manuscript No.
(will be inserted by the editor)

Construction bent functions using the Maiorana McFarland class

Juan Carlos Ku-Cauich · Javier Diaz-Vargas

Received: August 26, 2024/ Accepted: date

Abstract We are using the extended Maiorana-McFarland construction to create new bent functions. When we start with a bent function of dimension $s - r$, we can produce a new function of dimension $s + r$ while ensuring that its balance is limited to the set of vectors with an even Hamming weight in its domain. We also compare this approach with the case where $r = 1$ and apply it multiple times. Finally, we provide an algorithm as an example, focusing on the case where $r = 2$ and another algorithm using $r = 1$ two times.

Kewords: Bent functions, Maiorana-McFarland, Affine spaces, Balancedness

1 Introduction

The bent functions are a special kind of boolean function [9]. These functions reach maximum non-linearity, a maximum distance from the affine functions, using Hamming distance. The mentioned functions are used in cryptography, for example, to resist linear attacks, and various methods are used to find good cryptographic properties [1], [8]. There are many methods to obtain unique characteristics of boolean functions, and there is a particular interest due to the large size of the search space (2^{2^n} boolean functions with domain $\mathbb{F}_2^n$). We find distinct constructions in Tokareva's book Chapter 8 [10].

We used the extended Maiorana-McFarland's class [2]. We are generalizing the particular case given in [4]. Hence, we consider an initial bent function $g : \mathbb{F}_2^{s-r} \to \mathbb{F}_2$. We define 2^r affine spaces subsets of $\mathbb{F}_2^s$ on which bent functions are

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

defined, extensions of the original g. Finally, considering a specific $\phi : \mathbb{F}_2^s \to \mathbb{F}_2^r$ function and using the previous definitions, we obtain a new bent function on $\mathbb{F}_2^{r+s}$.

Is this general case $r = l$ equal to applying l times the case $r = 1$. To answer this, we give a specific expression of the last case, obtaining a similar expression of the general case but with distinct new bent functions. To support this, we provide an algorithm that considers $r = 2$ and one more, considering the case $r = 1$ two times.

The particular way to array the elements of $\mathbb{F}_2^s$ is significant because it allows one to easily understand the structure of the affine spaces and helps demonstrate the distinct results.

2 Background

Before introducing the bent functions, we need definitions, such as the Hamming distance, affine functions, Fourier transform, and non-linearity. The literature provides all these, for example, [4], [5], [7], [10].

A **boolean function** is such that its images are 0 or 1. In general, they are defined with domain $\mathbb{F}_2^n$

Definition 1 Let f and g boolean functions. The **Hamming distance** between f and g is denoted $d_H(f, g)$, where $d_H(f, g) := \sharp\{x \mid f(x) \neq g(x)\}$.

Definition 2 The **algebraic normal** form (ANF) of a boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is expressed

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

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

Definition 3 A **linear function** is defined as $l_a(x) := a \cdot x$, for some $a \in \mathbb{F}_2^n$. The set of **affine functions** is denoted $\mathcal{A}_n$,

$$\mathcal{A}_n := \{l_a, l_a \oplus \bar{1} \mid a, \bar{1} \in \mathbb{F}_2^n\}.$$

$a \cdot x = a_1 x_1 \oplus \cdots \oplus a_n x_n$, $a = (a_1, \ldots, a_n)$, $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$.

The **non-linearity** of a boolean function f is the Hamming distance between f and the set of affine functions.

Theorem 1 *The non-linearity of a boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is characterized by*

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

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

$\widehat{\mathcal{W}_f}$ is called the **Hadamard Transform** of f.

Now, the definition of bent functions is extended to an affine subspace $\mathcal{C}$ (a subset of $\mathbb{F}_2^n$), as is mentioned in Proposition 1 of [2]. The non-linearity is characterized as follows:

Theorem 2 *Let be a function $f : \mathcal{C} \subset \mathbb{F}_2^n \to \mathbb{F}_2$, $\mathcal{C}$ be of dimension m. Then*

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

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

Theorem 3 *(Parseval's equation) Let be a function $f : \mathcal{C} \subseteq \mathbb{F}_2^n \to \mathbb{F}_2$, $\mathcal{C}$ be of dimension m. Then*

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

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

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

Theorem 4 *[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 $s - r$. Let also 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.*

3 Constructing new Maiorana bent functions

We desire to construct bent functions using the above theorem. In [4], the particular case $r = 1$ is considered. Using a similar technique, we consider a general case r.

First of all, let $g : \mathbb{F}_2^{s-r} \to \mathbb{F}_2$ be a bent function. Now, we define the functions ϕ and g_e:

Let $g_{e|\mathcal{C}_i} := g_{e_i}$, $i = 1, \ldots, 2^r$, such that $g_{e_i} : \mathcal{C}_i \subset \mathbb{F}_2^s \to \mathbb{F}_2$, where $\mathcal{C}_i$ is an affine space, and

$$g_{e_i}(\bar{x}_1 | \bar{x}_2) := g(\bar{x}_1),\ \bar{x}_1 \in \mathbb{F}_2^{s-r},\ \bar{x}_2 \in \mathbb{F}_2^r.$$

For a good definition of g_e, we need to define $\mathcal{C}_i$, $i = 1, \ldots, 2^r$, in such a way that there is a partition of $\mathbb{F}_2^s$. First, we define ϕ in the following way,

$$\mathcal{C}_1 := \phi^{-1}(0, \ldots, 0), \ldots, \mathcal{C}_{2^{r-1}} := \phi^{-1}(0, 1, \ldots, 1), \mathcal{C}_{2^{r-1}+1} := \phi^{-1}(1, 0, \ldots, 0), \ldots, \mathcal{C}_{2^r} := \phi^{-1}(1, \ldots, 1).$$

The images can be considered in any order with respect to the affine spaces. We illustrate the definition using lexicographic order.

In the case $r = 1$ given in [4], there are two inverse images, $\mathcal{C}_1 = \phi^{-1}(0)$ and $\mathcal{C}_2 = \phi^{-1}(1)$, where $\mathcal{C}_1$ and $\mathcal{C}_2$ are the sets of elements of even and odd Hamming weight of $\mathbb{F}_2^s$, respectively. We maintain this definition for $r = 1$.

Now, we define the affine spaces for the general case. In this work, the elements of $\mathbb{F}_2^s$ are considered vectors, words, or rows of $\mathbb{F}_2^s$ (assuming the vector space is an array).

