Construction of Bent Functions of $2k$ Variables from a Basis of $\mathbb{F}_2^{2k*}$

Joan-Josep Climent¹ Francisco J. García²
Verónica Requena¹

¹ Departament d'Estadística i Investigació Operativa, Universitat d'Alacant

² Departament de Fonaments de l'Anàlisi Econòmica, Universitat d'Alacant

February 21, 2012

Abstract

Starting with a basis of $\mathbb{F}_2^{2k}$, we define some sets in $\mathbb{F}_2^{2k}$ that are the supports of bent functions of $2k$ variables. We also establish some results in order to count the number of bent functions we can construct, and we provide a complete classification of all bases of $\mathbb{F}_2^{2k}$ (for $k = 2$) providing the same supports of bent functions.

Keywords: Boolean function, bent function, support of a Boolean function, Gauss-Jordan basis, cryptography.

1 Introduction

A Boolean function maps a number of input bits into a single bit. Boolean functions are widely used in different types of cryptographic applications such as block ciphers, stream ciphers and hash functions [3, 5, 21], in coding theory [2, 15], among others. A cryptographic function should have high nonlinearity in order to prevent attacks based on linear approximation [1, 13, 19, 22]. The functions achieving the maximal possible nonlinearity possess the best resistance to the linear attack and they are called bent functions [27, 29]. Bent functions have been the subject of some interest in coding theory [17, 18], in logic synthesis [31] and in cryptography [21].

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

*This work was partially supported by Spanish grants MTM2008-06674-C02-01 and MTM2011-24858 of the Ministerio de Ciencia e Innovación of the Gobierno de España and ACOMP/2010/039 and ACOMP/2011/005 of the Generalitat Valenciana.

896 bent functions, for $n = 6$, Preneel [25] and Chang [8] proved that the number of bent functions is 5 425 430 528, and for $n = 8$, Langevin and Leander [16] 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 [20] on sets of finite differences in finite non-cyclic groups. One year after, Dillon [11] systematized and extended the ideas of McFarland, proving a great quantity of properties. The name *bent* for these functions is due to Rothaus [26]. There are different ways to obtain bent functions, most of them are based on the algebraic normal form of a Boolean function, see, for example, [7, 6, 8, 11, 12, 14, 20, 22, 26, 29, 32]. However, there are very few constructions of bent functions based on the support (or equivalently, on the truth table) of Boolean functions; for example the partial spread class of bent functions introduced by Dillon [11].

The use of the algebraic normal form or the truth table, both have 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 state that $f(\mathbf{x})$ is not a bent function (see [26]); nevertheless, we do not know the cardinality of its support (that is, its weight). On the other hand, if we know the truth table of $f(\mathbf{x})$, we know if its support has the necessary number of elements to be a bent function, although we do not know its degree. To see the relation between the algebraic normal form of a Boolean function and its support see, for example, [9].

The rest of the paper is organized as follows. Firstly, in Section 2 we introduce some basic definitions and notations that are used hereafter. In Section 3, starting with a bases of $\mathbb{F}_2^{2k}$ we introduce some sets of $\mathbb{F}_2^{2k}$ with the property that they are the supports of bent functions of $2k$ variables. In Section 4 we introduce some results in order to count how many bent functions we can construct using the method introduce in Section 3 and finally, in Section 5 we present some conclusions and open problems.

2 Preliminary results

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 of dimension n over $\mathbb{F}_2$ with the usual addition (denoted also by $\oplus$). If for $i = 0, 1, 2, \dots, 2^n - 1$, we denote by $\mathbf{i}$ the binary expansion of i of n digits, then $\mathbb{F}_2^n = \{\mathbf{i} \mid 0 \leq i \leq 2^n - 1\}$. Furthermore, we denote by $\text{Span}\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_l\}$ the linear subspace of $\mathbb{F}_2^n$ generated by the vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_l \in \mathbb{F}_2^n$. We say that the set $\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_l\}$ is a **Gauss-Jordan basis of cardinality l** if the matrix whose rows are $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_l$ is in reduced row echelon form (see also [4, 10]). Moreover, if $S \subseteq \mathbb{F}_2^n$

and $\mathbf{a} \oplus S = \{\mathbf{a} \oplus \mathbf{u} \mid \mathbf{u} \in S\}$ for $\mathbf{a} \in \mathbb{F}_2^n$, then it is evident that

$$|\mathbf{a} \oplus S| = |S|,$$

where $|S|$ denotes the number of elements of S . We will use this property without mentioning it explicitly.

A **Boolean function** of n variables is a map $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$. The set of all Boolean functions of n variables is denoted by $\mathcal{B}_n$; it is well known that $\mathcal{B}_n$, with the usual addition of functions (that we also denote by $\oplus$), is a linear space of dimension 2^n over $\mathbb{F}_2$. The complementary function of $f \in \mathcal{B}_n$ is the Boolean function $1 \oplus f$.

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

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

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

$$\text{Supp}(f) = \{\mathbf{a} \in \mathbb{F}_2^n \mid f(\mathbf{a}) = 1\}.$$

Furthermore, we call **weight** of f , denoted by $w(f)$, the number of 1s of the truth table of f and therefore, $w(f) = |\text{Supp}(f)|$.

If $f, g \in \mathcal{B}_n$, it can be checked that $\text{Supp}(f \oplus g) = \text{Supp}(f) \Delta \text{Supp}(g)$ where Δ denotes the symmetric difference of sets. As a consequence $\text{Supp}(1 \oplus f) = \mathbb{F}_2^n \setminus \text{Supp}(f)$ and so $w(1 \oplus f) = 2^n - w(f)$.

Furthermore, if $f \in \mathcal{B}_n$ and $\mathbf{a} \in \mathbb{F}_2^n$, then $\text{Supp}(g_{\mathbf{a}}) = \mathbf{a} \oplus \text{Supp}(f)$ where $g_{\mathbf{a}} \in \mathcal{B}_n$ is the Boolean function of n variables given by $g_{\mathbf{a}}(\mathbf{x}) = f(\mathbf{a} \oplus \mathbf{x})$ for all $\mathbf{x} \in \mathbb{F}_2^n$.

We said that f is **balanced** if $w(f) = 2^{n-1}$. It is evident that f is balanced if and only if $1 \oplus f$ is balanced.

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

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

where $\mathbf{a} \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$ and $\langle \mathbf{a}, \mathbf{x} \rangle$ denotes the dot product of $\mathbf{a}$ and $\mathbf{x}$. If $b = 0$, f is called a **linear function**. Affine functions are balanced, but not all balanced functions are affine.

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

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

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, for example, [21, 29]) by

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

The Boolean functions that achieve the maximum nonlinearity are called **bent functions** (see, for example, [21, 29]). As a consequence, bent functions of n variables only exist for n even.

The following result gives us a characterization of a bent function.

Theorem 1 ([28, 29]): *Let $f(\mathbf{x})$ be a Boolean function of n variables with n even. The following statements are equivalent.*

- (a) $f(\mathbf{x})$ is a bent function.
- (b) The Boolean function $f(\mathbf{x}) \oplus f(\mathbf{a} \oplus \mathbf{x})$ is balanced for all $\mathbf{a} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$.
- (c) The number of 1s in the truth table of the Boolean function $f(\mathbf{x}) \oplus \langle \mathbf{a}, \mathbf{x} \rangle$ is $2^{n-1} \pm 2^{\frac{n}{2}-1}$ for all $\mathbf{a} \in \mathbb{F}_2^n$.

As a consequence of the previous result we have the following characterization of the support of a bent function that we will use in the rest of the paper.

Corollary 1: *Assume that $S \subseteq \mathbb{F}_2^n$ with n even. Then S is the support of a bent function of n variables if and only if $S \Delta(\mathbf{a} \oplus S)$ is the support of a balanced function of n variables for all $\mathbf{a} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$.*

PROOF: Let $f \in \mathcal{B}_n$. If $S = \text{Supp}(f)$, then the result follows by Theorem 1 and from the fact that $S \Delta(\mathbf{a} \oplus S)$ is the support of the Boolean function $f(\mathbf{x}) \oplus f(\mathbf{a} \oplus \mathbf{x})$. $\square$

Another consequence of Theorem 1 is that if $f \in \mathcal{B}_n$ is a bent function, then $w(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$. Also, $1 \oplus f \in \mathcal{B}_n$ is a bent function and $w(1 \oplus f) = 2^{n-1} \mp 2^{\frac{n}{2}-1}$.

