A New Iterative Method to Construct Bent Functions[1]

JOAN-JOSEP CLIMENT[(a)], FRANCISCO J. GARCÍA[(b)], VERÓNICA REQUENA[(a)]
[(a)]Departament de Ciència de la Computació i Intel·ligència Artificial
[(b)]Departament de Fonaments de l'Anàlisi Econòmica
Universitat d'Alacant
Ap. 99 E-03080 Alacant
SPAIN

Abstract: In this paper we present a new method to construct iteratively new bent functions of $n+2$ variables from a bent functions of n variables. We generate bent functions using the concept of minterm for Boolean functions.

Key-words: Boolean function, cryptography, nonlinearity, bent function, balanced sequence, minterm.

1 Introduction

Boolean functions, components of S-boxes, are used in different types of cryptographic applications such as in block ciphers, stream ciphers and hash functions [3, 4, 8], and coding theory [2, 5, 6]. A variety of criteria for choosing Boolean functions determine their ability to provide security and its importance to be used in different applications. A high value of the nonlinearity ensure that the best affine approximation attack will fail [7, 10]. Boolean function achieving the maximum nonlinearity are called bent functions [11, 13]. In this paper we present a method to construct bent functions for any value of n. Bent functions with 4 variables have been very studied, and therefore we know the number of bent functions that there are. However a general method to generate all the bent functions in n variables is unknown for $n \geq 6$ (see for example [1, 9, 11, 12]). All the bent functions are only known for $n = 4$; so, we use this fact and the concept of minterm to construct iteratively bent functions for $n \geq 6$.

2 Preliminaries

Let $B = \{0, 1\}$, a **Boolean function** of n variables is a function $f : B^n \longrightarrow B$. For $i = 0, 1, \ldots, 2^n - 1$, let $\boldsymbol{\beta}_i$ be the vector in B^n whose integer representation is i. Obviously, $B^n = \{\boldsymbol{\beta}_i\}_{i=0}^{2^n-1}$. For $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ in B^n, let $\boldsymbol{\alpha} \oplus \boldsymbol{\beta}$ be the component-wise binary addition $\oplus$. For a Boolean function f, the $(0, 1)$-sequence

$$\xi_f = (f(\boldsymbol{\beta_0}),\ f(\boldsymbol{\beta_1}),\ \ldots\ , f(\boldsymbol{\beta_{2^n-1}}))$$

is called the **truth table** of f.

We say that a Boolean function f is an **affine function** if it takes the form

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{i=1}^{n} a_i x_i \oplus b,$$

where $a_i, b \in B$ for $i = 1, 2, \ldots, n$. We denote by $\mathcal{A}_n$ the set of all affine functions; if $b = 0$, we said that f is a **linear function**.

The **Hamming weight** of a $(0, 1)$-sequence $\boldsymbol{\alpha}$, denoted by $\mathrm{w}(\boldsymbol{\alpha})$, is the number of 1 in $\boldsymbol{\alpha}$. A $(0, 1)$-sequence is **balanced** if it contains an equal number of 0 and 1. A Boolean function f is **balanced** if its truth table is balanced. The **Hamming distance** between two $(0, 1)$-sequences $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, denoted by $\mathrm{d}(\boldsymbol{\alpha}, \boldsymbol{\beta})$, is the number of positions where the two sequences differ, that is $\mathrm{d}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \mathrm{w}(\boldsymbol{\alpha} \oplus \boldsymbol{\beta})$. For two Boolean functions f and g we have that $\mathrm{w}(f) = \mathrm{w}(\xi_f)$ and $\mathrm{d}(f, g) = \mathrm{d}(\xi_f, \xi_g)$.

The **nonlinearity** NL of a Boolean function f is

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

and it is well known (see [13]) that

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

The Boolean functions that attains the maximum nonlinearity are called **bent functions** (see [13]), in this case, n must be even. It follows then that $f(\boldsymbol{x})$ is a bent function if and only $1 \oplus f(\boldsymbol{x})$ is a bent function.

