbol{v}}$ are the truth tables of

$$\begin{array}{llll} f^+(\boldsymbol{x}), & (f \oplus l_{\boldsymbol{a}})^+(\boldsymbol{x}), & (g \oplus l_{\boldsymbol{b}})^+(\boldsymbol{x}), & (g \oplus l_{\boldsymbol{a}\oplus\boldsymbol{b}})^+(\boldsymbol{x}), \\ p^+(\boldsymbol{x}), & (p \oplus l_{\boldsymbol{u}})^+(\boldsymbol{x}), & (q \oplus l_{\boldsymbol{v}})^+(\boldsymbol{x}), & (q \oplus l_{\boldsymbol{u}\oplus\boldsymbol{v}})^+(\boldsymbol{x}) \end{array}$$

respectively, then the truth tables of $D_{f,g,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x})$ and $D_{p,q,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x})$ have four blocks (not necessarily in that order and not the same order for all):

$$\begin{array}{llllll} D_{f,g,\boldsymbol{a},\boldsymbol{b},\sigma}: & \boldsymbol{\xi}_f & \boldsymbol{\xi}_{f,\boldsymbol{a}} & \boldsymbol{\xi}_{g,\boldsymbol{b}} & \boldsymbol{I} \oplus \boldsymbol{\xi}_{g,\boldsymbol{a}\oplus\boldsymbol{b}} \\ D_{p,q,\boldsymbol{u},\boldsymbol{v},\tau}: & \boldsymbol{\xi}_p & \boldsymbol{\xi}_{p,\boldsymbol{u}} & \boldsymbol{\xi}_{q,\boldsymbol{v}} & \boldsymbol{I} \oplus \boldsymbol{\xi}_{q,\boldsymbol{u}\oplus\boldsymbol{v}} \end{array}$$

where $\boldsymbol{I}$ is the truth table of the constant function 1.

If $D_{f,g,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x}) = D_{p,q,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x})$, then the four blocks of the second row are a permutation of the four blocks of the first row. But, if we consider the 4! cases corresponding to these permutations we obtain, using Corollaries 2 and 3, that

$$f(\boldsymbol{x}) = p(\boldsymbol{x}), \quad f(\boldsymbol{x}) = p(\boldsymbol{x}) \oplus l_{\boldsymbol{u}}(\boldsymbol{x}), \quad f(\boldsymbol{x}) = q(\boldsymbol{x}) \oplus l_{\boldsymbol{v}}(\boldsymbol{x}), \quad \text{or} \quad f(\boldsymbol{x}) = 1 \oplus q(\boldsymbol{x}) \oplus l_{\boldsymbol{v}}(\boldsymbol{x})$$

which is a contradiction. Consequently, $D_{f,g,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x}) \neq D_{p,q,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x})$. □

Now, as a consequence of the previous lemma, we have the following result which establishes the number of different bent functions of $n+2$ variables that we can construct according to Theorem 9.

Theorem 11: *If* ν_n *is the number of bent functions of* n *variables, then*

$$3\left(2^{2n-1} - 3 \cdot 2^{n-1} + 1\right) \frac{\nu_n(\nu_n - 2^{n+1})}{2^{2n-2}} \tag{15}$$

is the number of different bent functions of $n+2$ *variables that we can construct according to Theorem 9.*

Proof: As a consequence of Lemma 6 we can choose $f(\boldsymbol{x})$ of $\nu_n/2^n$ different ways and, fixed $f(\boldsymbol{x})$, we can choose $g(\boldsymbol{x})$ of $\nu_n/2^{n+1} - 1$ different ways. On the other hand, since we can choose the vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ of $\binom{2^n-1}{2}$ different ways and since there are 4! different permutations of $\{0,1,2,3\}$, we have that

$$\frac{\nu_n}{2^n}\left(\frac{\nu_n}{2^{n+1}} - 1\right)\binom{2^n-1}{2} 4! = 3\left(2^{2n-1} - 3 \cdot 2^{n-1} + 1\right) \frac{\nu_n(\nu_n - 2^{n+1})}{2^{2n-2}}$$

is the number of different bent functions of $n+2$ variables provided by Theorem 9. □

The following result, whose proof is analogous to that of Lemmas 5 and 6 and, therefore, we omit, establishes that none of the bent functions constructed according to Theorem 8 coincides with none of the bent functions provides by Theorem 9 and viceversa.