3 Main results

In this section we introduce an iterative process in order to provide the supports of some bent functions of n variables from a basis of $\mathbb{F}_2^n$. From now on, we assume that $n = 2k$ and that $\mathcal{U} = \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_{2k-1}, \mathbf{u}_{2k}\}$ is a basis of $\mathbb{F}_2^n$. For $i = 1, 2, \dots, k$, consider the linear subspaces of $\mathbb{F}_2^n$ given by

$$G_i = \text{Span}\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_{2i-1}, \mathbf{u}_{2i}\} \quad \text{and} \quad H_i = \text{Span}\{\mathbf{u}_{2i-1}, \mathbf{u}_{2i}\}.$$

Clearly, $\dim G_i = 2i$ and $\dim H_i = 2$. Furthermore, if we consider $G_0 = \{\mathbf{0}\}$, then

$$G_i = G_{i-1} \oplus H_i \quad \text{and} \quad G_{i-1} \cap H_i = \{\mathbf{0}\}, \tag{1}$$

and therefore, G_i is the direct sum of G_{i-1} and H_i . In particular, $G_1 = H_1$.

For convenience in the notation, we refer the elements of H_i , for $i = 1, 2, \dots, k$, as

$$\mathbf{a}_0^{(i)} = \mathbf{0}, \quad \mathbf{a}_1^{(i)} = \mathbf{u}_{2i-1}, \quad \mathbf{a}_2^{(i)} = \mathbf{u}_{2i} \quad \text{and} \quad \mathbf{a}_3^{(i)} = \mathbf{u}_{2i-1} \oplus \mathbf{u}_{2i}.$$

Using the sets G_{i-1} and the elements of H_i , for $i = 1, 2, \dots, k$, we define a series of subsets of G_i with some properties in a way that at the end of the process, the obtained subsets of G_k are the supports of bent functions of $2k$ variables.

For $p \in \{0, 1, 2, 3\}$ consider the sets

$$B(p) = \{\mathbf{a}_p^{(1)}\} \quad \text{and} \quad \widehat{B}(p) = \bigcup_{\substack{q=0 \\ q \neq p}}^3 \{\mathbf{a}_q^{(1)}\}.$$

It is evident that

$$G_1 = B(p) \cup \widehat{B}(p) \quad \text{and} \quad B(p) \cap \widehat{B}(p) = \emptyset. \quad (2)$$

Furthermore, if $r, s \in \{0, 1, 2, 3\}$ with $r \neq s$, then $B(r) \neq B(s)$.

Now, let $(p_1, p_2, \dots, p_{i-1}, p_i) \in \{0, 1, 2, 3\}^i$ and assume that we have defined the sets $B(p_1, p_2, \dots, p_{i-1})$ and $\widehat{B}(p_1, p_2, \dots, p_{i-1})$. Then, we define

$$\begin{aligned} & B(p_1, p_2, \dots, p_{i-1}, p_i) \\ &= \left(\mathbf{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^3 \left(\mathbf{a}_q^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right), \end{aligned} \quad (3)$$

$$\begin{aligned} & \widehat{B}(p_1, p_2, \dots, p_{i-1}, p_i) \\ &= \left(\mathbf{a}_{p_i}^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^3 \left(\mathbf{a}_q^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right). \end{aligned} \quad (4)$$

Our goal is to prove that for all $(p_1, p_2, \dots, p_k) \in \{0, 1, 2, 3\}^k$, the sets

$$B(p_1, p_2, \dots, p_k) \quad \text{and} \quad \widehat{B}(p_1, p_2, \dots, p_k)$$

are the supports of two bent functions of $2k$ variables, such that one is the complementary function of the other. However, we need to prove beforehand some technical lemmas which will simplify the proof of the above mentioned result.

The following result establishes that the sets of expressions (3) and (4) are complementary sets in G_i .

Lemma 1: For $i = 1, 2, \dots, k$, and for all $(p_1, p_2, \dots, p_i) \in \{0, 1, 2, 3\}^i$, we have that

$$G_i = B(p_1, p_2, \dots, p_i) \cup \widehat{B}(p_1, p_2, \dots, p_i) \quad \text{and} \quad B(p_1, p_2, \dots, p_i) \cap \widehat{B}(p_1, p_2, \dots, p_i) = \emptyset.$$

PROOF: We proceed by induction over i . For $i = 1$ the result is true by expression (2). Assume that the result is true for $i - 1 < k$, we will prove that it is also true for i .

First, by the induction hypothesis, we have that

$$B(p_1, p_2, \dots, p_{i-1}) \cup \widehat{B}(p_1, p_2, \dots, p_{i-1}) = G_{i-1}$$

and therefore

$$\begin{aligned}
& B(p_1, p_2, \dots, p_{i-1}, p_i) \cup \widehat{B}(p_1, p_2, \dots, p_{i-1}, p_i) \\
&= \left(\mathbf{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^3 \left(\mathbf{a}_q^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right) \\
&\quad \cup \left(\mathbf{a}_{p_i}^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^3 \left(\mathbf{a}_q^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \\
&= \left(\mathbf{a}_{p_i}^{(i)} \oplus \left(B(p_1, p_2, \dots, p_{i-1}) \cup \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \right) \\
&\quad \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^3 \left(\mathbf{a}_q^{(i)} \oplus \left(B(p_1, p_2, \dots, p_{i-1}) \cup \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \right) \\
&= \left(\mathbf{a}_{p_i}^{(i)} \oplus G_{i-1} \right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^3 \left(\mathbf{a}_q^{(i)} \oplus G_{i-1} \right) = \left\{ \mathbf{a}_0^{(i)}, \mathbf{a}_1^{(i)}, \mathbf{a}_2^{(i)}, \mathbf{a}_3^{(i)} \right\} \oplus G_{i-1} = G_i
\end{aligned}$$

where the last equality follows from the first equality in expression (1).

Analogously, after some algebraic manipulations, we have that

$$\begin{aligned}
& B(p_1, p_2, \dots, p_{i-1}, p_i) \cap \widehat{B}(p_1, p_2, \dots, p_{i-1}, p_i) \\
&= \left(\left(\mathbf{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^3 \left(\mathbf{a}_q^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right) \right) \\
&\quad \cap \left(\left(\mathbf{a}_{p_i}^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^3 \left(\mathbf{a}_q^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \right) \\
&= \bigcup_{r=0}^3 \left(\left(\mathbf{a}_r^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right) \cap \left(\mathbf{a}_r^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \right) \tag{5a}
\end{aligned}$$

$$\cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^3 \left(\left(\mathbf{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \cap \left(\mathbf{a}_q^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \right) \tag{5b}$$

$$\cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^3 \left(\left(\mathbf{a}_{p_i}^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right) \cap \left(\mathbf{a}_q^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right) \right) \tag{5c}$$

$$\cup \bigcup_{\substack{q,r=0 \\ q,r \neq p_i \\ q \neq r}}^3 \left(\left(\mathbf{a}_q^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right) \cap \left(\mathbf{a}_r^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \right) \tag{5d}$$

In order to obtain that $B(p_1, p_2, \dots, p_{i-1}, p_i) \cap \widehat{B}(p_1, p_2, \dots, p_{i-1}, p_i) = \emptyset$, it is therefore

sufficient to prove that all the intersections that appear in expressions (5a), (5b), (5c) and (5d) are empty.

By the induction hypothesis we have that

$$\begin{aligned} (\mathbf{a}_r^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1})) \cap (\mathbf{a}_r^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1})) \\ = \mathbf{a}_r^{(i)} \oplus (B(p_1, p_2, \dots, p_{i-1}) \cap \widehat{B}(p_1, p_2, \dots, p_{i-1})) = \emptyset, \end{aligned}$$

therefore, all the intersections in expression (5a) are empty.

Assume now that $q \in \{0, 1, 2, 3\} \setminus \{p_i\}$. If

$$\mathbf{x} \in (\mathbf{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1})) \cap (\mathbf{a}_q^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1})),$$

then

$$\mathbf{x} = \mathbf{a}_{p_i}^{(i)} \oplus \mathbf{u} = \mathbf{a}_q^{(i)} \oplus \mathbf{v}$$

for some $\mathbf{u}, \mathbf{v} \in \widehat{B}(p_1, p_2, \dots, p_{i-1}) \subseteq G_{i-1}$. But then, taking into account that G_{i-1} and H_i are linear subspaces, we have that

$$\mathbf{u} \oplus \mathbf{v} = \mathbf{a}_{p_i}^{(i)} \oplus \mathbf{a}_q^{(i)} \in G_{i-1} \cap H_i = \{\mathbf{0}\}$$

by expression (1), and so, $\mathbf{a}_{p_i}^{(i)} = \mathbf{a}_q^{(i)}$ which is a contradiction. Consequently, the intersections that appear in expression (5b) are all empty.

By a similar argument, we obtain that all the intersections in expressions (5c) and (5d) are also empty. $\square$

Next result establishes the number of elements of the sets defined by expressions (3) and (4).

Lemma 2: For $i = 1, 2, \dots, k$, and for all $(p_1, p_2, \dots, p_i) \in \{0, 1, 2, 3\}^i$, we have that

$$|B(p_1, p_2, \dots, p_i)| = 2^{2i-1} - 2^{i-1} \quad \text{and} \quad |\widehat{B}(p_1, p_2, \dots, p_i)| = 2^{2i-1} + 2^{i-1}.$$

PROOF: We proceed by induction over i . For $i = 1$ and for all $p \in \{0, 1, 2, 3\}$, we have that

$$|B(p)| = 1 = 2^{2 \cdot 1 - 1} - 2^{1 - 1} \quad \text{y} \quad |\widehat{B}(p)| = 3 = 2^{2 \cdot 1 - 1} + 2^{1 - 1}.$$

Assume now that the result is true for $i - 1 < k$, we will prove that it is also true for i .