Let $\mathcal{A}_1 \cup \mathcal{B}_1 = \mathbb{F}_2^s$, where $\mathcal{A}_1$ is the set of elements of even Hamming weight and $\mathcal{B}_1$ the set of elements of odd Hamming weigh. For $0 < r < s$, $i = 1, \ldots, r$, we can see that we are using the fundamental relations:

$$\begin{matrix} \mathcal{A}_{i+1} & \bar{0}_i \\ \mathcal{B}_{i+1} & \bar{1}_i \end{matrix} = \mathcal{A}_i \quad \text{and} \quad \begin{matrix} \mathcal{A}_{i+1} & \bar{1}_i \\ \mathcal{B}_{i+1} & \bar{0}_i \end{matrix} = \mathcal{B}_i, \quad i = 1, \ldots, r.$$

$$\bar{0}_i = \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}, \quad \bar{1}_i = \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \text{ are sets in arrays of dimension } 2^{s-(i+1)} \times 1.$$

Then, we can write a general case:

$$\mathbb{F}_2^s = \begin{matrix} \mathcal{A}_1 \\ -- \\ \mathcal{B}_1 \end{matrix} = \begin{matrix} \mathcal{C}_1 \\ \vdots \\ \mathcal{C}_{2^{r-1}} \\ --- \\ \mathcal{C}_{2^{r-1}+1} \\ \vdots \\ \mathcal{C}_{2^r} \end{matrix} = \begin{matrix} \mathcal{A}_{r+1} & \bar{0}_r \bar{x}_1^r \\ \mathcal{B}_{r+1} & \bar{1}_r \bar{x}_1^r \\ & \vdots \\ \mathcal{A}_{r+1} & \bar{1}_r \bar{x}_{2^{r-1}}^r \\ \mathcal{B}_{r+1} & \bar{0}_r \bar{x}_{2^{r-1}}^r \\ ---------- & \\ \mathcal{A}_{r+1} & \bar{0}_r \bar{x}_{2^{r-1}+1}^r \\ \mathcal{B}_{r+1} & \bar{1}_r \bar{x}_{2^{r-1}+1}^r \\ & \vdots \\ \mathcal{A}_{r+1} & \bar{1}_r \bar{x}_{2^r}^r \\ \mathcal{B}_{r+1} & \bar{0}_r \bar{x}_{2^r}^r \end{matrix}.$$

The sets $\bar{x}_i^r$, $i = 1, \ldots, 2^r$, are considered as arrays of dimensions $2^{s-(r+1)} \times (r-1)$, with each row (an element of the set) a bit string of length r. For $i = 1, \ldots, 2^r$, $\mathcal{C}_i$ is a $2^{s-r} \times s$ array, where

$$\mathcal{C}_i := \begin{matrix} \mathcal{A}_{r+1} & \bar{0}_r \bar{x}_i^r \\ \mathcal{B}_{r+1} & \bar{1}_r \bar{x}_i^r \end{matrix} \text{ if } i \text{ is odd }, \quad \mathcal{C}_i := \begin{matrix} \mathcal{A}_{r+1} & \bar{1}_r \bar{x}_i^r \\ \mathcal{B}_{r+1} & \bar{0}_r \bar{x}_i^r \end{matrix} \text{ if } i \text{ is even.}$$

Remark 1
1. $\mathcal{A}_{r+1}$ and $\mathcal{B}_{r+1}$ are sets ordered as arrays of dimensions $2^{s-(r+1)} \times (s-r)$.
2. The union of $\mathcal{A}_{r+1}$ and $\mathcal{B}_{r+1}$ is the set of all vectors in $\mathbb{F}_2^{s-r}$ of even and odd Hamming weights, respectively.

3. For each $i = 1, \ldots, 2^r$, all the rows of $\bar{x}_i^r$ are equal. Also,

$$\left[\bigcup_{i=1}^{2^{r-1}-1}(\bar{0}_r\bar{x}_i^r)\cup(\bar{1}_r\bar{x}_i^r)\right] \bigcup \left[\bigcup_{j=2}^{2^{r-1}}(\bar{1}_r\bar{x}_j^r)\cup(\bar{0}_r\bar{x}_j^r)\right] = \mathbb{F}_2^r,$$

$$\left[\bigcup_{i=2^{r-1}+1}^{2^r-1}(\bar{0}_r\bar{x}_i^r)\cup(\bar{1}_r\bar{x}_i^r)\right] \bigcup \left[\bigcup_{j=2^{r-1}+2}^{2^r}(\bar{1}_r\bar{x}_j^r)\cup(\bar{0}_r\bar{x}_j^r)\right] = \mathbb{F}_2^r,$$

   i odd, j even.
4. For $i = 1, \ldots, 2^{r-1}$, the element of $\bar{x}_i^r$ has an even Hamming weight if i is odd and an odd Hamming weight if i is even. For $i = 2^{r-1}+1, \ldots, 2^r$, the element of $\bar{x}_i^r$ has an odd Hamming weight if i is odd and an even Hamming weight if i is even.

Let's provide an example using $s = 5$ and $r = 3$ to illustrate the general array and definitions. Consider $\mathbb{F}_2^5 = \mathcal{A}_1 \cup \mathcal{B}_1$.

$$\mathbb{F}_2^5 = \begin{matrix}\mathcal{A}_1\\ --\\ \mathcal{B}_1\end{matrix} = \begin{matrix}\mathcal{C}_1\\ --\\ \mathcal{C}_2\\ --\\ \mathcal{C}_3\\ --\\ \mathcal{C}_4\\ --\\ \mathcal{C}_5\\ --\\ \mathcal{C}_6\\ --\\ \mathcal{C}_7\\ --\\ \mathcal{C}_8\end{matrix} = \begin{matrix}\mathcal{A}_4\ \bar{0}_3\ \bar{0}_2\\ \mathcal{B}_4\ \bar{1}_3\\ ----\ \bar{0}_1\\ \mathcal{A}_4\ \bar{1}_3\ \bar{1}_2\\ \mathcal{B}_4\ \bar{0}_3\\ ----\\ \mathcal{A}_4\ \bar{0}_3\ \bar{1}_2\\ \mathcal{B}_4\ \bar{1}_3\\ ----\ \bar{1}_1\\ \mathcal{A}_4\ \bar{1}_3\ \bar{0}_2\\ \mathcal{B}_4\ \bar{0}_3\\ ----\\ \mathcal{A}_4\ \bar{0}_3\ \bar{0}_2\\ \mathcal{B}_4\ \bar{1}_3\\ ---\ \bar{1}_1\\ \mathcal{A}_4\ \bar{1}_3\ \bar{1}_2\\ \mathcal{B}_4\ \bar{0}_3\\ ----\\ \mathcal{A}_4\ \bar{0}_3\ \bar{1}_2\\ \mathcal{B}_4\ \bar{1}_3\\ ----\ \bar{0}_1\\ \mathcal{A}_4\ \bar{1}_3\ \bar{0}_2\\ \mathcal{B}_4\ \bar{0}_3\end{matrix}$$

$$\mathcal{A}_1 = \begin{matrix}00000\\11000\\10100\\01100\\00110\\11110\\10010\\01010\\---\\00011\\11011\\10111\\01111\\00101\\11101\\10001\\01001\end{matrix} \qquad \mathcal{B}_1 = \begin{matrix}00001\\11001\\10101\\01101\\00111\\11111\\10011\\01011\\---\\00010\\11010\\10110\\01110\\00100\\11100\\10000\\01000\end{matrix}$$

