Characterization of Symmetric Bent Functions – An Elementary Proof

Subhamoy Maitra
Computer and Statistical Service Centre
Indian Statistical Institute
203, B.T. Road,
Calcutta 700 035, INDIA
e-mail: subho@isical.ac.in

Palash Sarkar
Department of Combinatorics and Optimization
University of Waterloo
200 University Avenue West
Waterloo, Ontario
Canada N2L 3G1
e-mail: psarkar@cacr.math.uwaterloo.ca

Abstract

A characterization of symmetric bent functions has been presented in [3]. Here we provide a simple proof of the same result.

1 Introduction

A particularly interesting subclass of Boolean functions is the set of bent functions [2]. Bent functions achieve the maximum possible nonlinearity and exist only if the number of input variables is even. For even n, the maximum nonlinearity of an n-variable (bent) function is $2^{n-1} - 2^{\frac{n}{2}-1}$. A small subclass of Boolean functions is the set of symmetric Boolean functions where the output of the function depends only on the weight of the input vector. In [3], the set of symmetric bent functions has been characterized. It is interesting to note that all the possible symmetric bent functions can be represented by contiguous odd length binary substrings of $(1100)^*$. We provide an alternative simple proof of this result. We would like to mention that we became aware of [3] after obtaining our proof.

An n-variable symmetric function can be represented by an $(n+1)$ length binary string, where the i-th location contains the output corresponding to any input vector of Hamming weight i. Let f be a symmetric function. We denote the reduced form of f by $re(f)$, a binary string of length $(n+1)$, defined as follows. For $0 \leq i \leq n$, $re(f)[i] = f(a_1, \ldots, a_n)$, where the number of 1's in $(a_1, \ldots, a_n)$ is exactly i.

We denote the addition operator over GF(2) by $\oplus$. An n-variable function of the form $a_1X_1 \oplus a_2X_2 \oplus \ldots a_nX_n$ is called a linear function. We denote the set of all n-variable linear functions by $L(n)$. Given two n-variable functions f_1 and f_2 we define $wd(f_1, f_2)$ to be the number of values where f_1 and f_2 are equal minus the number of values where f_1 and f_2 are not equal. The nonlinearity $nl(f)$ of a function f, is defined as $nl(f) = 2^{n-1} - \frac{1}{2}\max_{l \in L(n)} |wd(f,l)|$. For n even, a function f on n variables is bent iff $wd(f,l) = \pm 2^{\frac{n}{2}}$ for any linear function l on n variables [2].

2 The Proof

Lemma 2.1 *Let n be even and $F(X_n, X_{n-1}, \ldots, X_1)$ be an n-variable bent function. Consider $F = (1 \oplus X_n)(1 \oplus X_{n-1})f_0 \oplus (1 \oplus X_n)X_{n-1}f_1 \oplus X_n(1 \oplus X_{n-1})f_2 \oplus X_nX_{n-1}f_3$ where f_0, f_1, f_2, f_3 are $(n-2)$-variable functions on the variables $X_{n-2}, \ldots, X_1$. If $f_1 = f_2$, then each of f_0, f_1, f_2, f_3 are bent and $f_0 = 1 \oplus f_3$.*

Proof : Let $\lambda \in L(n)$ be arbitrary. We write $\lambda(X_n, \ldots, X_1) = c_nX_n \oplus c_{n-1}X_{n-1} \oplus l(X_{n-2}, \ldots, X_1)$, where $l \in L(n-2)$. Let $wd(f_0, l) = a_l$, $wd(f_1, l) = wd(f_2, l) = b_l$ and $wd(f_3, l) = c_l$. Varying the pair c_nc_{n-1} over the strings $00, 01, 10, 11$ we respectively get the n-variable linear functions $\lambda_0, \lambda_1, \lambda_2, \lambda_3$. Since F is bent, $wd(F, \lambda_i) = \pm 2^{\frac{n}{2}}$. We thus get the following set of equations. Let $x = 2^{\frac{n}{2}}$.

$$\begin{array}{lcccccll} wd(F,\lambda_0) & = & a_l & +2b_l & +c_l & = & \pm x & (1) \\ wd(F,\lambda_1) & = & a_l & & -c_l & = & \pm x & (2) \\ wd(F,\lambda_3) & = & a_l & -2b_l & +c_l & = & \pm x & (3) \end{array}$$

Subtracting (3) from (1) we get $b_l = 0, \pm\frac{x}{2}$. We claim that for no l can b_l be 0. In contradiction if $b_l = 0$, for some l, then $\sum_{l \in L(n-2)}(wd(f_1, l))^2 <$

$2^{2(n-2)}$. However, this is not possible, since from Parseval's Theorem [1, Page 15] we have, $\sum_{l \in L(n-2)} (wd(f_1, l))^2 = 2^{2(n-2)}$. Hence, for each l, we have $b_l \neq 0$ and hence the signs of x in (1) and (3) must be opposite. Also $b_l = \pm\frac{x}{2}$ implies that $f_1 (= f_2)$ is bent.