Let $(p_1, p_2, \dots, p_{i-1}, p_i) \in \{0, 1, 2, 3\}^i$. By a similar argument as in the proof of Lemma 1, if $q \in \{0, 1, 2, 3\} \setminus \{p_i\}$, then

$$(\mathbf{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1})) \cap (\mathbf{a}_q^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1})) = \emptyset,$$

and if $q, r \in \{0, 1, 2, 3\} \setminus \{p_i\}$ with $q \neq r$, then

$$(\mathbf{a}_q^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1})) \cap (\mathbf{a}_r^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1})) = \emptyset.$$

Therefore, from expression (3) we have that

$$\begin{aligned}
& |B(p_1, p_2, \dots, p_i)| \\
&= \left| \mathbf{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right| + \sum_{\substack{q=0 \\ q \neq p_i}}^3 \left| \mathbf{a}_q^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right| \\
&= 2^{2(i-1)-1} + 2^{i-1-1} + 3(2^{2(i-1)-1} - 2^{i-1-1}) = 2^{2i-1} - 2^{i-1}.
\end{aligned}$$

Now, since $\widehat{B}(p_1, p_2, \dots, p_i) = G_i \setminus B(p_1, p_2, \dots, p_i)$ we have that

$$|\widehat{B}(p_1, p_2, \dots, p_i)| = 2^{2i} - |B(p_1, p_2, \dots, p_i)| = 2^{2i-1} + 2^{i-1}. \quad \square$$

By a similar argument as in the previous lemmas we can prove the following result.

Lemma 3: For $i = 1, 2, \dots, k$, if $(p_1, p_2, \dots, p_i) \in \{0, 1, 2, 3\}^i$ and $\mathbf{u} \in G_i \setminus \{\mathbf{0}\}$, then:

- (a) $\left| B(p_1, p_2, \dots, p_i) \cap \left(\mathbf{u} \oplus B(p_1, p_2, \dots, p_i) \right) \right| = 2^{2i-2} - 2^{i-1},$
- (b) $\left| \widehat{B}(p_1, p_2, \dots, p_i) \cap \left(\mathbf{u} \oplus \widehat{B}(p_1, p_2, \dots, p_i) \right) \right| = 2^{2i-2} + 2^{i-1},$
- (c) $\left| B(p_1, p_2, \dots, p_i) \cap \left(\mathbf{u} \oplus \widehat{B}(p_1, p_2, \dots, p_i) \right) \right| = 2^{2i-2},$
- (d) $\left| \widehat{B}(p_1, p_2, \dots, p_i) \cap \left(\mathbf{u} \oplus B(p_1, p_2, \dots, p_i) \right) \right| = 2^{2i-2}.$

PROOF: We proceed, as in the previous results, by induction over i . For $i = 1$, we have that $G_1 = \{\mathbf{a}_p^{(1)}, \mathbf{a}_q^{(1)}, \mathbf{a}_r^{(1)}, \mathbf{a}_s^{(1)}\}$ where $\{p, q, r, s\} = \{0, 1, 2, 3\}$, so

$$B(p) = \{\mathbf{a}_p^{(1)}\} \quad \text{and} \quad \widehat{B}(p) = \{\mathbf{a}_q^{(1)}, \mathbf{a}_r^{(1)}, \mathbf{a}_s^{(1)}\}.$$

If $\mathbf{u} \in G_1 \setminus \{\mathbf{0}\}$, we can assume that

$$\mathbf{u} \oplus \mathbf{a}_p^{(1)} = \mathbf{a}_q^{(1)},$$

(the same argument follows if $\mathbf{u} \oplus \mathbf{a}_p^{(1)} = \mathbf{a}_r^{(1)}$ or $\mathbf{u} \oplus \mathbf{a}_p^{(1)} = \mathbf{a}_s^{(1)}$).

So

$$B(p) \cap \left(\mathbf{u} \oplus B(p) \right) = \{\mathbf{a}_p^{(1)}\} \cap \{\mathbf{u} \oplus \mathbf{a}_p^{(1)}\} = \{\mathbf{a}_p^{(1)}\} \cap \{\mathbf{a}_q^{(1)}\} = \emptyset,$$

and therefore

$$\left| B(p) \cap \left(\mathbf{u} \oplus B(p) \right) \right| = 0 = 2^{2 \cdot 1 - 2} - 2^{1-1}.$$

On the other hand, since G_1 is a linear subspace we have that

$$\begin{aligned}
\widehat{B}(p) \cap \left(\mathbf{u} \oplus \widehat{B}(p) \right) &= \{\mathbf{a}_q^{(1)}, \mathbf{a}_r^{(1)}, \mathbf{a}_s^{(1)}\} \cap \{\mathbf{u} \oplus \mathbf{a}_q^{(1)}, \mathbf{u} \oplus \mathbf{a}_r^{(1)}, \mathbf{u} \oplus \mathbf{a}_s^{(1)}\} \\
&= \{\mathbf{a}_q^{(1)}, \mathbf{a}_r^{(1)}, \mathbf{a}_s^{(1)}\} \cap \{\mathbf{a}_p^{(1)}, \mathbf{a}_s^{(1)}, \mathbf{a}_r^{(1)}\}
\end{aligned}$$

$$= \{\mathbf{a}_r^{(1)}, \mathbf{a}_s^{(1)}\}$$

and therefore

$$\left| \widehat{B}(p) \cap (\mathbf{u} \oplus \widehat{B}(p)) \right| = 2 = 2^{2 \cdot 1 - 2} + 2^{1 - 1}.$$

Furthermore

$$B(p) \cap (\mathbf{u} \oplus \widehat{B}(p)) = \{\mathbf{a}_p^{(1)}\} \cap \{\mathbf{a}_p^{(1)}, \mathbf{a}_s^{(1)}, \mathbf{a}_r^{(1)}\} = \{\mathbf{a}_p^{(1)}\}$$

and then

$$\left| B(p) \cap (\mathbf{u} \oplus \widehat{B}(p)) \right| = 1 = 2^{2 \cdot 1 - 2}.$$

Finally

$$\widehat{B}(p) \cap (\mathbf{u} \oplus B(p)) = \{\mathbf{a}_q^{(1)}, \mathbf{a}_r^{(1)}, \mathbf{a}_s^{(1)}\} \cap \{\mathbf{u} \oplus \mathbf{a}_p^{(1)}\} = \{\mathbf{a}_q^{(1)}\}$$

and so

$$\left| \widehat{B}(p) \cap (\mathbf{u} \oplus B(p)) \right| = 1 = 2^{2 \cdot 1 - 2}.$$

Therefore, properties (a), (b), (c) and (d) hold for $i = 1$.

Assume now that properties (a), (b), (c) and (d) hold for $i - 1 < k$. We will prove that these properties also hold for i . Let $(p_1, p_2, \dots, p_{i-1}, p_i) \in \{0, 1, 2, 3\}^i$ and assume that $\mathbf{u} \in G_i \setminus \{\mathbf{0}\}$. From expression (3) we have that

$$\begin{aligned} & B(p_1, p_2, \dots, p_{i-1}, p_i) \cap (\mathbf{u} \oplus B(p_1, p_2, \dots, p_{i-1}, p_i)) \\ &= \left(\left(\mathbf{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \cap \left(\mathbf{u} \oplus \mathbf{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \right) \end{aligned} \quad (6a)$$

$$\cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^3 \left(\left(\mathbf{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \cap \left(\mathbf{u} \oplus \mathbf{a}_q^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right) \right) \quad (6b)$$

$$\cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^3 \left(\left(\mathbf{a}_q^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right) \cap \left(\mathbf{u} \oplus \mathbf{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \right) \quad (6c)$$

$$\cup \bigcup_{\substack{q,r=0 \\ q,r \neq p_i}}^3 \left(\left(\mathbf{a}_q^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right) \cap \left(\mathbf{u} \oplus \mathbf{a}_r^{(i)} \oplus B(p_1, p_2, \dots, p_{i-1}) \right) \right). \quad (6d)$$

From expression (1) we have that $\mathbf{u} = \mathbf{v} \oplus \mathbf{a}_l^{(i)}$ with $\mathbf{v} \in G_{i-1}$ and $l \in \{0, 1, 2, 3\}$.