A **minterm** on n variables $x_1, x_2, \ldots, x_n$ is a Boolean function

$$m_{e_1 e_2 \cdots e_n}(x_1, x_2, \ldots, x_n) = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$$

where

$$x^e = \begin{cases} x, & \text{if } e = 1, \\ 1 \oplus x, & \text{if } e = 0. \end{cases}$$

[1]This work was partially supported by Spanish grant MTM2005-05759

We write $m_i(\boldsymbol{x})$ instead of $m_{\boldsymbol{\beta}_i}(\boldsymbol{x})$, and therefore $m_i(\boldsymbol{x}) = 1$ if only if $\boldsymbol{x} = \boldsymbol{\beta}_i$. So, the truth table of $m_i(\boldsymbol{x})$ has a 1 in the ith position and 0 elsewhere. Consequently,

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

It is well known that any Boolean function f can be expressed as

$$f(\boldsymbol{x}) = \bigoplus_{i \in I} m_i(\boldsymbol{x})$$

for a subset I of $\{1, 2, \ldots, n\}$.

According with the above comments, f is a bent function if and only if $f(\boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{x})$ is a balanced function [13]; in addition, $g(\boldsymbol{x}) = f(\boldsymbol{x} \oplus \boldsymbol{\alpha})$ is also a bent function. In addition if f is a bent function, then it has exactly $2^{n-1} \pm 2^{\frac{n}{2}-1}$ minterms; so that f is not balanced.

3 Main results

In the following, we consider that (i_0, i_1, i_2, i_3) and (j_0, j_1, j_2, j_3) are permutations of $(0, 1, 2, 3)$. Also, let $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, y_2)$ (i_0, i_1, i_2, i_3).

The following two technical lemmas, whose proofs can be obtain directly from the definition of minterm, are the keys to proof our main result.

Lemma 1: *For each minterm in n variables, it is possible to construct 4 different minterms in $n+2$ variables.*

Lemma 2: $m_{\boldsymbol{\alpha}}(\boldsymbol{\beta} \oplus \boldsymbol{x}) = m_{\boldsymbol{\alpha}\oplus\boldsymbol{\beta}}(\boldsymbol{x})$ *for* $\boldsymbol{\alpha}, \boldsymbol{\beta} \in B^n$.

Next theorem, which is the main result of this paper, allow us to construct a new bent function of $n+2$ variables starting with a bent function of n variables.

Theorem 1: *Let $f(\boldsymbol{x})$ be a bent function with n variables. Assume that for nonzero $\boldsymbol{\lambda}, \boldsymbol{\mu} \in B^n$ the equality*

$$f(\boldsymbol{x}) \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\mu} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x}) = 1 \quad (1)$$

holds. Then

$$\begin{aligned} H(\boldsymbol{y}, \boldsymbol{x}) &= m_{i_0}(\boldsymbol{y}) f(\boldsymbol{x}) \oplus m_{i_1}(\boldsymbol{y}) f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \\ &\oplus m_{i_2}(\boldsymbol{y}) f(\boldsymbol{\mu} \oplus \boldsymbol{x}) \\ &\oplus m_{i_3}(\boldsymbol{y}) \left(f(\boldsymbol{x}) \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\mu} \oplus \boldsymbol{x}) \right) \end{aligned}$$

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

PROOF: For all nonzero $(\boldsymbol{\beta}, \boldsymbol{\alpha}) \in B^2 \times B^n$ we need to prove that the function

$$H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x}) = H(\boldsymbol{y}, \boldsymbol{x}) \oplus H((\boldsymbol{\beta}, \boldsymbol{\alpha}) \oplus (\boldsymbol{y}, \boldsymbol{x}))$$

is balanced.

Firstly, observe that from lemma 2

$$\begin{aligned} &H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x}) \\ &\quad = m_{i_0}(\boldsymbol{y}) f(\boldsymbol{x}) \oplus m_{i_1}(\boldsymbol{y}) f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \\ &\qquad \oplus m_{i_2}(\boldsymbol{y}) f(\boldsymbol{\mu} \oplus \boldsymbol{x}) \\ &\qquad \oplus m_{i_3}(\boldsymbol{y}) \left(f(\boldsymbol{x}) \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\mu} \oplus \boldsymbol{x}) \right) \\ &\qquad \oplus m_{i_0 \oplus \boldsymbol{\beta}}(\boldsymbol{y}) f(\boldsymbol{\alpha} \oplus \boldsymbol{x}) \\ &\qquad \oplus m_{i_1 \oplus \boldsymbol{\beta}}(\boldsymbol{y}) f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x}) \\ &\qquad \oplus m_{i_2 \oplus \boldsymbol{\beta}}(\boldsymbol{y}) f(\boldsymbol{\alpha} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x}) \\ &\qquad \oplus m_{i_3 \oplus \boldsymbol{\beta}}(\boldsymbol{y}) \left(f(\boldsymbol{\alpha} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x}) \right. \\ &\qquad\quad \left. \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x}) \right). \end{aligned}$$

