On a new invariant of Boolean functions

Sugata Gangopadhyay and Deepmala Sharma
Department of Mathematics
Indian Institute of Technology Roorkee - 247 667 INDIA

Abstract

A new invariant of the set of n-variable Boolean functions with respect to the action of $AGL(n,2)$ is studied. Application of this invariant to prove affine nonequivalence of two Boolean functions is outlined. The value of this invariant is computed for PS_{ap} type bent functions. It has been demonstrated by an example how this helps us to decide affine nonequivalence of a given bent function to a bent function belonging to the PS_{ap} class.

1 Introduction

A function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ is called a Boolean function on n variables. The set of all such functions is denoted by $\mathcal{B}_n$. Two Boolean function f and g are said to be affinely equivalent if there exists an $A \in GL(n,2)$ - the group of all invertible $\mathbb{F}_2$-linear transformations over $\mathbb{F}_{2^n}$ - and $b \in \mathbb{F}_{2^n}$ such that $g(x) = f(Ax + b)$ for all $x \in \mathbb{F}_{2^n}$. The group of transformations containing all the invertible affine transformations of the form $x \mapsto Ax + b$ where $A \in GL(n,2)$ and $b \in \mathbb{F}_{2^n}$ is denoted by $AGL(n,2)$ and a general element in the group is written as (A, b). The $\{Tr_1^n(\lambda x) | \lambda \in \mathbb{F}_{2^n}\}$ is the set of linear functions from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$, where $Tr_1^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}$ is called the trace function. Walsh-Hadamard transformation of $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_{2^n}$ is $\hat{f}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\lambda x)}$. The multiset $[\hat{f}(\lambda) | \lambda \in \mathbb{F}_{2^n}]$ is called the Walsh-Hadamard spectrum of f. A function is called bent if and only in its Walsh-Hadamard spectrum takes the values $\pm 2^{\frac{n}{2}}$. The autocorrelation of a Boolean function is defined by $C_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(x+\lambda)}$. The autocorrelation spectrum of a Boolean functtsugataion the multiset $[C_f(\lambda) | \lambda \in \mathbb{F}_{2^n}]$. For any bent function the all the entries in the autocorrelation spectrum is zero - in fact is a characterization of a bent function. Probably the most well known invariants of a Boolean function are its Walsh-Hadamard spectrum and autocorrelation spectrum along with algebraic degree. These may be used for partial solution to the problem of deciding whether any two given Boolean functions are not affinely equivalent. However in case of bent functions the first two invariants are identical over the complete class and therefore if two bent fucntions have the same algebraic degree we cannot distinguish them by using these invariants. The action of $AGL(m,2)$ bent functions has been studied by Hou [5, 6]. An algorithm to decide whether two Boolean functions are affinely equivalent or not and in case so to compute the matrix A and the element b is proposed by Meng, Yang and Zhang [7]. It is to be noted that introduction of new invariants of Boolean functions has the potential of improving any algorithm in this direction. Moreover given any bent function to decide that it is not affinely equivalent to a partial spreads bent is a particularly difficult problem [1, 3, 4]. In this paper we introduce a new invariant and provide a partial solution to this problem.

2 Description of the invariant

Suppose $f \in \mathcal{B}_n$ and $supp(f) = \{x \in \mathbb{F}_{2^n} | f(x) = 1\}$. Consider the set

$$S_n(f(x)) = \{\{a, b\} | f(a) = f(b) = f(a + b) = 1\}.$$

Define $M_n : \mathcal{B}_n \longrightarrow \mathbb{Z}$ by $M_n(f(x)) = |S_n(f(x))|$.