If $l = p_i$, then the set in expression (6a) becomes

$$\mathbf{a}_{p_i}^{(i)} \oplus \left(\widehat{B}(p_1, p_2, \dots, p_{i-1}) \cap \left(\mathbf{v} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \right), \quad (7)$$

the sets in expressions (6b) and (6c) become the empty set, and the set in expression (6d) becomes

$$\bigcup_{\substack{q=0 \\ q \neq p_i}}^3 \mathbf{a}_q^{(i)} \oplus (B(p_1, p_2, \dots, p_{i-1}) \cap (\mathbf{v} \oplus B(p_1, p_2, \dots, p_{i-1}))). \quad (8)$$

Furthermore, it is not difficult to prove that the set in expression (7) is disjoint with each one of the three sets that appear in expression (8). It is also easy to prove that these three sets are pairwise disjoint. Therefore, by the induction hypothesis,

$$\begin{aligned}
& |B(p_1, p_2, \dots, p_{i-1}, p_i) \cap (\mathbf{u} \oplus B(p_1, p_2, \dots, p_{i-1}, p_i))| \\
&= \left| \widehat{B}(p_1, p_2, \dots, p_{i-1}) \cap \left(\mathbf{v} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \right| \\
&\quad + 3 \cdot |B(p_1, p_2, \dots, p_{i-1}) \cap (\mathbf{v} \oplus B(p_1, p_2, \dots, p_{i-1}))| \\
&= 2^{2(i-1)-2} + 2^{(i-1)-1} + 3(2^{2(i-1)-2} - 2^{(i-1)-1}) = 2^{2i-2} - 2^{i-1}.
\end{aligned}$$

However, if $p_i \neq l$, then the set in expression (6a) becomes the empty set, the sets in expressions (6b) and (6c) become the sets

$$\mathbf{a}_{p_i}^{(i)} \oplus \left(\widehat{B}(p_1, p_2, \dots, p_{i-1}) \cap (\mathbf{v} \oplus B(p_1, p_2, \dots, p_{i-1})) \right) \quad (9)$$

and

$$\mathbf{a}_l^{(i)} \oplus \left(B(p_1, p_2, \dots, p_{i-1}) \cap \left(\mathbf{v} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \right) \quad (10)$$

respectively, and the set in expression (6d) becomes the set

$$(\mathbf{a}_r^{(i)} \oplus (B(p_1, p_2, \dots, p_{i-1}) \cap (\mathbf{v} \oplus B(p_1, p_2, \dots, p_{i-1})))) \quad (11a)$$

$$\cup (\mathbf{a}_s^{(i)} \oplus (B(p_1, p_2, \dots, p_{i-1}) \cap (\mathbf{v} \oplus B(p_1, p_2, \dots, p_{i-1})))) \quad (11b)$$

for some $r, s \in \{0, 1, 2, 3\} \setminus \{p_i, l\}$.

Furthermore, it is not difficult to prove that each one of the sets in expressions (9), (10), (11a) and (11b) is disjoint with the other. So, by the induction hypothesis,

$$\begin{aligned}
& |B(p_1, p_2, \dots, p_{i-1}, p_i) \cap (\mathbf{u} \oplus B(p_1, p_2, \dots, p_{i-1}, p_i))| \\
&= \left| \widehat{B}(p_1, p_2, \dots, p_{i-1}) \cap (\mathbf{v} \oplus B(p_1, p_2, \dots, p_{i-1})) \right| \\
&\quad + \left| B(p_1, p_2, \dots, p_{i-1}) \cap \left(\mathbf{v} \oplus \widehat{B}(p_1, p_2, \dots, p_{i-1}) \right) \right| \\
&\quad + 2 \cdot |B(p_1, p_2, \dots, p_{i-1}) \cap (\mathbf{v} \oplus B(p_1, p_2, \dots, p_{i-1}))| \\
&= 2^{2(i-1)-2} + 2^{2(i-1)-2} + 2(2^{2(i-1)-2} - 2^{(i-1)-1}) = 2^{2i-2} - 2^{i-1}.
\end{aligned}$$

Consequently, property (a) holds for i .

By a similar argument, we also have that properties (b), (c) and (d) hold for i . $\square$

We are now able to prove that the sets $B(p_1, p_2, \dots, p_k)$ and $\widehat{B}(p_1, p_2, \dots, p_k)$ are the supports of a bent function of $2k$ variables and its complementary, respectively.

Theorem 2: For all $(p_1, p_2, \dots, p_k) \in \{0, 1, 2, 3\}^k$ the sets

$$B(p_1, p_2, \dots, p_k) \quad \text{and} \quad \widehat{B}(p_1, p_2, \dots, p_k)$$

are the supports of two bent functions of $2k$ variables so that one is the complementary function of the other.

PROOF: Assume that $\mathbf{u} \in \mathbb{F}_2^{2k} \setminus \{\mathbf{0}\}$. Since $\mathbb{F}_2^{2k} = G_k$, by Lemmas 1, 2 and 3 we have that

$$\begin{aligned} & |B(p_1, p_2, \dots, p_k) \Delta (\mathbf{u} \oplus B(p_1, p_2, \dots, p_k))| \\ &= |B(p_1, p_2, \dots, p_k)| + |\mathbf{u} \oplus B(p_1, p_2, \dots, p_k)| \\ &\quad - 2|B(p_1, p_2, \dots, p_k) \cap (\mathbf{u} \oplus B(p_1, p_2, \dots, p_k))| \\ &= 2^{2k-1} - 2^{k-1} + 2^{2k-1} - 2^{k-1} - 2(2^{2k-2} - 2^{k-1}) = 2^{2k-1}, \end{aligned}$$

and therefore, $B(p_1, p_2, \dots, p_k) \Delta (\mathbf{u} \oplus B(p_1, p_2, \dots, p_k))$ is the support of a balanced function of $2k$ variables. So, by Corollary 1, we have that $B(p_1, p_2, \dots, p_k)$ is the support of a bent function $f(\mathbf{x})$ of $2k$ variables.

Moreover, from Lemma 1, we have that $\widehat{B}(p_1, p_2, \dots, p_k) = G_k \setminus B(p_1, p_2, \dots, p_k)$ and, consequently, the set $\widehat{B}(p_1, p_2, \dots, p_k)$ is the support of the complementary function $1 \oplus f(\mathbf{x})$. $\square$

4 Counting bent functions

In order to count the number of bent functions provided by Theorem 2, we need the following result.

Theorem 3: For $i = 1, 2, \dots, k$, let $(p_1, p_2, \dots, p_i), (q_1, q_2, \dots, q_i) \in \{0, 1, 2, 3\}^i$. If $p_1 = q_1, p_2 = q_2, \dots, p_l = q_l$, but $p_{l+1} \neq q_{l+1}$ for some $l \in \{1, 2, \dots, i-1\}$, then

$$\begin{aligned} B(p_1, p_2, \dots, p_l, p_{l+1}, p_{l+2}, \dots, p_{l+m}) &\neq B(p_1, p_2, \dots, p_l, q_{l+1}, q_{l+2}, \dots, q_{l+m}), \\ \widehat{B}(p_1, p_2, \dots, p_l, p_{l+1}, p_{l+2}, \dots, p_{l+m}) &\neq \widehat{B}(p_1, p_2, \dots, p_l, q_{l+1}, q_{l+2}, \dots, q_{l+m}) \end{aligned}$$

for $m = 1, 2, \dots, i-l$.

PROOF: We proceed by induction over m . Assume that $m = 1$. Since $p_{l+1} \neq q_{l+1}$, we can assume that $\{0, 1, 2, 3\} = \{p_{l+1}, q_{l+1}, r, s\}$ with $r \neq s$. Therefore, if

$$B(p_1, p_2, \dots, p_l, p_{l+1}) = B(p_1, p_2, \dots, p_l, q_{l+1}),$$

from expression (3) we have that

$$\begin{aligned} & \left(\mathbf{a}_{p_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \dots, p_l) \right) \cup \left(\mathbf{a}_{q_{l+1}}^{(l+1)} \oplus B(p_1, p_2, \dots, p_l) \right) \\ &= \left(\mathbf{a}_{q_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \dots, p_l) \right) \cup \left(\mathbf{a}_{p_{l+1}}^{(l+1)} \oplus B(p_1, p_2, \dots, p_l) \right). \end{aligned}$$

Let $\mathbf{x} \in \mathbf{a}_{p_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \dots, p_l)$, then

$$\mathbf{x} \in \mathbf{a}_{q_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \dots, p_l) \quad \text{or} \quad \mathbf{x} \in \mathbf{a}_{p_{l+1}}^{(l+1)} \oplus B(p_1, p_2, \dots, p_l).$$

In the first case,

$$\mathbf{x} = \mathbf{a}_{p_{l+1}}^{(l+1)} \oplus \mathbf{u} = \mathbf{a}_{q_{l+1}}^{(l+1)} \oplus \mathbf{v}$$

with $\mathbf{u}, \mathbf{v} \in \widehat{B}(p_1, p_2, \dots, p_l) \subseteq G_l$; but then

$$\mathbf{u} \oplus \mathbf{v} = \mathbf{a}_{p_{l+1}}^{(l+1)} \oplus \mathbf{a}_{q_{l+1}}^{(l+1)} \in G_l \cap H_{l+1} = \{\mathbf{0}\}$$

and therefore $\mathbf{a}_{p_{l+1}}^{(l+1)} = \mathbf{a}_{q_{l+1}}^{(l+1)}$ which is a contradiction.