$$\mathcal{C}_1 = \begin{matrix}00000\\11000\\10100\\01100\end{matrix} \quad \mathcal{C}_2 = \begin{matrix}00110\\11110\\10010\\01010\end{matrix} \quad \mathcal{C}_3 = \begin{matrix}00011\\11011\\10111\\01111\end{matrix} \quad \mathcal{C}_4 = \begin{matrix}00101\\11101\\10001\\01001\end{matrix}$$

$$\mathcal{C}_5 = \begin{matrix} 00001 \\ 11001 \\ 10101 \\ 01101 \end{matrix} \quad \mathcal{C}_6 = \begin{matrix} 00111 \\ 11111 \\ 10011 \\ 01011 \end{matrix} \quad \mathcal{C}_7 = \begin{matrix} 00010 \\ 11010 \\ 10110 \\ 01110 \end{matrix} \quad \mathcal{C}_8 = \begin{matrix} 00100 \\ 11100 \\ 10000 \\ 01000 \end{matrix}$$

$$\mathcal{A}_4 = \begin{matrix} 00 \\ 11 \end{matrix} \quad \mathcal{B}_4 = \begin{matrix} 10 \\ 01 \end{matrix} \quad \bar{0}_3 = \begin{matrix} 0 \\ 0 \end{matrix} \quad \bar{1}_3 = \begin{matrix} 1 \\ 1 \end{matrix}$$

Considering an arbitrary order,

$\mathcal{C}_i := \phi^{-1}(x_1, x_2, x_3)$, $i = 1, \ldots, 8$, $(x_1, x_2, x_3) \in \mathbb{F}_2^3$, $\mathcal{A}_4 \cup \mathcal{B}_4 = \mathbb{F}_2^2$.
$\mathcal{A}_4$ is the set of elements of even Hamming weight of $\mathbb{F}_2^2$.
$\mathcal{B}_4$ is the set of elements of odd Hamming weight of $\mathbb{F}_2^2$.

In order to have a good definition of g_e and g_{e_i}, $i = 1, \ldots, 2^r$:

Proposition 1 *The set $\{\mathcal{C}_1, \ldots, \mathcal{C}_{2^r}\}$ is a partition of $\mathbb{F}_2^s$ and each element is an affine space.*

Proof We know that

1. For $i = 1, \ldots, 2^r$. If i is odd,

$$a) \quad \mathcal{C}_i = \begin{matrix} & 0, x_{i(s-r+2)}, \ldots, x_{is} \\ \mathcal{A}_{r+1} & \vdots \\ & 0, x_{i(s-r+2)}, \ldots, x_{is} \\ & - - - - - - - - - - \\ & 1, x_{i(s-r+2)}, \ldots, x_{is} \\ \mathcal{B}_{r+1} & \vdots \\ & 1, x_{i(s-r+2)}, \ldots, x_{is} \end{matrix}.$$

In particular, $\mathcal{C}_1$ is an vectorial subspace of dimension $s-r$ and $(x_{1(s-r+2)}, \ldots, x_{1s}) = (0, \ldots, 0)$.

If i is even,

$$b) \quad \mathcal{C}_i = \begin{matrix} & 1, x_{i(s-r+2)}, \ldots, x_{is} \\ \mathcal{A}_{r+1} & \vdots \\ & 1, x_{i(s-r+2)}, \ldots, x_{is} \\ & - - - - - - - - - - \\ & 0, x_{i(s-r+2)}, \ldots, x_{is} \\ \mathcal{B}_{r+1} & \vdots \\ & 0, x_{i(s-r+2)}, \ldots, x_{is} \end{matrix}.$$

Now, we can write C_i, $i = 1, \ldots, 2^r$ as affine spaces:
Let $\mathcal{C}_i$ be of the form $a)$ and $\bar{x}_i = (\bar{x}_i', 0, x_{i(s-r+2)}, \ldots, x_{is}) \in \mathcal{C}_i$, $\bar{x}_i' \in \mathcal{A}_{r+1}$ a fix element. Then

$$\bar{x}_i + \mathcal{C}_1 = \mathcal{C}_i.$$

Let $\mathcal{C}_i$ be of the form b) and $\bar{x}_i = (\bar{x}'_i, 1, x_{i(s-r+2)}, \ldots, x_{is})$, $\bar{x}'_i \in \mathcal{A}_{r+1}$ a fix element. Then

$$\bar{x}_i + \mathcal{C}_1 = \mathcal{C}_i.$$

Additionally, the sets $\mathcal{C}_i$, $i = 1, \ldots, 2^r$ are distinct. Even more, their intersections are empty. We divide the demonstration into two cases: when $\mathcal{C}_i$, $i \in \{1, \ldots, 2^{r-1}\}$, has an empty intersection with the other affine spaces and when $\mathcal{C}_i$, $i \in \{2^{r-1}+1, \ldots, 2^r\}$ has an empty intersection.

In the first case, let $\bar{x}_i \in \mathcal{C}_i$, $i \in \{1, \ldots, 2^{r-1}\}$, $\bar{x}_i = (\bar{x}'_i, k, \bar{x}''_i)$, $k = 0$ or $k = 1$, $\bar{x}'_i \in \mathcal{A}_{r+1}$ or $\bar{x}'_i \in \mathcal{B}_{r+1}$, and $\bar{x}''_i$ a row of $\bar{x}^r_i$.

We claim, $\bar{x}_i \notin \mathcal{C}_j$, $j \neq i$, $j = 1, \ldots, 2^{r-1}$, because $\bar{x}''_i$ is not a row of $\bar{x}^r_j$. Also, $\bar{x}_i \notin \mathcal{C}_j$, $j \neq i$, $j = 2^{r-1}+1, \ldots, 2^r$, since in the unique case ,when $\bar{x}''_i = \bar{x}''_j$, we have $j = 2^r - i + 1$. In this case, $\bar{x}'_j \in \mathcal{B}_{r+1}$ if $\bar{x}'_i \in \mathcal{A}_{r+1}$ and $\bar{x}'_j \in \mathcal{A}_{r+1}$ if $\bar{x}'_i \in \mathcal{B}_{r+1}$. Thus, $\bar{x}_i \notin \mathcal{C}_j$.

In the other case, when $\bar{x}_i \in \mathcal{C}_i$, $i \in \{2^{r-1}+1, \ldots, 2^r\}$, the proof is similar.

The union of the affine spaces is the set $\mathbb{F}_2^s$. Therefore, we have the desired result.