We considerer different cases depending on $(\boldsymbol{\beta}, \boldsymbol{\alpha})$.

- Assume that $\boldsymbol{\alpha} = \boldsymbol{0}_n$ and $\boldsymbol{\beta} \neq \boldsymbol{0}_2$. Then, we have that

  $$\begin{aligned} &H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x}) \\ &\quad = \left(m_{i_0}(\boldsymbol{y}) \oplus m_{i_0 \oplus \boldsymbol{\beta}}(\boldsymbol{y}) \right) f(\boldsymbol{x}) \\ &\qquad \oplus \left(m_{i_1}(\boldsymbol{y}) \oplus m_{i_1 \oplus \boldsymbol{\beta}}(\boldsymbol{y}) \right) f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \\ &\qquad \oplus \left(m_{i_2}(\boldsymbol{y}) \oplus m_{i_2 \oplus \boldsymbol{\beta}}(\boldsymbol{y}) \right) f(\boldsymbol{\mu} \oplus \boldsymbol{x}) \\ &\qquad \oplus \left(m_{i_3}(\boldsymbol{y}) \oplus m_{i_3 \oplus \boldsymbol{\beta}}(\boldsymbol{y}) \right) \left(f(\boldsymbol{x}) \right. \\ &\qquad\quad \left. \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\mu} \oplus \boldsymbol{x}) \right). \end{aligned}$$

  – If $\boldsymbol{\beta} = 1$, then, after some tedious algebraic manipulations, we obtain

  $$H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x}) = f(\boldsymbol{x}) \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x})$$

  and consequently, if $\boldsymbol{\xi}_{\boldsymbol{\lambda}}$ is the truth table of $f(\boldsymbol{x}) \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x})$, then the truth table of $H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x})$ has 4 blocs,

  $$\boldsymbol{\xi}_{\boldsymbol{\lambda}} \quad \boldsymbol{\xi}_{\boldsymbol{\lambda}} \quad \boldsymbol{\xi}_{\boldsymbol{\lambda}} \quad \boldsymbol{\xi}_{\boldsymbol{\lambda}}$$

  which is balanced, because $\boldsymbol{\xi}_{\boldsymbol{\lambda}}$ is balanced.

  – If $\boldsymbol{\beta} = 2$, then

  $$H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x}) = f(\boldsymbol{x}) \oplus f(\boldsymbol{\mu} \oplus \boldsymbol{x})$$

  which is analogous to the previous case.

- If $\boldsymbol{\beta} = 3$,

$$H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x}) = f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\mu} \oplus \boldsymbol{x}).$$

which also is analogous to the first case, because

$$f(\boldsymbol{\lambda}\oplus\boldsymbol{x})\oplus f(\boldsymbol{\mu}\oplus\boldsymbol{x}) = f(\boldsymbol{z})\oplus f(\boldsymbol{\mu}\oplus\boldsymbol{\lambda}\oplus\boldsymbol{z})$$

for $\boldsymbol{z} = \boldsymbol{\lambda} \oplus \boldsymbol{x}$ and $\boldsymbol{\lambda} \neq \boldsymbol{\mu}$.

