**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: March 7, 2024/ Accepted: date

**Abstract** In a particular case, we consider the extended Maiorana-McFarland's class to obtain balanced bent functions restricted to vectors with even Hamming weight, an equal number of pre-images for each element in the range. Additionally, we demonstrate that all bent functions are balanced when we restrict to vectors of even Hamming weight or vectors with odd Hamming weight. Given the necessary tools, we provide a simple algorithm to obtain new bent functions using Maiorana-McFarland.

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

## 1 Introduction

The functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ are called boolean functions. They are important in cryptography and code theory because they have important properties such as non-linearity, balance, low auto-correlation and high algebraic immunity. The search space of these functions is very large, $2^{2^n}$, and different methods exist to search for these functions: random search, algebraic and heuristic methods, see for example [1], [8].

We are interested in the non-linearity of a function, defined as the distance between a boolean function and the set of affine functions. Functions with maximum non-linearity are called bent functions; Rothaus introduced

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

the name in 1976 [4]. These functions have been classified and constructed, as examples we have the Maiorana-McFarland class [6] and Rothaus [4].

In this work, we use a particular case of the extended Maiorana-McFarland class [2], i.e. $f$ bent given by $f : \mathbb{F}_2^{s+1} \to \mathbb{F}_2, \quad x \mapsto x \cdot \phi(y) \oplus g_e(y)$, where $\phi(y) : \mathbb{F}_2^s \to \mathbb{F}_2$ is such that $\phi^{-1}(a)$ is an affine space of dimension $s-1$, and $g_e(y) : \mathbb{F}_2^s \to \mathbb{F}_2$, $g_{e|\phi^{-1}(a)}$ is a bent function.

First, $\phi$ and $g_e$ are defined and, after a series of results, we find the direct relationship between a bent function and a bent function with a higher dimensional domain. Finally, we provide a pair of algorithms that simplify this relationship.

Additionally, we show that any bent function is balanced when restricted to an even Hamming weight or to an odd Hamming weight in its domain. This result is crucial, since it allows us to obtain a bent function $g_e : \mathcal{C}_0 \to \mathbb{F}_2$ from a bent function $g : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$, where $\mathcal{C}_0 := \phi^{-1}(0)$ is a linear code with a vector of even Hamming weight and $\mathcal{C}_1 := \phi^{-1}(1)$ the affine space of odd Hamming weight.

## 2 Background

Definitions and results about boolean functions, particularly bent functions, are recalled in this section. These can be found, for example, in [5], [7], [3].

**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,*

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

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

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

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

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

**Definition 4** The **Walsh-Hadamard Transform** of a boolean function, $f$ , is defined as

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

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

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

The boolean functions with maximum non-linearity are called **bent** functions and their non-linearity is $2^{n-1} - 2^{n/2-1}$.

## 3 Bent functions balancedness, restricted to even or odd Hamming weight

We will need bent functions over an affine space to find new bent functions when using the Extended Maiorana-McFarland class [2]. 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 that we need is: for all bent functions $f \in \mathcal{B}_n$, we have that $f_{|\{x \in \mathbb{F}_2^n | w_H(x) \ even\}}$ is balanced or $f_{|\{x \in \mathbb{F}_2^n | w_H(x) \ odd\}}$ is balanced.

In the following, we prove this claim. For this, we first give the particular cases $n = 2$ and $n = 4$.

*Example 2* In the case $\mathcal{B}_2$, all the bent functions satisfy this property because these must have three images 0 and one image 1, or three images 1 and one image 0.

$f(x_1, x_2) = x_1 x_2$,

| $x_1$ | $x_2$ | $ev(f)$ |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |

.

*Remark 1* 1. Let $g : \mathbb{F}_2^n \to \mathbb{F}_2$ be a bent function such that $g_{|\{x\in\mathbb{F}_2^n | w_H(x)\ even\}}$ is balanced.

(a) If $\widehat{\mathcal{W}}_g(a) = 2^{\frac{n}{2}}$, then
$|(g)^{-1}_{|\{x\in\mathbb{F}_2^n|w_H(x)\ even\}}(0)| = 2^{n-2}$
$|(g)^{-1}_{|\{x\in\mathbb{F}_2^n|w_H(x)\ even\}}(1)| = 2^{n-2}$
$|(g)^{-1}_{|\{x\in\mathbb{F}_2^n|w_H(x)\ odd\}}(0)| = 2^{n-2} + 2^{\frac{n-2}{2}}$.
$|(g)^{-1}_{|\{x\in\mathbb{F}_2^n|w_H(x)\ odd\}}(1)| = 2^{n-2} - 2^{\frac{n-2}{2}}$.

(b) If $\widehat{\mathcal{W}}_g(a) = -2^{\frac{n}{2}}$, then
$|(g)^{-1}_{|\{x\in\mathbb{F}_2^n|w_H(x)\ even\}}(0)| = 2^{n-2}$
$|(g)^{-1}_{|\{x\in\mathbb{F}_2^n|w_H(x)\ even\}}(1)| = 2^{n-2}$
$|(g)^{-1}_{|\{x\in\mathbb{F}_2^n|w_H(x)\ odd\}}(0)| = 2^{n-2} - 2^{\frac{n-2}{2}}$.
$|(g)^{-1}_{|\{x\in\mathbb{F}_2^n|w_H(x)\ odd\}}(1)| = 2^{n-2} + 2^{\frac{n-2}{2}}$.

