**manuscript No.**
(will be inserted by the editor)

# Bent functions construction using extended Maiorana-McFarland's class

**Juan Carlos Ku-Cauich · Javier Diaz-Vargas · Sara Mandujano-Velazquez**

Received: August 20, 2024/ Accepted: date

**Abstract** We use the extended Maiorana-McFarland's class to obtain bent functions. Additionally, we obtain balanced functions when we restrict its domain to vectors with even Hamming weight, i.e., an equal number of pre-images for 0 and 1. We have defined a bent function on an affine space to achieve this. Additionally, we demonstrate that the bent functions, in general, are balanced by restricting them to vectors of even Hamming or odd Hamming weight. Since that we have all the necessary tools, we present an algorithm for generating new bent functions of any dimension using the Maiorana-McFarland approach multiple times.

**Kewords**: Bent functions, Maiorana-McFarland, Balancedness, affine spaces

## 1 Introduction

The boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ are essential in cryptography and coding theory. They have various properties, such as non-linearity, balancedness, low auto-correlation, and high algebraic immunity. The search space of these functions is very large, $2^{2^n}$, and different methods exist to find them: random search, algebraic, and heuristic methods, see for example [1], [2].

We are interested in the non-linearity, defined as the distance between a boolean function and the set of affine functions. The boolean functions with

The authors acknowledge the support of Mexican Conacyt

Juan Carlos Ku-Cauich
Computer Science, CINVESTAV-IPN, Mexico City, Mexico, E-mail: jcku@cs.cinvestav.mx

Javier Diaz-Vargas
Facultad de Matemáticas, UADY, Mérida Yucatán, Mexico, E-mail: javier.diaz@correo.uady.mx

Sara Mandujano-Velazquez
ESFM, IPN, Mexico City, Mexico, E-mail: smandujanov2000@alumno.ipn.mx

maximum non-linearity are called bent functions, and this name was introduced by Rothaus in 1976 [3]. These functions have been classified and constructed in many ways, such as the Maiorana-McFarland class [4] and Rothaus [3]. In others works, a boolean function's balancedness is restricted to specific subsets of its domain depending of the Hamming weight [5]. We analyse the balancedness when the domain of a bent function is restricted to vectors of even Hamming weight or vectors of odd Hamming weight.

In this work, we use a particular case of the extended Maiorana-McFarland class [4]: given a function $\phi(y) : \mathbb{F}_2^s \to \mathbb{F}_2$ such that $\phi^{-1}(a)$ is an affine space of dimension $s-1$ and a function $g_e(y) : \mathbb{F}_2^s \to \mathbb{F}_2$, such that $g_{e|\phi^{-1}(a)}$ is a bent function, then $f : \mathbb{F}_2^{s+1} \to \mathbb{F}_2$ is a bent function, where $x \mapsto x \cdot \phi(y) \oplus g_e(y)$.

We proceed as follows: in Section 2, preliminaries are remembered. Then, in Section 3, we demonstrate that a bent function is balanced when we restrict its domain to the set of vectors of even Hamming weight or the set of odd Hamming weight. This process shows a distribution of the number of preimages of 0 and 1 in all the domain of the bent function. Finally, in Section 4, we remember and give brief proofs about bent functions on affine functions. Subsequently, we define the necessary elements $\phi : \mathbb{F}_2^s \to \mathbb{F}_2$, $g_e : \mathbb{F}_2^s \to \mathbb{F}_2$, a previous bent function $g : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$, and the affine spaces to construct the new Maiorana bent function $f : \mathbb{F}_2^{1+s} \to \mathbb{F}_2$. Furthermore, we give an algorithm to find a new bent function of any dimension, using Theorem 10 repeatedly.

Additionally, boolean functions $g_{e_0}$ and $g_{e_1}$ on affine spaces of dimension $s-1$ are defined and demonstrated to be bent functions. Even more, we see that uniquely $f_{|\{\text{even Hamming weight}\}}$ is balanced. Besides, the balancedness of $g_{e_0}$, $g_{e_1}$, and $f \oplus l_a$ is analysed, where $l_a$ is a linear function defined by $l_a(x) = a \cdot x$, $a, x \in \mathbb{F}_2^{1+s}$.

## 2 Background

Definitions and results about boolean functions, particularly bent functions, are recalled in this section. These can be found, for example, in [6], [7], [8].

**Definition 1** A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called a **boolean function**. $\mathcal{B}_n$ is the set of all boolean functions with domain $\mathbb{F}_2^n$.

All boolean functions $f \in \mathcal{B}_n$ have an **algebraic normal form** (ANF):

$$f(x) = \bigoplus\nolimits_{u \in \mathbb{F}_2^n} a_u x^u,$$

$a_u \in \mathbb{F}_2$, $x^u = x_1^{u_1} \cdots x_n^{u_n}$, $\quad x = (x_1, \ldots, x_n), u = (u_1, \ldots, u_n)$.

*Example 1* The boolean function $f(x) \in \mathcal{B}_3$, $\quad f(x_1, x_2, x_3) = 1 \oplus x_1 x_2 \oplus x_1 x_2 x_3$ is in its ANF.

**Theorem 1** *Let $f \in \mathcal{B}_n$. Then,*

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u,$$

$a_u = \oplus_{x \leq u} f(x)$, $x \leq u \Leftrightarrow x_i \leq u_i$, $x = (x_1, \ldots, x_n)$, $u = (u_1, \ldots, u_n)$.

**Definition 2** The set of all **affine** boolean functions with domain $\mathbb{F}_2^n$, denoted by $\mathcal{A}_n$, is defined as

$$\mathcal{A}_n := \{a \cdot x \oplus a_0 \mid a, x \in \mathbb{F}_2^n,\ a_0 \in \mathbb{F}_2\},$$

where $\cdot$ is the dot product.

Note that the number of affine functions is $2^{n+1}$ and the number of linear functions is $2^n$.

