On the bent boolean functions which are symmetric

Petr Savický
Department of logic, Faculty of Philosophy,
Charles University, Prague,
Czech Republic

Abstract

Bent functions are the boolean functions having the maximal possible Hamming distance from the linear boolean functions. Bent functions were introduced and studied first by Rothaus (1976).

We prove that there are exactly four symmetric bent functions on every even number of variables. These functions are exactly the four symmetric quadratic polynomials of the given number of variables.

1 Introduction

It is well-known (see [6]) that for every boolean function of n variables there exists a linear boolean function such that the Hamming distance of these two functions is at most $2^{n-1} - 2^{n/2-1}$. If n is even then there exist boolean functions such that the Hamming distance of any of them from every linear boolean function is at least $2^{n-1} - 2^{n/2-1}$. These functions are called bent in [6]. They are naturally defined in [6] through their discrete Fourier transform.

If n is odd, the $n-1$ variable bent function has the distance $2^{n-1} - 2^{(n-1)/2}$ from all the linear boolean functions of n variables. The maximum possible distance of a boolean function from the set of all linear boolean functions is studied in coding theory as the covering radius of the first order Reed-Muller code. In this setting some more results are known for the case of odd number of variables. See e.g. [3] and [5].

Every boolean function of n variables can be expressed as a polynomial over the two-element field in variables $x_1, x_2, \ldots, x_n$, which is of degree at most one in every variable. This polynomial is unique, see for instance [2], chapter 13, §2. We shall call the degree of the boolean function the degree of its corresponding polynomial.

The following results are proved in [6]. Every bent function of $n > 2$ variables has the degree at most $n/2$. For every even $n > 2$ there are bent functions of degree exactly $n/2$. These results can be found in [2] as well.

A boolean function is called symmetric if it does not depend on the order of variables. It means that it depends only on the number of unit values among the input variables. We prove that a symmetric boolean function of an even number of variables is bent if and only if it is quadratic. There are exactly four such functions for every even number of variables.

The symmetric bent functions and so called semibent functions were used in [1] to separate two classes of circuits constructed from specific threshold gates. If desired, more information on boolean functions and their complexity can be found in [4] or [7].

2 Preliminaries

We denote by B_n the set $\{0,1\}^n$. We use the symbols x, t for the elements of B_n throughout the paper. We denote the number of unit values in $x \in B_n$ as $|x|$. Linear functions are the functions of the form $a_0 \oplus a_1x_1 \oplus \ldots \oplus a_nx_n$, where $a_0, a_1, \ldots, a_n \in \{0,1\}$ and $\oplus$ denotes the addition in the two-element field.

We use the Fourier transform of a boolean function in the same way as in [2].

Definition 2.1 *If $t, x \in B_n$ then let $\langle t, x\rangle = \bigoplus_{j=1}^n t_jx_j$.*

Definition 2.2 Let f be a boolean function. We define its Fourier transform as

$$\widehat{F}(t) = \sum_{x\in B_n} (-1)^{f(x)\oplus\langle t,x\rangle}.$$

Definition 2.3 ([6]) A boolean function of n variables is bent if and only if $|\widehat{F}(t)| = 2^{n/2}$ for all t.

3 Symmetric functions

A symmetric boolean function of n variables is any function expressible in the form $f(x) = c_{|x|}$, where $c_0, \ldots, c_n \in \{0,1\}$. Let f be such a function. Directly from Definiton 2.2, we get the following:

$$\widehat{F}(t) = \sum_{k=0}^{n} (-1)^{c_k} \sum_{|x|=k} (-1)^{\langle t,x\rangle}. \tag{1}$$

Note, that

$$\sum_{|x|=k} (-1)^{\langle t,x\rangle} = \sum_{j=0}^{k} (-1)^j \binom{|t|}{j}\binom{n-|t|}{k-j} = P_k(|t|, n),$$

where P_k is the Krawtchouk polynomial (see [2]). It may be easily verified, that these polynomials have the following generating function:

$$(1-z)^{|t|}(1+z)^{n-|t|} = \sum_{k=0}^{n} P_k(|t|, n)z^k. \tag{2}$$

The main result is presented after two technical lemmas.

Lemma 3.1 *Let f be a symmetric boolean function of n variables. If there exists $t \in B_n$ such that $|t| = n/2$ and $|\widehat{F}(t)| = 2^{n/2}$ then $c_{2l+2} = c_{2l} \oplus 1$ holds for all $l = 0, \dots, n/2 - 1$.*

Proof: If $|t| = n/2$, then using (2) we obtain

$$\sum_{|x|=k} (-1)^{\langle t,x\rangle} = \begin{cases} 0 & \text{if } k \text{ odd,} \\ (-1)^l \binom{n/2}{l} & \text{if } k = 2l \end{cases}$$

Therefore, the expression (1) for $\widehat{F}(t)$ can be written as

$$\widehat{F}(t) = \sum_{l=0}^{n/2} (-1)^{c_{2l}} (-1)^l \binom{n/2}{l}.$$

If c_{2l+2} is equal to c_{2l} for some $l \in \{0, \dots, n/2 - 1\}$, then this sum contains nonzero members of opposite sign and hence

$$|\widehat{F}(t)| < \sum_{l=0}^{n/2} \binom{n/2}{l} = 2^{n/2}.$$

Since it contradicts our assumptions, we have $c_{2l+2} = c_{2l} \oplus 1$ for all $l = 0, \dots, n/2 - 1$. $\square$

Lemma 3.2 *Let f be a symmetric boolean function of n variables. If there exists $t \in B_n$ such that $|t| = n/2 - 1$ and $|\widehat{F}(t)| = 2^{n/2}$ and $c_{2l+2} = c_{2l} \oplus 1$ for all $l = 0, \dots, n/2 - 1$, then $c_{2l+3} = c_{2l+1} \oplus 1$ holds for all $l = 0, \dots, n/2 - 2$.*