2. Similar observations if $g_{|\{x\in\mathbb{F}_2^n|w_H(x)\ odd\}}$ is balanced.

*Remark 2* Let $\mathcal{A} := \{x \in \mathbb{F}_2^n \mid w_H(x) \text{ even}\}$ and $\mathcal{B} := \{x \in \mathbb{F}_2^n \mid w_H(x) \text{ odd}\}$. We can write,

$$[\mathbb{F}_2^n] = \begin{bmatrix} \mathcal{A} \\ \mathcal{B} \end{bmatrix} = \begin{bmatrix} \mathcal{A}' & \bar{0} \\ \mathcal{B}' & \bar{1} \\ \mathcal{A}' & \bar{1} \\ \mathcal{B}' & \bar{0} \end{bmatrix} = \begin{bmatrix} \mathbb{F}_2^{n-1}| & \bar{0} \\ & \bar{1} \\ \mathbb{F}_2^{n-1}| & \bar{1} \\ & \bar{0} \end{bmatrix} = \begin{bmatrix} I \\ II \\ III \\ 1V \end{bmatrix},$$

where $\bar{0} = \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}$ and $\bar{1} = \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix}$ are $2^{n-2} \times 1$ arrays.

Note that $\mathcal{A}$ is a MDS linear code of dimension $n-1$ and $\mathcal{B}$ is an affine space. Also, $\mathcal{A}' = \{x \in \mathbb{F}_2^{n-1} \mid w_H(x) \text{ even}\}$ and $\mathcal{B}' = \{x \in \mathbb{F}_2^{n-1} \mid w_H(x) \text{ odd}\}$.

The following result is the particular case $n = 4$. We use the notation of the Observation 2.

**Theorem 3** *Every bent function $f : \mathbb{F}_2^4 \to \mathbb{F}_2$ is such that $f_{|\mathcal{A}}$ is balanced or $f_{|\mathcal{B}}$ is balanced.*

*Proof* Let $f$ be a bent function and $l_a$ an affine function. Observe that, $w_H(f \oplus l_a) = 6$ or $w_H(f \oplus l_a) = 10$. In particular, the linear functions $l_0 := 0$ and $l_{\bar{1}}(x) := x_1 \oplus x_2 \oplus x_3 \oplus x_4$ satisfy the above observation. Additionally, notice that $l_{\bar{1}}(\mathcal{A}) = \{0\}$ and $l_{\bar{1}}(\mathcal{B}) = \{1\}$.

Since $f$ is a bent function:

**Case 1**. If $f_{|\mathcal{A}}$ has zero images 1, then $f_{|\mathcal{B}}$ has six images 1. Hence, $(f \oplus l_{\bar{1}})(\mathcal{A})$ has zero images 1 and $(f \oplus l_{\bar{1}})(\mathcal{B})$ has four images 1. Therefore, $f \oplus l_{\bar{1}}$ is not a bent function; consequently, $f$ is not a bent function.

**Case 2**. If $f_{|\mathcal{A}}$ has two images 1, then $f_{|\mathcal{B}}$ has four or eight images 1. If $f_{|\mathcal{B}}$ has four images 1, that means $f_{|\mathcal{B}}$ is balanced. Hence, the theorem is proven. If $f_{|\mathcal{B}}$ has eight images 1, $(f \oplus l_{\bar{1}})(\mathcal{A})$ has two 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; consequently, $f$ is not a bent function.

**Case 3**. If $f_{|A}$ has four images 1, that means $f_{|\mathcal{A}}$ is balanced. Hence, the theorem is proven.

**Case 4**. If $f_{|A}$ has six images 1, $f_{|\mathcal{A}}$ has two images 0, then $f_{|\mathcal{B}}$ has four or eight images 0. If $f_{|\mathcal{B}}$ has four images 0, that means $f_{|\mathcal{B}}$ is balanced. Hence, the theorem is proven. If $f_{|\mathcal{B}}$ has eight images 0, $(f \oplus l_{\bar{1}})(\mathcal{A})$ has two images 0 and $(f \oplus l_{\bar{1}})(\mathcal{B})$ has zero images 0. Therefore, $f \oplus l_{\bar{1}}$ is not a bent function; consequently, $f$ is not a bent function.

**Case 5**. If $f_{|A}$ has eight images 1, $f_{|\mathcal{A}}$ has zero images 0, then $f_{|\mathcal{B}}$ has six images 0. Hence, $(f \oplus l_{\bar{1}})(\mathcal{A})$ has zero images 0 and $(f \oplus l_{\bar{1}})(\mathcal{B})$ has four images 0. Therefore, $f \oplus l_{\bar{1}}$ is not a bent function; consequently, $f$ is not a bent function.

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

□

We note the symmetry of the cases 1 and 2 with cases 5 and 4, respectively, interchanging the number of images 1 by number of images 0. This will be very important to the general case.

The following result is a general case, $n$ even. As far as we have looking for, we do not know this result. We use the notation of the Observation 2.