Lemma 7: *Assume that $f(\boldsymbol{x})$, $p(\boldsymbol{x})$, and $q(\boldsymbol{x})$ are bent functions of n variables such that*

$$q(\boldsymbol{x}) \neq p(\boldsymbol{x}) \oplus l_{\boldsymbol{c}}(\boldsymbol{x}) \oplus c \quad \text{for all } (\boldsymbol{c}, c) \in \mathbb{F}_2^n \times \mathbb{F}_2.$$

Assume that $C_{f,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x})$ is the bent function constructed according to Theorem 8 using the bent function $f(\boldsymbol{x})$, the Gauss-Jordan basis $\{\boldsymbol{a},\boldsymbol{b}\}$ of $\mathbb{F}_2^n$ of cardinality 2, and the permutation σ of $\{0,1,2,3\}$. Assume also that $D_{p,q,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x})$ is the bent function constructed according to Theorem 9 using the bent functions $p(\boldsymbol{x})$ and $q(\boldsymbol{x})$, the vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ of $\mathbb{F}_2^n$ (with $\boldsymbol{u} \neq \boldsymbol{v}$), and the permutation τ of $\{0,1,2,3\}$. Then $C_{f,\boldsymbol{a},\boldsymbol{b},\sigma}(\boldsymbol{y},\boldsymbol{x}) \neq D_{p,q,\boldsymbol{u},\boldsymbol{v},\tau}(\boldsymbol{y},\boldsymbol{x})$.

Now, as a consequence of Lemma 7 and Theorems 10 and 11 we have the following result which establishes the number of different bent functions of $n+2$ variables that we can construct according to Theorems 8 and 9.

Corollary 4: *If ν_n is the number of bent functions of n variables, then*

$$\left(2^{2n-1} - 3 \cdot 2^{n-1} + 1\right)\left(\frac{3\nu_n^2}{2^{2n-2}} + \frac{(2^n-3)\nu_n^2}{2^{n-3}}\right)$$

is the number of different bent functions of $n+2$ variables that we can construct according to Theorems 8 and 9.

Proof: It is enough to add expressions (14) and (15) to obtain the result, because by Lemma 7, the bent functions constructed according to Theorems 8 and 9 are different to each other. □

Finally, as we commented at the beginning of this section, any other possible choice of the vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ can be reduced to one of the cases considered on Theorems 4, 5, 8 and 9 (together with the additional conditions of Lemma 6). For example:

- If $\boldsymbol{a} = \boldsymbol{0}$ and $\boldsymbol{b} \neq \boldsymbol{0}$, then the 4-tuple of expression (12) becomes

  $$(f(\boldsymbol{x}), f(\boldsymbol{x}), g(\boldsymbol{x}) \oplus l_{\boldsymbol{b}}(\boldsymbol{x}), 1 \oplus g(\boldsymbol{x}) \oplus l_{\boldsymbol{b}}(\boldsymbol{x}))$$

  which corresponds to Theorem 4 if $f(\boldsymbol{x}) = g(\boldsymbol{x}) \oplus l_{\boldsymbol{b}}(\boldsymbol{x})$, or to Theorem 5 if $f(\boldsymbol{x}) \neq g(\boldsymbol{x}) \oplus l_{\boldsymbol{b}}(\boldsymbol{x})$.

- If $\boldsymbol{a} \neq \boldsymbol{0}$ and $\boldsymbol{b} = \boldsymbol{0}$, then the 4-tuple of expression (12) becomes

  $$(f(\boldsymbol{x}), f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}), g(\boldsymbol{x}), 1 \oplus g(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}))$$

  which corresponds to Theorem 4 if $g(\boldsymbol{x}) = f(\boldsymbol{x})$, $g(\boldsymbol{x}) = 1 \oplus f(\boldsymbol{x})$, $g(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$, or $g(\boldsymbol{x}) = 1 \oplus f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$; or to Theorem 9 (together with the additional conditions of Lemma 6) if $g(\boldsymbol{x}) \neq f(\boldsymbol{x})$, $g(\boldsymbol{x}) \neq 1 \oplus f(\boldsymbol{x})$, $g(\boldsymbol{x}) \neq f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$, or $g(\boldsymbol{x}) \neq 1 \oplus f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$.

