A characterization of bent functions on $n+1$ variables[1]

JOAN-JOSEP CLIMENT[(a)(b)2], FRANCISCO J. GARCÍA[(c)], VERÓNICA REQUENA[(b)3]
[(a)]Institut Universitari d'Investigació Informàtica
[(b)]Departament de Ciència de la Computació i Intel·ligència Artificial
[(c)]Departament de Fonaments de l'Anàlisi Econòmica
Universitat d'Alacant
Campus de Sant Vicent del Raspeig
Ap. correus 99, E-03080 Alacant
SPAIN

Abstract: In this paper we construct a Boolean function of $n+1$ variables starting with two Boolean functions of n variables and we we introduce a necessary and sufficient condition in order to new function be a bent function when n is a positive odd integer.

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

1 Introduction

Boolean functions are used in cryptography [3, 5], coding theory [2, 9], among others. Boolean functions in cryptography are the basic elements and should have high nonlinearity in order to prevent attacks based on linear approximation. For n a positive even integer, Boolean functions achieving the maximum nonlinearity are called bent functions [8, 11].

There are different ways to obtain bent functions, most of them are based on the algebraic normal form of a Boolean function, see, for example, [1, 4, 10, 12, 13, 14]. Climent, García, and Requena [6, 7] using the concept of minterm, presented some constructions in order to obtain a bent function of $n+2$ variables starting with some bent functions of n variables (with n a positive even integer).

The rest of the paper is organized as follows. In Section 2 we introduce some basic concepts and the notation we will use in the paper. In Section 3 we consider two Boolean functions of n variables and introduce a necessary and sufficient condition in order to a Boolean function of $n+1$ variables (with n a positive odd integer) be a bent function, and then, we derive some properties. Finally, in Section 4 we present some conclusions.

2 Preliminaries

Let n be a positive integer. It is well-known that $\mathbb{Z}_2^n$ is a linear space over $\mathbb{Z}_2$ with the addition $\oplus$ given by

$$\boldsymbol{a} \oplus \boldsymbol{b} = (a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_n \oplus b_n)$$

where $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ and $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)$, and the addition $a_i \oplus b_i$, for $i = 1, 2, \ldots, n$, is the addition modulo 2 in $\mathbb{Z}_2$. In $\mathbb{Z}_2^n$ we also consider the inner product

$$\langle \boldsymbol{a}, \boldsymbol{b} \rangle = a_1 b_1 \oplus a_2 b_2 \oplus \cdots \oplus a_n b_n.$$

We call a **Boolean function** of n variables any map $f : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$. For $i = 0, 1, \ldots, 2^n - 1$, let $\boldsymbol{e}_i$ be the vector in $\mathbb{Z}_2^n$ corresponding to the binary expansion of the integer i. The **truth table** of a Boolean function $f(\boldsymbol{x})$ of n variables is the $(0,1)$-sequence

$$\boldsymbol{\xi}_f = (f(\boldsymbol{e_0}),\ f(\boldsymbol{e_1}),\ \ldots\ , f(\boldsymbol{e_{2^n-1}})).$$

The set $\mathcal{B}_n$ of all Boolean functions of n variables is also a linear space with the addition $f \oplus g$ of $f, g \in \mathcal{B}_n$ given by

$$(f \oplus g)(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus g(\boldsymbol{x}).$$

We say that a Boolean function $f(\boldsymbol{x})$ of n variables is an **affine function** if it takes the form

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

where $\boldsymbol{a} \in \mathbb{Z}_2^n$ and $b \in \mathbb{Z}_2$. In addition, we call f a **linear function** if $b = 0$. In the rest of the paper we

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

[2]The work of this author was partially developed during a stay at the University of Zurich supportted by Spanish grant PR2007-0181 of the Secretaría de Estado de Universidades e Investigación of the Ministerio de Educación y Ciencia.