**Theorem 4** *Every bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $n \geq 6$, is such that $f_{|\mathcal{A}}$ is balanced or $f_{|\mathcal{B}}$ is balanced.*

*Proof* Let $f$ be a bent function and $l_a$ an affine function. Observe that, $w_H(f \oplus l_a) = 2^{n-1} - 2^{\frac{n-2}{2}}$ or $w_H(f \oplus l_a) = 2^{n-1} + 2^{\frac{n-2}{2}}$. In particular, the linear functions $l_0(x) := 0$ and $l_{\bar{1}}(x) := x_1 \oplus \cdots \oplus x_n$ satisfy the observation. Additionally, notice that $l_{\bar{1}}(\mathcal{A}) = \{0\}$ and $l_{\bar{1}}(\mathcal{B}) = \{1\}$.

**Case 1**. If $f_{|A}$ 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, remember that, $n \geq 6$, then $2^{\frac{n-2}{2}} < 2^{n-2} - 2^{\frac{n-2}{2}}$.

**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, $c = 2^{n-2}$, and $f_{|\mathcal{A}}$ is balanced. But, remember that, $n \geq 6$, then $2^{\frac{n-2}{2}} < 2^{n-2}$.

**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 $2^{n-2}+(2^{n-2}-22^{\frac{n-2}{2}}-c)$ 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 $22^{\frac{n-2}{2}}+c$ images 1.

**Case 2a1** $(f\oplus l_{\bar{1}})$ has $(a)$ $c+2^{\frac{n-2}{2}}+22^{\frac{n-2}{2}}+c=2^{n-1}-2^{\frac{n-2}{2}}$ 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 $c+2^{\frac{n-2}{2}}+22^{\frac{n-2}{2}}+c=2^{n-1}+2^{\frac{n-2}{2}}$ 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 don't consider this case.

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 $f_{|\mathcal{A}}$ in place 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. Indeed, if $f$ is a bent function, it must satisfy, $f_{|\mathcal{A}}$ is balanced or $f_{|\mathcal{B}}$ is balanced.

□

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

We extend the definition of bent functions over $\mathbb{F}_2^n$ to an affine subspace included in $\mathbb{F}_2^n$ as suggested in the extended Maiorana–McFarland's Proposition 1 [2].

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

The following two results are easily obtained, similarly to the traditional bent function proofs.

**Theorem 5** *Let a function* $f:\mathcal{C}\rightarrow\mathbb{F}_2$. *Then* $Nl(f)=2^{m-1}-\frac{1}{2}\max_{a\in\mathbb{F}_2^n}|\widehat{\mathcal{W}}_f(a)|$, *where* $\widehat{\mathcal{W}}_f(a):=\sum_{x\in\mathcal{C}}(-1)^{f(x)\oplus a\cdot x}$.

□

Observe that all $a \in \mathbb{F}_2^n$ are considered.

**Theorem 6** *If $f : \mathcal{C} \subset \mathbb{F}_2^n \to \mathbb{F}_2$, $\dim \mathcal{C} = m$, is a bent function, then $\widehat{\mathcal{W}}_f(a) = \pm 2^{m/2}$.*

□

The following theorem corresponds to a class of bent functions: the extended **Maiorana**–**McFarland** class.

**Theorem 7** *[2] 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 a bent function.*

**Here in after**, according to Theorem 7, particular case $r = 1$, we denote $\phi(y) : \mathbb{F}_2^s \to \mathbb{F}_2$, $g_e : \mathbb{F}_2^s \to \mathbb{F}_2$, and define

$g : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$ a bent function,

$\mathcal{C}_0 = \phi^{-1}(0) := \{x \in \mathbb{F}_2^s \mid w_H(x) \text{ even}\}$ and $\mathcal{C}_1 = \phi^{-1}(1) := \{x \in \mathbb{F}_2^s \mid w_H(x) \text{ odd}\}$,

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

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

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

*Remark 3* 1. We can see that, $\mathcal{C}_0 = \phi^{-1}(0)$ is a linear code of dimension $s-1$.
2. $b \oplus \mathcal{C}_0 = \mathcal{C}_1$, for any $b \in \mathbb{F}_2^s$ with odd Hamming weight.
3. $\mathcal{C}_0$ is an MDS linear code.
4. In $\mathcal{C}_0$, if $x \in \mathbb{F}_2^{s-1}$ has an even Hamming weight, then $x_s$ is 0 and, if $x \in \mathbb{F}_2^{s-1}$ has and odd Hamming weight, then $x \in \mathbb{F}_2$ is 1.
5. In $\mathcal{C}_1$, if $x \in \mathbb{F}_2^{s-1}$ has an even Hamming weight, then $x_s$ is 1 and, if $x \in \mathbb{F}_2^{s-1}$ has an odd Hamming weight, then $x_s$ is 0.

In the proof of the following theorem, it is essential that if $g$ is a bent function, then $g_{|\{x|w_H(x) \ even\}}$ is balanced or $g_{|\{x|w_H(x) \ odd\}}$ is balanced.

Using the above notation.

**Theorem 8** *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* We will rely on the fact that, if $g$ is a bent function, then $g_{|\{x \in \mathbb{F}_2^{s-1}|w_H(x) \ even\}}$ is balanced or $g_{|\{x \in \mathbb{F}_2^{s-1}|w_H(x) \ odd\}}$ is balanced.