Reasoning as in Lemmas 5, 6 and 7, we can prove that none of the bent functions constructed according to Theorems 4 and 5 can be obtained by Theorems 8 and 9 and viceversa. Therefore, as a consequence of Corollary 4 we have the following result.

Corollary 5: *If ν_n is the number of bent functions of n variables and ω_n is the number of 4-tuples of bent functions which satisfy equation (6), excluded the corresponding cases to Theorems 4 and 5, then*

$$\omega_n \geq \left(2^{2n-1} - 3 \cdot 2^{n-1} + 1\right)\left(\frac{3\nu_n^2}{2^{2n-2}} + \frac{(2^n-3)\nu_n^2}{2^{n-3}}\right)$$

Finally, from Theorem 7 and the previous corollary, we have that Theorem 3 provides, at least,

$$\frac{3(2^{2n+1} - 9 \cdot 2^{n-1} + 3)}{2^{2n-2}}\nu_n^2 + \frac{3 \cdot 2^{3n-1} - 9 \cdot 2^{2n} + 131 \cdot 2^{n-3} - 9}{2^{n-6}}\nu_n$$

different bent functions of $n+2$ variables.

5 Comparison with other methods

The following three examples show some bent functions constructed according to Theorem 3, that are not Rothaus functions, Maiorana-McFarland functions or Carlet functions.

Example 7: Assume that $n = 4$ and consider the bent functions of 4 variables

$$\begin{aligned}
f_0(\boldsymbol{x}) &= m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_8(\boldsymbol{x}) \oplus m_{15}(\boldsymbol{x}),\\
f_1(\boldsymbol{x}) &= m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_9(\boldsymbol{x}) \oplus m_{14}(\boldsymbol{x}),\\
f_2(\boldsymbol{x}) &= m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_{10}(\boldsymbol{x}) \oplus m_{13}(\boldsymbol{x}),\\
f_3(\boldsymbol{x}) &= m_3(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_6(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_{11}(\boldsymbol{x}) \oplus m_{12}(\boldsymbol{x}),
\end{aligned}$$

then

$$\begin{aligned}
f_0^+(\boldsymbol{x}) &= m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_5(\boldsymbol{x})\\
&\quad \oplus m_6(\boldsymbol{x}) \oplus m_8(\boldsymbol{x}) \oplus m_9(\boldsymbol{x}) \oplus m_{10}(\boldsymbol{x}) \oplus m_{12}(\boldsymbol{x}),\\
f_1^+(\boldsymbol{x}) &= m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_6(\boldsymbol{x}) \oplus m_8(\boldsymbol{x})\\
&\quad \oplus m_9(\boldsymbol{x}) \oplus m_{10}(\boldsymbol{x}) \oplus m_{11}(\boldsymbol{x}) \oplus m_{12}(\boldsymbol{x}) \oplus m_{13}(\boldsymbol{x}),\\
f_2^+(\boldsymbol{x}) &= m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_8(\boldsymbol{x})\\
&\quad \oplus m_9(\boldsymbol{x}) \oplus m_{10}(\boldsymbol{x}) \oplus m_{11}(\boldsymbol{x}) \oplus m_{12}(\boldsymbol{x}) \oplus m_{14}(\boldsymbol{x}),\\
f_3^+(\boldsymbol{x}) &= m_3(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_8(\boldsymbol{x}) \oplus m_{13}(\boldsymbol{x}) \oplus m_{14}(\boldsymbol{x}) \oplus m_{15}(\boldsymbol{x}).
\end{aligned}$$