□

Remark 2 [4]

1. Let $g : \mathbb{F}_2^{s-r} \to \mathbb{F}_2$ be a bent function such that $g_{|\mathcal{A}_{r+1}}$ is balanced.
   (a) If $\widehat{\mathcal{W}}_g(\bar{0}) = 2^{\frac{s-r}{2}}$, then
   $|g^{-1}_{|\mathcal{A}_{r+1}}(0)| = 2^{s-r-2}$
   $|g^{-1}_{|\mathcal{A}_{r+1}}(1)| = 2^{s-r-2}$
   $|g^{-1}_{|\mathcal{B}_{r+1}}(0)| = 2^{s-r-2} + 2^{\frac{s-r-2}{2}}$.
   $|g^{-1}_{|\mathcal{B}_{r+1}}(1)| = 2^{s-r-2} - 2^{\frac{s-r-2}{2}}$.
   (b) If $\widehat{\mathcal{W}}_g(\bar{0}) = -2^{\frac{s-r}{2}}$, then
   $|g^{-1}_{|\mathcal{A}_{r+1}}(0)| = 2^{s-r-2}$
   $|g^{-1}_{|\mathcal{A}_{r+1}}(1)| = 2^{s-r-2}$
   $|g^{-1}_{|\mathcal{B}_{r+1}}(0)| = 2^{s-r-2} - 2^{\frac{s-r-2}{2}}$.
   $|g^{-1}_{|\mathcal{B}_{r+1}}(1)| = 2^{s-r-2} + 2^{\frac{s-r-2}{2}}$.
2. Similar observations if $g_{|\mathcal{B}_{r+1}}$ is balanced.

The claim that if g is a bent function, then $g_{|\mathcal{A}_{r+1}}$ is balanced or $g_{|\mathcal{B}_{r+1}}$ is balanced [4] is essential to proving the following theorem.

Using the notation accorded above.

Theorem 5 *Let $g : \mathbb{F}_2^{s-r} \to \mathbb{F}_2$ be a bent function. Then, $g_{e_i} : \mathcal{C}_i \to \mathbb{F}_2$, $i = 1, \ldots, 2^r$, are bent functions.*

Proof Let $\bar{b} = (\bar{b}_1, b_{s-r+1}, \bar{b}_2) \in \mathbb{F}_2^s$, $\bar{b}_1 \in \mathbb{F}_2^{s-r}$, $\bar{b}_2 \in \mathbb{F}_2^{r-1}$, $b_{s-r+1} \in \mathbb{F}_2$ and $\bar{x} = (\bar{x}_1, x_{s-r+1}, \bar{x}_2) \in \mathcal{C}_i$, $\bar{x}_1 \in \mathbb{F}_2^{s-r}$, $\bar{x}_2 \in \mathbb{F}_2^{r-1}$, $x_{s-r+1} \in \mathbb{F}_2$, $i \in \{1, \ldots, 2^r\}$. Let $l_c(\bar{x}_1) = c \cdot \bar{x}_1$ be a linear function.

Let's prove that $g_{e_i} : \mathcal{C}_i \to \mathbb{F}_2$ is a bent function.

If $\bar{x} = (\bar{x}_1, x_{s-r+1}, \bar{x}_2) \in \mathcal{C}_i$, then $\bar{x}_2 = \bar{c}_2$, where $\bar{c}_2$ is a constant vector.

$$\begin{aligned}&\widehat{\mathcal{W}}_{g_{e_i}}(\bar{b})\\ &= \sum_{\bar{x} \in \mathcal{C}_i} (-1)^{g_{e_i}(\bar{x}) + \bar{x} \cdot \bar{b}} = \sum_{\bar{x} \in \mathcal{C}_i} (-1)^{g_{e_i}(\bar{x}) + \bar{x}_1 \cdot \bar{b}_1 + x_{s-r+1} b_{s-r+1} + \bar{c}_2 \bar{b}_2}.\end{aligned}$$

If $b_{s-r+1} = 0$,

$$\begin{aligned}&\widehat{\mathcal{W}}_{g_{e_i}}(b)\\ &= (-1)^{\bar{c}_2 \cdot \bar{b}_2} \sum_{\bar{x}_1 \in \mathbb{F}_2^{s-r}} (-1)^{g(\bar{x}_1) + \bar{x}_1 \cdot b_1} = (-1)^{\bar{c}_2 \cdot \bar{b}_2} \widehat{\mathcal{W}}_g(\bar{b}_1).\end{aligned}$$

If $b_{s-r+1} = 1$ and i is odd,

$$\begin{aligned}&\widehat{\mathcal{W}}_{g_{e_i}}(b)\\ &= (-1)^{\bar{c}_2 \bar{b}_2} \sum_{\bar{x} \in \mathcal{C}_i} (-1)^{g_{e_i}(\bar{x}_1, 0, \bar{x}_2) + \bar{x}_1 \cdot \bar{b}_1} + (-1)^{\bar{c}_2 \bar{b}_2} \sum_{\bar{x} \in \mathcal{C}_i} (-1)^{g_{e_i}(\bar{x}_1, 1, \bar{x}_2) + \bar{x}_1 \cdot \bar{b}_1 + 1}\\ &= (-1)^{\bar{c}_2 \bar{b}_2} \sum_{\bar{x}_1 \in \mathcal{A}_{r+1}} (-1)^{g_{e_i}(\bar{x}_1, 0, \bar{x}_2) + \bar{x}_1 \cdot \bar{b}_1} + (-1)^{\bar{c}_2 \bar{b}_2 + 1} \sum_{\bar{x}_1 \in \mathcal{B}_{r+1}} (-1)^{g_{e_i}(\bar{x}_1, 1, \bar{x}_2) + \bar{x}_1 \cdot \bar{b}_1}\end{aligned}$$

If $b_{s-r+1} = 1$ and i is even,

$$\begin{aligned}&\widehat{\mathcal{W}}_{g_{e_i}}(b)\\ &= (-1)^{\bar{c}_2 \bar{b}_2} \sum_{\bar{x}_1 \in \mathcal{B}_{r+1}} (-1)^{g_{e_i}(\bar{x}_1, 0, \bar{x}_2) + \bar{x}_1 \cdot \bar{b}_1} + (-1)^{\bar{c}_2 \bar{b}_2 + 1} \sum_{\bar{x}_1 \in \mathcal{A}_{r+1}} (-1)^{g_{e_i}(\bar{x}_1, 1, \bar{x}_2) + \bar{x}_1 \cdot \bar{b}_1}\end{aligned}$$

In all the cases when $b_{s-r+1} = 1$, given that $(g + l_{\bar{b}_1})_{|\mathcal{A}_{r+1}}$ is balanced or $(g + l_{\bar{b}_1})_{|\mathcal{B}_{r+1}}$ is balanced, then $\widehat{\mathcal{W}}_{g_{e_i}}(b) = \pm \widehat{\mathcal{W}}_g(\bar{b}_1)$. Since g is a bent function, then g_{e_i} is a bent function.

□

Using the previous definitions, we can use Theorem 4 to give bent functions.

Theorem 6 *Let $g : \mathbb{F}_2^{s-r} \to \mathbb{F}_2$ be a bent function, g_e, and ϕ defined as above. Then, the function*

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

is a bent function.

Proof By definition of ϕ, g_e, Proposition 1, and Theorem 5, we have all the elements satisfying the conditions of Theorem 4. Then, f is a bent function. □

We want to achieve specific balancedness in the domain of a Maiorana bent function. Hence, we will make some observations and provide additional conditions in the following theorem.