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

$$\begin{aligned}&\widehat{\mathcal{W}}_{g_{e_0}}(b)\\ &= \sum_{\bar{x}\in\mathcal{C}_0} (-1)^{g_{e_0}(x_1,\ldots,x_{s-1},x_s)+(x_1\ldots\cdot x_{s-1},x_s)\cdot b}\\ &= \sum_{\bar{x}\in\mathcal{C}_0} (-1)^{g_{e_0}(x_1,\ldots,x_{s-1},x_s)+x_1b_1+\cdots+x_{s-1}b_{s-1}+x_sb_s}.\end{aligned}$$

If $b_s = 0$,

$$\widehat{\mathcal{W}}_{g_{e_0}}(b) = \sum_{\bar{x}\in\mathcal{C}_0} (-1)^{g(x_1,\ldots,x_{s-1})+x_1b_1+\cdots+x_{s-1}b_{s-1}} = \widehat{\mathcal{W}}_g(b_1, \ldots, b_{s-1}).$$

If $b_s = 1$

$$\begin{aligned}&\widehat{\mathcal{W}}_{g_{e_0}}(b)\\ &= \sum_{\bar{x}\in\mathcal{C}_0} (-1)^{g_{e_0}(x_1,\ldots,x_{s-1},x_s)+x_1b_1+\cdots+x_{s-1}b_{s-1}+x_s}\\ &= \sum_{\bar{x}\in\mathcal{C}_0} (-1)^{g_{e_0}(x_1,\ldots,x_{s-1},0)+x_1b_1+\cdots+x_{s-1}b_{s-1}} + \sum_{\bar{x}\in\mathcal{C}_0} (-1)^{g_{e_0}(x_1,\ldots,x_{s-1},1)+x_1b_1+\cdots+x_{s-1}b_{s-1}+1}\\ &= \sum_{\bar{x}\in\mathcal{C}_0} (-1)^{g_{e_0}(x_1,\ldots,x_{s-1},0)+x_1b_1+\cdots+x_{s-1}b_{s-1}} + (-1)\sum_{\bar{x}\in\mathcal{C}_0} (-1)^{g_{e_0}(x_1,\ldots,x_{s-1},1)+x_1b_1+\cdots+x_{s-1}b_{s-1}}\\ &= \sum_{\{x\in\mathbb{F}_2^{s-1}\ \mid\ w_H(x)\ even\}} (-1)^{g(x_1,\ldots,x_{s-1})+x_1b_1+\cdots+x_{s-1}b_{s-1}}\\ &+ (-1)\sum_{\{x\in\mathbb{F}_2^{s-1}\ \mid\ w_H(x)\ odd\}} (-1)^{g(x_1,\ldots,x_{s-1})+x_1b_1+\cdots+x_{s-1}b_{s-1}}\end{aligned}$$

The last equality, by Observation 3, Item 4.

If $g_{|\{x\in\mathbb{F}_2^{s-1}|w_H(x)\ even\}}$ is balanced,

$$\widehat{\mathcal{W}}_{g_{e_0}}(b) = (-1)\sum_{\{x\in\mathbb{F}_2^{s-1}\ \mid\ w_H(x)\ odd\}} (-1)^{g(x_1,\ldots,x_{s-1})+x_1b_1+\cdots+x_{s-1}b_{s-1}} = \widehat{\mathcal{W}}_g((b_1, \ldots, b_{s-1})).$$

If $g_{|\{x\in\mathbb{F}_2^{s-1}|w_H(x)\ odd\}}$ is balanced,

$$\widehat{\mathcal{W}}_{g_{e_0}}(b) = \sum_{\{x\in\mathbb{F}_2^{s-1}\ \mid\ w_H(x)\ even\}} (-1)^{g(x_1,\ldots,x_{s-1})+x_1b_1+\cdots+x_{s-1}b_{s-1}} = \widehat{\mathcal{W}}_g((b_1, \ldots, b_{s-1})).$$

In both cases, since $g$ is a bent function, then $g_{e_0}$ 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 $g_{|\{x\in\mathbb{F}_2^{s-1}|w_H(x)\ even\}}$ 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 $g_{|\{x\in\mathbb{F}_2^{s-1}|w_H(x)\ odd\}}$ 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* $\widehat{\mathcal{W}}_{g_{e_1}}(a,1) = -2^{\frac{s-1}{2}}$.

□

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

In the following theorem, we always have that $f_{|\{(x,y)|w_H((x,y))\ even\}}$ is uniquely balanced.

**Theorem 9** *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*

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

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

*Proof* Since, $\phi$ y $g_e$ satisfy the conditions of Theorem 7 (Observation 3 and Theorem 8), then $f$ is a bent function.

We will rely on the fact that, $g_{|\{\bar{x}\in\mathbb{F}_2^{s-1}|w_H(\bar{x})\ even\}}$ is balanced or $g_{|\{\bar{x}\in\mathbb{F}_2^{s-1}|w_H(\bar{x})\ odd\}}$ is balanced.

Let's see the balance. Let $g_{|\{\bar{x}|w_H(\bar{x})\ even\}}$ be balanced and $\widehat{\mathcal{W}}_g(0) = 2^{\frac{s-1}{2}}$. If we consider $\bar{x} = (y_1, \ldots, y_{s-1})$, we can write $f$ as

$$f(x, y_1, \ldots, y_{s-1}, y_s) = x\phi(y_1, \ldots, y_{s-1}, y_s) \oplus g_e(y_1, \ldots, y_{s-1}, y_s).$$

Let $x = 0$ and $y_s = 0$.

