Hindawi Publishing Corporation
Algebra
Volume 2014, Article ID 701298, 11 pages
http://dx.doi.org/10.1155/2014/701298

Research Article

A Construction of Bent Functions of $n + 2$ Variables from a Bent Function of n Variables and Its Cyclic Shifts

Joan-Josep Climent,[1] Francisco J. García,[2] and Verónica Requena[3]

[1] *Departament d'Estadística i Investigació Operativa, Universitat d'Alacant, Sant Vicent del Raspeig, 03690 Alacant, Spain*
[2] *Departament de Mètodes Quantitatius i Teoria Econòmica, Universitat d'Alacant, Sant Vicent del Raspeig, 03690 Alacant, Spain*
[3] *Departamento de Estadística, Matemáticas e Informática, Universidad Miguel Hernández de Elche, 03202 Alacant, Spain*

Correspondence should be addressed to Joan-Josep Climent; jcliment@ua.es

Received 9 October 2013; Accepted 17 March 2014; Published 17 April 2014

Academic Editor: Masoud Hajarian

We present a method to iteratively construct new bent functions of $n + 2$ variables from a bent function of n variables and its cyclic shift permutations using minterms of n variables and minterms of 2 variables. In addition, we provide the number of bent functions of $n + 2$ variables that we can obtain by applying the method here presented, and finally we compare this method with a previous one introduced by us in 2008 and with the Rothaus and Maiorana-McFarland constructions.

1. Introduction

Boolean functions are widely used in different types of cryptographic applications, such as block ciphers, stream ciphers, and hash functions [1–3], and in coding theory [4, 5], among others. For example, the implementation of an S-box needs nonlinear Boolean functions to resist attacks such as the linear and differential cryptanalysis [6–9]. For an even number of variables, Boolean functions bearing maximum nonlinearity are called bent functions [10, 11]. The construction of one-to-one S-boxes so that any linear combination of the output functions is balanced has already been explained [12, 13] and also the issue of making such linear combination a bent function [14]. However, no conclusive approaches have been presented yet for the construction of all S-boxes so that they satisfy the property that any linear combination of the outputs is also bent. It is precisely for this reason that a thorough study of the properties of bent functions as well as of the methods to construct them has occupied the minds of many authors in the last decades (see, e.g., [9, 11, 15–35] and the references therein).

Bent functions constitute a fascinating issue in cryptography but, unfortunately, there is a mist hovering over their properties, their classification, and their actual number. The origin of the concept of bent function takes us back to a theoretical article by McFarland [36] where he discussed difference sets in finite noncyclic groups. Dillon [24], a year later, systematized and further elaborated McFarland's insights and provided proofs for a great number of properties; Dillon's Ph.D. dissertation has been an excellent source in the field of bent functions up to the mid 1970s. But it was Rothaus [37] who came up with the name for the concept. These functions are called perfect nonlinear Boolean functions by Meier and Staffelbach [30].

There are different ways to obtain bent functions; most of them are based on the algebraic normal form of a Boolean function and the Walsh transform. However, there are very few constructions of bent functions based on the truth table of Boolean functions, for example, the partial spread class of bent functions introduced by Dillon [24]; moreover, from the truth tables of linear functions and bent functions, it is possible to construct bent functions with a greater number of

variables [38]. But not all the bent functions in 6 variables can be obtained from bent functions and linear functions with a smaller number of variables, as proved by Chang [21]. Hou and Langevin [28] described how, from a well-known bent function, new bent functions can be obtained with the same number of variables.

Charnes et al. [39, 40] discovered a surprising relation with the classical invariant theory. Qu et al. [41] have found, by computer enumeration, an interesting class of bent functions with 6 variables. Carlet and Guillot [19], Dobbertin [25], Kumar et al. [29], and Langevin [42] have analyzed some bent function constructions, characterizations, properties, and generalizations. Tokareva [34] introduces lower bound on the number of bent functions that can be obtained by the iterative constructions proposed by Canteaut and Charpin [43].

A general method for generating all bent functions is not known to exist yet, except for some particular cases. For example, it is well known that, for $n = 4$, there are only 896 different bent functions, for $n = 6$, Preneel [32] (see also [21]) proved that the number of different bent functions is 5 425 430 528, and, for $n = 8$, Langevin and Leander [44] proved recently that the number of bent functions is 99 270 589 265 934 370 305 785 861 242 880. Nevertheless, the classification and counting for $n > 8$ is still an open problem.

We refer the reader to the two excellent surveys in [18] and [23, Chapter 5] about bent functions.

The mentioned literature so far makes an intensive use of the representation of Boolean functions either in polynomial form, in matrix form, or in sequential form. Nevertheless, the classical concept of minterm, which, by the way, is directly related to the implementation of logic circuits and its complexity, has not been frequently applied (see [22]). This paper purports to practically generate bent functions using the representation of Boolean functions as a sum of minterms.

The use of the algebraic normal form or the truth table or both has its advantages and disadvantages. For example, the algebraic normal form of a Boolean function $f(\mathbf{x})$ of n variables provides directly its degree, and, if it is greater than $n/2$, we can ensure that $f(\mathbf{x})$ is not a bent function [37]; nevertheless, we do not know the cardinality of its support (i.e., the number of minterms). On the other hand, if we know the truth table of $f(\mathbf{x})$, then we know if its support has the necessary number of elements to be a bent function, although we do not know its degree.

The remainder of the paper is organized as follows. In Section 2, we present some basic definitions and notations used. In Section 3, we introduce a general method for the construction of bent functions of $n + 2$ variables using a bent function of n variables and some of its shifts; we also introduce some other important results required to prove the main theorems. In Section 4, we present the necessary results to count the number of bent functions we can construct based on the method dealt with in Section 3. Finally, in Section 5, we show that our construction generates bent functions which are not Rothaus or Maiorana-McFarland type (see, e.g., [29, 37]); we also show that the construction introduced in this paper is basically different from the construction introduced in [22] and we compute the number of bent functions we can obtain using one construction but not by the other one. In addition, we summarize the number of bent functions obtained by the different methods here considered.

2. Preliminaries

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

$$\mathbf{a} \oplus \mathbf{b} = (a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_n \oplus b_n), \tag{1}$$

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

$$\langle \mathbf{a}, \mathbf{b} \rangle = a_1 b_1 \oplus a_2 b_2 \oplus \cdots \oplus a_n b_n, \tag{2}$$

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

$$a_1 = b_1, \qquad a_2 = b_2, \ldots, a_{k-1} = b_{k-1} \quad \text{with } a_k = 0,\ b_k = 1. \tag{3}$$

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

$$\mathbf{e}_0 < \mathbf{e}_1 < \cdots < \mathbf{e}_{2^n-1}. \tag{4}$$

Furthermore, if $\mathbf{e}_i = (\epsilon_1^{(i)}, \epsilon_2^{(i)}, \ldots, \epsilon_n^{(i)}) \in \mathbb{Z}_2^n$, then

$$\epsilon_1^{(i)} 2^{n-1} + \epsilon_2^{(i)} 2^{n-2} + \cdots + \epsilon_{n-1}^{(i)} 2^1 + \epsilon_n^{(i)} 2^0 = i \in \mathbb{Z}_{2^n} \tag{5}$$

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

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

$$(f \oplus g)(\mathbf{x}) = f(\mathbf{x}) \oplus g(\mathbf{x}), \tag{6}$$

for $f, g \in \mathscr{B}_n$. For a function f of $\mathscr{B}_n$, the $(0,1)$-sequence of length 2^n,

$$\boldsymbol{\xi}_f = (f(\mathbf{e}_0), f(\mathbf{e}_1), \ldots, f(\mathbf{e}_{2^n-1})), \tag{7}$$

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

$$\begin{aligned} &m_{(u_1,u_2,\ldots,u_n)}(x_1, x_2, \ldots, x_n) \\ &\quad = (1 \oplus u_1 \oplus x_1)(1 \oplus u_2 \oplus x_2) \cdots (1 \oplus u_n \oplus x_n), \end{aligned} \tag{8}$$

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

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

$$(m_i(\mathbf{e}_0), m_i(\mathbf{e}_1), \ldots, m_i(\mathbf{e}_{2^n-1})), \tag{9}$$

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

$$\bigoplus_{i=0}^{2^n-1} m_i(\mathbf{x}) = 1. \tag{10}$$

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

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

$$f(\mathbf{x}) = \bigoplus_{i=0}^{2^n-1} f(\mathbf{e}_i)\, m_i(\mathbf{x}) \tag{11}$$

and since the identity

$$\bigoplus_{i=0}^{2^n-1} a_i m_i(\mathbf{x}) = 0 \tag{12}$$

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

For all $f \in \mathscr{B}_n$, we call the *support* of f the set

$$M = \{\mathbf{a} \in \mathbb{Z}_2^n \mid f(\mathbf{a}) = 1\} \text{ or } M = \{i \in \mathbb{Z}_{2^n} \mid f(\mathbf{e}_i) = 1\}, \tag{13}$$

according to expression (11) and the identification of $\mathbb{Z}_2^n$ with $\mathbb{Z}_{2^n}$. So, we can identify M as the set of minterms of $f(\mathbf{x})$. Therefore, we can rewrite expression (11) as

$$f(\mathbf{x}) = \bigoplus_{i \in M} m_i(\mathbf{x}), \tag{14}$$

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

The *Hamming weight* of a $(0,1)$-sequence $\boldsymbol{\alpha}$, denoted by $w(\boldsymbol{\alpha})$, is the number of 1s in $\boldsymbol{\alpha}$. The Hamming weight of a Boolean function $f(\mathbf{x})$, 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 $f(\mathbf{x})$ taken as a sum of minterms. A $(0,1)$-sequence is balanced if it contains an equal number of 0s and 1s, so a function f in $\mathscr{B}_n$ is balanced if its truth table is balanced.