**Definition 3** The **non-linearity** of a boolean function $f \in \mathcal{B}_n$ is defined as the Hamming distance between $f$ and the set of affine functions:

$$Nl(f) := \text{ mín }_{g \in \mathcal{A}_n} d_H(f, g).$$

The boolean functions with maximum non-linearity are called **bent** functions.

We define the following function to characterize the non-linearity:

**Definition 4** The **Walsh-Hadamard Transform** of a boolean function $f \in \mathcal{B}_n$ is defined as

$$\widehat{\mathcal{W}}_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x}, \quad a \in \mathbb{F}_2^n.$$

**Theorem 2** *The non-linearity of the boolean function $f \in \mathcal{B}_n$ is characterized as*

$$Nl(f) = 2^{n-1} - \frac{1}{2} max_{a \in \mathbb{F}_2^n} |\widehat{\mathcal{W}}_f(a)|.$$

**Theorem 3** *If $f \in \mathcal{B}_n$ is a bent function, then $\widehat{\mathcal{W}}_f(a) = \pm 2^{n/2}$ for all $a \in \mathbb{F}_2^n$.*

The bent functions have non-linearity $2^{n-1} - 2^{n/2-1}$.

## 3 Bent functions, balanced on a restricted domain

We will need bent functions over an affine space to find new bent functions when using the Extended Maiorana-McFarland class [4]. Following this idea, given a bent function with the traditional definition, we want to find a bent function over an affine space with the same dimension. For that purpose, the main characteristic we need is that for all bent functions $f \in \mathcal{B}_n$, $f_{|\{x\in\mathbb{F}_2^n | w_H(x)\ even\}}$ balanced or $f_{|\{x\in\mathbb{F}_2^n | w_H(x)\ odd\}}$ balanced. In this section, we prove this claim.

Let $\mathcal{A} := \{x \in \mathbb{F}_2^n | w_H(x)\ even\}$ and $\mathcal{B} := \{x \in \mathbb{F}_2^n | w_H(x)\ odd\}$. As far as we have searched, we have not yet found a result similar to the following.

**Theorem 4** *Every bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $n \geq 2$, $n$ even, is such that $f_{|\mathcal{A}}$ is balanced or $f_{|\mathcal{B}}$ is balanced.*

*Proof* Let $f$ be a bent function, $l'_a$ an affine function, and $l_{\bar{0}}(x) := 0$, $l_{\bar{1}}(x) := x_1 \oplus \cdots \oplus x_n$, $x = (x_1, \ldots, x_n)$, linear functions. Observe that, $w_H(f \oplus l'_a) = 2^{n-1} - 2^{\frac{n-2}{2}}$ or $w_H(f \oplus l'_a) = 2^{n-1} + 2^{\frac{n-2}{2}}$. Additionally, notice that $l_{\bar{1}}(\mathcal{A}) = \{0\}$ and $l_{\bar{1}}(\mathcal{B}) = \{1\}$.

First, we assume that $n \geq 6$.

**Case 1**. If $f_{|\mathcal{A}}$ has $c$ images 1, $0 \leq c \leq 2^{\frac{n-2}{2}}$.

**Case 1a**. $f_{|\mathcal{B}}$ has $2^{n-1} - (2^{\frac{n-2}{2}} + c)$ images 1. Then, $(f \oplus l_{\bar{1}})(\mathcal{A})$ has $c$ images 1 and $(f \oplus l_{\bar{1}})(\mathcal{B})$ has $2^{\frac{n-2}{2}} + c$ images 1.

**Case 1a1** $(f \oplus l_{\bar{1}})$ has $c + (2^{\frac{n-2}{2}} + c) = 2^{n-1} - 2^{\frac{n-2}{2}}$ images 1. Therefore, $c = 2^{n-2} - 2^{\frac{n-2}{2}}$ and $f_{|\mathcal{B}}$ is balanced. But since $n \geq 6$, then $2^{\frac{n-2}{2}} < c$. So, we have a contradiction.

**Case 1a2** $(f \oplus l_{\bar{1}})$ has $c + (2^{\frac{n-2}{2}} + c) = 2^{n-1} + 2^{\frac{n-2}{2}}$ images 1. Therefore, $c = 2^{n-2}$. Then, $2^{\frac{n-2}{2}} < c$. So, we have a contradiction.

**Case 1b** $f_{|\mathcal{B}}$ has $2^{n-1} + (2^{\frac{n-2}{2}} - c)$ images 1. Hence, $c = 2^{\frac{n-2}{2}}$. Then, $(f \oplus l_{\bar{1}})(\mathcal{A})$ has $2^{\frac{n-2}{2}}$ images 1 and $(f \oplus l_{\bar{1}})(\mathcal{B})$ has zero images 1. Therefore, $(f \oplus l_{\bar{1}})$ is not a bent function when $n \geq 6$; consequently, $f$ is not a bent function.

**Case 2**. If $f_{|\mathcal{A}}$ has $c + 2^{\frac{n-2}{2}}$ images 1, $0 < c \leq 2^{n-2} - 2^{\frac{n-2}{2}}$.

**Case 2a**. $f_{|\mathcal{B}}$ has $2^{n-2} + (2^{n-2} - 2 \cdot 2^{\frac{n-2}{2}} - c)$ images 1. $(f \oplus l_{\bar{1}})(\mathcal{A})$ has $c + 2^{\frac{n-2}{2}}$ images 1 and $(f \oplus l_{\bar{1}})(\mathcal{B})$ has $2 \cdot 2^{\frac{n-2}{2}} + c$ images 1.

**Case 2a1** $(f \oplus l_{\bar{1}})$ has $c + 2^{\frac{n-2}{2}} + 2 \cdot 2^{\frac{n-2}{2}} + c = 2^{n-1} - 2^{\frac{n-2}{2}}$ images 1. Therefore, $c = 2^{n-2} - 2^{\frac{n}{2}}$. Then, $f_{|\mathcal{B}}$ has $2^{n-2}$ images 1. Hence, $f_{|\mathcal{B}}$ is balanced.