**Case 1**. If $w_H(y_1, \ldots, y_{s-1})$ is even,
$f(0, y_1, \ldots, y_{s-1}, 0) = 0 \cdot 0 \oplus g_e(y_1, \ldots, y_{s-1}, 0) = g_{e_0}(y_1, \ldots, y_{s-1}, 0) = 0,\ 2^{s-3}$ times.

**Case 2**. If $w_H(y_1, \ldots, y_{s-1})$ is odd,
$f(0, y_1, \ldots, y_{s-1}, 0) = 0 \cdot 1 \oplus g_e(y_1, \ldots, y_{s-1}, 0) = g_{e_1}(y_1, \ldots, y_{s-1}, 0) = 0,\ 2^{s-3} + 2^{\frac{s-3}{2}}$ times.

Let $x = 0$ and $y_s = 1$.

**Case 3**. If $w_H(y_1, \ldots, y_{s-1})$ is even,
$f(0, y_1, \ldots, y_{s-1}, 1) = 0 \cdot 1 \oplus g_e(y_1, \ldots, y_{s-1}, 1) = g_{e_1}(y_1, \ldots, y_{s-1}, 1) = 0,\ 2^{s-3}$ times.

**Case 4**. If $w_H(y_1, \ldots, y_{s-1})$ is odd,
$f(0, y_1, \ldots, y_{s-1}, 1) = 0 \cdot 0 \oplus g_e(y_1, \ldots, y_{s-1}, 1) = g_{e_0}(y_1, \ldots, y_{s-1}, 1) = 0,\ 2^{s-3} + 2^{\frac{s-3}{2}}$ times.

Let $x = 1$ and $y_s = 0$.

**Case 5**. If $w_H(y_1, \ldots, y_{s-1})$ is even,
$f(1, y_1, \ldots, y_{s-1}, 0) = 1 \cdot 0 \oplus g_e(y_1, \ldots, y_{s-1}, 0) = g_{e_0}(y_1, \ldots, y_{s-1}, 0) = 0,\ \ 2^{s-3}$ times.

**Case 6**. If $w_H(y_1, \ldots, y_{s-1})$ is odd,
$f(1, y_1, \ldots, y_{s-1}, 1) = 1 \cdot 1 \oplus g_e(y_1, \ldots, y_{s-1}, 0) = 1 \oplus g_{e_1}(y_1, \ldots, y_{s-1}, 0) = 0,\ \ 2^{s-3} - 2^{\frac{s-3}{2}}$ times.

Let $x = 1$ and $y_s = 1$.

**Case 7**. If $w_H(y_1, \ldots, y_{s-1})$ is even,
$f(1, y_1, \ldots, y_{s-1}, 1) = 1 \cdot 1 \oplus g_e(y_1, \ldots, y_{s-1}, 1) = 1 \oplus g_{e_1}(y_1, \ldots, y_{s-1}, 1) = 0,\ \ 2^{s-3}$ times.

**Case 8**. If $w_H(y_1, \ldots, y_{s-1})$ is odd,
$f(1, y_1, \ldots, y_{s-1}, 1) = 1 \cdot 0 \oplus g_e(y_1, \ldots, y_{s-1}, 1) = 0 \oplus g_{e_0}(y_1, \ldots, y_{s-1}, 1) = 0,\ \ 2^{s-3} + 2^{\frac{s-3}{2}}$ times.

The elements with even Hamming weight in $\mathbb{F}_2^{s+1}$ are in: **Case 1**, **Case 4**, **Case 6**, **Case 7**. Hence,

$$|f^{-1}_{|\{(x,\bar{y})\in\mathbb{F}_2^{s+1}|w_H(x)\ even\}}(0)| = (2^{s-3}) + (2^{s-3} + 2^{\frac{s-3}{2}}) + (2^{s-3} - 2^{\frac{s-3}{2}}) + (2^{s-3}) = 2^{s-1}.$$

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

Similarly,

When $g_{|\{\bar{x}\in\mathbb{F}_2^{s-1}|w_H(\bar{x})\ even\}}$ is balanced and $\widehat{\mathcal{W}}_g(0) = -2^{\frac{s-1}{2}}$ :

$f_{|\{(x,\bar{y})\in\mathbb{F}_2^{s+1}|w_H((x,\bar{y}))\ even\}}$ is balanced.

When $g_{|\{\bar{x}\in\mathbb{F}_2^{s-1}|w_H(\bar{x})\ odd\}}$ is balanced and $\widehat{\mathcal{W}}_g(0) = 2^{\frac{s-1}{2}}$ :

$f_{|\{(x,\bar{y})\in\mathbb{F}_2^{s+1}|w_H((x,\bar{y}))\ even\}}$ is balanced.

When $g_{|\{\bar{x}\in\mathbb{F}_2^{s-1}|w_H(\bar{x})\ odd\}}$ is balanced and $\widehat{\mathcal{W}}_g(0) = -2^{\frac{s-1}{2}}$ :

$f_{|\{(x,\bar{y})\in\mathbb{F}_2^{s+1}|w_H((x,\bar{y}))\ even\}}$ is balanced.

□

The additional cases, from the above theorem, with odd Hamming weight in $\mathbb{F}_2^{s+1}$ will be necessary for the development of the subsequent algorithm, to obtain $f$ from $g$.