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

$$f(\mathbf{x}) = l_{\mathbf{a}}(\mathbf{x}) \oplus b, \tag{15}$$

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

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

$$\mathrm{NL}(f) = \min\{d(f, \varphi) \mid \varphi \in \mathscr{A}_n\}, \tag{16}$$

where $\mathscr{A}_n \subseteq \mathscr{B}_n$ is the set of all affine functions and the distance $d(f, g)$, for $f, g \in \mathscr{B}_n$, is defined as $d(f, g) = w(f \oplus g)$. The nonlinearity of $f \in \mathscr{B}_n$ is upper bounded (see, e.g., [11, 18, 23, 30]) by

$$\mathrm{NL}(f) \leq 2^{n-1} - 2^{n/2-1}. \tag{17}$$

The Boolean functions achieving the maximum nonlinearity are called *bent functions* (see, e.g., [11, 18, 23, 30]). As a consequence, bent functions only exist for n even.

It is well know that the above upper bound on the nonlinearity of a Boolean function of n variables coincides with the covering radius of the first order binary Reed-Muller code of length 2^n (see, e.g., [30, 45]).

The following result (see, e.g., [11, 46]) that we quote for further references gives us a characterization of a bent function.

Theorem 1. *Let $f(\mathbf{x})$ be a function of n variables. The following statements are equivalent.*

(1) *$f(\mathbf{x})$ is a bent function.*

(2) *The Boolean function $f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{a})$ is balanced for all $\mathbf{a} \in \mathbb{Z}_2^n \setminus \{\mathbf{0}\}$.*

(3) *The number of 1s in the truth table of the Boolean function $f(\mathbf{x}) \oplus l_{\mathbf{a}}(\mathbf{x})$ is $2^{n-1} \pm 2^{n/2-1}$ for all $\mathbf{a} \in \mathbb{Z}_2^n$.*

Taking into account that, and as a consequence of the previous theorem, if $f(\mathbf{x})$ is a bent function of n variables, then the number of 1s in its truth table is $2^{n-1} \pm 2^{n/2-1}$; so that $w(f) = 2^{n-1} \pm 2^{n/2-1}$ and $f(\mathbf{x})$ is not balanced. Equivalently, $f(\mathbf{x})$ is expressed as a sum of $2^{n-1} \pm 2^{n/2-1}$ minterms.

Finally, it is well known that for any bent function $f(\mathbf{x})$, the functions $1 \oplus f(\mathbf{x})$ and $f(\mathbf{x} \oplus \mathbf{u})$, for all $\mathbf{u} \in \mathbb{Z}_2^n$, are also bent functions.

Before moving onto the next section, remember that two Boolean functions $f(\mathbf{x})$ and $g(\mathbf{x})$ are called *affine equivalent* if there exist an $n \times n$ invertible matrix A, two vectors $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^n$, and a bit $c \in \mathbb{Z}_2$ such that $g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{a}) \oplus l_{\mathbf{b}}(\mathbf{x}) \oplus c$.

It is known (see, e.g., [47]) that affine equivalent functions are both bent or both not bent. So, many authors work on the problem of *finding the number and representatives of affine equivalent classes of bent functions*. Nevertheless, we are interested in the problem of *finding how many different bent functions there exist 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

$$f(\mathbf{x}) = m_0(\mathbf{x}) \oplus m_1(\mathbf{x}) \oplus m_2(\mathbf{x}) \oplus m_4(\mathbf{x}) \oplus m_8(\mathbf{x}) \oplus m_{15}(\mathbf{x}), \tag{18}$$

of 4 variables; the invertible matrix

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}, \tag{19}$$

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

3. Main Results

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

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

Lemma 3 (see Lemma 1 of [22]). *Suppose that $a \in \mathbb{Z}_{2^n}$ and $b \in \mathbb{Z}_{2^2}$. If $m_a(\mathbf{x})$ is a minterm of n variables and $m_b(\mathbf{y})$ is a minterm of 2 variables, then $m_c(\mathbf{y},\mathbf{x}) = m_b(\mathbf{y})m_a(\mathbf{x})$ is a minterm of $n+2$ variables, where*

$$c = b_1 2^{n+1} + b_2 2^n + a, \qquad b = b_1 2 + b_2. \tag{20}$$

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

$$\begin{aligned} &m_a(\mathbf{y},\mathbf{x}), \qquad m_{2^n+a}(\mathbf{y},\mathbf{x}), \\ &m_{2^{n+1}+a}(\mathbf{y},\mathbf{x}), \qquad m_{2^n+2^{n+1}+a}(\mathbf{y},\mathbf{x}). \end{aligned} \tag{21}$$

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 $m_{\mathbf{a}}(\mathbf{x})$ of n variables are

$$\begin{aligned} &m_{(0,0,\mathbf{a})}(\mathbf{y},\mathbf{x}), \qquad m_{(0,1,\mathbf{a})}(\mathbf{y},\mathbf{x}), \\ &m_{(1,0,\mathbf{a})}(\mathbf{y},\mathbf{x}), \qquad m_{(1,1,\mathbf{a})}(\mathbf{y},\mathbf{x}). \end{aligned} \tag{22}$$

Furthermore, minterms have the following property that makes them operative from the algebraic point of view.

Lemma 4. *One has $m_{\mathbf{u}}(x \oplus \mathbf{v}) = m_{\mathbf{u}\oplus\mathbf{v}}(\mathbf{x})$ for all $\mathbf{u},\mathbf{v} \in \mathbb{Z}_2^n$.*

Proof. Assume that

$$\mathbf{u} = (u_1, u_2, \ldots, u_n), \qquad \mathbf{v} = (v_1, v_2, \ldots, v_n); \tag{23}$$

then

$$\begin{aligned} m_{\mathbf{u}}(\mathbf{x}\oplus\mathbf{v}) &= (1 \oplus u_1 \oplus x_1 \oplus v_1)(1 \oplus u_2 \oplus x_2 \oplus v_2) \\ &\quad \cdots (1 \oplus u_n \oplus x_n \oplus v_n) = m_{\mathbf{u}\oplus\mathbf{v}}(\mathbf{x}). \end{aligned} \tag{24}$$

□

The following theorem is the main result of this paper. Here, we present a construction of bent functions of $n+2$ variables from a bent function $f(\mathbf{x})$ of n variables and some cyclic shifts of $f(\mathbf{x})$.

Theorem 5. *Let $f(\mathbf{x})$ be a bent function of n variables and consider $\mathbf{u},\mathbf{v} \in \mathbb{Z}_2^n$. If σ is any permutation of $\{0,1,2,3\}$, then*

$$\begin{aligned} B(\mathbf{y},\mathbf{x}) &= m_{\sigma(0)}(\mathbf{y}) f(\mathbf{x}) \oplus m_{\sigma(1)}(\mathbf{y}) f(\mathbf{x}\oplus\mathbf{u}) \\ &\quad \oplus m_{\sigma(2)}(\mathbf{y}) f(\mathbf{x}\oplus\mathbf{v}) \\ &\quad \oplus m_{\sigma(3)}(\mathbf{y})(1 \oplus f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v})) \end{aligned} \tag{25}$$

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

Proof. According to Theorem 1 we must prove that the Boolean function,

$$B_{(\mathbf{b},\mathbf{a})}(\mathbf{y},\mathbf{x}) = B(\mathbf{y},\mathbf{x}) \oplus B((\mathbf{y},\mathbf{x}) \oplus (\mathbf{b},\mathbf{a})), \tag{26}$$

is balanced for all $(\mathbf{b},\mathbf{a}) \in \mathbb{Z}_2^2 \times \mathbb{Z}_2^n$ with $(\mathbf{b},\mathbf{a}) \neq (\mathbf{0}_2,\mathbf{0}_n)$. In the following, we use the vector $\mathbf{b} = (b_1,b_2) \in \mathbb{Z}_2^2$ as the argument of the functions and its integer representation $b = b_1 2 + b_2 \in \mathbb{Z}_{2^2}$ as subindex of a minterm. So, by Lemma 4,

$$\begin{aligned} B_{(\mathbf{b},\mathbf{a})}(\mathbf{y},\mathbf{x}) &= B(\mathbf{y},\mathbf{x}) \oplus B(\mathbf{y}\oplus\mathbf{b},\mathbf{x}\oplus\mathbf{b}) \\ &= m_{\sigma(0)}(\mathbf{y}) f(\mathbf{x}) \\ &\quad \oplus m_{\sigma(1)}(\mathbf{y}) f(\mathbf{x}\oplus\mathbf{u}) \oplus m_{\sigma(2)}(\mathbf{y}) f(\mathbf{x}\oplus\mathbf{v}) \\ &\quad \oplus m_{\sigma(3)}(\mathbf{y})(1 \oplus f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v})) \\ &\quad \oplus m_{\sigma(0)\oplus b}(\mathbf{y}) f(\mathbf{x}\oplus\mathbf{a}) \\ &\quad \oplus m_{\sigma(1)\oplus b}(\mathbf{y}) f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{a}) \\ &\quad \oplus m_{\sigma(2)\oplus b}(\mathbf{y}) f(\mathbf{x}\oplus\mathbf{v}\oplus\mathbf{a}) \\ &\quad \oplus m_{\sigma(3)\oplus b}(\mathbf{y})(1 \oplus f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v}\oplus\mathbf{a})). \end{aligned} \tag{27}$$

Now, for each $b \in \mathbb{Z}_{2^2}$, if we denote by μ_b the permutation of $\{0,1,2,3\}$ given by

$$\mu_b(i) = \sigma(i) \oplus b \quad \text{for } i = 0,1,2,3, \tag{28}$$

then it is not difficult to prove that the $4!\cdot 4$ cases, corresponding to the different values of σ and b, are reduced to one of the following four cases for some permutation η of $\{0,1,2,3\}$.