**Case 2a2** $(f \oplus l_{\bar{1}})$ has $c + 2^{\frac{n-2}{2}} + 2 \cdot 2^{\frac{n-2}{2}} + c = 2^{n-1} + 2^{\frac{n-2}{2}}$ images 1. Therefore, $c = 2^{n-2} - 2^{\frac{n-2}{2}}$. Then, $f_{|\mathcal{A}}$ has $2^{n-2}$ images 1. Hence, $f_{|\mathcal{A}}$ is balanced.

**Case 2b** $f_{|\mathcal{B}}$ has $2^{n-2} + (2^{n-2} - c)$ images 1. Hence, $(f \oplus l_{\bar{1}})(\mathcal{A})$ has $c + 2^{\frac{n-2}{2}}$ images 1 and $(f \oplus l_{\bar{1}})(\mathcal{B})$ has $c$ images 1.

**Case 2b1** $(f \oplus l_{\bar{1}})$ has $c + (c + 2^{\frac{n-2}{2}}) = 2^{n-1} - 2^{\frac{n-2}{2}}$ images 1. Therefore, $c = 2^{n-2} - 2^{\frac{n-2}{2}}$. Hence, $f_{|\mathcal{A}}$ is balanced.

**Case 2b2** $(f \oplus l_{\bar{1}})$ has $c + (c + 2^{\frac{n-2}{2}}) = 2^{n-1} + 2^{\frac{n-2}{2}}$ images 1. Therefore, $c = 2^{n-2}$. But, $0 < c \leq 2^{n-2} - 2^{\frac{n-2}{2}}$. Thus, we have a contradiction.

When $f_{|\mathcal{A}}$ has more than $2^{n-2}$ images 1, the proof is similar to the previous cases, but we use the number of images 0 of $f_{|\mathcal{A}}$ instead of number of images 1 of $f_{|\mathcal{A}}$. Also, we use the fact that $w_H(\bar{1} \oplus f) = 2^{n-1} - 2^{\frac{n-2}{2}}$ or $w_H(\bar{1} \oplus f) = 2^{n-1} + 2^{\frac{n-2}{2}}$. That means the number of zeros of $f$ is $2^{n-1} - 2^{\frac{n-2}{2}}$ or $2^{n-1} + 2^{\frac{n-2}{2}}$.

In all the cases where $f_{|\mathcal{A}}$ is not balanced and $f_{|\mathcal{B}}$ is not balanced, we obtain a contradiction. Therefore, if $f$ is a bent function, it must satisfy, $f_{|\mathcal{A}}$ is balanced or $f_{|\mathcal{B}}$ is balanced.

The case $n = 2$ is direct and the case $n = 4$ only need light observations.

□

Due to the previous result, the cardinality distribution of the preimages of a bent function is as follows:

*Remark 1* Let $g : \mathbb{F}_2^n \to \mathbb{F}_2$ be a bent function such that $g_{|\mathcal{A}}$ is balanced.

(a) If $\widehat{\mathcal{W}_g}(\bar{0}) = 2^{\frac{n}{2}}$, then
$|(g)^{-1}_{|\mathcal{A}}(0)| = 2^{n-2}$
$|(g)^{-1}_{|\mathcal{A}}(1)| = 2^{n-2}$
$|(g)^{-1}_{|\mathcal{B}}(0)| = 2^{n-2} + 2^{\frac{n-2}{2}}$.
$|(g)^{-1}_{|\mathcal{B}}(1)| = 2^{n-2} - 2^{\frac{n-2}{2}}$.

(b) If $\widehat{\mathcal{W}_g}(\bar{0}) = -2^{\frac{n}{2}}$, then
$|(g)^{-1}_{|\mathcal{A}}(0)| = 2^{n-2}$
$|(g)^{-1}_{|\mathcal{A}}(1)| = 2^{n-2}$
$|(g)^{-1}_{|\mathcal{B}}(0)| = 2^{n-2} - 2^{\frac{n-2}{2}}$.
$|(g)^{-1}_{|\mathcal{B}}(1)| = 2^{n-2} + 2^{\frac{n-2}{2}}$.

We obtain a similar observation if $g_{|\mathcal{B}}$ is balanced.

## 4 Construction of a particular family from the extended Maiorana-McFarland class

We extend the definition of bent functions with domain $\mathbb{F}_2^n$ to bent functions with domain an affine subspace, as suggested in the extended Maiorana-McFarland's Proposition 1 [4].

**Definition 5** A function $f : \mathcal{C} \to \mathbb{F}_2$, $\mathcal{C} \subseteq \mathbb{F}_2^n$ an affine space, $m \leq n$, $\dim \mathcal{C} = m$, is bent if $Nl(f) := d_H(f, \mathcal{A}_n)$ is maximum.

The following results are easy to obtain; the demonstrations are similar to the traditional boolean function proofs.

**Theorem 5** *Let a function $f : \mathcal{C} \to \mathbb{F}_2$. Then*

$$Nl(f) = 2^{m-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |\widehat{\mathcal{W}}_f(a)|,$$

*where $\widehat{\mathcal{W}}_f(a) := \sum_{x \in \mathcal{C}} (-1)^{f(x) \oplus a \cdot x}$.*

*Proof* We can see that, for all $a \in \mathbb{F}_2^n$,

$$\widehat{\mathcal{W}}_f(a) = 2^m - 2d_H(f, a \cdot x) \text{ and } -\widehat{\mathcal{W}}_f(a) = 2^m - 2d_H(f, a \cdot x \oplus 1).$$

Resolving $d_H$ on the left side, we obtain the result in both cases.