If we consider the permutation $\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 2 & 3 \end{pmatrix}$, then we obtain the function

$$\begin{aligned}
F(\boldsymbol{y},\boldsymbol{x}) &= m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_3(\boldsymbol{y},\boldsymbol{x}) \oplus m_5(\boldsymbol{y},\boldsymbol{x}) \oplus m_7(\boldsymbol{y},\boldsymbol{x}) \oplus m_{14}(\boldsymbol{y},\boldsymbol{x})\\
&\quad \oplus m_{15}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{16}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{23}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{27}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{29}(\boldsymbol{y},\boldsymbol{x})\\
&\quad \oplus m_{30}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{31}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{32}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{35}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{38}(\boldsymbol{y},\boldsymbol{x})\\
&\quad \oplus m_{39}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{45}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{47}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{48}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{49}(\boldsymbol{y},\boldsymbol{x})\\
&\quad \oplus m_{50}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{52}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{53}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{54}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{57}(\boldsymbol{y},\boldsymbol{x})\\
&\quad \oplus m_{58}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{59}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{60}(\boldsymbol{y},\boldsymbol{x})\\
&= 1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus y_1y_2x_2\\
&\quad \oplus y_1y_2x_3 \oplus y_1y_2x_4 \oplus y_1x_2x_3 \oplus y_1x_2x_4 \oplus y_2x_2x_4 \oplus y_2x_3x_4
\end{aligned}$$

which is not a Rothaus function, because its ANF does not contain the monomial y_1y_2. ■

Example 8: Assume that $n = 2$ and consider the bent functions of 2 variables

$$\begin{aligned}
f_0(\boldsymbol{x}) &= f_1(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}),\\
f_2(\boldsymbol{x}) &= m_2(\boldsymbol{x}),\\
f_3(\boldsymbol{x}) &= m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}),
\end{aligned}$$

then

$$f_0^+(\boldsymbol{x}) = f_1^+(\boldsymbol{x}) = m_0(\boldsymbol{x}),\ f_2^+(\boldsymbol{x}) = m_1(\boldsymbol{x}),\ \text{and}\ f_3^+(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}),$$

Variables	4	6	8	10
bent	896	5 425 430 528	2^{106}	?
Rothauss	512	?	?	?
Maiorana-McFarland	384	10 321 920	2^{60}	2^{150}
Carlet	320	?	?	?
Theorem 4	32	3 584	$2^{34.3}$	$2^{108.3}$
Theorem 5	288	4 806 144	$2^{67.25}$	$2^{215.17}$
Theorem 8	192	752 640	$2^{46.26}$	$2^{124.27}$
Theorem 9	0	68 040	$2^{40.85}$	$2^{116.85}$

Table 4: Number of bent functions constructed with different methods

If σ is the identity permutation, then we obtain the function

$$\begin{aligned} F(\boldsymbol{y},\boldsymbol{x}) &= m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_4(\boldsymbol{y},\boldsymbol{x}) \oplus m_9(\boldsymbol{y},\boldsymbol{x}) \oplus m_{12}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{14}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{15}(\boldsymbol{y},\boldsymbol{x}) \\ &= 1 \oplus x_1 \oplus x_2 \oplus x_1x_2 \oplus y_1 \oplus y_1x_1 \oplus y_1y_2 \end{aligned}$$

which is not a Maiorana-McFarland function. ■

Example 9: Assume now that $n = 2$ and consider the bent functions of 2 variables

$$\begin{aligned} f_0(\boldsymbol{x}) &= m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}), \\ f_1(\boldsymbol{x}) &= m_2(\boldsymbol{x}), \\ f_2(\boldsymbol{x}) &= m_1(\boldsymbol{x}), \\ f_3(\boldsymbol{x}) &= m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}), \end{aligned}$$

then

$$f_0^+(\boldsymbol{x}) = m_0(\boldsymbol{x}),\ f_1^+(\boldsymbol{x}) = m_1(\boldsymbol{x}),\ f_2^+(\boldsymbol{x}) = m_2(\boldsymbol{x}),\ f_3^+(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}).$$

If $\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix}$, then we obtain the function

$$F(\boldsymbol{y},\boldsymbol{x}) = m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_1(\boldsymbol{y},\boldsymbol{x}) \oplus m_2(\boldsymbol{y},\boldsymbol{x}) \oplus m_4(\boldsymbol{y},\boldsymbol{x}) \oplus m_9(\boldsymbol{y},\boldsymbol{x}) \oplus m_{14}(\boldsymbol{y},\boldsymbol{x}).$$