(1) Consider

$$\begin{aligned} B_{(\mathbf{b},\mathbf{a})}(\mathbf{y},\mathbf{x}) &= m_{\eta(0)}(\mathbf{y})(f(\mathbf{x}) \oplus f(\mathbf{x}\oplus\mathbf{a})) \\ &\quad \oplus m_{\eta(1)}(\mathbf{y})(f(\mathbf{x}\oplus\mathbf{u}) \oplus f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{a})) \\ &\quad \oplus m_{\eta(2)}(\mathbf{y})(f(\mathbf{x}\oplus\mathbf{v}) \oplus f(\mathbf{x}\oplus\mathbf{v}\oplus\mathbf{a})) \\ &\quad \oplus m_{\eta(3)}(\mathbf{y})(f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v}) \oplus f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v}\oplus\mathbf{a})). \end{aligned} \tag{29}$$

(2) Consider

$$\begin{aligned} B_{(\mathbf{b},\mathbf{a})}(\mathbf{y},\mathbf{x}) &= m_{\eta(0)}(\mathbf{y})(f(\mathbf{x}) \oplus f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{a})) \\ &\quad \oplus m_{\eta(1)}(\mathbf{y})(f(\mathbf{x}\oplus\mathbf{u}) \oplus f(\mathbf{x}\oplus\mathbf{a})) \\ &\quad \oplus m_{\eta(2)}(\mathbf{y})(f(\mathbf{x}\oplus\mathbf{v}) \oplus f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v}\oplus\mathbf{a}) \oplus 1) \\ &\quad \oplus m_{\eta(3)}(\mathbf{y})(f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v}) \oplus f(\mathbf{x}\oplus\mathbf{v}\oplus\mathbf{a}) \oplus 1). \end{aligned} \tag{30}$$

(3) Consider

$$\begin{aligned} B_{(\mathbf{b},\mathbf{a})}(\mathbf{y},\mathbf{x}) &= m_{\eta(0)}(\mathbf{y})\left(f(\mathbf{x}) \oplus f(\mathbf{x}\oplus\mathbf{v}\oplus\mathbf{a})\right) \\ &\oplus m_{\eta(1)}(\mathbf{y})\left(f(\mathbf{x}\oplus\mathbf{u}) \oplus f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v}\oplus\mathbf{a}) \oplus 1\right) \\ &\oplus m_{\eta(2)}(\mathbf{y})\left(f(\mathbf{x}\oplus\mathbf{v}) \oplus f(\mathbf{x}\oplus\mathbf{a})\right) \\ &\oplus m_{\eta(3)}(\mathbf{y})\left(f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v}) \oplus f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{a}) \oplus 1\right). \end{aligned} \tag{31}$$

(4) Consider

$$\begin{aligned} B_{(\mathbf{b},\mathbf{a})}(\mathbf{y},\mathbf{x}) &= m_{\eta(0)}(\mathbf{y})\left(f(\mathbf{x}) \oplus f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v}\oplus\mathbf{a}) \oplus 1\right) \\ &\oplus m_{\eta(1)}(\mathbf{y})\left(f(\mathbf{x}\oplus\mathbf{u}) \oplus f(\mathbf{x}\oplus\mathbf{v}\oplus\mathbf{a})\right) \\ &\oplus m_{\eta(2)}(\mathbf{y})\left(f(\mathbf{x}\oplus\mathbf{v}) \oplus f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{a})\right) \\ &\oplus m_{\eta(3)}(\mathbf{y})\left(f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v}) \oplus f(\mathbf{x}\oplus\mathbf{a}) \oplus 1\right). \end{aligned} \tag{32}$$

Observe that each one of the factors which multiply to $m_{\eta(i)}(\mathbf{y})$ for $i = 0, 1, 2, 3$ can be written as

$$\begin{aligned} &f(\mathbf{z}) \oplus f(\mathbf{z}\oplus\mathbf{a}) \quad \text{or } f(\mathbf{z}) \oplus f(\mathbf{z}\oplus\mathbf{a}) \oplus 1 \\ &\text{for } \mathbf{z} \in \{\mathbf{x}, \mathbf{x}\oplus\mathbf{u}, \mathbf{x}\oplus\mathbf{v}, \mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v}\}. \end{aligned} \tag{33}$$

Now, by Theorem 1, since $f(\mathbf{z}) \oplus f(\mathbf{z}\oplus\mathbf{a})$ is balanced for all nonzero $\mathbf{a}$, we have that $B_{(\mathbf{b},\mathbf{a})}(\mathbf{y},\mathbf{x})$ is balanced, unless $\mathbf{a} = \mathbf{b} = \mathbf{0}$. □

Note that, as a consequence of Lemma 4, if M is the support of $f(\mathbf{x})$, then

$$M_{\mathbf{w}} = \{\mathbf{a}\oplus\mathbf{w} \mid \mathbf{a} \in M\} \tag{34}$$

is the support of $f(\mathbf{x}\oplus\mathbf{w})$ for all $\mathbf{w} \in \mathbb{Z}_2^n$. Furthermore, as a consequence of Lemma 3, if we use the decimal notation for the indices of the minterms and consider the permutation $\begin{pmatrix} 0 & 2^n & 2^{n+1} & 2^n+2^{n+1} \\ b_0 & b_1 & b_2 & b_3 \end{pmatrix}$, then the support of the bent function $B(\mathbf{y},\mathbf{x})$ constructed in Theorem 5 is the set

$$\begin{aligned} &\{b_0 + a \mid a \in M\} \cup \{b_1 + a \mid a \in M_{\mathbf{u}}\} \\ &\cup \{b_2 + a \mid a \in M_{\mathbf{v}}\} \cup \{b_3 + a \mid a \in M_{\mathbf{u}\oplus\mathbf{v}}\}. \end{aligned} \tag{35}$$

Nevertheless, if we use the vector notation for the indices of the minterms and consider the permutation $\begin{pmatrix} (0,0) & (0,1) & (1,0) & (1,1) \\ \mathbf{b}_0 & \mathbf{b}_1 & \mathbf{b}_2 & \mathbf{b}_3 \end{pmatrix}$, then the support of $B(\mathbf{y},\mathbf{x})$ is the set

$$\begin{aligned} &\{(\mathbf{b}_0,\mathbf{a}) \mid \mathbf{a} \in M\} \cup \{(\mathbf{b}_1,\mathbf{a}) \mid \mathbf{a} \in M_{\mathbf{u}}\} \\ &\cup \{(\mathbf{b}_2,\mathbf{a}) \mid \mathbf{a} \in M_{\mathbf{v}}\} \cup \{(\mathbf{b}_3,\mathbf{a}) \mid \mathbf{a} \in M_{\mathbf{u}\oplus\mathbf{v}}\}. \end{aligned} \tag{36}$$

Note that the sets of expression (35) (resp., (36)) are pairwise disjoints by Lemma 3.

4. Counting Bent Functions

In this section we introduce some results in order to compute the number of bent functions we can construct using Theorem 5. Firstly, we consider three particular cases (see Corollaries 6, 7, and 8) which we can derive directly from Theorem 5. The first one corresponds to the case $\mathbf{u} = \mathbf{v} = \mathbf{0}$; the second one to the case $\mathbf{u} = \mathbf{v} \neq \mathbf{0}$, and the third one to the case $\mathbf{0} \neq \mathbf{u} \neq \mathbf{v} \neq \mathbf{0}$.