Proof: If $|t| = n/2 - 1$, then using (2) we obtain

$$\sum_{|x|=k} (-1)^{\langle t,x\rangle} = \begin{cases} (-1)^l \left[\binom{n/2-1}{l} - \binom{n/2-1}{l-1}\right] & k = 2l \\ \\ 2(-1)^l \binom{n/2-1}{l} & k = 2l+1 \end{cases}$$

Consequently, the terms for even k in (1) sum up to

$$\sum_{l=0}^{n/2} (-1)^{c_{2l}} (-1)^l \left[\binom{n/2-1}{l} - \binom{n/2-1}{l-1}\right]$$

Since $c_{2l+2} = c_{2l} \oplus 1$ by assumptions of the lemma, $(-1)^{c_{2l}}(-1)^l = (-1)^{c_0}$ for all $l = 0, \dots, n$ and hence the sum of even k terms in (1) is zero. It follows that

$$\widehat{F}(t) = 2 \sum_{l=0}^{n/2-1} (-1)^{c_{2l+1}} (-1)^l \binom{n/2-1}{l}.$$

If c_{2l+1} is equal to c_{2l+3} for some $l \in \{0, \dots, n/2 - 2\}$, then

$$|\widehat{F}(t)| < 2 \sum_{l=0}^{n/2-1} \binom{n/2-1}{l} = 2^{n/2}.$$

It is a contradiction. Hence $c_{2l+3} = c_{2l+1} \oplus 1$ for all $l = 0, \dots, n/2 - 2$. $\square$

Now we can formulate the characterization of the symmetric bent functions.

Theorem 3.3 *If $f(x) = c_{|x|}$ is a symmetric function of an even number n of variables then the following statements are equivalent:*
(a) The function f is a bent function.
(b) For all $k = 0, \ldots, n-2$ the identity $c_{k+2} = c_k \oplus 1$ is satisfied.
(c) There exist constants $c, d \in \{0,1\}$ such that for all x

$$f(x) = \bigoplus_{i<j} x_i x_j \oplus \left(\bigoplus_i c x_i \right) \oplus d$$

.

Proof:

(a)$\Rightarrow$(b): It is a direct consequence of Lemmas 3.1 and 3.2.

(b)$\Rightarrow$(a): In this step we use the complex numbers and so we use i to denote the imaginary unit. Let us denote $\alpha = (-1)^{c_0} - i(-1)^{c_1}$. If (b) is satisfied then one can prove by induction $(-1)^{c_k} = \operatorname{Re}(\alpha i^k)$ for all $k = 0, \ldots, n-2$. By substituting this into (1), we obtain that for all $t \in B_n$

$$\widehat{F}(t) = \operatorname{Re}\left[\sum_{k=0}^{n} \alpha i^k \sum_{|x|=k} (-1)^{\langle t,x \rangle} \right].$$

Using (2) with $z = i$ we get:

$$\widehat{F}(t) = \operatorname{Re}\left[\alpha (1-i)^{|t|} (1+i)^{n-|t|} \right]$$

$$= \operatorname{Re}\left[\alpha (1+i)^n (-i)^{|t|} \right] = \operatorname{Re}\left[\alpha (2i)^{n/2} (-i)^{|t|} \right]$$

$$= 2^{n/2} \operatorname{Re}\left[\alpha i^{n/2} (-i)^{|t|} \right].$$

Since both real and imaginary part of α are 1 or -1 and $n/2$ is a natural number, we get $|\widehat{F}(t)| = 2^{n/2}$ for all $t \in B_n$ and hence f is a bent function.

(c)$\Leftrightarrow$(b): Let $k \in \{0, \ldots, n\}$. It is easy to see that if (c) is satisfied and $|x| = k$ then

$$c_k = f(x) \equiv \binom{k}{2} + ck + d \bmod 2$$

Since $\binom{k+2}{2} - \binom{k}{2} = 2k+1$ we get $c_{k+2} = c_k \oplus 1$ for $k = 0, \ldots, n-2$.

Let (b) be satisfied. If $c = c_1 \oplus c_0$ and $d = c_0$ then

$$c_k \equiv \binom{k}{2} + ck + d \bmod 2$$

is satisfied for $k = 0, 1$. Hence this identity is satisfied for all $k = 0, \ldots, n$ due to the fact that c_k and the parity of the right hand side of this identity satisfy the same recurrence relation. Since $f(x) = c_{|x|}$, it implies (c). $\square$

References

[1] J. Bruck: Harmonic Analysis of Polynomial Threshold Functions, *SIAM J. Disc. Math.,* Vol. 3, No. 2, 168-177, 1990

[2] F. J. MacWilliams, N. J. A. Sloane: *The theory of error correcting codes,* Amsterdam-New York-Oxford: North Holland 1977

[3] J. Mykkeltveit: The Covering radius of the $(128, 8)$ Reed–Muller code is 56, *IEEE Trans. Inform. Theory,* vol. IT-26, pp. 359–362, 1980

[4] R. G. Nigmatullin: *The complexity of boolean functions* (in Russian), Kazan University Press 1983

[5] N. J. Patterson, D. H. Wiedemann: The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276, *IEEE Trans. Inform. Theory,* vol. IT-29, pp. 354–356, 1983

[6] O. S. Rothaus: On "bent" functions, *Journal of Combinatorial Theory* 20A, pp. 300–305, 1976

[7] I. Wegener: *The complexity of boolean functions,* Stuttgart: B.G.Teubner/New York 1987