□

**Theorem 6** *(Parseval's equation) Let $f : \mathcal{C} \to \mathbb{F}_2$. Then,*

$$\sum_{a \in \mathbb{F}_2^n} \widehat{\mathcal{W}}_f^2(a) = 2^{m+n}.$$

*Proof* Resolving,

$$\sum_{a \in \mathbb{F}_2^n} \widehat{\mathcal{W}}_f(a)\widehat{\mathcal{W}}_f(a) = \sum_{x,y \in \mathcal{C}} (-1)^{f(x)+f(y)} \sum_{a \in \mathbb{F}_2^n} (-1)^{a \cdot (x+y)} = 2^{m+n}.$$

□

**Theorem 7** *If $f : \mathcal{C} \subset \mathbb{F}_2^n \to \mathbb{F}_2$, $\dim \mathcal{C} = m$, is a bent function, then $\widehat{\mathcal{W}}_f(a) = \pm 2^{m/2}$ for all $a \in \mathbb{F}_2^n$.*

*Proof* If $|\widehat{\mathcal{W}}_f(b)| < 2^{m/2}$, then, by Parseval's equation exists $b' \in \mathbb{F}_2^n$ such that $|\widehat{\mathcal{W}}_f(b')| > 2^{m/2}$. Hence, by Theorem 5, the non-linearity of $f$ is the greatest when $\widehat{\mathcal{W}}_f(a) = \pm 2^{m/2}$ for all $a \in \mathbb{F}_2^n$.

□

The following theorem corresponds to a class of bent functions known as the extended **Maiorana-McFarland** class.

**Theorem 8** *[4] Let the function $\phi(y) : \mathbb{F}_2^s \to \mathbb{F}_2^r$ such that for all $a \in \mathbb{F}_2^r$, $\phi^{-1}(a)$ is an affine space of dimension $s - r$. Also, let a function $g_e(y) : \mathbb{F}_2^s \to \mathbb{F}_2$, where $g_{e|\phi^{-1}(a)}$ is a bent function. Then, the function $f : \mathbb{F}_2^{r+s} \to \mathbb{F}_2$, $(x, y) \mapsto x \cdot \phi(y) \oplus g_e(y)$, $x \in \mathbb{F}_2^r$, is bent.*

In this work, we consider $\mathbb{F}_2^s$ an array, where each element is a row, and we order the elements in a particular way:

Let $\mathcal{C}_0 := \{\bar{x} \in \mathbb{F}_2^s \mid w_H(\bar{x}) \text{ even}\}$ and $\mathcal{C}_1 := \{\bar{x} \in \mathbb{F}_2^s \mid w_H(\bar{x}) \text{ odd}\}$. We can write,

$$\mathbb{F}_2^s = \begin{array}{c} \mathcal{C}_0 \\ -- \\ \mathcal{C}_1 \end{array} = \begin{array}{ccc} \mathcal{C}_0' & \bar{0} \\ \mathcal{C}_1' & \bar{1} \\ - & - & - \\ \mathcal{C}_0' & \bar{1} \\ \mathcal{C}_1' & \bar{0} \end{array},$$

where $\bar{0} = \begin{array}{c} 0 \\ \vdots \\ 0 \end{array}$ and $\bar{1} = \begin{array}{c} 1 \\ \vdots \\ 1 \end{array}$ are $2^{s-2} \times 1$ arrays, and

$\mathcal{C}_0' := \{x \in \mathbb{F}_2^{s-1} \mid w_H(x) \text{ even}\}$, $\mathcal{C}_1' := \{x \in \mathbb{F}_2^{s-1} \mid w_H(x) \text{ odd}\}$.

Observe that $\mathcal{C}_0$ is a linear code of dimension $s-1$ and $\mathcal{C}_1$ is an affine space, such that $\bar{b} \oplus \mathcal{C}_0 = \mathcal{C}_1$ for any $\bar{b} \in \mathbb{F}_2^s$ with odd Hamming weight.

**From now on**, according to Theorem 8 (particular case $r = 1$) we consider a bent function $g : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$, and we define $\phi : \mathbb{F}_2^s \to \mathbb{F}_2$ and $g_e : \mathbb{F}_2^s \to \mathbb{F}_2$ as

$\phi^{-1}(0) = \mathcal{C}_0$ and $\phi^{-1}(1) = \mathcal{C}_1$,

$g_{e|\mathcal{C}_0} := g_{e_0}$ and $g_{e|\mathcal{C}_1} := g_{e_1}$ so that,

$g_{e_0} : \mathcal{C}_0 \to \mathbb{F}_2$, $g_{e_0}(x|x_s) := g(x)$, $x \in \mathbb{F}_2^{s-1}$, $x_s \in \mathbb{F}_2$,

$g_{e_1} : \mathcal{C}_1 \to \mathbb{F}_2$, $g_{e_1}(x|x_s) := g(x)$, $x \in \mathbb{F}_2^{s-1}$, $x_s \in \mathbb{F}_2$.

*Remark 2* In $\mathcal{C}_0$, if $x \in \mathbb{F}_2^{s-1}$ has even Hamming weight, then $x_s$ is 0. If $x \in \mathbb{F}_2^{s-1}$ has odd Hamming weight, then $x_s \in \mathbb{F}_2$ is 1. Similarly in $\mathcal{C}_1$.

In the proof of the following theorem, the restricted balancedness of a bent function is essential.

Using the above notation.

**Theorem 9** *Let $g : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$ be a bent function. Then, $g_{e_0} : \mathcal{C}_0 \to \mathbb{F}_2$ is a bent function and $g_{e_1} : \mathcal{C}_1 \to \mathbb{F}_2$ is a bent function.*

*Proof* Let $\bar{b} = (b, b_s) \in \mathbb{F}_2^s$ and $\bar{x} = (x, x_s) \in \mathcal{C}_0$, $b = (b_1, \ldots, b_{s-1})$ and $x = (x_1, \ldots, x_{s-1})$.

$$\widehat{\mathcal{W}}_{g_{e_0}}(\bar{b}) = \sum_{\bar{x} \in \mathcal{C}_0} (-1)^{g_{e_0}(\bar{x}) + \bar{x} \cdot \bar{b}} = \sum_{\bar{x} \in \mathcal{C}_0} (-1)^{g_{e_0}(x, x_s) + x \cdot b + x_s b_s}.$$