Corollary 6. *If $f(\mathbf{x})$ is a bent function of n variables and σ is any permutation of $\{0, 1, 2, 3\}$, then*

$$\begin{aligned} F_f(\mathbf{y},\mathbf{x}) &= \left(m_{\sigma(0)}(\mathbf{y}) \oplus m_{\sigma(1)}(\mathbf{y}) \oplus m_{\sigma(2)}(\mathbf{y})\right) \\ &\times f(\mathbf{x}) \oplus m_{\sigma(3)}(\mathbf{y})\left(1 \oplus f(\mathbf{x})\right) \end{aligned} \tag{37}$$

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

Corollary 7. *If $f(\mathbf{x})$ is a bent function of n variables, $\mathbf{u} \in \mathbb{Z}_2^n \setminus \{\mathbf{0}\}$, and σ is any permutation of $\{0, 1, 2, 3\}$, then*

$$\begin{aligned} G_{f,\mathbf{u}}(\mathbf{y},\mathbf{x}) &= m_{\sigma(0)}(\mathbf{y})\, f(\mathbf{x}) \oplus \left(m_{\sigma(1)}(\mathbf{y}) \oplus m_{\sigma(2)}(\mathbf{y})\right) \\ &\times f(\mathbf{x}\oplus\mathbf{u}) \oplus m_{\sigma(3)}(\mathbf{y})\left(1 \oplus f(\mathbf{x})\right) \end{aligned} \tag{38}$$

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

Corollary 8. *If $f(\mathbf{x})$ is a bent function of n variables, $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^n \setminus \{\mathbf{0}\}$, with $\mathbf{u} \neq \mathbf{v}$, and σ is any permutation of $\{0, 1, 2, 3\}$, then*

$$\begin{aligned} H_{f,\mathbf{u},\mathbf{v}}(\mathbf{y},\mathbf{x}) &= m_{\sigma(0)}(\mathbf{y})\, f(\mathbf{x}) \oplus m_{\sigma(1)}(\mathbf{y})\, f(\mathbf{x}\oplus\mathbf{u}) \\ &\oplus m_{\sigma(2)}(\mathbf{y})\, f(\mathbf{x}\oplus\mathbf{v}) \\ &\oplus m_{\sigma(3)}(\mathbf{y})\left(1 \oplus f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v})\right) \end{aligned} \tag{39}$$

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

The following result establishes that the bent functions constructed in Corollary 6 are all different from one another.

Lemma 9. *Let $f(\mathbf{x})$ and $g(\mathbf{x})$ be bent functions of n variables. Assume that $F_f(\mathbf{y},\mathbf{x})$ is the bent function constructed in Corollary 6 using $f(\mathbf{x})$ and the permutation σ of $\{0, 1, 2, 3\}$. Assume also that $F_g(\mathbf{y},\mathbf{x})$ is the bent function constructed in Corollary 6 using $g(\mathbf{x})$ and the permutation τ of $\{0, 1, 2, 3\}$. If $f(\mathbf{x}) \neq g(\mathbf{x})$, then $F_f(\mathbf{y},\mathbf{x}) \neq F_g(\mathbf{y},\mathbf{x})$.*

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

$$\begin{aligned} F_f: &\quad \boldsymbol{\xi} \quad \boldsymbol{\xi} \quad \boldsymbol{\xi} \quad \mathbf{1}\oplus\boldsymbol{\xi} \\ F_g: &\quad \boldsymbol{\eta} \quad \boldsymbol{\eta} \quad \boldsymbol{\eta} \quad \mathbf{1}\oplus\boldsymbol{\eta}. \end{aligned} \tag{40}$$

If $F_f(\mathbf{y},\mathbf{x}) = F_g(\mathbf{y},\mathbf{x})$, 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 that $f(\mathbf{x}) = g(\mathbf{x})$, or that $f(\mathbf{x})$

and $g(\mathbf{x})$ both have the same number of minterms and the complementary number of minterms. So, in all cases, we obtain a contradiction and, therefore, $F_f(\mathbf{y},\mathbf{x}) \neq F_g(\mathbf{y},\mathbf{x})$. □

Our next result, whose proof is similar to the previous one, establishes that the bent functions constructed in Corollary 7 are all different from one another.

Lemma 10. *Let $f(\mathbf{x})$ and $g(\mathbf{x})$ be bent functions of n variables. Assume that $G_{f,\mathbf{u}}(\mathbf{y},\mathbf{x})$ is the bent function constructed in Corollary 7 using $f(\mathbf{x})$, the vector $\mathbf{u} \in \mathbb{Z}_2^n \setminus \{\mathbf{0}\}$, and the permutation σ of $\{0,1,2,3\}$. Assume also that $G_{g,\mathbf{a}}(\mathbf{y},\mathbf{x})$ is the bent function constructed in Corollary 7 using $g(\mathbf{x})$, the vector $\mathbf{a} \in \mathbb{Z}_2^n \setminus \{\mathbf{0}\}$, and the permutation τ of $\{0,1,2,3\}$. If $f(\mathbf{x}) \neq g(\mathbf{x})$, then $G_f(\mathbf{y},\mathbf{x}) \neq G_g(\mathbf{y},\mathbf{x})$.*

The same result is not true for the bent functions constructed using Corollary 8 as we can see in the following example.

Example 11. Assume that $n = 2$. Consider the vectors $\mathbf{u} = \mathbf{1} = (0,1)$, $\mathbf{v} = \mathbf{2} = (1,0)$ and the bent function $f(\mathbf{x}) = m_0(\mathbf{x})$. Then, according to expression (10), Lemmas 3 and 4, and Corollary 8, we have that

$$\begin{aligned} H_{f,\mathbf{1},\mathbf{2}}(\mathbf{y},\mathbf{x}) &= m_0(\mathbf{y})\, f(\mathbf{x}) \oplus m_1(\mathbf{y})\, f(\mathbf{x}\oplus\mathbf{1}) \oplus m_2(\mathbf{y})\, f(\mathbf{x}\oplus\mathbf{2}) \\ &\quad \oplus m_3(\mathbf{y})\,(1 \oplus f(\mathbf{x}\oplus\mathbf{3})) \\ &= m_0(\mathbf{y})\, m_0(\mathbf{x}) \oplus m_1(\mathbf{y})\, m_1(\mathbf{x}) \oplus m_2(\mathbf{y})\, m_2(\mathbf{x}) \\ &\quad \oplus m_3(\mathbf{y})\,(1 \oplus m_3(\mathbf{x})) \\ &= m_0(\mathbf{y},\mathbf{x}) \oplus m_5(\mathbf{y},\mathbf{x}) \oplus m_{10}(\mathbf{y},\mathbf{x}) \oplus m_{12}(\mathbf{y},\mathbf{x}) \\ &\quad \oplus m_{13}(\mathbf{y},\mathbf{x}) \oplus m_{14}(\mathbf{y},\mathbf{x}) \end{aligned} \tag{41}$$

is a bent function of $n + 2 = 4$ variables.

On the other hand, consider the vectors $\mathbf{a} = \mathbf{1} = (0,1)$ and $\mathbf{b} = \mathbf{3} = (1,1)$ and the bent function $g(\mathbf{x}) = m_1(\mathbf{x})$. Again, by expression (10), Lemmas 3 and 4, and Corollary 8, we have that

$$\begin{aligned} H_{g,\mathbf{1},\mathbf{3}}(\mathbf{y},\mathbf{x}) &= m_1(\mathbf{y})\, g(\mathbf{x}) \oplus m_0(\mathbf{y})\, g(\mathbf{x}\oplus\mathbf{1}) \\ &\quad \oplus m_2(\mathbf{y})\, g(\mathbf{x}\oplus\mathbf{3}) \oplus m_3(\mathbf{y})\,(1 \oplus g(\mathbf{x}\oplus\mathbf{2})) \\ &= m_0(\mathbf{y},\mathbf{x}) \oplus m_5(\mathbf{y},\mathbf{x}) \oplus m_{10}(\mathbf{y},\mathbf{x}) \\ &\quad \oplus m_{12}(\mathbf{y},\mathbf{x}) \oplus m_{13}(\mathbf{y},\mathbf{x}) \oplus m_{14}(\mathbf{y},\mathbf{x}), \end{aligned} \tag{42}$$

is a bent function of $n + 2 = 4$ variables. Clearly $H_{g,\mathbf{1},\mathbf{3}}(\mathbf{y},\mathbf{x}) = H_{f,\mathbf{1},\mathbf{2}}(\mathbf{y},\mathbf{x})$.

Note that, in the previous example, $g(\mathbf{x}) = f(\mathbf{x}\oplus\mathbf{1})$ and that $\{\mathbf{1},\mathbf{2}\}$ and $\{\mathbf{1},\mathbf{3}\}$ are bases of the same linear subspace $\{\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3}\}$ of $\mathbb{Z}_2^2$. With the aim to avoid this situation which provides equal bent functions, we will consider only vectors $\mathbf{u},\mathbf{v} \in \mathbb{Z}_2^n$ such that $\{\mathbf{u},\mathbf{v}\}$ is a Gauss-Jordan basis of cardinality 2. Remember that a set $\{\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_k\} \subseteq \mathbb{Z}_2^n$ is a Gauss-Jordan basis of cardinality k if the matrix whose rows are $\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_k$ is in reduced row echelon form (see also [48, 49]).

So, our next result establishes that the bent functions constructed in Corollary 8 are all different if $\{\mathbf{u},\mathbf{v}\}$ is a Gauss-Jordan basis of cardinality 2 of $\mathbb{Z}_2^n$.

