International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 6 (2018) pp. 3461-3463
© Research India Publications. http://www.ripublication.com

On Affine Non-Equivalence of Monomial Bi-quadratic Boolean Functions

Rashmeet Kaur and Deepmala Sharma

Department of Mathematics, National Institute of Technology
Raipur, Chhattisgarh, 492010, India.

Abstract

In this article, we present results on affine non-equivalence of monomial bi-quadratic Boolean functions to Kasami bent functions. In addition, we also proved that there exists no monomial bi-quadratic Boolean function which is also negabent function.

INTRODUCTION

Boolean functions are the basic components for the design and security of cryptosystem. Cryptographic properties of Boolean function resist the system from various attacks. Among the desired characteristic of Boolean function, the most important requirement is the nonlinearity profile of a Boolean function. It is defined as the minimum hamming distance between the Boolean functions and the set of all affine functions. For cryptographic use of Boolean functions, the nonlinearity must be as high as possible. For even number of variables, the Boolean function achieving the maximum possible nonlinearity is known as bent functions. Bent functions have been widely studied because of their importance in the coding theory, cryptography and graph theory. Several constructions of bent functions are presented in [1, 2, 6]. While dealing with the construction of Boolean functions, a Boolean function is considered to be new if it is not affine equivalent to any known function. Thus determining affine equivalence of Boolean function is quite observant. Partial solutions are obtained by dealing several characteristic of Boolean functions. But, the problem is most difficult while dealing with bent functions having same algebraic degree. In [4] Gangopadhyay *et. al* use the weight distribution to classify affine non-equivalent Boolean functions.

In this article, we induct the study of monomial bi-quadratic Boolean function of the form $tr_1^n(\lambda x)$, for all $x \in \mathbb{F}_{2^n}$ and $\lambda \in \mathbb{F}_{2^n}^*$, where

1. $d = 2^i + 2^j + 2^k + 1$ i, j, k are integers such that $i > j > k \geq 1$ and $n > 2i$.
2. $d = 2^{3l} + 2^{2l} + 2^l + 1, l$ is a positive integer such that $gcd(i,n) = 1$.

We investigate the affine non-equivalence of these functions by using the second derivative spectrum and prove that monomial bi-quadratic Boolean functions are affine non-equivalent to kasami bent functions. We also proved that there is no monomial bi-quadratic Boolean function which is negabent.

PRELIMINARIES

Boolean function is a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, where $\mathbb{F}_{2^n}$ is an n-dimensional vector space over $\mathbb{F}_2$. The set of all Boolean functions is denoted by $\mathcal{B}_n$. The Hamming weight of $f \in \mathcal{B}_n$ is defined by the set $wt(f) = \{x \in \mathbb{F}_{2^n} : f(x) = 1\}$. The Hamming distance of two Boolean functions $f, g \in \mathcal{B}_n$ is defined by the set $\{x \in \mathbb{F}_{2^n} : f(x) \neq g(x)\}$.

The trace function, denoted by $tr_1^n(x)$ is a function from $\mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$, which is defined by

$$tr_1^n(x) = x + x^2 + x^{2^2} + \cdots x^{2^{n-1}},$$

for all $x \in \mathbb{F}_{2^n}$.

Affine Boolean functions are the functions with degree at most one. Affine Boolean functions can be written as $tr_1^n(\lambda x) + \epsilon$ for some $\lambda \in \mathbb{F}_{2^n}$ and $\epsilon \in \mathbb{F}_2$. The set of all n-variable affine Boolean functions is denoted by $\mathcal{A}_n$.

The Walsh transform of f at any point $\lambda \in \mathbb{F}_{2^n}$ is defined by

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + tr_1^n(\lambda x)}.$$

Nonlinearity and Walsh transform are related as

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_{2^n}} |W_f(\lambda)|.$$

–

By using Parsevals equality

$$\sum_{\lambda \in \mathbb{F}_{2^n}} W_f(\lambda)^2 = 2^{2n},$$

we have

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

A Boolean function $f \in \mathcal{B}_n$ is said to be a Bent function if they possesses maximum nonlinearity.