Now, we consider the addition of a linear function.

**Theorem 10** *Let* $g : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$ *be a bent function and* $f : \mathbb{F}_2^{s+1} \to \mathbb{F}_2,\ (x, \bar{y}) \mapsto x\phi(\bar{y}) \oplus g_e(\bar{y})$ *be a Maiorana-McFarland bent function. The function* $f \oplus l_b$, $l_{\bar{b}}(\bar{x}, \bar{y}) = \bar{b} \cdot (\bar{x}, \bar{y})$, $\bar{y} = (\bar{x}, y_s)$, $\bar{x} \in \mathbb{F}_2^{s-1}$, $\bar{b} = (a_0, \bar{a}, a_s)$, $a_0, a_s \in \mathbb{F}_2$, $\bar{a} \in \mathbb{F}_2^{s-1}$ *is as follows:*

$$\text{If}\ \ a_0 = 1,\ (f \oplus l_{\bar{b}})_{|\{(x,\bar{y})|w_H((x,\bar{y}))\ odd\}}\ \ \text{is balanced.}$$
$$\text{If}\ \ a_0 = 0,\ (f \oplus l_{\bar{b}})_{|\{(x,\bar{y})|w_H((x,\bar{y}))\ even\}}\ \ \text{is balanced.}$$

*Proof* Let $\bar{x} = (y_1, \ldots, y_{s-1})$. Given $g$ a bent function, then $(g_e \oplus l_{(\bar{a},a_s)})_{|\{(\bar{x},y_s)|\bar{x}\in\mathbb{F}_2^{s-1}, w_H(\bar{x})\ even\}}$ is balanced or $(g_e \oplus l_{(\bar{a},a_s)})_{|\{(\bar{x},y_s)|\bar{x}\in\mathbb{F}_2^{s-1}, w_H(\bar{x})\ odd\}}$ is balanced.

Suppose w.l.o.g. that $(g_e \oplus l_{(\bar{a},a_s)})_{|\{(\bar{x},y_s)|\bar{x}\in\mathbb{F}_2^{s-1}, w_H(\bar{x})\ even\}}$ is balanced and $\widehat{\mathcal{W}}_{g_e}(\bar{a}, a_s) = 2^{\frac{s-1}{2}}$.

We can write $f \oplus l_{\bar{b}}$ as,

$$f(x, y_1, \ldots, y_{s-1}, y_s) \oplus l_{\bar{b}} = x\phi(y_1, \ldots, y_{s-1}, y_s) \oplus g_e(y_1, \ldots, y_{s-1}, y_s) \oplus a_0 x \oplus (\bar{a}, a_s)\cdot\bar{y},\ \ \bar{y} = (y_1, \ldots, y_s).$$

Let $a_0 = 1$. The elements with odd Hamming weight in $\mathbb{F}_2^{s+1}$ are in the following cases:

**Case 1**. Let $x = 0$, $y_s = 0$, and $w_H(y_1, \ldots, y_{s-1})$ odd. Then $f(0, y_1, \ldots, y_{s-1}, 0) \oplus l_{\bar{b}} = 0\cdot 1 \oplus g_e(y_1, \ldots, y_{s-1}, 0) \oplus l_{(\bar{a},a_s)} = g_{e_1}(y_1, \ldots, y_{s-1}, 0) \oplus l_{(\bar{a},a_s)} = 0$, $\ 2^{s-3} + 2^{\frac{s-3}{2}}$ times.

**Case 2**. Let $x = 0$, $y_s = 1$, and $w_H(y_1, \ldots, y_{s-1})$ even. Then, $f(0, y_1, \ldots, y_{s-1}, 1) \oplus l_{\bar{b}} = 0\cdot 1 \oplus g_e(y_1, \ldots, y_{s-1}, 1) \oplus l_{(\bar{a},a_s)} = g_{e_1}(y_1, \ldots, y_{s-1}, 1) \oplus l_{(\bar{a},a_s)} = 0$, $\ 2^{s-3}$ times.

**Case 3**. Let $x = 1$, $y_s = 0$, and $w_H(y_1, \ldots, y_{s-1})$ even. Then, $f(1, y_1, \ldots, y_{s-1}, 0) \oplus l_{\bar{b}} = 1\cdot 0 \oplus g_e(y_1, \ldots, y_{s-1}, 0) \oplus l_{(\bar{a},a_s)} \oplus 1 = g_{e_0}(y_1, \ldots, y_{s-1}, 0) \oplus l_{(\bar{a},a_s)} \oplus 1 = 0$, $\ 2^{s-3}$ times.

**Case 4**. Let $x = 1$, $y_s = 1$, and $w_H(y_1, \ldots, y_{s-1})$ odd. Then, $f(1, y_1, \ldots, y_{s-1}, 1) \oplus l_{\bar{b}} = 1 \cdot 0 \oplus g_e(y_1, \ldots, y_{s-1}, 1) \oplus l_{(\bar{a},a_s)} \oplus 1 = 0 \oplus g_{e_0}(y_1, \ldots, y_{s-1}, 1) \oplus l_{(\bar{a},a_s)} \oplus 1 = 0$, $\ 2^{s-3} - 2^{\frac{s-3}{2}}$ times.