Adding (1) and (3) we get $a_l + c_l = 0$. This combined with (2) gives $a_l = -c_l = \pm\frac{x}{2}$ for each $l \in L(n-2)$. Thus $f_0 = 1 \oplus f_3$ and both f_0 and f_3 are bent. ■

We introduce a notation which will be used in the sequel. Let s be a binary string. By s^* we will denote the one-way infinite binary string $sss\ldots$, i.e. the binary string formed by the repeated concatenation of the string s.

Theorem 2.1 *[3] For even $n \geq 2$, F is a symmetric bent function on n variables iff $re(F)$ is a contiguous $(n+1)$ length substring of $(1100)^*$. Consequently, there are only four symmetric bent functions on n variables.*

Proof : First suppose F is bent and let $re(F) = s_0 s_1 \ldots s_{n-1} s_n$, where $s_i \in \{0, 1\}$, $0 \leq i \leq n$. Consider $F = (1 \oplus X_n)(1 \oplus X_{n-1}) f_0 \oplus (1 \oplus X_n) X_{n-1} f_1 \oplus X_n (1 \oplus X_{n-1}) f_2 \oplus X_n X_{n-1} f_3$ where f_0, f_1, f_2, f_3 are $(n-2)$-variable functions. It is clear that they are also symmetric and it is not difficult to check that $re(f_0) = s_0 s_1 \ldots s_{n-3} s_{n-2}$, $re(f_1) = re(f_2) = s_1 s_2 \ldots s_{n-2} s_{n-1}$ and $re(f_3) = s_2 s_3 \ldots s_{n-1} s_n$.

Since F is bent and $f_1 = f_2$ (since F is symmetric), using Lemma 2.1, we have that f_0, f_1, f_2, f_3 are also bent and $f_0 = 1 \oplus f_3$. This implies that $re(f_3)$ is the bitwise complement of $re(f_0)$. Hence, $s_{i+2} = s_i^c$ for $0 \leq i \leq n-2$. Thus, if F is symmetric bent then $re(F)$ is a contiguous $(n+1)$ length substring of $(1100)^*$.

We prove the other direction by induction on the number of variables. The induction base is $n = 2$. In this case, the 4 possible length 3 contiguous substrings of $(1100)^*$ are $110, 100, 001, 011$. It is easy to check that if F is a 2-variable symmetric function such that $re(F)$ is one of these strings, then F is bent.

Now we turn to the inductive step. Assume the result is true for all n-variable (n even) functions. Let F be an $(n+2)$-variable symmetric function and let $g = re(F)$ be a contiguous substring of $(1100)^*$. We write $g = s_0 s_1 \ldots s_{n-1} s_n s_{n+1} s_{n+2}$, where each $s_i \in \{0, 1\}$. Since g is a contiguous substring of $(1100)^*$ we get $s_{n+1} = s_{n-1}^c$ and $s_{n+2} = s_n^c$. We define $g_0 = s_0 s_1 \ldots s_{n-1} s_n$, $g_1 = g_2 = s_1 \ldots s_{n-1} s_n s_{n+1}$ and $g_3 = s_2 \ldots s_{n+1} s_{n+2}$. The strings g_0, g_1, g_2, g_3 are contiguous substring of $(1100)^*$ of length $n+1$ and also g_3 is the bitwise complement of g_0. Define symmetric functions f_i such that $re(f_i) = g_i$ for $0 \leq i \leq 3$. Then $F = (1 \oplus X_{n+2})(1 \oplus X_{n+1})f_0 \oplus (1 \oplus X_{n+2})X_{n+1}f_1 \oplus X_{n+2}(1 \oplus X_{n+1})f_2 \oplus X_{n+2}X_{n+1}f_3$. By induction hypothesis the f_i's are all bent. Again let $\lambda \in L(n+2)$ and write $\lambda(X_{n+2}, \ldots, X_1) = c_{n+2}X_{n+2} \oplus c_{n+1}X_{n+1} \oplus l(X_n, \ldots, X_1)$. It is easy to check that $wd(F, \lambda)$ is either $2wd(f_0, l)$ or $\pm 2wd(f_1, l)$. This shows that F has two valued spectra $\pm 2 \cdot 2^{\frac{n-2}{2}} = \pm 2^{\frac{n}{2}}$ and hence F is bent. This proves the other direction.

There are exactly four distinct contiguous substrings of $(1100)^*$ of length $n+1$, since there are four choices for selecting the first two bits. Hence there are exactly 4 distinct n-variable symmetric bent function. ■

References

[1] C. Ding, G. Xiao, and W. Shan. *The Stability Theory of Stream Ciphers.* Number 561 in Lecture Notes in Computer Science. Springer-Verlag, 1991.

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

[3] P. Savicky. On the bent Boolean functions that are symmetric. *European Journal of Combinatorics*, 15:407–410, 1994.