In the second case,

$$\mathbf{x} = \mathbf{a}_{p_{l+1}}^{(l+1)} \oplus \mathbf{u} = \mathbf{a}_{p_{l+1}}^{(l+1)} \oplus \mathbf{v}$$

with $\mathbf{u} \in \widehat{B}(p_1, p_2, \dots, p_l)$ and $\mathbf{v} \in B(p_1, p_2, \dots, p_l)$; but then

$$\mathbf{u} = \mathbf{v} \in \widehat{B}(p_1, p_2, \dots, p_l) \cap B(p_1, p_2, \dots, p_l) = \emptyset$$

which is a contradiction.

So, none of the elements of $\mathbf{a}_{p_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \dots, p_l)$ belongs to the set

$$\left(\mathbf{a}_{q_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \dots, p_l) \right) \cup \left(\mathbf{a}_{p_{l+1}}^{(l+1)} \oplus B(p_1, p_2, \dots, p_l) \right).$$

An analogous argument shows that none of the elements of $\mathbf{a}_{q_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \dots, p_l)$ belongs to the set

$$\left(\mathbf{a}_{q_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \dots, p_l) \right) \cup \left(\mathbf{a}_{p_{l+1}}^{(l+1)} \oplus B(p_1, p_2, \dots, p_l) \right).$$

Consequently, $B(p_1, p_2, \dots, p_l, p_{l+1}) \neq B(p_1, p_2, \dots, p_l, q_{l+1})$ and from Lemma 1, we also have that $\widehat{B}(p_1, p_2, \dots, p_l, p_{l+1}) \neq \widehat{B}(p_1, p_2, \dots, p_l, q_{l+1})$.

Assume now that the result is true for $m - 1$, we will prove that it is also true for m .
If

$$B(p_1, p_2, \dots, p_l, p_{l+1}, p_{l+2}, \dots, p_{l+m}) = B(p_1, p_2, \dots, p_l, q_{l+1}, q_{l+2}, \dots, q_{l+m})$$

from expression (3) we have that

$$\begin{aligned} & \left(\mathbf{a}_{p_{l+m}}^{(l+m)} \oplus \widehat{B}(p_1, p_2, \dots, p_l, p_{l+1}, \dots, p_{l+m-1}) \right) \\ & \cup \bigcup_{\substack{r=0 \\ r \neq p_{l+m}}}^3 \left(\mathbf{a}_r^{(l+m)} \oplus B(p_1, p_2, \dots, p_l, p_{l+1}, \dots, p_{l+m-1}) \right) \\ & = \left(\mathbf{a}_{q_{l+m}}^{(l+m)} \oplus \widehat{B}(p_1, p_2, \dots, p_l, q_{l+1}, \dots, q_{l+m-1}) \right) \\ & \cup \bigcup_{\substack{s=0 \\ s \neq q_{l+m}}}^3 \left(\mathbf{a}_s^{(l+m)} \oplus B(p_1, p_2, \dots, p_l, q_{l+1}, \dots, q_{l+m-1}) \right) \end{aligned}$$

Now, by a similar argument to the previous one, but considering the cases $p_{l+m} = q_{l+m}$ and $p_{l+m} \neq q_{l+m}$, we obtain that none of the elements of the set of the left hand side of the previous expression belongs to the set of the right hand side. So,

$$B(p_1, p_2, \dots, p_l, p_{l+1}, p_{l+2}, \dots, p_{l+m}) \neq B(p_1, p_2, \dots, p_l, q_{l+1}, q_{l+2}, \dots, q_{l+m})$$

and from Lemma 1, we have that

$$\widehat{B}(p_1, p_2, \dots, p_l, p_{l+1}, p_{l+2}, \dots, p_{l+m}) \neq \widehat{B}(p_1, p_2, \dots, p_l, q_{l+1}, q_{l+2}, \dots, q_{l+m}). \quad \square$$

Thus, as a consequence of this result, we have the following corollary.

Corollary 2: *For a basis of $\mathbb{F}_2^{2k}$ the number of bent functions of $2k$ variables that we can construct using the procedure described in Section 3 is 2^{2k+1} .*

PROOF: For a fixed basis $\mathcal{U}$, we can construct as many sets of type $B(p_1, p_2, \dots, p_k)$ as elements are in $\{0, 1, 2, 3\}^k$. The same is true for the sets of type $\widehat{B}(p_1, p_2, \dots, p_k)$. Therefore, the number of bent functions of $2k$ variables that we can construct is

$$2 |\{0, 1, 2, 3\}^k| = 2^{2k+1}. \quad \square$$

One question that arises at this point is the following: starting with two different bases $\mathcal{U}$ and $\mathcal{V}$ of $\mathbb{F}_2^{2k}$, the 2^{2k+1} bent functions obtained from basis $\mathcal{U}$ are different of the 2^{2k+1} bent functions obtained from basis $\mathcal{V}$?

Since the number of different bases in $\mathbb{F}_2^{2k}$ (see [30, page 46]) is $\prod_{i=0}^{2k-1} (2^{2k} - 2^i)$ we can construct

$$2^{2k+1} \prod_{i=0}^{2k-1} (2^{2k} - 2^i)$$

bent functions of $2k$ variables. For example, for $k = 2$, we can construct 645 120 bent functions. Nevertheless, it is well known that the number of different bent functions of 4 variables is 896. So there are different bases that provide the same bent functions as we can see in the following example.

Example 1: Assume that $k = 2$ and consider the basis $\mathcal{U} = \{1, 2, 4, 8\}$ of $\mathbb{F}_2^4$. The supports of the bent functions we can construct using the procedure described in Section 3 are given in Table 1. On the other hand, if we consider the basis $\mathcal{V} = \{6, 7, 9, 13\}$, then the supports of the bent functions we can construct using the procedure described in Section 3 are given in Table 2. As we can see, we obtain the same bent functions in both cases, although for different values of $(p_1, p_2) \in \{0, 1, 2, 3\}^2$. $\square$

From now on, if we need to emphasize the basis $\mathcal{U} = \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_{2k-1}, \mathbf{u}_{2k}\}$ used in the construction of the supports of the bent functions provided by the process described in Section 3, we write

$$B_{\mathcal{U}}(p_1, p_2, \dots, p_k) \quad \text{and} \quad \widehat{B}_{\mathcal{U}}(p_1, p_2, \dots, p_k).$$

Moreover, if we look closely expressions (3) and (4) we see that the above sets depend on the linear subspaces $H_i = \text{Span}\{\mathbf{u}_{2i-1}, \mathbf{u}_{2i}\}$, for $i = 1, 2, \dots, k$, rather than the basis $\{\mathbf{u}_{2i-1}, \mathbf{u}_{2i}\}$ considered. Therefore, we can establish the following result.

Lemma 4: *Let $\mathcal{U} = \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_{2k-1}, \mathbf{u}_{2k}\}$ and $\mathcal{V} = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{2k-1}, \mathbf{v}_{2k}\}$ be two bases of $\mathbb{F}_2^{2k}$. Assume that there exists $r \in \{1, 2, \dots, k\}$ such that*

(p_1, p_2)	$B(p_1, p_2)$	$\widehat{B}(p_1, p_2)$
(0, 0)	1, 2, 3, 4, 8, 12	0, 5, 6, 7, 9, 10, 11, 13, 14, 15
(0, 1)	0, 5, 6, 7, 8, 12	1, 2, 3, 4, 9, 10, 11, 13, 14, 15
(0, 2)	0, 4, 9, 10, 11, 12	1, 2, 3, 5, 6, 7, 8, 13, 14, 15
(0, 3)	0, 4, 8, 13, 14, 15	1, 2, 3, 5, 6, 7, 9, 10, 11, 12
(1, 0)	0, 2, 3, 5, 9, 13	1, 4, 6, 7, 8, 10, 11, 12, 14, 15
(1, 1)	1, 4, 6, 7, 9, 13	0, 2, 3, 5, 8, 10, 11, 12, 14, 15
(1, 2)	1, 5, 8, 10, 11, 13	0, 2, 3, 4, 6, 7, 9, 12, 14, 15
(1, 3)	1, 5, 9, 12, 14, 15	0, 2, 3, 4, 6, 7, 8, 10, 11, 13
(2, 0)	0, 1, 3, 6, 10, 14	2, 4, 5, 7, 8, 9, 11, 12, 13, 15
(2, 1)	2, 4, 5, 7, 10, 14	0, 1, 3, 6, 8, 9, 11, 12, 13, 15
(2, 2)	2, 6, 8, 9, 11, 14	0, 1, 3, 4, 5, 7, 10, 12, 13, 15
(2, 3)	2, 6, 10, 12, 13, 15	0, 1, 3, 4, 5, 7, 8, 9, 11, 14
(3, 0)	0, 1, 2, 7, 11, 15	3, 4, 5, 6, 8, 9, 10, 12, 13, 14
(3, 1)	3, 4, 5, 6, 11, 15	0, 1, 2, 7, 8, 9, 10, 12, 13, 14
(3, 2)	3, 7, 8, 9, 10, 15	0, 1, 2, 4, 5, 6, 11, 12, 13, 14
(3, 3)	3, 7, 11, 12, 13, 14	0, 1, 2, 4, 5, 6, 8, 9, 10, 15