[3]The work of this author was supported by a grant of the Vicerectorat d'Investigació, Desenvolupament i Innovació of the Universitat d'Alacant for PhD students and was partially developed during a stay at the University of Zurich also supported by the Vicerectorat d'Investigació, Desenvolupament i Innovació of the Universitat d'Alacant.

write $l_{\boldsymbol{a}}(\boldsymbol{x})$ for the linear function defined by $\boldsymbol{a} \in \mathbb{Z}_2^n$, that is, $l_{\boldsymbol{a}}(\boldsymbol{x}) = \langle \boldsymbol{a}, \boldsymbol{x} \rangle$.

The **Hamming weight** of a $(0,1)$-sequence $\boldsymbol{\alpha}$, denoted by $w(\boldsymbol{\alpha})$, is the number of 1s in $\boldsymbol{\alpha}$. A $(0,1)$-sequence is **balanced** if it contains an equal number of 0s and 1s. The **Hamming distance** between two $(0,1)$-sequences $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, denoted by $d(\boldsymbol{\alpha}, \boldsymbol{\beta})$, is the number of positions where the two sequences differ, that is $d(\boldsymbol{\alpha}, \boldsymbol{\beta}) = w(\boldsymbol{\alpha} \oplus \boldsymbol{\beta})$.

For two Boolean functions $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ of n variables we have that $d(f,g) = d(\boldsymbol{\xi}_f, \boldsymbol{\xi}_g)$. Also, we have that $w(f) = w(\boldsymbol{\xi}_f)$ and, therefore, $f(\boldsymbol{x})$ is **balanced** if $\boldsymbol{\xi}_f$ is balanced; that is, if $w(f) = 2^{n-1}$. In this paper we consider 0 and 1 as elements in $\mathbb{Z}_2$ or in $\mathbb{Z}$ as we need, so

$$w(f) = \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} f(\boldsymbol{x}).$$

The **nonlinearity** NL of a Boolean function $f(\boldsymbol{x})$ of n variables is given by

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

where $\mathcal{A}_n$ is the set of all affine functions; it is well known (see [13]) that

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

The Boolean functions that attains the maximum nonlinearity are called **bent functions** (see [13]), in this case, n must be even.

The following result (see [12, 13]), that we quote for further references, give us a characterization of bent functions.

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

1. *$f(\boldsymbol{x})$ is a bent function,*
2. *$f(\boldsymbol{x}) \oplus f(\boldsymbol{a} \oplus \boldsymbol{x})$ is balanced for all $\boldsymbol{a} \in \mathbb{Z}_2^n$ with $\boldsymbol{a} \neq \boldsymbol{0}$.*
3. *$w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$ for all $\boldsymbol{a} \in \mathbb{Z}_2^n$.*

As a consequence of this theorem, if $f(\boldsymbol{x})$ is a bent function, then the number of 1s of its truth table is $2^{n-1} \pm 2^{\frac{n}{2}-1}$, and consequently, $w(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$.

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

$$\begin{aligned} & m_{(u_1,u_2,\ldots,u_n)}(x_1, x_2, \ldots, x_n) \\ & = (1 \oplus u_1 \oplus x_1)(1 \oplus u_2 \oplus x_2) \cdots (1 \oplus u_n \oplus x_n). \end{aligned}$$

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

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

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

for a subset M of $\mathbb{Z}_{2^n}$, that we call the **support** of f, and defined as

$$M = \{i \in \mathbb{Z}_2^n \mid f(\boldsymbol{e}_i) = 1\}.$$

So, $w(f) = \mathrm{card}(M)$.

Next results, whose proof is immediate, that we will use later, establishes that for each minterm of n variables we can obtain two minterms of $n+1$ variables.

Lemma 1: *Assume that $a \in \mathbb{Z}_{2^n}$ and $b \in \mathbb{Z}_2$. If $m_a(\boldsymbol{x})$ is a minterm of n variables and $m_b(y)$ is a minterm of one variable, then $m_c(y, \boldsymbol{x}) = m_b(y) m_a(\boldsymbol{x})$ is a minterm of $n+1$ variables, where $c = b \cdot 2^n + a \in \mathbb{Z}_{2^{n+1}}$.*

3 Main results

In the rest of the paper we assume that $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ are two Boolean functions of n variables, and let $f(y, \boldsymbol{x})$ be the Boolean function of $n+1$ variables given by

$$f(y, \boldsymbol{x}) = m_0(y) f_0(\boldsymbol{x}) \oplus m_1(y) f_1(\boldsymbol{x}). \qquad (1)$$

If M_0 and M_1 are the supports of $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ respectively, then by lemma 1 we have that

$$M_0 \cup \{2^n + a \mid a \in M_1\}$$

is the support of $f(y, \boldsymbol{x})$ and, consequently,

$$w(f) = w(f_0) + w(f_1)$$

because $M_0 \cap \{2^n + a \mid a \in M_1\} = \emptyset$.