Remark 3 1. Let $l_a : \{x \in \mathbb{F}_2^n : w_H(x) \text{ even}\} \to \mathbb{F}_2$, $l_a(x) := a \cdot x$.
If $w_H(a) \neq n$ and $w_H(a) \neq 0$, then l_a is balanced.
If n is even and $a = \bar{1}$, then $l_a(\{x \in \mathbb{F}_2^n : w_H(x) \text{ even}\}) = \{0\}$.
2. Let $l_a : \{x \in \mathbb{F}_2^n : w_H(x) \text{ odd}\} \to \mathbb{F}_2$, $l_a(x) := a \cdot x$.
If $w_H(a) \neq n$ and $w_H(a) \neq 0$, then l_a is balanced.
If n is odd and $a = \bar{1}$, then $l_a(\{x \in \mathbb{F}_2^n : w_H(x) \text{ odd }\}) = \{1\}$.

Theorem 7 *Let r an integer odd, $g : \mathbb{F}_2^{s-r} \to \mathbb{F}_2$ be a bent function, and g_e defined as above. Also, let $\phi(\mathcal{C}_i)$ an image even if $i = 1, \ldots, 2^{r-1}$ and $\phi(\mathcal{C}_i)$ an image odd if $i = 2^{r-1} + 1, \ldots, 2^r$. Then, the bent function*

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

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

Proof Consider without loss of generality the case $g_{|\mathcal{A}_{r+1}}$ balanced and $\widehat{\mathcal{W}_g}(0) = 2^{\frac{s-r}{2}}$.

Since we desire to find balancedness in $\mathbb{F}_2^{r+s}$ restricted to the set of vectors of even Hamming weight, then we consider the following necessary subcases:

1. $\bar{x}$ even and $\bar{y} \in \mathcal{C}_i$, $i = 1, \ldots, 2^{r-1}$
2. $\bar{x}$ odd and $\bar{y} \in \mathcal{C}_i$, $i = 2^{r-1} + 1, \ldots, 2^r$

In the first subcase, we know $\phi(\mathcal{C}_i)$ has a constant even image, and $g_{e|\mathcal{C}_i} = g_{e_i}$ has $2^{s-r-2} + 2^{s-r-2} + 2^{\frac{s-r-2}{2}}$ images zero (Remark 2). Then, for each $\bar{x} \in \mathbb{F}_2^r$, depending if $\bar{x} \cdot \phi(\mathcal{C}_i)$ is zero or one, we have that $f(\bar{x}, \mathcal{C}_i) = \bar{x} \cdot \phi(\mathcal{C}_i) \oplus g_e(\mathcal{C}_i)$ has

$2^{s-r-2} + 2^{s-r-2} + 2^{\frac{s-r-2}{2}}$ images zero or
$2^{s-r-2} + 2^{s-r-2} - 2^{\frac{s-r-2}{2}}$ images zero respectively.

On the other hand, $\bar{y} \mapsto \bar{x} \cdot \phi(\bar{y})$ is balanced in $\mathcal{A}_1$ if $x \neq \bar{0}$ given $\bar{z} \mapsto \bar{x} \cdot \bar{z}$ is balanced when $\bar{z}$ is restricted to the set of vectors of even Hamming weight

of $\mathbb{F}_2^r$ (by Remark 3 item 1). Since there are $2^{r-1}-1$ elements $\bar{x} \in \mathbb{F}_2^r$ of even Hamming weight, distinct of vector zero, the total number of images zero is

$$(2^{r-1}-1)\left[2^{r-2}[(2^{s-r-2} + 2^{s-r-2} + 2^{\frac{s-r-2}{2}}) + (2^{s-r-2} + 2^{s-r-2} - 2^{\frac{s-r-2}{2}})]\right].$$

Also, $\bar{0} \cdot \phi(\bar{y}) = 0$, $\forall y \in \mathcal{A}_1$. Then, we have additionally

$2^{r-1}(2^{s-r-2} + 2^{s-r-2} + 2^{\frac{s-r-2}{2}})$ images zero.

The second subcase is similar, but $\bar{y} \mapsto \bar{x} \cdot \phi(\bar{y})$ is balanced if $w_H(\bar{x}) \neq n$, now in $\mathcal{B}_1$. Since there are $2^{r-1}-1$ elements $\bar{x} \in \mathbb{F}_2^r$ of odd Hamming weight, the total number of images zero is

$$(2^{r-1}-1)\left[2^{r-2}[(2^{s-r-2} + 2^{s-r-2} + 2^{\frac{s-r-2}{2}}) + (2^{s-r-2} + 2^{s-r-2} - 2^{\frac{s-r-2}{2}})]\right].$$

Also, $\bar{1} \cdot \phi(\bar{y}) = 1$, $\forall y \in \mathcal{B}_1$ by Remark 3 item 2. Then, we have additionally

$2^{r-1}(2^{s-r-2} + 2^{s-r-2} - 2^{\frac{s-r-2}{2}})$ images zero.

Finally, we can see that adding the number of all images equal to zero is 2^{s+r-2} Hence, f is balanced when restricted to the set of vectors of even Hamming weight.

If we consider the other cases, following a similar analysis, we obtain the same result.

□

The previous results generalise the case $r = 1$ given in [4]. Now, we desire to provide a relation between the particular case $r = 1$ and the general r.

4 Applying Maiorana many times

Suppose we have a bent function $g : \mathbb{F}_2^{s-l} \to \mathbb{F}_2$, $\bar{y} \mapsto g(\bar{y})$, and want to obtain a bent function over $\mathbb{F}_2^{l+s}$, but applying l times the Theorem 6 using the particular case $r = 1$. This is done in Algorithm 1 of [4] but does not obtain a specific expression of this new function. First, we consider the function ϕ_1' using the case $r = 1$ as in Theorem 6 over $\mathbb{F}_2^{s-l}$, then repeat the process l times. Hence, we obtain l functions:

$$\phi_1' : \mathbb{F}_2^{s-l+2(1)-1} \to \mathbb{F}_2,\ \phi_2' : \mathbb{F}_2^{s-l+2(2)-1} \to \mathbb{F}_2,\ \ldots,\ \phi_l' : \mathbb{F}_2^{s-l+2(l)-1} \to \mathbb{F}_2.$$

And then, we can define a function $\phi' : \mathbb{F}_2^{s+l-1} \to \mathbb{F}_2^l$ as follows:

$$\begin{aligned} &\phi'(x_2, \ldots, x_l, \bar{y}_1, \bar{y}_2) \\ &:= [\phi_l'(x_2, \ldots, x_l, \bar{y}_1, \bar{y}_2), \ldots, \phi_2'(x_l, \bar{y}_1, y_{s-l+1}, y_{s-l+2}), \phi_1'(\bar{y}_1, y_{s-l+1})], \end{aligned}$$

where $\bar{y}_1 \in \mathbb{F}_2^{s-l}$, $\bar{y}_2 = (y_{s-1+1}, \ldots, y_s) \in \mathbb{F}_2^l$ and $x_2, \ldots, x_l \in \mathbb{F}_2$.