An exhaustive computer search shows that there are no bent functions of 2 variables $f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x})$, $g_0(\boldsymbol{y})$ and $g_1(\boldsymbol{y})$ such that

$$F(\boldsymbol{y},\boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus g_0(\boldsymbol{y}) \oplus (f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}))\,(g_0(\boldsymbol{y}) \oplus g_1(\boldsymbol{y}))\,.$$

Therefore, $F(\boldsymbol{y},\boldsymbol{x})$ is not a bent function of Carlet type. ■

Finally, Table 4 summarizes the number of bent functions we can construct using Theorems 4, 5, 8, and 9, compared with the number of bent functions of the classes of Rothaus, Mairona-McFarland and Carlet. Both the number of bent functions for 8 variables and the number of Rothaus functions of 6 and 8 variables are unknown.

Note that for 4 variables the number of bent functions provided by Theorems 4, 5, 8, and 9 is the same that the number of bent functions provided by the Rothaus construction; nevertheless, our construction and the Rothaus construction provide different bent functions as we see in Example 7 before.

Note also that for 4 variables the number of bent functions provided by Theorems 4, 5 is the same that the number of bent functions provided by the Carlet construction; nevertheless, these constructions provide different bent functions as we see in Example 9 before.

6 Conclusions

In this paper we have introduced a method to obtain bent functions of n variables from bent functions of n variables. With the new bent functions (which we have called max-weight and min-weight functions of the old bent functions) and with the four minterms of two variables, we constructed new bent functions of $n+2$ variables. With this method we obtain $6\nu_n^2 - 8\nu_n + 24\omega_n$ bent functions of $n+2$ variables, where ν_n is the number of bent functions of n variables (which is unknown for $n \geq 8$) and ω_n is the number of quadruplets of Boolean functions which satisfies Identity (6) leaving out the particular cases studied. We have established a lower bounded for the value ω_n, namely $\omega_n \geq \binom{2^n-1}{2}\nu_n\left(\nu_n - 2^{n+1}\right)$. We have also noted that if we take $f_j(\boldsymbol{x})$, for $j = 0, 1, 2, 3$, in Theorem 3 rather than $f_j^+(\boldsymbol{x})$, the resulting function of $n+2$ variables may not be bent. Moreover, our construction provides some bent functions which are not Rothaus nor Maiorana-McFarland type.

References

[1] Yuri Borissov, An Braeken, Svetla Nikova, and Bart Preneel. On the covering radii of binary Reed-Muller codes in the set of resilient Boolean functions. *IEEE Transactions on Information Theory*, 51(3):1182–1189, 2005.

[2] An Braeken, Yuri Borissov, Svetla Nikova, and Bart Preneel. Classification of Boolean functions of 6 variables or less with respect to some cryptographic properties. In Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *Automata, Languages and Programming*, volume 3580 of *Lecture Notes in Computer Science*, pages 324–334. Springer-Verlag, Berlin, 2005.

[3] An Braeken, Ventzislav Nikov, Svetla Nikova, and Bart Preneel. On Boolean functions with generalized cryptographic properties. In Anne Canteaut and Kapaleeswaran Viswanathan, editors, *Progress in Cryptology – INDOCRYPT 2004*, volume 3348 of *Lecture Notes in Computer Science*, pages 120–135. Springer-Verlag, Berlin, 2004.

[4] Anne Canteaut, Magnus Daum, Hans Dobbertin, and Gregor Leander. Finding nonnormal bent functions. *Discrete Applied Mathematics*, 154:202–218, 2006.

[5] C. Carlet and Yu. Tarannikov. Covering sequences of Boolean functions and their cryptographic significance. *Designs, Codes and Cryptography*, 25:263–279, 2002.

[6] Claude Carlet. Two new classes of bent functions. In Tor Helleseth, editor, *Advances in Cryptology – EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 77–101. Springer-Verlag, Berlin, 1994.

[7] Claude Carlet. On the secondary constructions of resilient and bent functions. *Progress in Computer Science and Applied Logic*, 23:3–28, 2004.

[8] Claude Carlet. On bent and highly nonlinear balanced/resilient functions and their algebraic immunities. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-16)*, volume 3857 of *Lecture Notes in Computer Science*, pages 1–28. Springer-Verlag, Berlin, 2006.