If $b_s = 0$,

$$\widehat{\mathcal{W}}_{g_{e_0}}(\bar{b}) = \sum_{x \in \mathbb{F}_2^{s-1}} (-1)^{g(x) + x \cdot b} = \widehat{\mathcal{W}}_g(b).$$

If $b_s = 1$,

$$\begin{aligned}\widehat{\mathcal{W}}_{g_{e_0}}(\bar{b}) &= \sum_{\bar{x}\in\mathcal{C}_0}(-1)^{g_{e_0}(x,0)+x\cdot b} + \sum_{\bar{x}\in\mathcal{C}_0}(-1)^{g_{e_0}(x,1)+x\cdot b+1} \\ &= \sum_{x\in\mathcal{C}_0'}(-1)^{g(x)+x\cdot b} + (-1)\sum_{x\in\mathcal{C}_1'}(-1)^{g(x)+x\cdot b}.\end{aligned}$$

The last equality, by Remark 2.

If $g_{|\mathcal{C}_0'}$ is balanced, $\widehat{\mathcal{W}}_{g_{e_0}}(\bar{b}) = -\widehat{\mathcal{W}}_g(b)$.
If $g_{|\mathcal{C}_1'}$ is balanced, $\widehat{\mathcal{W}}_{g_{e_0}}(\bar{b}) = \widehat{\mathcal{W}}_g(b)$.

In both cases, since $g$ is a bent function, $g_{e_0}$ is a bent function.

Proceeding similarly, $g_{e_1} : \mathcal{C}_1 \to \mathbb{F}_2$ is a bent function.

□

**Corollary 1** *Let $g : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$ be a bent function. For all $a \in \mathbb{F}_2^{s-1}$ :*

1. $\widehat{\mathcal{W}}_g(a) = \widehat{\mathcal{W}}_{g_{e_0}}(a,0) = \widehat{\mathcal{W}}_{g_{e_1}}(a,0)$.
2. *If $g_{|\mathcal{C}_0'}$ is balanced,*
   $\widehat{\mathcal{W}}_g(a) = 2^{\frac{s-1}{2}} \Leftrightarrow \widehat{\mathcal{W}}_{g_{e_0}}(a,1) = -2^{\frac{s-1}{2}}$ *and* $\widehat{\mathcal{W}}_{g_{e_1}}(a,1) = 2^{\frac{s-1}{2}}$.
3. *If $g_{|\mathcal{C}_1'}$ is balanced,*
   $\widehat{\mathcal{W}}_g(a) = -2^{\frac{s-1}{2}} \Leftrightarrow \widehat{\mathcal{W}}_{g_{e_0}}(a,1) = 2^{\frac{s-1}{2}}$ *and* $\widehat{\mathcal{W}}_{g_{e_1}}(a,1) = -2^{\frac{s-1}{2}}$.

□

Like $g$, the functions $g_{e_0}$ and $g_{e_1}$ are balanced when their domain is restricted. The balancedness is maintained even if we add a linear function.

**Proposition 1** *Let $g : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$ be a bent function. Then, for all $\bar{a} \in \mathbb{F}_2^s$, $g_{e_0} \oplus l_{\bar{a}} : \mathcal{C}_0 \to \mathbb{F}_2$ is a bent function, and it is balanced restricted to $\mathcal{C}_0'|\bar{0}$, or it is balanced restricted to $\mathcal{C}_1'|\bar{1}$. Also, $g_{e_1} \oplus l_{\bar{a}} : \mathcal{C}_1 \to \mathbb{F}_2$ is a bent function and balanced restricted to $\mathcal{C}_0'|\bar{1}$ or to $\mathcal{C}_1'|\bar{0}$.*

*Proof* Let us see first that the desired functions are bent:

Without loss of generality, we prove that $g_{e_0} \oplus l_{\bar{a}}$ is a bent function on $\mathcal{C}_0$ for all $\bar{a} \in \mathbb{F}_2^s$. We claim that $\widehat{\mathcal{W}}_{g_{e_0}}(\bar{b}) = \pm 2^{\frac{s-1}{2}}$ for all $\bar{b} \in \mathbb{F}_2^s$, and therefore we obtain the bentness. We know that the relation is true since $g : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$ is a bent function and the linearity properties of $l_{\bar{a}}$.

Similarly, we can see that $g_{e_1} \oplus l_{\bar{a}}$ is bent on $\mathcal{C}_1$.

Now, we prove the balancedness:

Without loss of generality, suppose that $g \oplus l_a : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$, $a \in \mathbb{F}_2^{s-1}$, is balanced restricted to $\mathcal{C}_0'$ (since $g \oplus l_a$ is a bent function). Therefore, $g_{e_0} \oplus l_{(a,a_s)}$ is balanced restricted to $\mathcal{C}_0'|\bar{0}$, and $g_{e_1} \oplus l_{(a,a_s)}$ is balanced restricted to $\mathcal{C}_0'|\bar{1}$, $a_s \in \mathbb{F}_2$ (since $a_s$ is a constant and the images of $g$, $g_{e_0}$, and $g_{e_1}$ are equal).

It is solved in a similar way, if the balancedness restricted to $\mathcal{C}_1'$ is considered.

□

In particular, if $g_{|\mathcal{C}_0'}$ is balanced, $g_{e_0}$ is balanced restricted to $\mathcal{C}_0'|\bar{0}$ and $g_{e_1}$ is balanced restricted to $\mathcal{C}_0'|\bar{1}$. If $g_{|\mathcal{C}_1'}$ is balanced, then $g_{e_0}$ is balanced restricted to $\mathcal{C}_1'|\bar{1}$ and $g_{e_1}$ is balanced restricted to $\mathcal{C}_1'|\bar{0}$.

Now, we are ready to use the extended Maiorana-McFarland, in the particular case where $r = 1$.