Observe that, if we consider a constant $\bar{c} = (c_2, \ldots, c_l)$, then for all $(\bar{y}_1, \bar{y}_2) \in \mathcal{C}_i$, for each $i \in \{1, \ldots, 2^l\}$, the images of $\phi'(\bar{c}, \bar{y}_1, \bar{y}_2)$ are equal. Also, the set of images of $\phi'(\bar{c}, \bar{y}_1, \bar{y}_2)$ have all the elements of $\mathbb{F}_2^l$, repeat 2^{s-l} times. Do not forget the initial order accorded of $\mathbb{F}_2^s$.

More details in the next result.

Theorem 8 *Let $g : \mathbb{F}_2^{s-l} \to \mathbb{F}_2$, $\bar{y}_1 \mapsto g(\bar{y}_1)$, be a bent function and ϕ' defined as above. Then, there is a bent function*

$$g_l : \mathbb{F}_2^{l+s} \to \mathbb{F}_2,\ (\bar{x}, \bar{y}_1, \bar{y}_2) \mapsto \bar{x} \cdot \phi'(x_2, \ldots, x_l, \bar{y}_1, \bar{y}_2) \oplus g_e(\bar{y}_1, \bar{y}_2),$$

$$g_e(\bar{y}_1, \bar{y}_2) = g(\bar{y}_1)\ \forall \bar{y}_1 \in \mathbb{F}_2^{s-l},\ \bar{y}_2 \in \mathbb{F}_2^l,\ \bar{x} = (x_1, x_2, \ldots, x_l) \in \mathbb{F}_2^l.$$

Proof We proceed considering l times the particular case $r = 1$:

Step 1. Let $g : \mathbb{F}_2^{s-l} \to \mathbb{F}_2$, $\bar{y}_1 \mapsto g(\bar{y}_1)$, be a bent function. Then, $g_e : \mathbb{F}_2^{s-l+1} \to \mathbb{F}_2$ and $\phi_1' : \mathbb{F}_2^{s-l+1} \to \mathbb{F}_2$ are defined as in Theorem 6 (particular case $r = 1$) in order to obtain a bent function $g_1 : \mathbb{F}_2^{s-l+2(1)} \to \mathbb{F}_2$. Hence,

$$g_1(x_l, \bar{\mathbf{y}}_1, y_{s-l+1}) = x_l \phi_1'(\bar{\mathbf{y}}_1, y_{s-l+1}) + g_e(\bar{\mathbf{y}}_1, y_{s-l+1}).$$

Step 2. Similarly to step 1, the bent function $g_1 : \mathbb{F}_2^{s-l+2(1)} \to \mathbb{F}_2$ define $g_{1e} : \mathbb{F}_2^{s-l+2(1)+1} \to \mathbb{F}_2$ and $\phi_2' : \mathbb{F}_2^{s-l+2(1)+1} \to \mathbb{F}_2$, as done in Theorem 6. Hence, we obtain a $g_2 : \mathbb{F}_2^{s-l+2(2)} \to \mathbb{F}_2$ bent function. This bent function can be expressed in the following way:

$$\begin{aligned}
&g_2(x_{l-1}, \mathbf{x}_l, \bar{\mathbf{y}}_1, \mathbf{y}_{s-l+1}, y_{s-l+2}) \\
&= x_{l-1}\phi_2'(\mathbf{x}_l, \bar{\mathbf{y}}_1, \mathbf{y}_{s-l+1}, y_{s-l+2}) + g_{1e}(\mathbf{x_l}, \bar{\mathbf{y}}_1, \mathbf{y}_{s-l+1}, y_{s-l+2}) \\
&= x_{l-1}\phi_2(x_l, \bar{y}_1, y_{s-l+1}, y_{s-l+2}) + x_l\phi_1'(\bar{y}_1, y_{s-l+1}) + g_e(\bar{y}_1, y_{s-l+1}) \\
&= (x_{l-1}, x_l) \cdot [\phi_2'(x_l, \bar{y}_1, y_{s-l+1}, y_{s-l+2}), \phi_1'(\bar{y}_1, y_{s-l+1})] + g_e(\bar{y}_1, y_{s-l+1}).
\end{aligned}$$

Note that the relation of the step 1 gives the second equality.

Step 3. Proceeding in the same way l times, a bent function $g_l : \mathbb{F}_2^{s-l+2l} \to \mathbb{F}_2$ is obtained:

$$\begin{aligned}
&g_l(x_1, \mathbf{x}_2, \ldots, \mathbf{x}_{l-1}, \mathbf{x}_l, \bar{\mathbf{y}}_1, \mathbf{y}_{s-l+1}, \mathbf{y}_{s-l+2}, \ldots, \mathbf{y}_{s-l+l-1}, y_{s-l+l}) \\
&= \bar{x} \cdot [\phi_l'(x_2, \ldots, x_l, \bar{y}_1, \bar{y}_2), \ldots, \phi_2'(x_l, \bar{y}_1, y_{s-l+1}, y_{s-l+2}), \phi_1'(\bar{y}_1, y_{s-l+1})] \\
&\quad + g_e(\bar{y}_1, y_{s-l+1}) \\
&= \bar{x} \cdot \phi'(x_2, \ldots, x_l, \bar{y}_1, \bar{y}_2) + g_e(\bar{y}_1, \bar{y}_2).
\end{aligned}$$

Observe that we are abusing notation by indistinctly using the extension of g, namely g_e, with $r = 1$ and $r = l$.

Therefore,

$$g_l(\bar{x}, \bar{y}_1, \bar{y}_2) = \bar{x} \cdot \phi'(x_2, \ldots, x_l, \bar{y}_1, \bar{y}_2) + g_e(\bar{y}_1, \bar{y}_2).$$

□

In the following result, we do not need r to be an odd integer to obtain balancedness on the domain (restricted to the set of vectors of even Hamming weight) of the obtained bent function. Also, we consider ϕ' as in Theorem 8.

Corollary 1 *Let $g : \mathbb{F}_2^{s-r} \to \mathbb{F}_2$ be a bent function, with g_e and ϕ' defined as above. Then, the bent function*

$$g_r : \mathbb{F}_2^{r+s} \to \mathbb{F}_2,\ (\bar{x}, \bar{y}_1, \bar{y}_2) \mapsto \bar{x} \cdot \phi'(x_2, \ldots, x_l, \bar{y}_1, \bar{y}_2) \oplus g_e(\bar{y}_1, \bar{y}_2),$$

will satisfy that $f_{|\{(\bar{x},\bar{y}_1,\bar{y}_2)|w_H((\bar{x},\bar{y}_1\bar{y}_2))\ even\}}$ is balanced, where $g_e(\bar{y}_1, \bar{y}_2) = g(\bar{y}_1)\ \forall \bar{y}_1 \in \mathbb{F}_2^{s-r}, \bar{x} \in \mathbb{F}_2^r,\ \bar{y}_2 \in \mathbb{F}_2^r,\ \bar{x} = (x_1, x_2, \ldots, x_r),\ \bar{y}_2 = (y_{s-r+1}, \ldots, y_s)$.

Proof The proof is direct. We use Theorem 8 many times (in particular case $l = 1$). Each time, a balanced bent function restricted to the set of vectors of even Hamming weight in its domain is constructed [4].