Lemma 1 *Suppose $g(x) = f(Ax)$ for some $A \in GL(n, 2)$. Then $M_n(f) = M_n(g)$.*

Proof : Consider $\phi : S_n(f(x)) \longrightarrow S_n(g(x))$, defined by $\phi : (a, b) \mapsto (A^{-1}a, A^{-1}b)$. Clearly this map is bijective hence $M_n(f(x)) = M_n(g(x))$. ■

Theorem 1 *If $g(x) = f(Ax + b)$ for some $A \in GL(n, 2)$ and $b \in \mathbb{F}_{2^n}$ then $M_n(g(x + A^{-1}b)) = M_n(f(x))$.*

Proof : Putting $x = y + A^{-1}b$ we obtain $g(y + A^{-1}b) = f(A(y + A^{-1}b) + b) = f(Ay)$. Since $M_n(f(Ay)) = M_n(f(y))$ by lemma 1, we obtain, $M_n(g(y + A^{-1}b)) = M_n(f(y))$. ■

By using the above theorem we outline a method of deciding whether two given Boolean functions $f, g \in \mathcal{B}_n$ are not affinely equivalent. Suppose ζ is a primitive element of $\mathbb{F}_{2^n}$.

- **Step 1:** Construct the following multiset:

  $[M_n(g(x)), M_n(g(x + 1)), M_n(g(x + \zeta)), M_n(g(x + \zeta^2)), \ldots, M_n(g(x + \zeta^{2^n-2}))]$

  Let us call this M-spectrum of $g(x)$.

- **Step 2:** Compute $M_n(f(x))$.

- **Step 3:** If $M_n(f(x)) \neq M_n(g(x+\zeta^i))$ for all $i = 0, 1, \ldots, 2^n-2$ along with $M_n(f(x)) \neq M_n(g(x))$ we conclude that $f(x)$ is not affinely equivalent to $g(x)$.

Clearly above is a necessary but not sufficient condition for affine equivalence, however in the next section it is shown that it is possible to distinguish between functions by using this invariant where the analysis of Walsh-Hadamard transform, autocorrelation transform or algebraic degree fail.

Remark 1 *It is to be noted that $M_n(f(x))$ is the number of triangles formed at each vertex of the Cayley graph corresponding to the function f.*

3 The invariant M_n on PS_{ap}

In this section the value of $M_n(f(x))$ for $f \in PS_{ap}$ is computed. It is to be noted that this is the only subclass of PS type bent functions which can be effectively constructed and till date no PS type bent function is known which is not affinely equivalent to a PS_{ap} type function. The class PS_{ap} is partitioned into two subclasses PS_{ap}^- and PS_{ap}^+ such that $PS_{ap} = PS_{ap}^- \cup PS_{ap}^+$. Their definitions are given below: For $n = 2p$ and ζ a primitive element of $\mathbb{F}_{2^n}$ define $V_i = \zeta^i \mathbb{F}_{2^p}$, $V_i^* = \zeta^i \mathbb{F}_{2^p} \setminus \{0\}$. $\mathbb{F}_{2^n} = \cup_{i \in C} V_i$ where $C = \{0, 1, 2, \ldots, 2^p\}$.

Definition 1 *A function $f \in \mathcal{B}_n$ is a PS_{ap}^- (PS_{ap}^+) type bent if and only if $supp(f) = \cup_{i \in I} V_i^*$ ($supp(f) = \cup_{i \in I} V_i$) where $I \subseteq C$ and $|I| = 2^{p-1}$ ($|I| = 2^{p-1} + 1$)*

We prove the following theorem.

Theorem 2 *Suppose $n = 2p$ and f is a PS_{ap} type bent function on n variables. Then*

1. *If $f \in PS_{ap}^-$ then*

$$M_n(f(x)) = \binom{2^p - 1}{2} 2^{p-1} + \binom{2^{p-1}}{2} (2^{p-1} - 2)(2^p - 1).$$

2. *If $f \in PS_{ap}^+$ then*

$$M_n(f(x)) = \binom{2^p - 1}{2} (2^{p-1} + 1) + \binom{2^{p-1} + 1}{2} (2^{p-1} - 1)(2^p - 1) + (2^p - 1)(2^{p-1} + 1).$$

Proof :
(a) We have to count the number of sets $\{a, b\}$ ($a \neq b$) such that $f(a) = f(b) = f(a + b) = 1$.Suppose $f \in PS_{ap}^-$, $V_i^* \subseteq supp(f)$. If $a, b \in V_i^*$ then $a + b \in V_i^*$. For each $i \in I$ there are $\binom{2^p - 1}{2}$ such $\{a, b\}$. Then the total number of such pairs is $\binom{2^p - 1}{2} 2^{p-1}$.