**Theorem 10** *Let $g : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$ be a bent function, $g_e$, and $\phi$ defined as above. Then, the function*

$$f : \mathbb{F}_2^{1+s} \to \mathbb{F}_2,\ (x_0, \bar{x}) \mapsto x_0\phi(\bar{x}) \oplus g_e(\bar{x}),\ x_0 \in \mathbb{F}_2,\ \bar{x} \in \mathbb{F}_2^s,$$

*is a bent function and $f_{|\{(x_0,\bar{x})|w_H((x_0,\bar{x}))\ even\}}$ is balanced.*

*Proof* Since $\phi$ y $g_e$ satisfy the conditions of Theorem 8, then $f$ is a bent function.

Let us see the balancedness of $f$. We have four cases. Without loss of generality, consider case $g_{|\mathcal{C}_0'}$ be balanced and $\widehat{\mathcal{W}_g}(\bar{0}) = 2^{\frac{s-1}{2}}$.

Let $\bar{x} = (x, x_s)$, $x \in \mathbb{F}_2^{s-1}$, $x_s \in \mathbb{F}_2$. The elements with even Hamming weight in $\mathbb{F}_2^{s+1}$ are in the following cases:

**Case 1**. Let $x_0 = 0$, $x_s = 0$ and $x \in \mathcal{C}_0'$. Then,
$f(0, x, 0) = g_{e_0}(x, 0) = 0$, $2^{s-3}$ times.

**Case 2**. Let $x_0 = 0$, $x_s = 1$ and $x \in \mathcal{C}_1'$. Then,
$f(0, x, 1) = g_{e_0}(x, 1) = 0$, $2^{s-3} + 2^{\frac{s-3}{2}}$ times.

**Case 3**. Let $x = 1$, $x_s = 0$ and $x \in \mathcal{C}_1'$. Then,
$f(1, x, 1) = 1 \oplus g_{e_1}(x, 0) = 0$, $2^{s-3} - 2^{\frac{s-3}{2}}$ times.

**Case 4**. Let $x_0 = 1$, $x_s = 1$ and $x \in \mathcal{C}_0'$. Then,
$f(1, x, 1) = 1 \oplus g_{e_1}(x, 1) = 0$, $2^{s-3}$ times.

Hence, adding the four cases,

$$|f^{-1}_{|\{(x_0,\bar{x})\in\mathbb{F}_2^{s+1}|w_H(x_0,\bar{x})\ even\}}(0)| = 2^{s-1}.$$

Therefore, $f_{|\{(x_0,\bar{x})|w_H((x_0,\bar{x}))\ even\}}$ is balanced.

Resolving similarly, we obtained the same result in the other cases.

□

Given a balanced bent function when we restrict to vectors of even Hamming weight (using Maiorana-McFarland), we want to have a balanced bent function if we add a linear function. We use principally the functions considered in Proposition 1, applying Remark 1.

**Theorem 11** *Let $g : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$ be a bent function and*

$$f : \mathbb{F}_2^{s+1} \to \mathbb{F}_2,\ (x_0, \bar{x}) \mapsto x_0\phi(\bar{x}) \oplus g_e(\bar{x}),\ x_0 \in \mathbb{F}_2,\ \bar{x} \in \mathbb{F}_2^s,$$

*be a Maiorana-McFarland bent function. Then, the function $f \oplus l_{(a_0,\bar{a})}$, where $l_{(a_0,\bar{a})}(x_0, \bar{x}) = a_0x_0 \oplus \bar{a}\cdot\bar{x}$, $a_0 \in \mathbb{F}_2$, $\bar{a} = (a_1, \ldots, a_s) \in \mathbb{F}_2^s$, satisfy the following:*

*If $(a_0 = 0 \wedge a_s = 0) \vee (a_0 = 1 \wedge a_s = 1)$, then*

$$(f \oplus l_{(a_0,\bar{a})})_{|\{(x_0,\bar{x})|w_H(x_0,\bar{x})\ even\}} \quad \textit{is balanced.}$$

*If $(a_0 = 0 \wedge a_s = 1) \vee (a_0 = 1 \wedge a_s = 0)$, then*

$$(f \oplus l_{(a_0,\bar{a})})_{|\{(x_0,\bar{x})|w_H(x_0,\bar{x})\ odd\}} \quad \textit{is balanced.}$$

*Proof* Let $\bar{a} = (a, a_s)$ and $\bar{x} = (x, x_s)$, $a, x \in \mathbb{F}_2^{s-1}$, $a_s, x_s \in \mathbb{F}_2$.

We have four possibilities for the pair $(a_0, a_s)$. For each one, we proceed by considering when $g_e \oplus l_{(a,a_s)}$ is balanced in

$$\mathcal{C}_0'|\bar{0} \text{ or } \mathcal{C}_1'|\bar{1} \text{ or } \mathcal{C}_0'|\bar{1} \text{ or } \mathcal{C}_1'|\bar{0},$$

and $\widehat{\mathcal{W}}_{g_e\oplus l_{(a,a_s)}}(\bar{0}) = 2^{\frac{s-1}{2}}$ or $\widehat{\mathcal{W}}_{g_e\oplus l_{(a,a_s)}}(\bar{0}) = -2^{\frac{s-1}{2}}$ in the corresponding complement of the affine space: in

$$\mathcal{C}_1'|\bar{1} \text{ or } \mathcal{C}_0'|\bar{0} \text{ or } \mathcal{C}_1'|\bar{0} \text{ or } \mathcal{C}_0'|\bar{1}$$

respectively.

We know that,

$$(f \oplus l_{(a_0,a,a_s)})(x_0, x, x_s) = x_0\phi(x, x_s) \oplus g_e(x, x_s) \oplus l_{(a,a_s)}(x, x_s) \oplus a_0x_0.$$

Without loss of generality, let us see the case $a_0 = 0$ and $a_s = 1$ when $g_e \oplus l_{(a,1)}$ is balanced in $\mathcal{C}_0'|\bar{1}$ and $\widehat{\mathcal{W}}_{g_e\oplus l_{(a,1)}}(\bar{0}) = -2^{\frac{s-1}{2}}$ in $\mathcal{C}_1'|\bar{0}$.