□

5 Comparing constructions

We have obtained a similar expression considering the case $r = l$ and the case $r = 1$ l times. However, the obtained functions are different. First, we can see the dependence of ϕ' with the variables $x_2, \ldots, x_l$. In the following result, we demonstrate this claim. In this way, it rises to a greater variety of bent functions.

Theorem 9 *Let f be the bent function obtained using Theorem 6 when $r = l$, and let g_l be the bent function obtained using Theorem 8, $r = 1$ l times. Then, $f \neq g_l$.*

Proof Let ϕ be defined as Theorem 6 and $\phi' = (\phi'_1, \ldots, \phi'_l)$ be as in Theorem 8. We can express, $\phi = (\phi_1, \ldots, \phi_l)$, where $\phi_1, \ldots, \phi_l$ are component functions.

Let $i \in \{1, \ldots, 2^l \mid i \text{ even}\}$.

Suppose $\phi_l(\mathcal{C}_i) = \{0\}$ for some i. Then, $\forall (\bar{y}_1, \bar{y}_2) \in \mathcal{C}_i,\quad \bar{y}_1 \in \mathbb{F}_2^{s-l}, \bar{y}_2 \in \mathbb{F}_2^l$,

$$\begin{aligned} f(0, \ldots, 0, 1, \bar{y}_1, \bar{y}_2) &= (0, \ldots, 0, 1) \cdot \phi(\bar{y}_1, \bar{y}_2) \oplus g_e(\bar{y}_1, \bar{y}_2) \\ &= \phi_l(\bar{y}_1, \bar{y}_2) \oplus g_e(\bar{y}_1, \bar{y}_2) = g_e(\bar{y}_1, \bar{y}_2). \end{aligned}$$

On the other side,

$$\begin{aligned} g_l(0, \ldots, 0, 1, \bar{y}_1, \bar{y}_2) &= (0, \ldots, 0, 1) \cdot \phi'(0, \ldots, 0, 1, \bar{y}_1, \bar{y}_2) \oplus g_e(\bar{y}_1, \bar{y}_2) \\ &= \phi'_1(\bar{y}_1, y_{s-l+1}) + g_e(\bar{y}_1, \bar{y}_2) = 1 \oplus g_e(\bar{y}_1, \bar{y}_2). \end{aligned}$$

Then, we have distinct images.

In other case, if $\phi_l(\mathcal{C}_i) = \{1\}$, $\forall i \in \{1, \ldots, 2^l \mid i \text{ even}\}$.

First, suppose $\phi_{l-1}(\mathcal{C}_i) \neq \phi'_2(0, \bar{y}_1, y_{s-l+1}, y_{s-l+2})$, $(\bar{y}_1, \bar{y}_2) \in \mathcal{C}_i$, $\bar{y}_2 = (y_{s-l+1}, y_{s-l+2}, \ldots, y_s)$, for some i. Then,

$$f(0, \ldots, 0, 1, 0, \bar{y}_1, \bar{y}_2) = (0, \ldots, 0, 1, 0) \cdot \phi(\bar{y}_1, \bar{y}_2) \oplus g_e(\bar{y}_1, \bar{y}_2)$$
$$= \phi_{l-1}(\bar{y}_1, \bar{y}_2) \oplus g_e(\bar{y}_1, \bar{y}_2).$$

On the other side,

$$g_l(0, \ldots, 0, 1, 0, \bar{y}_1, \bar{y}_2) = (0, \ldots, 0, 1, 0) \cdot \phi'(0, \ldots, 0, 1, 0, \bar{y}_1, \bar{y}_2) \oplus g_e(\bar{y}_1, \bar{y}_2)$$
$$= \phi'_2(0, \bar{y}_1, y_{s-l+1}, y_{s-l+2}) + g_e(\bar{y}_1, \bar{y}_2)$$

Hence, we obtain distinct images.

Now, suppose $\phi_{l-1}(\mathcal{C}_i) = \phi'_2(0, \bar{y}_1, y_{s-l+1}, y_{s-l+2}) = 0$, $(\bar{y}_1, \bar{y}_2) \in \mathcal{C}_i$, $\bar{y}_2 = (y_{s-l+1}, y_{s-l+2}, \ldots, y_s)$, for some i. We know that exist 2^{l-2} of the i even elements such that $\phi'_2(0, \bar{y}_1, y_{s-l+1}, y_{s-l+2}) = 0$.

For the same chosen i:

$$f(0, \ldots, 0, 1, 1, \bar{y}_1, \bar{y}_2) = (0, \ldots, 0, 1, 1) \cdot \phi(\bar{y}_1, \bar{y}_2) \oplus g_e(\bar{y}_1, \bar{y}_2)$$
$$= \phi_{l-1}(\bar{y}_1, \bar{y}_2) \oplus \phi_l(\bar{y}_1, \bar{y}_2) \oplus g_e(\bar{y}_1, \bar{y}_2) = 0 \oplus 1 \oplus g_e(\bar{y}_1, \bar{y}_2) = 1 \oplus g_e(\bar{y}_1, \bar{y}_2).$$

On the other side,

$$g_l(0, \ldots, 0, 1, 1, \bar{y}_1, \bar{y}_2) = (0, \ldots, 0, 1, 1) \cdot \phi'(0, \ldots, 0, 1, 1, \bar{y}_1, \bar{y}_2) \oplus g_e(\bar{y}_1, \bar{y}_2)$$
$$= \phi'_2(1, \bar{y}_1, y_{s-l+1}, y_{s-l+2}) \oplus \phi'_1(\bar{y}_1, y_{s-l+1}) \oplus g_e(\bar{y}_1, \bar{y}_2) = 1 \oplus 1 \oplus g_e(\bar{y}_1, \bar{y}_2).$$
$$= g_e(\bar{y}_1, \bar{y}_2).$$

Again, we obtain distinct images.

Given the conclusions of all the cases, we have images where f and g_l are distinct. In this way, we obtain the desired result.

□

In the following, we present two algorithms, one using the case $r = 2$ and the other using two times the case $r = 1$. The algorithms are obtained mainly by analysing the images of ϕ and ϕ' functions. As we demonstrate, we can see that, in this particular case, the bent functions constructed in each algorithm are different.

We present an example for the general case r. Using a particular case $r = 2$, we obtain bent functions over $\mathbb{F}_2^{s+3}$ given a bent function over $\mathbb{F}_2^{s-1}$. We are defining $\phi(\mathcal{C}_1) := (0, 0)$, $\phi(\mathcal{C}_2) := (1, 1)$, $\phi(\mathcal{C}_3) := (1, 0)$, and $\phi(\mathcal{C}_4) := (0, 1)$. Note that this is a particular case for the ϕ function.

In Algorithm 1,the union of $\mathcal{A}_3$ and $\mathcal{B}_3$ is the set of all vectors in $\mathbb{F}_2^{s-1}$ with even and odd Hamming weights, respectively, and we are using

$$\mathcal{C}_1 := \begin{matrix} \mathcal{A}_3 & \bar{0} & \bar{0} \\ \mathcal{B}_3 & \bar{1} & \bar{0} \end{matrix}.$$

Also, we give an algorithm using $r = 1$ twice (Algorithm 2). Comparing it with Algorithm 1, we can see that we obtain a different bent function.