The nega-hadamard transform of f at $u \in \mathbb{F}_{2^n}$ is given by

$$N_f(u) = \frac{1}{2^{\frac{n}{2}}}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{f(x)+u\cdot x}\sqrt{(-1)}^{wt(x)}$$

The nega spectrum of a Boolean function f contains all the values $\{N_f(u) | u \in \mathbb{F}_{2^n}\}$.

In terms of matrix, the nega-hadamard transform is defined by n-fold tensor product

$$\frac{1}{\sqrt{2^n}}(N\otimes N\otimes \ldots N)$$

Where

$$N = \begin{pmatrix}1 & I\\ 1 & -I\end{pmatrix}$$

A function is said to be negabent if $|N_f(u)|=1$,

for all $u \in \mathbb{F}_{2^n}$.

Suppose $f(x) = tr_1^n(\lambda x^k)$ for all $x \in \mathbb{F}_{2^n}$ such that

1. 3 does not divide n.
2. $k = 2^{2d} - 2^d + 1$ with $\gcd(n,d) = 1$, where gcd means greatest common divisor and 0 < d < n.
3. $\lambda \in F_2^n \setminus 0$ does not belong to $\{x^3 : x \in \mathbb{F}_{2^n}\}$.

Then f is a bent function. The bent functions which can be written in this form are said to be kasami bent function. If a function f satisfy only condition 2 then it is called kasami Boolean function.

The derivative of $f \in \mathcal{B}_n$with respect to $a \in \mathbb{F}_{2^n}$ denoted by $D_a f(x)$ is defined as

$$D_a f(x) = f(x) + f(x+a) \quad \text{for all } x \in \mathbb{F}_{2^n}.$$

The second derivative of f at $a, b \in \mathbb{F}_{2^n}$ is defined by

$D_aD_b(f) = f(x) + f(x+a) + f(x+b) + f(x+a+b)$ for all $x \in \mathbb{F}_{2^n}$.

Let

$S(f:a,b) = \sum_{x\in F_2^n}(f(x)+f(x+a)+f(x+b)+f(x+a+b))$ where $a, b \in \mathbb{F}_{2^n}$. It is to be noted that the sum in $D_aD_b(f)$ is over $\mathbb{F}_2$ and the sum in $\sum$ is over integers. The multiset $[S(f:a,b):\{a,b\}\in J_2^n]$ is called the second derivative spectrum of f. We use the following result proved in [4] to prove our result.

Theorem 1. Suppose $f, g \in \mathcal{B}_n$ such that $[S(f:a,b):\{a,b\}\in J_2^n] \neq [S(g:a,b):\{a,b\}\in J_2^n]$, then f is not affine equivalent to g.

MONOMIAL BI-QUADRATIC BOOLEAN FUNCTION ON 8-VARIABLES

In this section, we consider 8-variable monomial bi-quadratic Boolean function with algebraic degree 4. We generate all bi-quadratic monomial Boolean function on 8 variables and compute $[S(f:a,b):\{a,b\}\in J_2^n]$ for each of them. It is observed that there are 10 different multisets. This proves that there exists at least 10 affine non equivalent bi-quadratic Boolean functions on 8 variables. In Table 1, the first row corresponds to the possible value of $S(f:a,b)$ obtained by bi-quadratic Boolean functions. The remaining 10 rows contain different frequency distributions.

Theorem 2. There exist 8 variable monomial bi-quadratic Boolean functions which is not affine equivalent to kasami bent functions.

Proof. We compute the weight distribution of $S(f:a,b)$ of all 8-variable kasami bent functions with algebraic degree 4. We get only one distinct multiset which is listed in Table 2. It is observed that the multiset in Table 1 does not match with the multiset in Table 2. Hence by Theorem 1 there exists no monomial bi-quadratic Boolean function on 8 variables which is affine equivalent to kasami bent functions.