Table 1: Supports of the bent functions constructed with the basis $\mathcal{U}$ of Example 1

(p_1, p_2)	$B(p_1, p_2)$	$\widehat{B}(p_1, p_2)$
(0, 0)	3, 7, 11, 12, 13, 14	0, 1, 2, 4, 5, 6, 8, 9, 10, 15
(0, 1)	0, 1, 2, 7, 11, 15	3, 4, 5, 6, 8, 9, 10, 12, 13, 14
(0, 2)	0, 4, 9, 10, 11, 12	1, 2, 3, 5, 6, 7, 8, 13, 14, 15
(0, 3)	0, 5, 6, 7, 8, 12	1, 2, 3, 4, 9, 10, 11, 13, 14, 15
(1, 0)	0, 4, 8, 13, 14, 15	1, 2, 3, 5, 6, 7, 9, 10, 11, 12
(1, 1)	1, 2, 3, 4, 8, 12	0, 5, 6, 7, 9, 10, 11, 13, 14, 15
(1, 2)	3, 7, 8, 9, 10, 15	0, 1, 2, 4, 5, 6, 11, 12, 13, 14
(1, 3)	3, 4, 5, 6, 11, 15	0, 1, 2, 7, 8, 9, 10, 12, 13, 14
(2, 0)	0, 1, 3, 6, 10, 14	2, 4, 5, 7, 8, 9, 11, 12, 13, 15
(2, 1)	2, 6, 10, 12, 13, 15	0, 1, 3, 4, 5, 7, 8, 9, 11, 14
(2, 2)	1, 4, 6, 7, 9, 13	0, 2, 3, 5, 8, 10, 11, 12, 14, 15
(2, 3)	1, 5, 8, 10, 11, 13	0, 2, 3, 4, 6, 7, 9, 12, 14, 15
(3, 0)	0, 2, 3, 5, 9, 13	1, 4, 6, 7, 8, 10, 11, 12, 14, 15
(3, 1)	1, 5, 9, 12, 14, 15	0, 2, 3, 4, 6, 7, 8, 10, 11, 13
(3, 2)	2, 4, 5, 7, 10, 14	0, 1, 3, 6, 8, 9, 11, 12, 13, 15
(3, 3)	2, 6, 8, 9, 11, 14	0, 1, 3, 4, 5, 7, 10, 12, 13, 15

Table 2: Supports of the bent functions constructed with the basis $\mathcal{V}$ of Example 1

- $(\mathbf{v}_{2i-1}, \mathbf{v}_{2i}) = (\mathbf{u}_{2i-1}, \mathbf{u}_{2i})$ for $i \in \{1, 2, \dots, k\} \setminus \{r\}$,
- $\text{Span}\{\mathbf{v}_{2r-1}, \mathbf{v}_{2r}\} = \text{Span}\{\mathbf{u}_{2r-1}, \mathbf{u}_{2r}\}$,

then

$$B_{\mathcal{U}}(p_1, p_2, \dots, p_k) = B_{\mathcal{V}}(p_1, p_2, \dots, p_k) \quad \text{and} \quad \widehat{B}_{\mathcal{U}}(p_1, p_2, \dots, p_k) = \widehat{B}_{\mathcal{V}}(p_1, p_2, \dots, p_k)$$

for all $(p_1, p_2, \dots, p_k) \in \{0, 1, 2, 3\}^k$.

Furthermore, the order in which each pair of vectors appears within the basis is not important, as we can see in the following example.

Example 2: Assume that $k = 4$ and consider the bases

$$\mathcal{U} = \{\mathbf{1}, \mathbf{2}; \mathbf{4}, \mathbf{8}; \mathbf{16}, \mathbf{32}; \mathbf{64}, \mathbf{128}\} \quad \text{and} \quad \mathcal{V} = \{\mathbf{1}, \mathbf{2}; \mathbf{16}, \mathbf{32}; \mathbf{4}, \mathbf{8}; \mathbf{64}, \mathbf{128}\}$$

of $\mathbb{F}_2^8$. Then, following the process described in Section 3 we obtain the following sets from basis $\mathcal{U}$

$$\begin{aligned} B_{\mathcal{U}}(0) &= \{\mathbf{0}\}, \\ B_{\mathcal{U}}(0, 2) &= \{\mathbf{0}, \mathbf{4}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}\}, \\ B_{\mathcal{U}}(0, 2, 1) &= \{\mathbf{0}, \mathbf{4}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{17}, \mathbf{18}, \mathbf{19}, \mathbf{21}, \mathbf{22}, \mathbf{23}, \mathbf{24}, \mathbf{29}, \mathbf{30}, \mathbf{31}, \mathbf{32}, \mathbf{36}, \\ &\quad \mathbf{41}, \mathbf{42}, \mathbf{43}, \mathbf{44}, \mathbf{48}, \mathbf{52}, \mathbf{57}, \mathbf{58}, \mathbf{59}, \mathbf{60}\}, \\ B_{\mathcal{U}}(0, 2, 1, 3) &= \{\mathbf{0}, \mathbf{4}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{17}, \mathbf{18}, \mathbf{19}, \mathbf{21}, \mathbf{22}, \mathbf{23}, \mathbf{24}, \mathbf{29}, \mathbf{30}, \mathbf{31}, \mathbf{32}, \mathbf{36}, \\ &\quad \mathbf{41}, \mathbf{42}, \mathbf{43}, \mathbf{44}, \mathbf{48}, \mathbf{52}, \mathbf{57}, \mathbf{58}, \mathbf{59}, \mathbf{60}, \mathbf{64}, \mathbf{68}, \mathbf{73}, \mathbf{74}, \mathbf{75}, \mathbf{76}, \mathbf{81}, \\ &\quad \mathbf{82}, \mathbf{83}, \mathbf{85}, \mathbf{86}, \mathbf{87}, \mathbf{88}, \mathbf{93}, \mathbf{94}, \mathbf{95}, \mathbf{96}, \mathbf{100}, \mathbf{105}, \mathbf{106}, \mathbf{107}, \mathbf{108}, \\ &\quad \mathbf{112}, \mathbf{116}, \mathbf{121}, \mathbf{122}, \mathbf{123}, \mathbf{124}, \mathbf{128}, \mathbf{132}, \mathbf{137}, \mathbf{138}, \mathbf{139}, \mathbf{140}, \\ &\quad \mathbf{145}, \mathbf{146}, \mathbf{147}, \mathbf{149}, \mathbf{150}, \mathbf{151}, \mathbf{152}, \mathbf{157}, \mathbf{158}, \mathbf{159}, \mathbf{160}, \mathbf{164}, \\ &\quad \mathbf{169}, \mathbf{170}, \mathbf{171}, \mathbf{172}, \mathbf{176}, \mathbf{180}, \mathbf{185}, \mathbf{186}, \mathbf{187}, \mathbf{188}, \mathbf{193}, \mathbf{194}, \\ &\quad \mathbf{195}, \mathbf{197}, \mathbf{198}, \mathbf{199}, \mathbf{200}, \mathbf{205}, \mathbf{206}, \mathbf{207}, \mathbf{208}, \mathbf{212}, \mathbf{217}, \mathbf{218}, \\ &\quad \mathbf{219}, \mathbf{220}, \mathbf{225}, \mathbf{226}, \mathbf{227}, \mathbf{229}, \mathbf{230}, \mathbf{231}, \mathbf{232}, \mathbf{237}, \mathbf{238}, \mathbf{239}, \\ &\quad \mathbf{241}, \mathbf{242}, \mathbf{243}, \mathbf{245}, \mathbf{246}, \mathbf{247}, \mathbf{248}, \mathbf{253}, \mathbf{254}, \mathbf{255}\}, \end{aligned}$$

and the following sets from basis $\mathcal{V}$

$$\begin{aligned} B_{\mathcal{V}}(0) &= \{\mathbf{0}\}, \\ B_{\mathcal{V}}(0, 1) &= \{\mathbf{0}, \mathbf{17}, \mathbf{18}, \mathbf{19}, \mathbf{32}, \mathbf{48}\}, \\ B_{\mathcal{V}}(0, 1, 2) &= \{\mathbf{0}, \mathbf{4}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{17}, \mathbf{18}, \mathbf{19}, \mathbf{21}, \mathbf{22}, \mathbf{23}, \mathbf{24}, \mathbf{29}, \mathbf{30}, \mathbf{31}, \mathbf{32}, \mathbf{36}, \\ &\quad \mathbf{41}, \mathbf{42}, \mathbf{43}, \mathbf{44}, \mathbf{48}, \mathbf{52}, \mathbf{57}, \mathbf{58}, \mathbf{59}, \mathbf{60}\}, \\ B_{\mathcal{V}}(0, 1, 2, 3) &= \{\mathbf{0}, \mathbf{4}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{17}, \mathbf{18}, \mathbf{19}, \mathbf{21}, \mathbf{22}, \mathbf{23}, \mathbf{24}, \mathbf{29}, \mathbf{30}, \mathbf{31}, \mathbf{32}, \mathbf{36}, \end{aligned}$$