Next result will be used in the proof of the main theorem of this paper (see Theorem 2 below).

Lemma 2: *Let $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ be two Boolean functions of n variables and consider the Boolean function $f(y, \boldsymbol{x})$ of $n+1$ variables defined by expression (1). If $\boldsymbol{a} \in \mathbb{Z}_2^n$ and $b \in \mathbb{Z}_2$, then*

$$\begin{aligned} & w(f \oplus l_{(b,\boldsymbol{a})}) \\ & = \begin{cases} w(f_0 \oplus l_{\boldsymbol{a}}) + w(f_1 \oplus l_{\boldsymbol{a}}), & \text{if } b = 0, \\ w(f_0 \oplus l_{\boldsymbol{a}}) + 2^n - w(f_1 \oplus l_{\boldsymbol{a}}), & \text{if } b = 1. \end{cases} \end{aligned}$$

y	$\boldsymbol{x}$	$m_0(y)$	$m_1(y)$	$f_0(\boldsymbol{x})$	$f_1(\boldsymbol{x})$	by	$\lambda_{\boldsymbol{a}}(\boldsymbol{x})$	$f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{a})}(y,\boldsymbol{x})$
$\mathbf{0}$	$\boldsymbol{\tau}$	$\mathbf{1}$	$\mathbf{0}$	$\boldsymbol{\xi}_0$	$\boldsymbol{\xi}_1$	$\mathbf{0}$	$\boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\mathbf{1}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{1}$	$\boldsymbol{\xi}_0$	$\boldsymbol{\xi}_1$	$b\mathbf{1}$	$\boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus b\mathbf{1} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$

Table 1: Truth table of $f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{a})}(y,\boldsymbol{x})$

$b = 0$	$b = 1$
$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus \mathbf{1} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$

Table 2: Truth table of $f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{a})}(y,\boldsymbol{x})$ for the different values of b

PROOF: From expression (1) and the definition of $l_{(b,\boldsymbol{a})}(y,\boldsymbol{x})$ we have that

$$\begin{aligned} & f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{a})}(y,\boldsymbol{x}) \\ & = m_0(y) f_0(\boldsymbol{x}) \oplus m_1(y) f_1(\boldsymbol{x}) \oplus by \oplus l_{\boldsymbol{a}}(\boldsymbol{x}). \end{aligned}$$

So, if $\mathbf{0}$ and $\mathbf{1}$ are the $2^n \times 1$ arrays with all entries equal to 0 and 1 respectively; $\boldsymbol{\tau}$ is the $2^n \times n$ array whose ith row is $\boldsymbol{e}_i$; $\boldsymbol{\xi}_0$ and $\boldsymbol{\xi}_1$ are the truth tables of $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ respectively; and $\boldsymbol{\Lambda}_{\boldsymbol{a}}$ is the truth table of $l_{\boldsymbol{a}}(\boldsymbol{x})$, then the last column of Table 1 shows the truth table of the Boolean function $f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{a})}(y,\boldsymbol{x})$.

Now, the result follows clearly from Table 2 which represents the two blocks of the truth table of the Boolean function $f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{a})}(y,\boldsymbol{x})$ for the different values of b. ∎

From now to the end of the paper, we assume that n is odd, and consequently, that $n+1$ is even. Next theorem introduces a necessary and sufficient condition so that the Boolean function $f(y,\boldsymbol{x})$ defined by expression (1) is bent.