Lemma 12. *Let $f(\mathbf{x})$ and $g(\mathbf{x})$ be bent functions of n variables. Assume that $H_{f,\mathbf{u},\mathbf{v}}(\mathbf{y},\mathbf{x})$ is the bent function constructed in Corollary 8 using $f(\mathbf{x})$, the Gauss-Jordan basis $\{\mathbf{u},\mathbf{v}\}$ of cardinality 2 of $\mathbb{Z}_2^n$, and the permutation σ of $\{0,1,2,3\}$. Assume also that $H_{g,\mathbf{a},\mathbf{b}}(\mathbf{y},\mathbf{x})$ is the bent function constructed in Corollary 8 using $g(\mathbf{x})$, the Gauss-Jordan basis $\{\mathbf{a},\mathbf{b}\}$ of cardinality 2 of $\mathbb{Z}_2^n$, and the permutation τ of $\{0,1,2,3\}$. If $f(\mathbf{x}) \neq g(\mathbf{x})$, then $H_{f,\mathbf{u},\mathbf{v}}(\mathbf{y},\mathbf{x}) \neq H_{g,\mathbf{a},\mathbf{b}}(\mathbf{y},\mathbf{x})$.*

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

$$\begin{array}{lcccc} H_{f,\mathbf{u},\mathbf{v}}: & \boldsymbol{\xi} & \boldsymbol{\xi}_{\mathbf{u}} & \boldsymbol{\xi}_{\mathbf{v}} & \mathbf{1} \oplus \boldsymbol{\xi}_{\mathbf{u}\oplus\mathbf{v}} \\ H_{g,\mathbf{a},\mathbf{b}}: & \boldsymbol{\eta} & \boldsymbol{\eta}_{\mathbf{a}} & \boldsymbol{\eta}_{\mathbf{b}} & \mathbf{1} \oplus \boldsymbol{\eta}_{\mathbf{a}\oplus\mathbf{b}}, \end{array} \tag{43}$$

where $\boldsymbol{\xi}_{\mathbf{u}}$, $\boldsymbol{\xi}_{\mathbf{v}}$, $\boldsymbol{\xi}_{\mathbf{u}\oplus\mathbf{v}}$, $\boldsymbol{\eta}_{\mathbf{a}}$, $\boldsymbol{\eta}_{\mathbf{b}}$, and $\boldsymbol{\eta}_{\mathbf{a}\oplus\mathbf{b}}$ are the truth tables of $f(\mathbf{x}\oplus\mathbf{u})$, $f(\mathbf{x}\oplus\mathbf{v})$, $f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v})$, $g(\mathbf{x}\oplus\mathbf{a})$, $g(\mathbf{x}\oplus\mathbf{b})$, and $g(\mathbf{x}\oplus\mathbf{a}\oplus\mathbf{b})$, respectively.

If $H_{f,\mathbf{u},\mathbf{v}}(\mathbf{y},\mathbf{x}) = H_{g,\mathbf{a},\mathbf{b}}(\mathbf{y},\mathbf{x})$, 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 that $f(\mathbf{x}) = g(\mathbf{x})$ or that $f(\mathbf{x})$ and $g(\mathbf{x})$ both have the same number of minterms and the complementary number of minterms, or that

$$(\mathbf{a},\mathbf{b}) \in \{(\mathbf{u},\mathbf{u}\oplus\mathbf{v}),(\mathbf{v},\mathbf{u}\oplus\mathbf{v}),(\mathbf{u}\oplus\mathbf{v},\mathbf{u}),(\mathbf{u}\oplus\mathbf{v},\mathbf{v})\}; \tag{44}$$

note that if $\{\mathbf{u},\mathbf{v}\}$ is a Gauss-Jordan basis of cardinality 2, then $\{\mathbf{a},\mathbf{b}\}$ cannot be a Gauss-Jordan basis of cardinality 2. So, in all cases we obtain a contradiction and, therefore, $H_{f,\mathbf{u},\mathbf{v}}(\mathbf{y},\mathbf{x}) \neq H_{g,\mathbf{a},\mathbf{b}}(\mathbf{y},\mathbf{x})$. □

Our next result establishes that none of the bent functions, obtained by one of Corollaries 6, 7, and 8, can be obtained by any of the others involved.

Lemma 13. *Let $f(\mathbf{x})$, $g(\mathbf{x})$, and $h(\mathbf{x})$ be three bent functions of n variables (not necessarily different). Assume that $F_f(\mathbf{y},\mathbf{x})$ is the bent function constructed in Corollary 6 using $f(\mathbf{x})$ and the permutation σ of $\{0,1,2,3\}$. Assume that $G_{g,\mathbf{u}}(\mathbf{y},\mathbf{x})$ is the bent function constructed in Corollary 7 using $g(\mathbf{x})$, the vector $\mathbf{u} \in \mathbb{Z}_2^n \setminus \{\mathbf{0}\}$, and the permutation τ of $\{0,1,2,3\}$. Assume also that $H_{h,\mathbf{a},\mathbf{b}}(\mathbf{y},\mathbf{x})$ is the bent function constructed in Corollary 8 using $h(\mathbf{x})$, the Gauss-Jordan basis $\{\mathbf{a},\mathbf{b}\}$ of cardinality 2 of $\mathbb{Z}_2^n$, and the permutation ω of $\{0,1,2,3\}$. Then $F_f(\mathbf{y},\mathbf{x}) \neq G_{g,\mathbf{u}}(\mathbf{y},\mathbf{x})$, $F_f(\mathbf{y},\mathbf{x}) \neq H_{h,\mathbf{a},\mathbf{b}}(\mathbf{y},\mathbf{x})$, and $G_{g,\mathbf{u}}(\mathbf{y},\mathbf{x}) \neq H_{h,\mathbf{a},\mathbf{b}}(\mathbf{y},\mathbf{x})$.*

Proof. If $\boldsymbol{\xi}$, $\boldsymbol{\eta}$, and $\boldsymbol{\zeta}$ are the truth tables of $f(\mathbf{x})$, $g(\mathbf{x})$, and $h(\mathbf{x})$, respectively, then the truth tables of $F_f(\mathbf{y},\mathbf{x})$, $G_{g,\mathbf{u}}(\mathbf{y},\mathbf{x})$,

and $H_{h,\mathbf{u},\mathbf{v}}(\mathbf{y},\mathbf{x})$ have four blocks (not necessarily in that order and not the same order for all):

$$\begin{array}{lcccc} F_f: & \boldsymbol{\xi} & \boldsymbol{\xi} & \boldsymbol{\xi} & \mathbf{1}\oplus\boldsymbol{\xi} \\ G_{g,\mathbf{u}}: & \boldsymbol{\eta} & \boldsymbol{\eta}_{\mathbf{u}} & \boldsymbol{\eta}_{\mathbf{u}} & \mathbf{1}\oplus\boldsymbol{\eta} \\ H_{h,\mathbf{a},\mathbf{b}}: & \boldsymbol{\zeta} & \boldsymbol{\zeta}_{\mathbf{a}} & \boldsymbol{\zeta}_{\mathbf{b}} & \mathbf{1}\oplus\boldsymbol{\zeta}_{\mathbf{a}\oplus\mathbf{b}}, \end{array} \tag{45}$$

where $\boldsymbol{\eta}_{\mathbf{u}}$, $\boldsymbol{\zeta}_{\mathbf{a}}$, $\boldsymbol{\zeta}_{\mathbf{b}}$, and $\boldsymbol{\zeta}_{\mathbf{a}\oplus\mathbf{b}}$ are the truth tables of $g(\mathbf{x}\oplus\mathbf{u})$, $h(\mathbf{x}\oplus\mathbf{a})$, $h(\mathbf{x}\oplus\mathbf{b})$, and $h(\mathbf{x}\oplus\mathbf{a}\oplus\mathbf{b})$, respectively.

The result is now evident because $F_f(\mathbf{y},\mathbf{x})$ has three identical blocks, $G_{g,\mathbf{u}}(\mathbf{y},\mathbf{x})$ has only two identical blocks, and all the blocks of $H_{h,\mathbf{a},\mathbf{b}}(\mathbf{y},\mathbf{x})$ are different. □

Now, as a consequence of the previous lemmas, we can obtain the number of bent functions of $n+2$ variables that we can construct using Corollaries 6, 7, and 8.

Theorem 14. *If ν_n is the number of bent functions of n variables, then using Corollaries 6, 7, and 8 one can construct $2^{2n+2}\nu_n$ different bent functions of $n+2$ variables.*

Proof. According to Lemma 9, using Corollary 6, we can construct

$$\frac{4!}{3!}\nu_n, \tag{46}$$

bent functions of $n+2$ variables.

Similarly, according to Lemma 10, using Corollary 7, we can construct

$$\frac{4!}{2!}\nu_n\left(2^n-1\right), \tag{47}$$

bent functions of $n+2$ variables.

Finally, according to Lemma 12, using Corollary 8, we can construct

$$4!\nu_n N(n,2), \tag{48}$$

bent functions of $n+2$ variables where $N(n,2)$ is the number of Gauss-Jordan basis of cardinality 2 in $\mathbb{Z}_2^n$. Now, taking into account that each linear subspace of dimension 2 has a unique Gauss-Jordan basis of cardinality 2, we have that $N(n,2)$ is the number of linear subspaces of dimension 2 in $\mathbb{Z}_2^n$; so (see [50, page 46])

$$N(n,2)=\frac{\left(2^n-1\right)\left(2^n-2\right)}{\left(2^2-1\right)\left(2^2-2\right)}=\frac{\left(2^n-1\right)\left(2^{n-1}-1\right)}{3}. \tag{49}$$

The result follows now by replacing expression (49) in expression (48) and by adding expressions (46), (47), and (48) because Lemma 13 guarantees that bent functions constructed according to Corollaries 6, 7, and 8 are all different from one another. □

5. Comparison with Other Methods

Our examples now show some bent functions constructed according to Corollaries 7 and 8 that are not Maiorana-McFarland functions or Rothaus functions.