Hence,

$$|f^{-1}_{|\{(x,\bar{y})\in\mathbb{F}_2^{s+1}|w_H(x,\bar{y})\ odd\}}(0)| = (2^{s-3}+2^{\frac{s-3}{2}})+(2^{s-3})+(2^{s-3})+(2^{s-3}-2^{\frac{s-3}{2}}) = 2^{s-1}.$$

Therefore, $(f \oplus l_{\bar{b}})_{|\{(x,\bar{y})|w_H((x,\bar{y}))\ odd\}}$ is balanced.

The demonstration when $a_0 = 0$ is similar to **Case 1**, **Case 4**, **Case 6** and **Case 7** of Theorem 9, and we obtain that $(f \oplus l_{\bar{b}})_{|\{(x,\bar{y})|w_H((x,\bar{y}))\ even\}}$ is balanced.

Similarly,

When $(g_e \oplus l_{(\bar{a},a_s)})_{|\{\bar{x}\in\mathbb{F}_2^{s-1}|w_H(\bar{x})\ even\}}$ is balanced and $\widehat{\mathcal{W}}_{g_e}(\bar{a}, a_s) = -2^{\frac{s-1}{2}}$ :

If $a_0 = 1$,
$(f \oplus l_{\bar{b}})_{|\{(x,\bar{y})|w_H((x,\bar{y}))\ odd\}}$ is balanced.
If $a_0 = 0$,
$(f \oplus l_{\bar{b}})_{|\{(x,\bar{y})|w_H((x,\bar{y}))\ even\}}$ is balanced.

When $(g_e \oplus l_{(\bar{a},a_s)})_{|\{\bar{x}\in\mathbb{F}_2^{s-1}|w_H(\bar{x})\ odd\}}$ is balanced and $\widehat{\mathcal{W}}_{g_e}(\bar{a},a_s)=2^{\frac{s-1}{2}}$ :

If $a_0=1$,
$(f\oplus l_{\bar{b}})_{|\{(x,\bar{y})|w_H((x,\bar{y}))\ odd\}}$ is balanced.
If $a_0=0$,
$(f\oplus l_{\bar{b}})_{|\{(x,\bar{y})|w_H((x,\bar{y}))\ even\}}$ is balanced.

When $(g_e \oplus l_{(\bar{a},a_s)})_{|\{\bar{x}\in\mathbb{F}_2^{s-1}|w_H(\bar{x})\ odd\}}$ is balanced and $\widehat{\mathcal{W}}_{g_e}(\bar{a},a_s)=-2^{\frac{s-1}{2}}$ :

If $a_0=1$,
$(f\oplus l_{\bar{b}})_{|\{(x,\bar{y})|w_H((x,\bar{y}))\ odd\}}$ is balanced.
If $a_0=0$,
$(f\oplus l_{\bar{b}})_{|\{(x,\bar{y})|w_H((x,\bar{y}))\ even\}}$ is balanced.

□

We can use the demonstration of Theorem 10 to have a simple way to obtain bent functions of any even dimension in its domain, greater than dimension of given the bent function. These new functions are specifically balanced for even Hamming weight in its domain.

In Algorithms 1 and 2 we are considering $\mathcal{A}:=\{\bar{x}\in\mathbb{F}_2^{s-1}|w_H(\bar{x})\ even\}$, $\mathcal{B}:=\{\bar{x}\in\mathbb{F}_2^{s-1}|w_H(\bar{x})\ odd\}$.

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

```
Input: $s-1\geq 2$ odd, $g_{s-1}(\bar{y})$, $g_{s-1}:\mathbb{F}_2^{s-1}\to\mathbb{F}_2$ be a bent function, $\{(x,\bar{y},y)\in\mathbb{F}_2^{s+1}\mid x,y\in\mathbb{F}_2,\bar{y}\in\mathbb{F}_2^{s-1}\}$
Output: $g_{new}(x,\bar{y},y)$ a bent function, $g_{new|\mathcal{A}}$ balanced
Integer $end$;
$new:=s-1$
while $new\neq end$ do
    for $x,y$ from 0 to 1 do
        if $\bar{y}$ is even, $x=1$, $y=1$ or $\bar{y}$ is odd, $x=1$, $y=0$ then
            $g_{new+2}(x,\bar{y},y)=1\oplus g_{new}(\bar{y})$;
        else
            $g_{new+2}(x,\bar{y},y)=g_{new}(\bar{y})$;
            $new:=new+2$;
            $\bar{y}=(x,\bar{y},y)$;
        end if
    end for
end while
```

## 5 Conclusions

We found, using the Maiorana-McFarland class, a new subclass of bent functions such that it is uniquely balanced on the set $\{x \in \mathbb{F}_2^n | w_H((x)\ even\}$. For this, we see, first, that all bent functions in $\mathcal{B}_n$ satisfy $\{x \in \mathbb{F}_2^n | w_H(x)\ even\}$ is balanced or $\{x \in \mathbb{F}_2^n | w_H(x)\ even\}$ is balanced. Also, if we have a bent function $f$ obtained by the Maiorana-McFarland construction, to see the behaviour when we consider the addition of a linear function $l_b$, $b = (a_0, \bar{a}, a)$, we now know that, if $a_0 = 0$, $(f \oplus l_b)_{||\{(x,\bar{y})|w_H((x,\bar{y}))\ even\}}$ is balanced and if $a_0 = 1$, $(f \oplus l_b)_{||\{(x,\bar{y})|w_H((x,\bar{y}))\ odd\}}$ is balanced.