Theorem 2: *Let $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ be two Boolean functions of n variables. The Boolean function $f(y,\boldsymbol{x})$ of $n+1$ variables defined by expression (1) is bent if and only if for all $\boldsymbol{a} \in \mathbb{Z}_2^n$ one of the two following conditions hold:*

1. *$w(f_0 \oplus l_{\boldsymbol{a}}) = 2^{n-1} \pm 2^{\frac{n-1}{2}}$ and $w(f_1 \oplus l_{\boldsymbol{a}}) = 2^{n-1}$,*
2. *$w(f_0 \oplus l_{\boldsymbol{a}}) = 2^{n-1}$ and $w(f_1 \oplus l_{\boldsymbol{a}}) = 2^{n-1} \pm 2^{\frac{n-1}{2}}$.*

PROOF: Assume that $f(y,\boldsymbol{x})$ is a bent function. Then, according to Theorem 1 we have that

$$w(f \oplus l_{(b,\boldsymbol{a})}) = 2^n \pm 2^{\frac{n-1}{2}}$$

for all $(b,\boldsymbol{a}) \in \mathbb{Z}_2^{n+1}$.

Assume first that $w(f \oplus l_{(b,\boldsymbol{a})}) = 2^n + 2^{\frac{n-1}{2}}$ when $b = 0, 1$. Then, by Lemma 2,

$$2^n + 2^{\frac{n-1}{2}} = w(f_0 \oplus l_{\boldsymbol{a}}) + w(f_1 \oplus l_{\boldsymbol{a}}), \qquad (2)$$

$$2^n + 2^{\frac{n-1}{2}} = w(f_0 \oplus l_{\boldsymbol{a}}) + 2^n - w(f_1 \oplus l_{\boldsymbol{a}}). \qquad (3)$$

If we add equalities (2) and (3) we obtain that

$$2\left(2^n + 2^{\frac{n-1}{2}}\right) = 2w(f_0 \oplus l_{\boldsymbol{a}}) + 2^n$$

and consequently,

$$w(f_0 \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n-1}{2}}.$$

If instead to add equalities (2) and (3) we substract one to the other, then we obtain $w(f_1 \oplus l_{\boldsymbol{a}}) = 2^{n-1}$.

If we assume that $w(f \oplus l_{(b,\boldsymbol{a})}) = 2^n - 2^{\frac{n-1}{2}}$ when $b = 0, 1$, then, by a similar argument, we obtain that

$$w(f_0 \oplus l_{\boldsymbol{a}}) = 2^{n-1} - 2^{\frac{n-1}{2}} \quad \text{and} \quad w(f_1 \oplus l_{\boldsymbol{a}}) = 2^{n-1}.$$

Finally, if we assume that $w(f \oplus l_{(b,\boldsymbol{a})}) = 2^n + 2^{\frac{n-1}{2}}$ when $b = 0$ and $w(f \oplus l_{(b,\boldsymbol{a})}) = 2^n - 2^{\frac{n-1}{2}}$ when $b = 1$, or $w(f \oplus l_{(b,\boldsymbol{a})}) = 2^n - 2^{\frac{n-1}{2}}$ when $b = 0$ and $w(f \oplus l_{(b,\boldsymbol{a})}) = 2^n + 2^{\frac{n-1}{2}}$ when $b = 1$, then, by a similar argument, we obtain the equalities of part 2.

Conversely, assume first that condition 1 holds. If $b = 0$, then by Lemma 2

$$\begin{aligned} w(f \oplus l_{(b,\boldsymbol{a})}) &= w(f_0 \oplus l_{\boldsymbol{a}}) + w(f_1 \oplus l_{\boldsymbol{a}}) \\ &= 2^{n-1} \pm 2^{\frac{n-1}{2}} + 2^{n-1} \\ &= 2^n \pm 2^{\frac{n-1}{2}}. \end{aligned}$$

If $b = 1$, then, again by Lemma 2

$$\begin{aligned} w(f \oplus l_{(b,\boldsymbol{a})}) &= w(f_0 \oplus l_{\boldsymbol{a}}) + 2^n - w(f_1 \oplus l_{\boldsymbol{a}}) \\ &= 2^{n-1} \pm 2^{\frac{n-1}{2}} + 2^n - 2^{n-1} \\ &= 2^n \pm 2^{\frac{n-1}{2}}. \end{aligned}$$

Consequently, by Theorem 1, $f(y, \boldsymbol{x})$ is a bent function.