Algorithm 1 `Extended Maiorana-McFarland` $r = 2$

Input: $s-1 \geq 2$ even, $g_{s-1}(\bar{y})$, $g_{s-1} : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$ be a bent function, $\{(x_1, x_2, \bar{y}, y_1, y_2) \in \mathbb{F}_2^{s-1+4} \mid x_1, x_2, y_1, y_2 \in \mathbb{F}_2, \bar{y} \in \mathbb{F}_2^{s-1}\}$
Output: $f(x_1, x_2, \bar{y}, y_1, y_2)$ a bent function, $f_{|\mathcal{A}_1}$ balanced

for x_1, x_2 from 0 to 1 **do**
  if $(\bar{y}, y_1, y_2) \in \mathcal{C}_2 := \begin{matrix} \mathcal{A}_3 & \bar{1} & \bar{1} \\ \mathcal{B}_3 & \bar{0} & \bar{1} \end{matrix}$,
    $[(x_1, x_2) = (0,1)$ **and** $(x_1, x_2) = (1,0)]$
    or
  $(\bar{y}, y_1, y_2) \in \mathcal{C}_3 := \begin{matrix} \mathcal{A}_3 & \bar{0} & \bar{1} \\ \mathcal{B}_3 & \bar{1} & \bar{1} \end{matrix}$,
    $[(x_1, x_2) = (1,0)$ **and** $(x_1, x_2) = (1,1)]$
    or
  $(\bar{y}, y_1, y_2) \in \mathcal{C}_4 := \begin{matrix} \mathcal{A}_3 & \bar{1} & \bar{0} \\ \mathcal{B}_3 & \bar{0} & \bar{0} \end{matrix}$,
    $[(x_1, x_2) = (0,1)$ **and** $(x_1, x_2) = (1,1)]$ **then**
    $f(x_1, x_2, \bar{y}, y_1, y_2) = 1 \oplus g_{s-1}(\bar{y})$;
  else
    $f(x_1, x_2, \bar{y}, y_1, y_2) = g_{s-1}(\bar{y})$;
  end if
end for

Algorithm 2 `Extended Maiorana-McFarland` two times $r = 1$

Input: $s-1 \geq 2$ even, $g_{s-1}(\bar{y})$, $g_{s-1} : \mathbb{F}_2^{s-1} \to \mathbb{F}_2$ be a bent function, $\{(x_1, x_2, \bar{y}, y_1, y_2) \in \mathbb{F}_2^{s+3} \mid x_1, x_2, y_1, y_2 \in \mathbb{F}_2, \bar{y} \in \mathbb{F}_2^{s-1}\}$
Output: $g_{s+3}(x_1, x_2, \bar{y}, y_1, y_2)$ a bent function, $g_{s+3|\mathcal{A}_1}$ balanced

for x_1, x_2, y_1, y_2 from 0 to 1 **do**
  if $\bar{y}$ is even,
    $[(x_1, x_2) = (0,1)$ **and** $[(y_1, y_2) = (1,1)$ **or** $(1,0)]]$ **or**
    $[(x_1, x_2) = (1,0)$ **and** $[(y_1, y_2) = (0,1)$ **or** $(1,0)]]$ **or**
    $[(x_1, x_2) = (1,1)$ **and** $[(y_1, y_2) = (0,0)$ **or** $(1,0)]]$
    or
  $\bar{y}$ is odd,
    $[(x_1, x_2) = (0,1)$ **and** $[(y_1, y_2) = (0,1)$ **or** $(0,0)]]$ **or**
    $[(x_1, x_2) = (1,0)$ **and** $[(y_1, y_2) = (1,1)$ **or** $(0,0)]]$ **or**
    $[(x_1, x_2) = (1,1)$ **and** $[(y_1, y_2) = (1,0)$ **or** $(0,0)]]$ **then**
  $g_{s+3}(x_1, x_2, \bar{y}, y_1, y_2) = 1 \oplus g_{s-1}(\bar{y})$;
  else
    $g_{s+3}(x_1, x_2, \bar{y}, y_1, y_2) = g_{s-1}(\bar{y})$;
  end if
end for

6 Conclusions

We generalize Maiorana-McFarland's construction of [4], now for a general positive integer r; namely, given a bent function $g : \mathbb{F}_2^{s-r} \to \mathbb{F}_2$, we construct a bent function $f : \mathbb{F}_2^{s+r} \to \mathbb{F}_2$.

For this, a particular way to array the elements of $\mathbb{F}_2^s$ is considered, and 2^r affine spaces $\mathcal{C}_i$, $i = 1, \ldots, 2^r$, are provided, demonstrating that these are a partition of $\mathbb{F}_2^s$. Furthermore, a bent function on each $\mathcal{C}_i$ is defined for each affine space.

The images of $\phi : \mathbb{F}_2^s \to \mathbb{F}_2^r$ can be defined in any order. Then, we obtain many distinct bent functions only with one bent function, g. But if we want to get a bent function f with balancedness restricted to the set of vectors of even Hamming weight in its domain, we need to define the images $\phi(\mathcal{C}_i)$ of even Hamming weight if $i \in \{1, \ldots, 2^{r-1}\}$. And also, we need to consider r odd.

This new bent function is distinct concerning the constructed bent function when we repeat the case $r = 1$ many times: In Theorem 8, we obtain an expression of the new bent functions applying $r = 1$ l times (with balancedness restricted to the set of vectors of even Hamming weigh). The construction is similar to Maiorana-McFarland's expression, but ϕ' (in place of ϕ) depends on extras $l - 1$ variables of g_l, the new bent function.

The two given algorithms can obtain distinct bent functions incremented in four dimensions relative to the original bent function. We can follow the same procedure to get new bent functions by increasing the dimension by multiples of four.

A desired outcome is to find total balanced functions with high non-linearity, initializing from bent functions [3], [6]. In future research, starting from the Maiorana bent function's partial balancedness, one can find a total balancedness by reducing the non-linearity as little as possible.

References

1. 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
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. Dobbertin, H. "Construction of bent functions and balanced Boolean functions with high nonlinearity", In: Preneel, B. (eds) Fast Software Encryption. FSE 1994. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg vol. 1008, (1995). $https://doi.org/10.1007/3-540-60590-8\_5$
4. Ku-Cauich, J.C., Diaz-Vargas, J., Mandujano-Velazquez, S. "Bent functions construction using extended Maiorana-McFarland's class", Cryptology ePrint Archive, 2024. https://eprint.iacr.org/2024/413
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. 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, vol. 13774, pp. 449-470 (2022).
7. Mesnager, S. "Bent Functions Fundamentals and Results", Springer Cham, 2016.
8. 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.
9. Rothaus 0. S. "On bent functions", J. Comb. Theory, Vol. 20, 1976, pp. 300-305
10. Tokareva, N. "Bent Functions: Results and Application in Cryptography", Bent Functions: Results and Application in Cryptography, pp. 1-202, 2015.