## References

1. S. Picek, C. Carlet, S. Guilley, J. F. Miller and D. Jakobovic, "Evolutionary Algorithms for Boolean Functions in Diverse Domains of Cryptography", in Evolutionary Computation, vol. 24, no. 4, pp. 667-694, Dec. 2016.
2. C. Carlet, "On the confusion and diffusion properties of Maiorana–McFarland's and extended Maiorana–McFarland's functions", J. Complexity, pp. 182-204, vol. 20, 2004
3. Carlet, C. and Guillot, Ph. "A new representation of Boolean Functions", Springer-Verlag Berlin Heidelberg, 1999, pp. 94-103.
4. Rothaus 0. S. "On bent functions", J. Comb. Theory, Vol. 20, 1976, pp. 300-305
5. MacWilliams, F.J. and Sloane, N. J. *"The Theory of Error Correcting Codes"*, Elsevier Science Publisher B.V., North-Holland Mathematical Library, vol. 16, 1977.
6. J. F. Dillon. Elementary Hadamard Difference sets. Ph. D. Thesis, Univ. of Maryland (1974).
7. Natalia Tokareva "Bent Functions: Results and Application in Cryptography", Bent Functions: Results and Application in Cryptography, pp. 1-202, 2015.
8. 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

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

**Input:** $s-1 \geq 2$ odd, $g_{s-1}(\bar{x})$, $g_{s-1} : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$ a bent function, $b = (a_0, \bar{a}, a) \in \mathbb{F}_2^{s+1}$, $\{(x, \bar{x}, y) \in \mathbb{F}_2^{s+1} \mid x, y \in \mathbb{F}_2, \bar{x} \in \mathbb{F}_2^{s-1}\}$

**Output:** $(g_{new} \oplus l_{0,\bar{a},a})(x, \bar{x}, y)$ a bent function, $(g_{new} \oplus l_{0,\bar{a},a})_{|\mathcal{A}}$ balanced $(g_{new} \oplus l_{1,\bar{a},a})(x, \bar{x}, y)$ a bent function, $(g_{new} \oplus l_{1,\bar{a},a})_{|\mathcal{B}}$ balanced

```
Integer $end$;
$new := s - 1$
while $new \neq end$ do
    if $a_0 = 0$ and $a = 0$ then
        for $x, y$ from 0 to 1 do
            if ($\bar{y}$ is even, $x = 1$, $y = 1$) or ($\bar{y}$ is odd, $x = 1$, $y = 0$) then
                $(g_{new+2} \oplus l_{0,a,0})(x, \bar{x}, y) = 1 \oplus (g_{new} \oplus l_a)(\bar{x})$;
            else
                $(g_{new+2} \oplus l_{0,a,0})(x, \bar{x}, y) = (g_{new} \oplus l_a)(\bar{x})$;
            end if
            $new := new + 2$;    $\bar{y} = (x, \bar{y}, y)$;
        end for
    end if
    if $a_0 = 0$ and $a = 1$ then
        for $x, y$ from 0 to 1 do
            if ($\bar{y}$ is even, $x = 0$, $y = 1$) or $\{(\bar{y}$ is odd, $[(x = 0$, $y = 1)$ or $(x = 1$, $y = 0)$ or $(x = 1$, $y = 1)]\}$ then
                $(g_{new+2} \oplus l_{0,a,0})(x, \bar{x}, y) = 1 \oplus (g_{new} \oplus l_a)(\bar{x})$;
            else
                $(g_{new+2} \oplus l_{0,a,0})(x, \bar{x}, y) = (g_{new} \oplus l_a)(\bar{x})$;
            end if
            $new := new + 2$;    $\bar{y} = (x, \bar{y}, y)$;
        end for
    end if
    if $a_0 = 1$ and $a = 0$ then
        for $x, y$ from 0 to 1 do
            if ($\bar{y}$ is even, $x = 1$, $y = 0$) or ($\bar{y}$ is odd, $x = 1$, $y = 1$) then
                $(g_{new+2} \oplus l_{0,a,0})(x, \bar{x}, y) = 1 \oplus (g_{new} \oplus l_a)(\bar{x})$;
            else
                $(g_{new+2} \oplus l_{0,a,0})(x, \bar{x}, y) = (g_{new} \oplus l_a)(\bar{x})$;
            end if
            $new := new + 2$;    $\bar{y} = (x, \bar{y}, y)$;
        end for
    end if
    if $a_0 = 1$ and $a = 1$ then
        for $x, y$ from 0 to 1 do
            if $\{(\bar{y}$ is even, $[(x = 0$, $y = 1)$ or $(x = 1$, $y = 0)$ or $(x = 1$, $y = 1)]\}$ or ($\bar{y}$ is odd, $x = 0$, $y = 1$) then
                $(g_{new+2} \oplus l_{0,a,0})(x, \bar{x}, y) = 1 \oplus (g_{new} \oplus l_a)(\bar{x})$;
            else
                $(g_{new+2} \oplus l_{0,a,0})(x, \bar{x}, y) = (g_{new} \oplus l_a)(\bar{x})$;
            end if
            $new := new + 2$;    $\bar{y} = (x, \bar{y}, y)$;
        end for
    end if
end while
```