Now, if condition 2 holds, by a similar argument, we also obtain that $f(y, \boldsymbol{x})$ is a bent function. ■

As an immediate consequence of the previous theorem we have the following results.

Corollary 1: *Let $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ be two Boolean functions of n variables. If the Boolean function $f(y, \boldsymbol{x})$ of $n + 1$ variables defined by expression (1) is bent, then only one of the two functions $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ is balanced.*

Corollary 2: *Let $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ be two Boolean functions of n variables. If the Boolean function $f(y, \boldsymbol{x})$ of $n + 1$ variables defined by expression (1) is bent, then*

$$f_0(\boldsymbol{a} \oplus \boldsymbol{x}) \oplus f_1(\boldsymbol{x}) \quad \textit{and} \quad f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{a} \oplus \boldsymbol{x})$$

are balanced functions for all $\boldsymbol{a} \in \mathbb{Z}_2^n$.

Observe that if we take $\boldsymbol{a} = \boldsymbol{0}$ in Corollary 2, then the Boolean function $f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x})$ is balanced.

4 Conclusion

Starting with two Boolean functions $f_0(\boldsymbol{x})$ and $f_1(\boldsymbol{x})$ of n variables (with n a positive odd integer), we define the Boolean function

$$f(y, \boldsymbol{x}) = m_0(y) f_0(\boldsymbol{x}) \oplus m_1(y) f_1(\boldsymbol{x})$$

of $n + 1$ variables. Then, we introduce a necessary and sufficient condition in order to $f(y, \boldsymbol{x})$ is a bent functions and we derive some properties.

References:

[1] C. M. ADAMS and S. E. TAVARES. Generating and counting binary bent sequences. *IEEE Transactions on Information Theory*, **35(6)**: 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 A. CANTEAUT and K. VISWANATHAN (editors), *Progress in Cryptology – INDOCRYPT 2004*, volume 3348 of *Lecture Notes in Computer Science*, pages 120–135. Springer-Verlag, Berlin, 2004.

[4] C. CARLET and J. L. YUCAS. Piecewise constructions of bent and almost optimal Boolean functions. *Designs, Codes and Cryptography*, **37**: 449–464 (2005).

[5] C. CHARNES, M. RÖTTELER and T. BETH. Homogeneous bent functions, invariants, and designs. *Designs, Codes and Cryptography*, **26**: 139–154 (2002).

[6] J.-J. CLIMENT, F. J. GARCÍA and V. REQUENA. An iterative method to construct new bent funcions from old bent functions. *Transactions on Information Science and Applications*, **4(2)**: 245–250 (2007).

[7] J.-J. CLIMENT, F. J. GARCÍA and V. REQUENA. Iterative methods to construct boolean bent funcions. *Transactions on Information Science and Applications*, **4(2)**: 251–256 (2007).

[8] J. F. DILLON. *Elementary Hadamard Difference Sets*. PhD Thesis, University of Maryland, 1974.

[9] 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).

[10] W. MEIER and O. STAFFELBACH. Nonlinearity criteria for cryptographic functions. In J. QUISQUATER and J. VANDEWALLE (editors), *Advances in Cryptology – EUROCRYPT'89*, volume 434 of *Lecture Notes in Computer Science*, pages 549–562. Springer-Verlag, Berlin, 1998.

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

[12] J. SEBERRY and X.-M. ZHANG. Constructions of bent functions from two known bent functions. *Australasian Journal of Combinatorics*, **9**: 21–35 (1994).

[13] J. SEBERRY, X.-M. ZHANG and Y. ZHENG. Nonlinearity and propagation characteristics of balanced Boolean functions. *Information and Computation*, **119**: 1–13 (1995).

[14] N. Y. YU and G. GONG. Constructions of quadratic bent functions in polynomial forms. *IEEE Transactions on Information Theory*, **52(7)**: 3291–3299 (2006).