- Assume that $\boldsymbol{\alpha} \neq \mathbf{0}_n$ and $\boldsymbol{\beta} = \mathbf{0}_2$. Then, we have that

$$\begin{aligned}
&H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x})\\
&= m_{i_0}(\boldsymbol{y})\left(f(\boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{x})\right)\\
&\quad \oplus m_{i_1}(\boldsymbol{y})\left(f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x})\right)\\
&\quad \oplus m_{i_2}(\boldsymbol{y})\left(f(\boldsymbol{\mu} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x})\right)\\
&\quad \oplus m_{i_3}(\boldsymbol{y})\left(f(\boldsymbol{x}) \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\mu} \oplus \boldsymbol{x})\right.\\
&\qquad \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x})\\
&\qquad \left.\oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x})\right)\\
&= m_{i_0}(\boldsymbol{y})\left(f(\boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{x})\right)\\
&\quad \oplus m_{i_1}(\boldsymbol{y})\left(f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x})\right)\\
&\quad \oplus m_{i_2}(\boldsymbol{y})\left(f(\boldsymbol{\mu} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x})\right)\\
&\quad \oplus m_{i_3}(\boldsymbol{y})\left(f(\boldsymbol{\lambda} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x})\right.\\
&\qquad \left.\oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x})\right)
\end{aligned}$$

where the last equality follows from expression (1). Now, taking into account that the following functions

$$f(\boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{x}),$$

$$f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x}),$$
$$f(\boldsymbol{\mu} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x}),$$
$$f(\boldsymbol{\lambda} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x})$$

are balanced, we obtain that $H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x})$ is balanced.

- Assume that $\boldsymbol{\alpha} \neq \mathbf{0}_n$ and $\boldsymbol{\beta} \neq \mathbf{0}_2$. Then, from expression (1), we have that

$$\begin{aligned}
&H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x})\\
&= m_{i_0}(\boldsymbol{y})f(\boldsymbol{x}) \oplus m_{i_1}(\boldsymbol{y})f(\boldsymbol{\lambda} \oplus \boldsymbol{x})\\
&\quad \oplus m_{i_2}(\boldsymbol{y})f(\boldsymbol{\mu} \oplus \boldsymbol{x})\\
&\quad \oplus m_{i_3}(\boldsymbol{y})\left(1 \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x})\right)\\
&\quad \oplus m_{i_0\oplus\boldsymbol{\beta}}(\boldsymbol{y})f(\boldsymbol{\alpha} \oplus \boldsymbol{x})\\
&\quad \oplus m_{i_1\oplus\boldsymbol{\beta}}(\boldsymbol{y})f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x})\\
&\quad \oplus m_{i_2\oplus\boldsymbol{\beta}}(\boldsymbol{y})f(\boldsymbol{\alpha} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x})\\
&\quad \oplus m_{i_3\oplus\boldsymbol{\beta}}(\boldsymbol{y})\left(1 \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x})\right)
\end{aligned}$$

For $\boldsymbol{\beta} = 1$, then

$$\begin{aligned}
&H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x})\\
&= m_{i_0}(\boldsymbol{y})\left(f(\boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x})\right)\\
&\quad \oplus m_{i_1}(\boldsymbol{y})\left(f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{x})\right)\\
&\quad \oplus m_{i_2}(\boldsymbol{y})\left(f(\boldsymbol{\mu} \oplus \boldsymbol{x}) \oplus 1\right.\\
&\qquad \left.\oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x})\right)\\
&\quad \oplus m_{i_3}(\boldsymbol{y})\left(1 \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x})\right.\\
&\qquad \left.\oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x})\right)
\end{aligned}$$

- For $\boldsymbol{\alpha} = \boldsymbol{\lambda}$, we have that

$$H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x}) = m_{i_2}(\boldsymbol{y}) \oplus m_{i_3}(\boldsymbol{y})$$

which is balanced.

- For $\boldsymbol{\alpha} = \boldsymbol{\mu}$, we have that

$$\begin{aligned}
&H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x})\\
&= m_{i_0}(\boldsymbol{y})\left(f(\boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x})\right)\\
&\quad \oplus m_{i_1}(\boldsymbol{y})\left(f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{x})\right)\\
&\quad \oplus m_{i_2}(\boldsymbol{y})\left(f(\boldsymbol{\alpha} \oplus \boldsymbol{x}) \oplus 1 \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x})\right)\\
&\quad \oplus m_{i_3}(\boldsymbol{y})\left(1 \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{\alpha} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{x})\right)
\end{aligned}$$

which is balanced because $\boldsymbol{\alpha} \neq \boldsymbol{\lambda}$ and each one of the following functions

$$f(\boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x}),$$
$$f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{x}),$$
$$f(\boldsymbol{\alpha} \oplus \boldsymbol{x}) \oplus 1 \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x}),$$
$$1 \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{\alpha} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{x})$$

is balanced.