The elements with odd Hamming weight in $\mathbb{F}_2^{1+s}$ are in the following cases:

**Case 1**. Let $x_0 = 0$, $x_s = 0$, and $w_H(x)$ odd. Then,
$(f \oplus l_{(0,a,1)})(0, x, 0) = g_{e_1}(x, 0) \oplus l_{(a,1)}(x, 0) = 0$, $2^{s-3} - 2^{\frac{s-3}{2}}$ times.

Since, $g_e \oplus l_{(a,1)}$ is not balanced and $\widehat{\mathcal{W}}_{g_e\oplus l_{(a,1)}}(\bar{0}) = -2^{\frac{s-1}{2}}$ in $\mathcal{C}_1'|\bar{0}$.

**Case** 2. Let $x_0 = 0$, $x_s = 1$, and $w_H(x)$ even. Then,
$(f \oplus l_{(0,a,1)})(0, x, 1) = g_{e_1}(x, 1) \oplus l_{(a,1)}(x, 1) = 0$, $2^{s-3}$ times.

Since, $g_e \oplus l_{(a,1)}$ is balanced in $\mathcal{C}_0'|\bar{1}$.

**Case** 3. Let $x_0 = 1$, $x_s = 0$, and $w_H(x)$ even. Then,
$(f \oplus l_{(0,a,1)})(1, x, 0) = g_{e_0}(x, 0) \oplus l_{(a,1)}(x, 0) = 0$, $2^{s-3}$ times.

Since, $g_e \oplus l_{(a,1)}$ is balanced in $\mathcal{C}_0'|\bar{0}$.

**Case** 4. Let $x_0 = 1$, $x_s = 1$, and $w_H(x)$ odd. Then,

$(f \oplus l_{(0,a,1)})(1,x,1) = g_{e_0}(x,1) \oplus l_{(a,1)}(x,1) = 0, \quad 2^{s-3} + 2^{\frac{s-3}{2}}$ times.

Since, $g_e \oplus l_{(a,1)}$ is not balanced and $\widehat{\mathcal{W}}_{g_e \oplus l_{(a,1)}}(\bar{0}) = 2^{\frac{s-1}{2}}$ in $\mathcal{C}_1'|\bar{1}$.

Hence, adding the four cases,

$$|f^{-1}_{|\{(x_0,\bar{x}) \in \mathbb{F}_2^{s+1} | w_H(x_0,\bar{x}) \ odd\}}(0)| = 2^{s-1}.$$

Therefore, $f_{|\{(x_0,\bar{x})|w_H((x_0,\bar{x})) \ odd\}}$ is balanced.

Resolving similarly, we obtained the same result in the other cases.

□

We can use the demonstration of Theorem 11 to have a simple way to obtain bent functions of any even dimension in its domain greater than the dimension of the given bent function. These new bent functions are balanced explicitly when the domain is restricted to vectors of even Hamming weight.

In Algorithms 1 and 2, we consider $\mathcal{A}$ and $\mathcal{B}$ sets of vectors of length $o$ of even Hamming and odd Hamming weights, respectively. Also, in general, $l_a(x) := a_1x_1 \oplus \cdots \oplus a_rx_r$, $a = (a_1, \ldots, a_r), x = (x_1, \ldots, x_r) \in \mathbb{F}_2^r$, for any positive integer $r$.

**Algorithm 1** `Extended Maiorana-McFarland` $r = 1$

**Input:** $s-1 \geq 2$ even, $g_{s-1} : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$ be a bent function, $x'^{s-1}, x''^{s-1} \in \mathbb{F}_2, x^{s-1} \in \mathbb{F}_2^{s-1}$
**Output:** $g_o$ a bent function, $g_{o|\mathcal{A}}$ balanced

```
Integer o;
n := s − 1;
while n < o do
    for x'^n, x''^n from 0 to 1 do
        if x^n is even, x'^n = 1, x''^n = 1 or x^n is odd, x'^n = 1, x''^n = 0 then
            g_{n+2}(x'^n, x^n, x''^n) = 1 ⊕ g_n(x^n);
        else
            g_{n+2}(x'^n, x^n, x''^n) = g_n(x^n);
        end if
    end for
    x^n = (x'^n, x^n, x''^n);   n := n + 2;
end while
```

## 5 Conclusions

Initially, we prove that the bent functions are balanced on the set of vectors of even Hamming weight or the set of odd Hamming weight. Later, we use Maiorana-McFarland's class to construct bent functions. The bent functions obtained are balanced if the domain is restricted to vectors of even Hamming weight. In this case, we start using initial bent functions on $\mathbb{F}_2^{s-1}$, and $\phi$ and $g_e$ are defined as boolean functions. Besides, the affine spaces are the set of vectors of even Hamming weight and the set of vectors of odd Hamming weight.

**Algorithm 2** `Extended Maiorana-McFarland` $\oplus linear$ $r = 1$

**Input:** $s-1 \geq 2$ even, $g_{s-1} : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$ be a bent function, $l_{a^{s-1}}$ a linear function on $\mathbb{F}_2^{s-1}$, $x'^{s-1}, a'^{s-1}, x''^{s-1}, a''^{s-1} \in \mathbb{F}_2, x^{s-1}, a^{s-1} \in \mathbb{F}_2^{s-1}$

**Output:** $g_o \oplus l_{(a'^{o-2}, a^{o-2}, a''^{o-2})}$ a bent function. If $(a'^{o-2} = 0 \wedge a''^{o-2} = 0) \vee (a'^{o-2} = 1 \wedge a''^{o-2} = 1)$, $(g_o \oplus l_{(a'^{o-2}, a^{o-2}, a''^{o-2})})_{|\mathcal{A}}$ balanced. If $(a'^{o-2} = 0 \wedge a''^{o-2} = 1) \vee (a'^{o-2} = 1 \wedge a''^{o-2} = 0)$, $(g_o \oplus l_{(a'^{o-2}, a^{o-2}, a''^{o-2})})_{|\mathcal{B}}$ balanced