Example 15. Assume that $n=2$ and consider the bent function $f(\mathbf{x})=m_3(\mathbf{x})$, the vector $\mathbf{u}=\mathbf{3}=(1,1)$, and the permutation $\left(\begin{smallmatrix}0&1&2&3\\3&1&2&0\end{smallmatrix}\right)$. Then Corollary 7, expression (10), and Lemmas 3 and 4 provide the bent function

$$\begin{aligned} G(\mathbf{y},\mathbf{x}) &= m_3(\mathbf{y})m_3(\mathbf{x})\oplus\left(m_1(\mathbf{y})\oplus m_2(\mathbf{y})\right)m_0(\mathbf{x}) \\ &\quad\oplus m_0(\mathbf{y})\left(1\oplus m_3(\mathbf{x})\right) \\ &= m_{15}(\mathbf{y},\mathbf{x})\oplus m_4(\mathbf{y},\mathbf{x})\oplus m_8(\mathbf{y},\mathbf{x}) \\ &\quad\oplus m_0(\mathbf{y},\mathbf{x})\oplus m_1(\mathbf{y},\mathbf{x})\oplus m_2(\mathbf{y},\mathbf{x}) \\ &= 1\oplus x_1x_2\oplus y_1y_2\oplus y_1x_1 \\ &\quad\oplus y_1x_2\oplus y_2x_1\oplus y_2x_2, \end{aligned} \tag{50}$$

which is not a Maiorana-McFarland function.

Example 16. Assume that $n=2$ and consider the bent function $f(\mathbf{x})=m_1(\mathbf{x})$, the vectors $\mathbf{u}=\mathbf{2}=(1,0)$, $\mathbf{v}=\mathbf{1}=(0,1)$, and the permutation $\left(\begin{smallmatrix}0&1&2&3\\0&3&1&2\end{smallmatrix}\right)$. Then Corollary 8, expression (10), and Lemmas 3 and 4 provide the bent function

$$\begin{aligned} H(\mathbf{y},\mathbf{x}) &= m_0(\mathbf{y})m_1(\mathbf{x})\oplus m_3(\mathbf{y})m_3(\mathbf{x}) \\ &\quad\oplus m_1(\mathbf{y})m_0(\mathbf{x})\oplus m_2(\mathbf{y})\left(1\oplus m_2(\mathbf{x})\right) \\ &= m_1(\mathbf{y},\mathbf{x})\oplus m_{15}(\mathbf{y},\mathbf{x})\oplus m_4(\mathbf{y},\mathbf{x}) \\ &\quad\oplus m_8(\mathbf{y},\mathbf{x})\oplus m_9(\mathbf{y},\mathbf{x})\oplus m_{11}(\mathbf{y},\mathbf{x}) \\ &= x_2\oplus x_1x_2\oplus y_2\oplus y_2x_1 \\ &\quad\oplus y_1\oplus y_1x_2\oplus y_1x_1, \end{aligned} \tag{51}$$

which is not a Rothaus function, because it does not contain the monomial y_1y_2.

In [22] we introduced the following construction of bent functions of $n+2$ variables using bent functions of n variables and the minterms of two variables.

Theorem 17. *(1) (Corollary 1 of [22]). If $f(\mathbf{x})$ is a bent function of n variables and if $i\in\{0,1,2,3\}$, then*

$$A_f(\mathbf{y},\mathbf{x})=f(\mathbf{x})\oplus m_i(\mathbf{y}) \tag{52}$$

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

(2) (Corollary 2 of [22]). Let $f_0(\mathbf{x})$ and $f_1(\mathbf{x})$ be bent functions of n variables such that

$$f_1(\mathbf{x})\neq f_0(\mathbf{x}),\qquad f_1(\mathbf{x})\neq 1\oplus f_0(\mathbf{x}). \tag{53}$$

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

$$\begin{aligned} B_{f_0,f_1}(\mathbf{y},\mathbf{x}) &= \left(m_{\sigma(0)}(\mathbf{y})\oplus m_{\sigma(1)}(\mathbf{y})\right)f_0(\mathbf{x}) \\ &\quad\oplus m_{\sigma(2)}(\mathbf{y})f_1(\mathbf{x})\oplus m_{\sigma(3)}(\mathbf{y})\left(1\oplus f_1(\mathbf{x})\right) \end{aligned} \tag{54}$$

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

In addition, we also establish [22, Theorem 3] that the number of different bent functions of $n+2$ variables we can construct using the previous theorem is

$$6\nu_n^2 - 8\nu_n, \tag{55}$$

that is, $4\nu_n$ from Theorem 17(1) and $6\nu_n^2 - 12\nu_n$ from Theorem 17(2).

According to expression (10) it is evident that Corollary 6 and Theorem 17(1) provide the same bent functions. It is also evident that the bent functions constructed by Corollary 7 can be obtained by Theorem 17(2) if we take

$$\begin{aligned} &\left(f_0(\mathbf{x}), f_1(\mathbf{x})\right) = \left(f(\mathbf{x}\oplus\mathbf{u}), f(\mathbf{x})\right) \text{ or} \\ &\left(f_0(\mathbf{x}), f_1(\mathbf{x})\right) = \left(f(\mathbf{x}\oplus\mathbf{u}), 1\oplus f(\mathbf{x})\right). \end{aligned} \tag{56}$$

In fact, for $n = 2$, both constructions provide the same bent functions of $n+2 = 4$ variables. The following result establishes that this is the only case when both constructions provide the same bent functions.

Theorem 18. *Let $f_0(\mathbf{x})$, $f_1(\mathbf{x})$, and $f(\mathbf{x})$ be bent functions of n variables and consider $\mathbf{u} \in \mathbb{Z}_2^n \setminus \{\mathbf{0}\}$. If*

$$\begin{aligned} &\left(f_0(\mathbf{x}), f_1(\mathbf{x})\right) \neq \left(f(\mathbf{x}\oplus\mathbf{u}), f(\mathbf{x})\right), \\ &\left(f_0(\mathbf{x}), f_1(\mathbf{x})\right) \neq \left(f(\mathbf{x}\oplus\mathbf{u}), 1\oplus f(\mathbf{x})\right), \end{aligned} \tag{57}$$

then $B_{f_0,f_1}(\mathbf{y},\mathbf{x}) \neq G_{f,\mathbf{u}}(\mathbf{y},\mathbf{x})$.

Proof. If $\boldsymbol{\eta}_0$, $\boldsymbol{\eta}_1$, $\boldsymbol{\xi}$, and $\boldsymbol{\xi}_{\mathbf{u}}$ are the truth tables of the functions $f_0(\mathbf{x})$, $f_1(\mathbf{x})$, $f(\mathbf{x})$, and $f(\mathbf{x}\oplus\mathbf{u})$, respectively, then, according to Theorem 17(2) and Corollary 7, the truth tables of the functions $B_{f_0,f_1}(\mathbf{y},\mathbf{x})$ and $G_{f,\mathbf{u}}(\mathbf{y},\mathbf{x})$ have four blocks (not necessarily in that order and not the same order for all):

$$\begin{array}{lcccc} B_{f_0,f_1}: & \boldsymbol{\eta}_0 & \boldsymbol{\eta}_0 & \boldsymbol{\eta}_1 & \mathbf{1}\oplus\boldsymbol{\eta}_1 \\ G_{f,\mathbf{u}}: & \boldsymbol{\xi} & \boldsymbol{\xi}_{\mathbf{u}} & \boldsymbol{\xi}_{\mathbf{u}} & \mathbf{1}\oplus\boldsymbol{\xi}. \end{array} \tag{58}$$

If $B_{f_0,f_1}(\mathbf{y},\mathbf{x}) = G_{f,\mathbf{u}}(\mathbf{y},\mathbf{x})$, 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 that $\mathbf{u} = \mathbf{0}$, $(f_0(\mathbf{x}), f_1(\mathbf{x})) = (f(\mathbf{x}\oplus\mathbf{u}), f(\mathbf{x}))$, $(f_0(\mathbf{x}), f_1(\mathbf{x})) = (f(\mathbf{x}\oplus\mathbf{u}), 1\oplus f(\mathbf{x}))$, $f(\mathbf{x}\oplus\mathbf{u}) = 1\oplus f(\mathbf{x})$, or $f(\mathbf{x}) = 1\oplus f(\mathbf{x})$. So, in all cases, we obtain a contradiction and, therefore, $B_{f_0,f_1}(\mathbf{y},\mathbf{x}) \neq G_{f,\mathbf{u}}(\mathbf{y},\mathbf{x})$. □

Although, for $n = 2$, both constructions provide the same bent functions of $n+2 = 4$ variables, for $n \geq 4$, Theorems 18 and 14 ensure that Theorem 17(2) provides (see expression (47) and the comment explaining expression (55))

$$6\nu_n\left(\nu_n - 2^{n+1}\right), \tag{59}$$

bent functions of $n+2$ variables which cannot be obtained by Corollary 7.

Now, the following result, whose proof is similar to the previous one, establishes that none of the bent functions obtained by Corollary 8 can be obtained by Theorem 17(2) and vice versa.

Theorem 19. *Let $f_0(\mathbf{x})$, $f_1(\mathbf{x})$, and $f(\mathbf{x})$ be bent functions of n variables and assume that $\{\mathbf{u},\mathbf{v}\}$ is a Gauss-Jordan basis of cardinality 2 of $\mathbb{Z}_2^n$; then $B_{f_0,f_1}(\mathbf{y},\mathbf{x}) \neq H_{f,\mathbf{u},\mathbf{v}}(\mathbf{y},\mathbf{x})$.*

So, Theorem 19 and expressions (48) and (49) ensure that the number of different bent functions of $n+2$ variables constructed by Corollary 8, which cannot be obtained by Theorem 17(2), is

$$\left(2^{n+2}\left(2^n - 3\right) + 8\right)\nu_n. \tag{60}$$

Finally, adding expressions (55) and (60), we have the following result which establishes the number of different bent functions we can construct using Theorems 5 and 17.