- Finally, for $\boldsymbol{\alpha} \neq \boldsymbol{\lambda}$ and $\boldsymbol{\alpha} \neq \boldsymbol{\mu}$, we have that $H_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x})$ is balanced because each one of the functions

$$f(\boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x}),$$
$$f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{x}),$$
$$f(\boldsymbol{\mu} \oplus \boldsymbol{x}) \oplus 1 \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x}),$$
$$1 \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\mu} \oplus \boldsymbol{x})$$

is balanced.

For $\boldsymbol{\beta} = 2$ and $\boldsymbol{\beta} = 3$ the same argument follows. ■

For a given bent function $f(\boldsymbol{x})$ and a fixed $\boldsymbol{\lambda}$ our examples show that the values of $\boldsymbol{\mu}$ that satisfy equation (1) are those that correspond to indices of minterms that are not in $f(\boldsymbol{x}) \oplus f(\boldsymbol{x} \oplus \boldsymbol{\lambda})$. Since this function is balanced, we have 2^{n-1} possibles values for $\boldsymbol{\mu}$. Consequently, we claim that we can construct $(2^n - 1)2^{n-1}$ new bent functions according with the above theorem. Nevertheless, we cannot prove this claim.

4 Conclusion

We have presented one method to obtain new bent functions of $n+2$ variables from bent functions of n variables. This method is based in the expression of Boolean functions as sum of minterms. We have proved some properties of the minterms. We claim that the number of new bent functions of $n+2$ variables that we can construct with this method starting with a bent function of n variables is $(2^n-1)2^{n-1}$. In fact, tacking into account that $1 \oplus F$ is bent if F is bent, then the number of new bent functions will be $2^n(2^n-1)$. The results of this paper are valuable in both theory and practical applications.

References:

[1] C. M. Adams and S. E. Tavares. Generating and counting binary bent sequences. *IEEE Transactions on Information Theory*, 35(5):1170–1173, 1990.

[2] Y. Borissov, A. Braeken, S. Nikova, and B. Preneel. On the covering radii of binary reed-muller codes in the set of resilient boolean functions. *IEEE Transactions on Information Theory*, 51(3):1182–1189, 2005.

[3] A. Braeken, V. Nikov, S. Nikova, and B. Preneel. On Boolean functions with generalized cryptographic properties. In Anne Canteaut and Kapaleeswaran Viswanathan, editors, *Progress in Cryptology – INDOCRYPT 2004*, volume 3348 of *Lecture Notes in Computer Science*, pages 120–135. Springer-Verlag, Berlin, 2004.

[4] C. Charnes and T. Yu. Covering sequences of boolean functions and their cryptographic significance. *Designs, Codes and Cryptography*, 25:263–279, 2002.

[5] K. Kurosawa, T.Iwata, and T. Yoshiwara. New covering radius of reed-muller codes for t-resilient functions. *IEEE Transactions on Information Theory*, 50(3):468–475, 2004.

[6] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 6 edition, 1988.

[7] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology – EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, Berlin, 1994.

[8] W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In J.J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology – EUROCRYPT'89*, volume 434 of *Lecture Notes in Computer Science*, pages 549–562. Springer-Verlag, Berlin, 1998.

[9] K. Ren, J. Park, and K. Kim. On the construction of cryptographycally strong boolean functions with desirable trade-off. *Journal of Zhejiang University SCIENCE*, 6A(5):358–364, 2005.

[10] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory (Series A)*, 20:300–305, 1976.

[11] P. Sarkar and S. Maitra. Construction of nonlinear boolean functions with important cryptographyc properties. In B. Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 485–506. Springer-Verlag, Berlin, 2000.

[12] P. Sarkar and S. Maitra. Efficient implementation of cryptographically useful "large" boolean functions. *IEEE Transactions on Computers*, 52(4):410–417, 2003.

[13] J. Seberry, X.-M. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. *Information and Computation*, 119:1–13, 1995.