Integer $o$;
$n := s-1$;
**while** $n < o$ **do**
  **if** $a'^n = 0$ **and** $a''^n = 0$ **then**
    **for** $x'^n, x''^n$ from 0 to 1 **do**
      **if** ($x^n$ is even, $x'^n = 1$, $x''^n = 1$) or ($x^n$ is odd, $x'^n = 1$, $x''^n = 0$) **then**
        $(g_{n+2} \oplus l_{0,a^n,0})(x'^n, x^n, x''^n) = 1 \oplus (g_n \oplus l_{a^n})(x^n)$;
      **else**
        $(g_{n+2} \oplus l_{0,a^n,0})(x'^n, x^n, x''^n) = (g_n \oplus l_{a^n})(x^n)$;
      **end if**
    **end for**
    $x^n = (x'^n, x^n, x''^n)$; $a^n = (a'^n, a^n, a''^n)$; $n := n+2$;
  **end if**
  **if** $a'^n = 0$ **and** $a''^n = 1$ **then**
    **for** $x'^n, x''^n$ from 0 to 1 **do**
      **if** ($x^n$ is even, $x'^n = 0$, $x''^n = 1$) or {($x^n$ is odd, [($x'^n = 0$, $x''^n = 1$) or ($x'^n = 1$, $x''^n = 0$) or ($x'^n = 1$, $x''^n = 1$)]} **then**
        $(g_{n+2} \oplus l_{0,a^n,0})(x'^n, x^n, x''^n) = 1 \oplus (g_n \oplus l_{a^n})(x^n)$;
      **else**
        $(g_{n+2} \oplus l_{0,a^n,0})(x'^n, x^n, x''^n) = (g_n \oplus l_{a^n})(x^n)$;
      **end if**
    **end for**
    $x^n = (x'^n, x^n, x''^n)$; $a^n = (a'^n, a^n, a''^n)$; $n := n+2$;
  **end if**
  **if** $a'^n = 1$ **and** $a''^n = 0$ **then**
    **for** $x'^n, x''^n$ from 0 to 1 **do**
      **if** ($x^n$ is even, $x'^n = 1$, $x''^n = 0$) or ($x^n$ is odd, $x'^n = 1$, $x''^n = 1$) **then**
        $(g_{n+2} \oplus l_{0,a^n,0})(x'^n, x^n, x''^n) = 1 \oplus (g_n \oplus l_{a^n})(x^n)$;
      **else**
        $(g_{n+2} \oplus l_{0,a^n,0})(x'^n, x^n, x''^n) = (g_n \oplus l_{a^n})(x^n)$;
      **end if**
    **end for**
    $x^n = (x'^n, x^n, x''^n)$; $a^n = (a'^n, a^n, a''^n)$; $n := n+2$;
  **end if**
  **if** $a'^n = 1$ **and** $a''^n = 1$ **then**
    **for** $x'^n, x''^n$ from 0 to 1 **do**
      **if** {$x^n$ is even, [($x'^n = 0$, $x''^n = 1$) or ($x'^n = 1$, $x''^n = 0$) or ($x'^n = 1$, $x''^n = 1$)]} or ($x^n$ is odd, $x'^n = 0$, $x''^n = 1$) **then**
        $(g_{n+2} \oplus l_{0,a^n,0})(x'^n, x^n, x''^n) = 1 \oplus (g_n \oplus l_{a^n})(x^n)$;
      **else**
        $(g_{n+2} \oplus l_{0,a^n,0})(x'^n, x^n, x''^n) = (g_n \oplus l_{a^n})(x^n)$;
      **end if**
    **end for**
    $x^n = (x'^n, x^n, x''^n)$; $a^n = (a'^n, a^n, a''^n)$; $n := n+2$;
  **end if**
**end while**

Additionally, we analyse the balancedness by adding linear functions (also for $g_{e_0}$ and $g_{e_1}$), obtaining precise results. All this research can be important for future investigation to find boolean functions with total balancedness and high non-linearity, starting from bent functions, for example [9]. Observe that we already have half of the domain balanced concerning the images. For future research, we will only need the other half, reducing the non-linearity of the bent function as little as possible.

## References


1. Picek, S., Carlet, C., Guilley, S., Miller, J.F, Jakobovic, D. "Evolutionary Algorithms for Boolean Functions in Diverse Domains of Cryptography", in Evolutionary Computation, vol. 24, no. 4, pp. 667-694, Dec. 2016.
2. Behera, P.K., Gangopadhyay, S. "An improved hybrid genetic algorithm to construct balanced Boolean function with optimal cryptographic properties", Evol. Intel. vol. 15, pp. 639-653, 2022. https://doi.org/10.1007/s12065-020-00538-x
3. Rothaus, 0.S. "On bent functions", J. Comb. Theory, Vol. 20, 1976, pp. 300-305.
4. C. Carlet, "On the confusion and diffusion properties of Maiorana–McFarland's and extended Maiorana–McFarland's functions", J. Complexity, vol. 20, pp. 182-204, 2004
5. Gini, A., Pierrick, M. "S0-equivalence classes, a new direction to find better weightwise perfectly balanced functions, and more", Journal: Cryptography and Communications, 2024.
6. MacWilliams, F.J., Sloane, N. J. *"The Theory of Error Correcting Codes"*, Elsevier Science Publisher B.V., North-Holland Mathematical Library, vol. 16, 1977.
7. Tokareva, N. "Bent Functions: Results and Application in Cryptography", Bent Functions: Results and Application in Cryptography, pp. 1-202, 2015.
8. Carlet, C., Guillot, Ph. "A new representation of Boolean Functions", Springer-Verlag Berlin Heidelberg, pp. 94-103, 1999.
9. Maitra, S., Mandal, B., Roy, M. "Modifying Bent Functions to Obtain the Balanced Ones with High Nonlinearity", Progress in Cryptology – INDOCRYPT 2022, Springer International Publishing 13774, pp. 449–470, 2022.