Theorem 20. *If ν_n is the number of bent functions of n variables, then using Theorems 5 and 17 we can construct*

$$6\nu_n^2 + 2^{n+2}\left(2^n - 3\right)\nu_n, \tag{61}$$

different bent functions of $n+2$ variables.

Table 1 summarizes the number of bent functions we can construct using Theorems 5 and 17 compared with the number of bent functions of the classes of Rothaus and Maiorana-McFarland and the iterative construction. The number of Rothaus functions for more than 6 variables is unknown. Also, the number of bent functions of more than 10 variables is unknown. Note that for 4 variables the number of bent functions provided by Theorem 5 or by Theorem 17 (see comments after Theorem 18) is the same as the number of bent functions provided by Rothaus construction; nevertheless, both constructions provide different bent functions as we can see in Example 16. Using the iterative construction of Canteaut and Charpin [43], Tokareva [34] obtain the same number of bent functions for 4 variables and more functions for a greater number of variables, but for 8 and 10 variables, she only provides a lower bound on the number of bent functions that can be obtained. Finally, an exhaustive computer search shows that the 512 bent functions of 4 variables obtained by iterative construction and Theorem 17 are the same.

6. Some Remarks

Note that the bent functions obtained by Theorem 5 can be obtained from some affine transformations of the bent function

$$A_f(\mathbf{y},\mathbf{x}) = f(\mathbf{x}) \oplus m_3(\mathbf{y}), \tag{62}$$

obtained in Theorem 17(1).

For example, for $\mathbf{u},\mathbf{v} \in \mathbb{F}_2^n$, consider the $(n+2)\times(n+2)$ matrix,

$$M = \left[\begin{array}{cc|c} 1 & 0 & \mathbf{v} \\ 0 & 1 & \mathbf{u} \\ \hline \mathbf{0}^T & \mathbf{0}^T & I_n \end{array}\right], \tag{63}$$

Table 1: Number of bent functions constructed with different methods.

Variables	4	6	8	10
Bent	896	5 425 430 528	99 270 589 265 934 370 305 785 861 242 880 $\approx 2^{106}$	?
Rothaus	512	?	?	?
Maiorana-McFarland	384	10 321 920	1 371 195 958 099 968 000 $\approx 2^{60}$	2^{150}
Iterative construction	512	333 961 408	$2^{87.35}$	$2^{262.16}$
Theorem 17	320	4 809 728	176 611 778 441 522 708 480 $\approx 2^{68}$	2^{214}
Theorem 5	512	752 640	84 766 926 569 472 $\approx 2^{47}$	2^{128}
Theorems 5 and 17	512	5 562 368	176 611 863 208 449 277 952 $\approx 2^{68}$	2^{214}

where I_n is the $n \times n$ identity matrix. It is not difficult to see that the bent function

$$A_f\left(\left(\mathbf{y}, \mathbf{x}\right) M\right) = f\left(y_1 \mathbf{v} \oplus y_2 \mathbf{u} \oplus \mathbf{x}\right) \oplus y_1 y_2 \tag{64}$$

has the same truth table as the bent function

$$\begin{aligned} B\left(\mathbf{y}, \mathbf{x}\right) = {} & m_0\left(\mathbf{y}\right) f\left(\mathbf{x}\right) \oplus m_1\left(\mathbf{y}\right) f\left(\mathbf{x} \oplus \mathbf{u}\right) \oplus m_2\left(\mathbf{y}\right) f\left(\mathbf{x} \oplus \mathbf{v}\right) \\ & \oplus m_3\left(\mathbf{y}\right)\left(1 \oplus f\left(\mathbf{x} \oplus \mathbf{u} \oplus \mathbf{v}\right)\right), \end{aligned} \tag{65}$$

and, therefore, both expressions define the same bent function. Analogously, for the $(n+2) \times (n+2)$ matrix

$$N = \left[\begin{array}{cc|c} 1 & 0 & \mathbf{u} \oplus \mathbf{v} \\ 0 & 1 & \mathbf{u} \\ \hline \mathbf{0}^T & \mathbf{0}^T & I_n \end{array}\right], \tag{66}$$

the bent function

$$\begin{aligned} & A_f\left(\left(\mathbf{y}, \mathbf{x}\right) N \oplus \left(\mathbf{0}_2, \mathbf{u}\right)\right) \\ & \quad = f\left(y_1\left(\mathbf{u} \oplus \mathbf{v}\right) \oplus \left(y_2 \oplus 1\right) \mathbf{u} \oplus \mathbf{x}\right) \oplus y_1 y_2 \end{aligned} \tag{67}$$

has the same truth table as the bent function

$$\begin{aligned} B\left(\mathbf{y}, \mathbf{x}\right) = {} & m_1\left(\mathbf{y}\right) f\left(\mathbf{x}\right) \oplus m_0\left(\mathbf{y}\right) f\left(\mathbf{x} \oplus \mathbf{u}\right) \oplus m_2\left(\mathbf{y}\right) f\left(\mathbf{x} \oplus \mathbf{v}\right) \\ & \oplus m_3\left(\mathbf{y}\right)\left(1 \oplus f\left(\mathbf{x} \oplus \mathbf{u} \oplus \mathbf{v}\right)\right), \end{aligned} \tag{68}$$

and, therefore, both expressions define the same bent function.

We use the construction of Theorem 5 instead of the affine transformations because of the following.

(i) As we explained in Example 2, not all the bent functions that are affine equivalent to a given function are different. This fact makes the computation of the number of functions we can construct a difficult task.

(ii) The simplicity of the operations with minterms makes the computation of the support of the new bent functions evident.

(iii) Finally, in Example 11, using two different bent functions of n variables and two different pairs of vectors, we have obtained the same bent function of $n+2$ variables faster and in a clearer fashion. However, to achieve the same result using the affine equivalence, we need a greater number of algebraic manipulations and, besides, it is far from evident the choice of the appropriate pair of vectors to prevent the equality of the obtained functions.

The following example emphasizes the latter two items.

Example 21. For the functions $f(\mathbf{x})$ and $g(\mathbf{x})$ of Example 11, using the first and the second affine transformations introduced at the beginning of this section, we have, after some algebraic manipulations, the following functions:

$$\begin{aligned} H_{f,\mathbf{1},\mathbf{2}}\left(\mathbf{y}, \mathbf{x}\right) &= f\left(y_1 \mathbf{2} \oplus y_2 \mathbf{1} \oplus \mathbf{x}\right) \oplus m_3\left(\mathbf{y}\right) \\ &= m_0\left(y_1 \oplus x_1, y_2 \oplus x_2\right) \oplus y_1 y_2, \\ H_{g,\mathbf{1},\mathbf{3}}\left(\mathbf{y}, \mathbf{x}\right) &= g\left(y_1\left(\mathbf{1} \oplus \mathbf{3}\right) \oplus \left(y_2 \oplus 1\right) \mathbf{1} \oplus \mathbf{x}\right) \oplus m_3\left(\mathbf{y}\right) \\ &= m_1\left(y_1 \oplus x_1, 1 \oplus y_2 \oplus x_2\right) \oplus y_1 y_2. \end{aligned} \tag{69}$$

As we know, both functions are the same, but, in this way, it is our contention that the support of those functions is not obtainable straightforwardly. Nevertheless, from Example 11, the support of the above functions is the set $\{\mathbf{0}, \mathbf{5}, \mathbf{10}, \mathbf{12}, \mathbf{13}, \mathbf{14}\}$.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The work of the first author was partially supported by Spanish Grant MTM2011-24858 of the Ministerio de Economía y Competitividad of the Gobierno de España.

References

[1] A. Braeken, V. Nikov, S. Nikova, and B. Preneel, "On Boolean functions with generalized cryptographic properties," in *Progress in Cryptology—INDOCRYPT 2004*, A. Canteaut and K. Viswanathan, Eds., vol. 3348 of *Lecture Notes in Computer Science*, pp. 120–135, Springer, Berlin, Germany, 2004.

[2] C. Carlet and Y. Tarannikov, "Covering sequences of Boolean functions and their cryptographic significance," *Designs, Codes and Cryptography*, vol. 25, no. 3, pp. 263–279, 2002.

[3] K. Kurosawa and R. Matsumoto, "Almost security of cryptographic boolean functions," *IEEE Transactions on Information Theory*, vol. 50, no. 11, pp. 2752–2761, 2004.

[4] Y. Borissov, A. Braeken, S. Nikova, and B. Preneel, "On the covering radii of binary Reed-Muller codes in the set of resilient boolean functions," *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 1182–1189, 2005.

[5] K. Kurosawa, T. Iwata, and T. Yoshiwara, "New covering radius of Reed-Muller codes for t-resilient functions," *IEEE Transactions on Information Theory*, vol. 50, no. 3, pp. 468–475, 2004.

[6] C. M. Adams, "Constructing symmetric ciphers using the CAST design procedure," *Designs, Codes, and Cryptography*, vol. 12, no. 3, pp. 283–316, 1997.