[9] Claude Carlet and Joseph L. Yucas. Piecewise constructions of bent and almost optimal Boolean functions. *Designs, Codes and Cryptography*, 37:449–464, 2005.

[10] Derek K. Chang. Binary bent sequences of order 64. *Utilitas Mathematica*, 52:141–151, 1997.

[11] Joan-Josep Climent, Francisco J. García, and Verónica Requena. On the construction of bent functions of $n + 2$ variables from bent functions of n variables. *Advances in Mathematics of Communications*, 2(4):421–431, 2008.

[12] M. Daum, H. Dobbertin, and G. Leander. An algorithm for checking normality of Boolean functions. In *Proceedings of the 2003 International Workshop on Coding and Cryptography (WCC 2003)*, pages 133–142, March 2003.

[13] John F. Dillon. *Elementary Hadamard Difference Sets*. PhD thesis, University of Maryland, 1974.

[14] Joanne Fuller, Ed Dawson, and William Millan. Evolutionary generation of bent functions for cryptography. In *Proceedings of the 2003 Congress on Evolutionary Computation*, volume 2, pages 1655–1661. IEEE, 2003.

[15] Xiang-Dong Hou and Philippe Langevin. Results on bent functions. *Journal of Combinatorial Theory (Series A)*, 80:232–246, 1997.

[16] P. V. Kumar, R. A. Scholtz, and L. R. Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory (Series A)*, 40:90–107, 1985.

[17] Kaoru Kurosawa, Tetsu Iwata, and Takayuki Yoshiwara. New covering radius of Reed-Muller codes for t-resilient functions. *IEEE Transactions on Information Theory*, 50(3):468–475, 2004.

[18] Philippe Langevin and Gregor Leander. Counting all bent functions in dimension eight 99270589265934370305785861242880. *Designs, Codes and Cryptography*, 59:193–201, 2011.

[19] V. V. Losev. Decoding of sequences of bent functions by means of a fast Hadamard transform. *Soviet Journal of Communications Technology and Electronics*, 32(10):155–157, 1987.

[20] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 6 edition, 1988.

[21] Robert L. McFarland. A family of difference sets in non-cyclic groups. *Journal of Combinatorial Theory (Series A)*, 15:1–10, 1973.

[22] Willi Meier and Othmar Staffelbach. Nonlinearity criteria for cryptographic functions. In J. J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology – EUROCRYPT'89*, volume 434 of *Lecture Notes in Computer Science*, pages 549–562. Springer-Verlag, Berlin, 1990.

[23] Daniel Olejár and Martin Stanek. On cryptographic properties of random Boolean functions. *Journal of Universal Computer Science*, 4(8):705–717, 1998.

[24] Enes Pasalic and Thomas Johansson. Further results on the relation between nonlinearity and resiliency for Boolean functions. In Michael Walker, editor, *Crytography and Coding*, volume 1746 of *Lecture Notes in Computer Science*, pages 35–44. Springer-Verlag, Berlin, 1999.

[25] J. Pieprzyk and G. Finkelstein. Towards effective nonlinear cryptosystem design. *IEEE Proceedings*, 135(6):325–335, 1988.

[26] Bart Preneel. *Analysis and Design of Cryptographic Hash Functions*. PhD thesis, Katholieke University Leuven, January 1993.

[27] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory (Series A)*, 20:300–305, 1976.

[28] Palash Sarkar and Subhamoy Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In B. Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 485–506. Springer-Verlag, Berlin, 2000.

[29] Jennifer Seberry and Xian-Mo Zhang. Constructions of bent functions from two known bent functions. *Australasian Journal of Combinatorics*, 9:21–35, 1994.

[30] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. Nonlinearity and propagation characteristics of balanced Boolean functions. *Information and Computation*, 119:1–13, 1995.

[31] Scott A. Vanstone and Paul C. van Oorschot. *An Introduction to Error Correcting Codes with Applications*. Kluwer Academic Publishers, Boston, MA, 1989.

[32] Rao Yarlagadda and John E. Hershey. Analysis and synthesis of bent sequences. *IEE Proceedings*, 136(2):112–123, 1989.

[33] Nam Yul Yu and Guang Gong. Constructions of quadratic bent functions in polynomial forms. *IEEE Transactions on Information Theory*, 52(7):3291–3299, 2006.