41, 42, 43, 44, 48, 52, 57, 58, 59, 60, 64, 68, 73, 74, 75, 76, 81,
82, 83, 85, 86, 87, 88, 93, 94, 95, 96, 100, 105, 106, 107, 108,
112, 116, 121, 122, 123, 124, 128, 132, 137, 138, 139, 140,
145, 146, 147, 149, 150, 151, 152, 157, 158, 159, 160, 164,
169, 170, 171, 172, 176, 180, 185, 186, 187, 188, 193, 194,
195, 197, 198, 199, 200, 205, 206, 207, 208, 212, 217, 218,
219, 220, 225, 226, 227, 229, 230, 231, 232, 237, 238, 239,
241, 242, 243, 245, 246, 247, 248, 253, 254, 255}.

Note that $B_{\mathcal{U}}(0) = B_{\mathcal{V}}(0)$ and $B_{\mathcal{U}}(0, 2) \neq B_{\mathcal{V}}(0, 1)$, but $B_{\mathcal{U}}(0, 2, 1) = B_{\mathcal{V}}(0, 1, 2)$ and consequently $B_{\mathcal{U}}(0, 2, 1, 3) = B_{\mathcal{V}}(0, 1, 2, 3)$. So, both bases $\mathcal{U}$ and $\mathcal{V}$ provide the same bent function of 8 variables, although the intermediate sets are not necessarily equal. $\square$

The following result establishes the property described in the previous example.

Lemma 5: *Let $\mathcal{U} = \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_{2k-1}, \mathbf{u}_{2k}\}$ and $\mathcal{V} = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{2k-1}, \mathbf{v}_{2k}\}$ be two bases of $\mathbb{F}_2^{2k}$. Assume that there exist $r, s \in \{1, 2, \dots, k\}$, with $r < s$, such that*

- $(\mathbf{v}_{2i-1}, \mathbf{v}_{2i}) = (\mathbf{u}_{2i-1}, \mathbf{u}_{2i})$ for $i \in \{1, 2, \dots, k\} \setminus \{r, s\}$,
- $(\mathbf{v}_{2r-1}, \mathbf{v}_{2r}) = (\mathbf{u}_{2s-1}, \mathbf{u}_{2s})$ and $(\mathbf{v}_{2s-1}, \mathbf{v}_{2s}) = (\mathbf{u}_{2r-1}, \mathbf{u}_{2r})$,

then

$$B_{\mathcal{U}}(p_1, p_2, \dots, p_k, \dots, p_r, \dots, p_s, \dots, p_k) = B_{\mathcal{V}}(p_1, p_2, \dots, p_k, \dots, p_s, \dots, p_r, \dots, p_k),$$

$$\widehat{B}_{\mathcal{U}}(p_1, p_2, \dots, p_k, \dots, p_r, \dots, p_s, \dots, p_k) = \widehat{B}_{\mathcal{V}}(p_1, p_2, \dots, p_k, \dots, p_s, \dots, p_r, \dots, p_k),$$

for all $(p_1, p_2, \dots, p_k) \in \{0, 1, 2, 3\}^k$.

PROOF: Without loss of generality we can assume that $s = r + 1$. From the choice of bases $\mathcal{U}$ and $\mathcal{V}$, we have that

$$B_{\mathcal{U}}(p_1, p_2, \dots, p_{r-1}) = B_{\mathcal{V}}(p_1, p_2, \dots, p_{r-1}) \quad \text{and} \quad \widehat{B}_{\mathcal{U}}(p_1, p_2, \dots, p_{r-1}) = \widehat{B}_{\mathcal{V}}(p_1, p_2, \dots, p_{r-1}).$$

Following similar arguments that in the proofs of the results in Section 3, it is not difficult to prove that

$$B_{\mathcal{U}}(p_1, p_2, \dots, p_{r-1}, p_r, p_{r+1}) = B_{\mathcal{V}}(p_1, p_2, \dots, p_{r-1}, p_{r+1}, p_r),$$

$$\widehat{B}_{\mathcal{U}}(p_1, p_2, \dots, p_{r-1}, p_r, p_{r+1}) = \widehat{B}_{\mathcal{V}}(p_1, p_2, \dots, p_{r-1}, p_{r+1}, p_r).$$

Now, the result follows from the choice of bases $\mathcal{U}$ and $\mathcal{V}$. $\square$

As a consequence of Lemmas 4 and 5 we have the following result.

Theorem 4: Let $\mathcal{U} = \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_{2k-1}, \mathbf{u}_{2k}\}$ and $\mathcal{V} = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{2k-1}, \mathbf{v}_{2k}\}$ be bases of $\mathbb{F}_2^{2k}$ such that $\{\mathbf{u}_{2i-1}, \mathbf{u}_{2i}\}$ and $\{\mathbf{v}_{2i-1}, \mathbf{v}_{2i}\}$ are Gauss-Jordan bases of cardinality 2. If σ is a permutation of $\{1, 2, \dots, k\}$, such that

$$(\mathbf{v}_{2i-1}, \mathbf{v}_{2i}) = (\mathbf{u}_{2\sigma(i)-1}, \mathbf{u}_{2\sigma(i)}) \quad \text{for } i = 1, 2, \dots, k,$$

then $\mathcal{U}$ and $\mathcal{V}$ provide the same bent functions of $2k$ variables.

Therefore, from now on, in addition to consider that $\{\mathbf{u}_{2i-1}, \mathbf{u}_{2i}\}$ is a Gauss-Jordan basis of cardinality 2 we will consider also that $\mathbf{u}_{2i-1} > \mathbf{u}_{2j-1}$ (lexicographical order) if $i < j$. Since each linear subspace of dimension 2 has 6 different basis, but only one is a Gauss-Jordan basis of cardinality 2, we have that the number of bases of $\mathbb{F}_2^{2k}$ satisfying these conditions is

$$\frac{\prod_{i=0}^{2k-1} (2^{2k} - 2^i)}{6^k \cdot k!}.$$

In particular, for $k = 2$ we have 280 bases satisfying these conditions. Consequently, according with Corollary 2, we can construct $2^5 \cdot 280 = 8960$ bent functions of 4 variables. Remember that the number of different bent functions of 4 variables is 896 (448 with weight 6 and 448 with weight 10). An exhaustive computer search shows that these 896 bent functions can be obtained from the following 28 bases of $\mathbb{F}_2^4$:

$$\begin{aligned} \mathcal{U}_1 &= \{8, 7; 5, 3\}, & \mathcal{U}_2 &= \{8, 7; 4, 2\}, & \mathcal{U}_3 &= \{8, 7; 4, 1\}, & \mathcal{U}_4 &= \{8, 7; 2, 1\}, \\ \mathcal{U}_5 &= \{8, 6; 5, 2\}, & \mathcal{U}_6 &= \{8, 6; 4, 3\}, & \mathcal{U}_7 &= \{8, 6; 4, 1\}, & \mathcal{U}_8 &= \{8, 6; 2, 1\}, \\ \mathcal{U}_9 &= \{8, 5; 6, 1\}, & \mathcal{U}_{10} &= \{8, 5; 4, 3\}, & \mathcal{U}_{11} &= \{8, 5; 4, 2\}, & \mathcal{U}_{12} &= \{8, 5; 2, 1\}, \\ \mathcal{U}_{13} &= \{8, 4; 6, 1\}, & \mathcal{U}_{14} &= \{8, 4; 5, 3\}, & \mathcal{U}_{15} &= \{8, 4; 5, 2\}, & \mathcal{U}_{16} &= \{8, 4; 2, 1\}, \\ \mathcal{U}_{17} &= \{8, 3; 6, 1\}, & \mathcal{U}_{18} &= \{8, 3; 5, 2\}, & \mathcal{U}_{19} &= \{8, 3; 4, 2\}, & \mathcal{U}_{20} &= \{8, 3; 4, 1\}, \\ \mathcal{U}_{21} &= \{8, 2; 6, 1\}, & \mathcal{U}_{22} &= \{8, 2; 5, 3\}, & \mathcal{U}_{23} &= \{8, 2; 4, 3\}, & \mathcal{U}_{24} &= \{8, 2; 4, 1\}, \\ \mathcal{U}_{25} &= \{8, 1; 5, 3\}, & \mathcal{U}_{26} &= \{8, 1; 5, 2\}, & \mathcal{U}_{27} &= \{8, 1; 4, 3\}, & \mathcal{U}_{28} &= \{8, 1; 4, 2\}. \end{aligned}$$