[7] K. C. Gupta and P. Sarkar, "Improved construction of nonlinear resilient S-boxes," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 339–348, 2005.

[8] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT '93*, T. Helleseth, Ed., vol. 765 of *Lecture Notes in Computer Science*, pp. 386–397, Springer, Berlin, Germany, 1994.

[9] K. Nyberg, "Perfect nonlinear S-boxes," in *Advances in Cryptology—EUROCRYPT '91*, D. W. Davies, Ed., vol. 547 of *Lecture Notes in Computer Science*, pp. 378–386, Springer, Berlin, Germany, 1991.

[10] P. Sarkar and S. Maitra, "Construction of nonlinear Boolean functions with important cryptographic properties," in *Advances in Cryptology—EUROCRYPT 2000*, B. Preneel, Ed., vol. 1807 of *Lecture Notes in Computer Science*, pp. 485–506, Springer, Berlin, Germany, 2000.

[11] J. Seberry, X.-M. Zhang, and Y. L. Zheng, "Nonlinearity and propagation characteristics of balanced Boolean functions," *Information and Computation*, vol. 119, no. 1, pp. 1–13, 1995.

[12] W. Millan, "How to improve the nonlinearity of bijective S-boxes," in *Information Security and Privacy*, C. Boyd and E. Dawson, Eds., vol. 1438 of *Lecture Notes in Computer Science*, pp. 181–192, Springer, Berlin, Germany, 1998.

[13] W. Millan, L. Burnet, G. Carter, A. Clark, and E. Dawson, "Evolutionary heuristics for finding cryptographically strong S-boxes," in *Information and Communication Security*, V. Varadharajan and Y. Mu, Eds., vol. 1726 of *Lecture Notes in Computer Science*, pp. 263–274, Springer, Berlin, Germany, 1999.

[14] J. Detombe and S. Tavares, "Constructing large cryptographically strong S-boxes," in *Advances in Cryptology—AUSCRYPT '92*, J. Seberry and Y. Zheng, Eds., vol. 718 of *Lecture Notes in Computer Science*, pp. 165–181, Springer, Berlin, Germany, 1993.

[15] C. Carlet, "Two new classes of bent functions," in *Advances in Cryptology—EUROCRYPT '93*, T. Helleseth, Ed., vol. 765 of *Lecture Notes in Computer Science*, pp. 77–101, Springer, Berlin, Germany, 1994.

[16] C. Carlet, "On the secondary constructions of resilient and bent functions," in *Coding, Cryptography and Combinatorics*, vol. 23 of *Progress in Computer Science and Applied Logic*, pp. 3–28, Birkhäuser, Basel, Switzerland, 2004.

[17] C. Carlet, "On bent and highly nonlinear balanced/resilient functions and their algebraic immunities," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, M. Fossorier, H. Imai, S. Lin, and A. Poli, Eds., vol. 3857 of *Lecture Notes in Computer Science*, pp. 1–28, Springer, Berlin, Germany, 2006.

[18] C. Carlet, "Boolean functions for cryptography and error-correcting codes," in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer, Eds., chapter 8, pp. 257–397, Cambridge University Press, New York, NY, USA, 2010.

[19] C. Carlet and P. Guillot, "A characterization of binary bent functions," *Journal of Combinatorial Theory A*, vol. 76, no. 2, pp. 328–335, 1996.

[20] C. Carlet and J. L. Yucas, "Piecewise constructions of bent and almost optimal boolean functions," *Designs, Codes, and Cryptography*, vol. 37, no. 3, pp. 449–464, 2005.

[21] D. K. Chang, "Binary bent sequences of order 64," *Utilitas Mathematica*, vol. 52, pp. 141–151, 1997.

[22] J.-J. Climent, F. J. Garćia, and V. Requena, "On the construction of bent functions of $n + 2$ variables from bent functions of n variables," *Advances in Mathematics of Communications*, vol. 2, no. 4, pp. 421–431, 2008.

[23] T. W. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications*, Academic Press, San Diego, Calif, USA, 2009.

[24] J. F. Dillon, *Elementary hadamard difference sets [Ph.D. thesis]*, University of Maryland, College Park, Md, USA, 1974.

[25] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," in *Fast Sofware Encription*, B. Preneel, Ed., vol. 1008 of *Lecture Notes in Computer Science*, pp. 61–74, Springer, Berlin, Germany, 1995.

[26] H. Dobbertin and G. Leander, "Cryptographer's toolkit for construction of 8-bit bent functions," Cryptology ePrint Archive 2005/089, 2005, http://eprint.iacr.org/.

[27] J. Fuller, E. Dawson, and W. Millan, "Evolutionary generation of bent functions for cryptography," in *Proceedings of the IEEE Congress on Evolutionary Computation*, vol. 2, pp. 1655–1661, December 2003.

[28] X.-D. Hou and P. Langevin, "Results on bent functions," *Journal of Combinatorial Theory A*, vol. 80, no. 2, pp. 232–246, 1997.

[29] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," *Journal of Combinatorial Theory A*, vol. 40, no. 1, pp. 90–107, 1985.

[30] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Advances in Cryptology—EUROCRYPT '89*, J. J. Quisquater and J. Vandewalle, Eds., vol. 434 of *Lecture Notes in Computer Science*, pp. 549–562, Springer, Berlin, Germany, 1990.

[31] Q. Meng, H. Zhang, J. Cui, and M. Yang, "Almost enumeration of eight-variable bent functions," Cryptology ePrint Archive 2005/100, 2005, http://eprint.iacr.org/.

[32] B. Preneel, *Analysis and design of cryptographic hash functions [Ph.D. thesis]*, Katholieke Universiteit Leuven, Leuven, Belgium, 1993.

[33] J. Seberry and X. M. Zhang, "Constructions of bent functions from two known bent functions," *The Australasian Journal of Combinatorics*, vol. 9, pp. 21–35, 1994.

[34] N. Tokareva, "On the number of bent functions from iterative constructions: lower bounds and hypothesis," *Advances in Mathematics of Communications*, vol. 5, no. 4, pp. 609–621, 2011.

[35] N. Y. Yu and G. Gong, "Constructions of quadratic bent functions in polynomial forms," *IEEE Transactions on Information Theory*, vol. 52, no. 7, pp. 3291–3299, 2006.

[36] R. L. McFarland, "A family of difference sets in noncyclic groups," *Journal of Combinatorial Theory A*, vol. 15, no. 1, pp. 1–10, 1973.

[37] O. S. Rothaus, "On "bent" functions," *Journal of Combinatorial Theory A*, vol. 20, no. 3, pp. 300–305, 1976.

[38] R. Yarlagadda and J. E. Hershey, "Analysis and synthesis of bent sequences," *IEE Proceedings E: Computers and Digital Techniques*, vol. 136, no. 2, pp. 112–123, 1989.

[39] C. Charnes, M. Rötteler, and T. Beth, "On homogeneous bent functions," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, S. Boztaş and I. E. Shparlinski, Eds., vol. 2227 of *Lecture Notes in Computer Science*, pp. 249–259, Springer, Berlin, Germany, 2001.

[40] C. Charnes, M. Rötteler, and T. Beth, "Homogeneous bent functions, invariants, and designs," *Designs, Codes and Cryptography*, vol. 26, no. 1–3, pp. 139–154, 2002.

[41] C. Qu, J. Seberry, and J. Pieprzyk, "On the symmetric property of homogeneous Boolean functions," in *Information Security and Privacy*, J. Pieprzyk, R. Safavi-Naini, and J. Seberry, Eds., vol. 1587 of *Lecture Notes in Computer Science*, pp. 26–35, Springer, Berlin, Germany, 1999.

[42] P. Langevin, "On generalized bent functions," in *Eurocode '92*, vol. 339 of *CISM Courses and Lectures*, pp. 147–157, Springer, New York, NY, USA, 1992.

[43] A. Canteaut and P. Charpin, "Decomposing bent functions," *IEEE Transactions on Information Theory*, vol. 49, no. 8, pp. 2004–2019, 2003.

[44] P. Langevin and G. Leander, "Counting all bent functions in dimension eight," in *Proceedings of the International Workshop on Coding and Cryptography*, Ullensvang, Norway, May 2009.

[45] G. D. Cohen, M. G. Karpovsky, H. F. Mattson Jr., and J. R. Schatz, "Covering radius—survey and recent results," *IEEE Transactions on Information Theory*, vol. 31, no. 3, pp. 328–343, 1985.

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

[47] A. Braeken, Y. Borissov, S. Nikova, and B. Preneel, "Classication of Boolean functions of 6 variables or less with respect to some cryptographic properties," in *Automata, Languages and Programming*, L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, Eds., vol. 3580 of *Lecture Notes in Computer Science*, pp. 324–334, Springer, Berlin, Germany, 2005.

[48] A. Canteaut, M. Daum, H. Dobbertin, and G. Leander, "Finding nonnormal bent functions," *Discrete Applied Mathematics*, vol. 154, no. 2, pp. 202–218, 2006.

[49] M. Daum, H. Dobbertin, and G. Leander, "An algorithm for checking normality of Boolean functions," in *Proceedings of the International Workshop on Coding and Cryptography (WCC '03)*, pp. 133–142, March 2003.

[50] S. A. Vanstone and P. C. van Oorschot, *An Introduction to Error Correcting Codes with Applications*, Kluwer Academic, Boston, Mass, USA, 1989.