Suppose $i, j \in I$ and $i \neq j$. For any $a \in V_i^*$ we have $|\{a + x | x \in V_j^*\} \cap V_k^*| = 1$ if $i \neq k$ and $j \neq k$, otherwise $|\{a + x | x \in V_j^*\} \cap V_k^*| = 0$. $|I \setminus \{i, j\}| = 2^{p-1} - 2$, Thus is a is fixed in V_i^* and x varies over V_j^* then $a + x$ is 1 exactly $2^{p-1} - 2$ times. Number of ways i, j can be chosen is $\binom{2^{p-1}}{2}$ and the number of ways a can be chosen is $2^p - 1$. Thus value of $|S_n(f(x))| = M_n(f(x))|$ is

$$M_n(f(x)) = \binom{2^p - 1}{2} 2^{p-1} + \binom{2^{p-1}}{2} (2^{p-1} - 2)(2^p - 1).$$

(b) Similar argument proves this part. It is to be remembered that in this case $f(0) = 1$. This explains the third term $(2^p - 1)(2^{p-1} + 1)$ in the expression for $M_n(f(x))$. ■

Example 1 *Consider the function $Tr_1^{10}(\zeta x^{57})$ where $\zeta \in \mathbb{F}_{2^{10}}$ is a primitive element with minimal polynomial $p(x) = x^{10} + x^3 + 1$ (corresponding to the string "10000001001"). This is a Kasami bent function on 10 variables. By theorem 2 if $f \in PS_{ap}$ then either $M_n(f)$ is 59520 or 71672. None of these numbers occur in the M-spectrum of $Tr_1^{10}(\zeta x^{57})$. Therefore we can immediately conclude that the given function is not affinely equivalent of any PS_{ap} type function.*

4 Conclusion

We know of no reference where this invariant is used to determine affine nonequivalence of two Boolean functions. The values of this invariant when $f \in PS_{ap}$ is determined using which it is possible to check whether a function is not affinely equivalent to a function belonging to PS_{ap} class. The study of M-spectrum - defined in this paper - of a Boolean function may also be important in the general affine equivalence problem for Boolean functions.

References

[1] C. Carlet. Two new classes of bent functions. In *Advances in cryptology - EUROCRYPT'93*. Lecture Notes in Computer Science, number 765, pages 77-101, 1994.

[2] C. Carlet. On secondary constructions of resilient and bent functions. *Coding, Cryptography and Combinatorics*. Progress in computer science and applied logic, vol. 23, Birkhauser Verlag, Basel, pp. 3 - 28, 2004.

[3] J. F. Dillon. Elementary Hadamard Difference sets. PhD Thesis, University of Maryland, 1974.

[4] J. F. Dillon. Elementary Hadamard difference sets. In *Proceedings of 6th S. E. Conference of Combinatorics, Graph Theory, and Computing*. Utility Mathematics, Winnipeg, Pages 237–249, 1975.

[5] X. Hou. $GL(m, 2)$ acting on $R(r, m)/R(r-1, m)$. In *Discrete Mathematics*. 149, (1996), Pages 99 - 122.

[6] X. Hou. Cubic bent functions. In *Discrete Mathematics*. 189, (1998), Pages 149 - 161.

[7] Q. Meng, M. Yang and H. Zhang. The Analysis of affinely equivalent Boolean functions. http://eprint.iacr.org/2005/025.

[8] R. Lidl and H. Niederreiter. Introduction to finite fields and their applications. Cambridge University Press, 1994.

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