Furthermore, if we consider the following 4×4 binary matrices

$$\begin{aligned} P_1 &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, & P_2 &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}, & P_3 &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}, & P_4 &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \\ P_5 &= \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}, & P_6 &= \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, & P_7 &= \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, & P_8 &= \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \\ P_9 &= \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}, & P_{10} &= \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \end{aligned}$$

k	Seconds	Number of supports
2	0.0276	2^5
3	0.2923	2^7
4	4.7412	2^9
5	74.5827	2^{11}
6	1215.0815	2^{13}
7	21347.9378	2^{15}

Table 3: For a given basis, time (in second) to obtain all the bent functions of $2k$ variables for different values of k

and for $i = 1, 2, \dots, 28$ and $j = 1, 2, \dots, 10$, we consider the new bases

$$\mathcal{V}_{i,j} = \left\{ P_j \mathbf{u}_1^{(i)}, P_j \mathbf{u}_2^{(i)}; P_j \mathbf{u}_3^{(i)}, P_j \mathbf{u}_4^{(i)} \right\}$$

where $\mathcal{U}_i = \{\mathbf{u}_1^{(i)}, \mathbf{u}_2^{(i)}; \mathbf{u}_3^{(i)}, \mathbf{u}_4^{(i)}\}$, then, the bent functions provided by the bases $\mathcal{V}_{i,j}$ and $\mathcal{U}_i$, for $j = 1, 2, \dots, 10$, are the same. Note that not all the bases $\mathcal{V}_{i,j}$ have the same properties that the basis $\mathcal{U}_i$ in the sense that $\{P_j \mathbf{u}_1^{(i)}, P_j \mathbf{u}_2^{(i)}\}$ and $\{P_j \mathbf{u}_3^{(i)}, P_j \mathbf{u}_4^{(i)}\}$ are not necessarily Gauss-Jordan bases of cardinality 2 and that not necessarily $P_j \mathbf{u}_1^{(i)} > P_j \mathbf{u}_3^{(i)}$ (lexicographical order), but after some elementary operations we can obtain a basis $\mathcal{V}'_{i,j}$ with such properties.

For $k = 3$ it is not possible to obtain a complete classification similar to the above classification for $k = 2$ because the number of bases satisfying the necessary conditions is 15 554 560.

Finally, we summarize in Table 3, the time required (in seconds) to obtain, on a standard personal computer (PC), the 2^{2k+1} supports of bent functions of $2k$ variables from the same basis of $\mathbb{F}_2^n$ using the iterative procedure described in Section 3. It is worth mentioning that the average time taken to obtain randomly the supports of 100 bent functions of 4 variables (that is, for $k = 2$) was 6.56 seconds; however, after more than 250 hours of computation, we did not obtain (randomly) any support corresponding to a bent function of 6 variables (that is, for $k = 3$).

5 Conclusions

In this paper we use a basis of $\mathbb{F}_2^{2k}$ to construct 2^{2k+1} sets in $\mathbb{F}_2^{2k}$ that are the supports of bent functions of $2k$ variables. Half of the bent functions obtained are the complementary functions of the other half.

We give some examples to point out that different bases can provide the same bent functions and we give a complete classification for the case $k = 2$; that is, for the bent

functions of 4 variables. However, we could not establish, for $k > 2$, any relationship between the bases that provide the same bent functions. Therefore, further work is needed to determine under what conditions two different bases provide the same bent functions.

References

- [1] C. M. ADAMS. Constructing symmetric ciphers using the CAST design procedure. *Designs, Codes and Cryptography*, **12**: 283–316 (1997).
- [2] 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*, **51(3)**: 1182–1189 (2005).
- [3] A. BRAEKEN, V. NIKOV, S. NIKOVA and B. PRENEEL. On Boolean functions with generalized cryptographic properties. In A. CANTEAUT and K. VISWANATHAN (editors), *Progress in Cryptology – INDOCRYPT 2004*, volume 3348 of *Lecture Notes in Computer Science*, pages 120–135. Springer-Verlag, Berlin, 2004.
- [4] A. CANTEAUT, M. DAUM, H. DOBBERTIN and G. LEANDER. Finding nonnormal bent functions. *Discrete Applied Mathematics*, **154**: 202–218 (2006).
- [5] C. CARLET and Y. TARANNIKOV. Covering sequences of Boolean functions and their cryptographic significance. *Designs, Codes and Cryptography*, **25**: 263–279 (2002).
- [6] C. CARLET. On the secondary constructions of resilient and bent functions. *Progress in Computer Science and Applied Logic*, **23**: 3–28 (2004).
- [7] C. CARLET and P. GUILLOT. A characterization of binary bent functions. *Journal of Combinatorial Theory (Series A)*, **76**: 328–335 (1996).
- [8] D. K. CHANG. Binary bent sequences of order 64. *Utilitas Mathematica*, **52**: 141–151 (1997).
- [9] J.-J. CLIMENT, F. J. GARCÍA and V. REQUENA. Computing the degree of a Boolean function from its support. In C.-C. CHAO and R. KOHNO (editors), *Proceedings of the 2010 International Symposium on Information Theory and its Applications (ISITA2010)*, pages 123–128. IEEE Press, 2010.
- [10] 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.

- [11] J. F. DILLON. *Elementary Hadamard Difference Sets*. PhD Thesis, University of Maryland, 1974.
- [12] H. DOBBERTIN. Construction of bent functions and balanced Boolean functions with high nonlinearity. In B. PRENEEL (editor), *Fast Software Encryption*, volume 1008 of *Lecture Notes in Computer Science*, pages 61–74. Springer-Verlag, Berlin, 1995.
- [13] K. C. GUPTA and P. SARKAR. Improved construction of nonlinear resilient S-boxes. *IEEE Transactions on Information Theory*, **51(1)**: 339–348 (2005).
- [14] 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).
- [15] K. KUROSAWA, T. IWATA and T. YOSHIWARA. New covering radius of Reed-Muller codes for t -resilient functions. *IEEE Transactions on Information Theory*, **50(3)**: 468–475 (2004).
- [16] P. LANGEVIN and G. LEANDER. Counting all bent functions in dimension eight 99270589265934370305785861242880. *Designs, Codes and Cryptography*, **59**: 193–201 (2011).
- [17] 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).
- [18] F. J. MACWILLIAMS and N. J. A. SLOANE. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 6th edition, 1988.
- [19] M. MATSUI. Linear cryptanalysis method for DES cipher. In T. HELLESETH (editor), *Advances in Cryptology – EUROCRYPT ’93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, Berlin, 1994.
- [20] R. L. MCFARLAND. A family of difference sets in non-cyclic groups. *Journal of Combinatorial Theory (Series A)*, **15**: 1–10 (1973).
- [21] W. MEIER and O. STAFFELBACH. Nonlinearity criteria for cryptographic functions. In 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.
- [22] K. NYBERG. Perfect nonlinear S-boxes. In D. W. DAVIES (editor), *Advances in Cryptology – EUROCRYPT ’91*, volume 547 of *Lecture Notes in Computer Science*, pages 378–386. Springer-Verlag, Berlin, 1991.

- [23] D. OLEJÁR and M. STANEK. On cryptographic properties of random Boolean functions. *Journal of Universal Computer Science*, **4(8)**: 705–717 (1998).
- [24] E. PASALIC and T. JOHANSSON. Further results on the relation between nonlinearity and resiliency for Boolean functions. In M. WALKER (editor), *Cryptography and Coding*, volume 1746 of *Lecture Notes in Computer Science*, pages 35–44. Springer-Verlag, Berlin, 1999.
- [25] B. PRENEEL. *Analysis and Design of Cryptographic Hash Functions*. PhD Thesis, Katholieke University Leuven, January 1993.
- [26] O. S. ROTH AUS. On “bent” functions. *Journal of Combinatorial Theory (Series A)*, **20**: 300–305 (1976).
- [27] P. SARKAR and S. 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.
- [28] J. SEBERRY and X.-M. ZHANG. Constructions of bent functions from two known bent functions. *Australasian Journal of Combinatorics*, **9**: 21–35 (1994).
- [29] J. SEBERRY, X.-M. ZHANG and Y. ZHENG. Nonlinearity and propagation characteristics of balanced Boolean functions. *Information and Computation*, **119**: 1–13 (1995).
- [30] S. A. VANSTONE and P. C. VAN OORSCHOT. *An Introduction to Error Correcting Codes with Applications*. Kluwer Academic Publishers, Boston, MA, 2000.
- [31] R. YARLAGADDA and J. E. HERSHEY. Analysis and synthesis of bent sequences. *IEEE Proceedings*, **136(2)**: 112–123 (1989).
- [32] N. Y. YU and G. GONG. Constructions of quadratic bent functions in polynomial forms. *IEEE Transactions on Information Theory*, **52(7)**: 3291–3299 (2006).