Table 1: Weight distribution of second derivative spectrum of all 8-variable degree 4 bi-quadratic Boolean functions

0	64	96	112	128	144	160	192
0	0	750	2800	3360	2800	1080	5
0	0	580	2480	4725	2400	610	0
0	0	25	450	2680	4110	2840	690
0	0	700	2840	5295	1560	400	0
0	0	940	2360	3885	2360	1220	30
0	26	696	2304	4921	2176	672	0
0	0	830	2448	4380	2448	688	1
0	34	744	2176	4945	2304	592	0
0	0	1360	0	8245	0	1190	0
0	25	450	2680	4110	2840	690	0

Table 2: Weight distribution of second derivative spectrum of all 8-variable degree 4 kasami Bent functions which do not have any second derivative zero

0	16	32	48	64	80	96	112	128	144	160	176	192
0	0	0	0	0	0	590	2448	4380	2448	928	0	1

Table 3: Weight distribution of second derivative spectrum of all 10-variable degree 4 bi-quadratic Boolean functions

0	256	384	448	480	512	544	576	640	768
0	0	250	12370	38496	72765	37600	12630	140	0
0	0	30	11245	41080	69060	40936	11855	45	0
0	5	230	12045	36676	75560	36700	12855	175	5
0	0	60	12735	37180	75930	36036	12065	245	0
0	0	520	12700	37776	76335	33520	13260	140	0
0	0	60	12100	38260	72735	38476	12560	60	0
0	0	190	11800	38076	74925	38020	11160	80	0
0	0	90	11200	40780	68775	41236	12140	30	0

Table 4: Weight distribution of second derivative spectrum of all 10-variable degree 4 kasami Bent functions which does not have any second derivative zero

0	384	448	480	512	544	576	640
0	345	11040	32576	88005	31680	10400	205
0	80	11625	38100	70110	41676	12595	65

MONOMIAL BIQUADRATIC BOOLEAN FUNCTION ON 10-VARIABLES

In this section, we examine the 10-variable bi-quadratic Boolean function with algebraic degree 4. While computing the S(f : a; b) for the 10 variable bi-quadratic Boolean functions, we observed that there are 8 distinct multiset. This proves that there are at least 8 affine non equivalent bi-quadratic Boolean functions on 10 variables.

Theorem 3. There exist 10 variable monomial bi-quadratic Boolean functions which is not affine equivalent to kasami bent functions.

Proof. We compute the weight distribution of $S(f : a, b)$ of all 10-variable kasami bent function with algebraic degree 4. We get only two distinct multiset which is listed in Table 4. It is observed that the multiset in Table 3 does not match with the multiset in Table 4. Hence by Theorem 1 there exists no monomial bi-quadratic Boolean function on 10 variables which is affine equivalent to kasami bent functions.

NEGABENT FUNCTION IN THE CLASS OF MONOMIAL BI-QUADRATIC BOOLEAN FUNCTIONS

In this section, we initiate the study of negabent function in the class of monomial bi-quadratic Boolean functions. We study negabent function in terms of negaperiodic autocorrelation. Using negaperiodic autocorrelation we completely enumerate negabent bi-quadratic Boolean function. Pott and Parker [5] compute the negaperiodic autocorrelation coefficient of Boolean functions as follows:

$$n_y = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(x+a)+x\cdot y}$$

We use the following theorem presented in [5] to prove our result.

Theorem 4. A Boolean function is negabent if and only if all its nontrivial negaperiodic autocorrelation coefficients are 0.

Theorem 5. There exist no monomial bi-quadratic Boolean functions which is negabent.

Proof. We investigate the monomial bi-quadratic

Boolean function which is negabent. We compute the negaperiodic autocorrelation values of these functions. We observe that all these values are not zero.

Hence by Theorem 4 there exists no monomial negabent bi-quadratic Boolean function.

REFERENCES

[1] Carlet C., 1994, ”Two new classes of bent functions,” Eurocrypt93. Lect. Notes Comput. Sci., 765, pp.77-101.

[2] Dillon J. F., 1974, ”Elementary hadamard difference sets,” Ph.D. Thesis, University of Maryland.

[3] Dobbertin H., 1995, ”Construction of bent functions and highly nonlinear balanced Boolean functions,” FSE, Lect. Notes Comput. Sci., 1008, pp.61-74.

[4] Gangopadhyay S., Sharma D., Sarkar S. and Maitra S., 2009, ”On affine (non)equivalence of Boolean functions,” Computing, 85, pp.37-55.

[5] Parker M. G. and Pott A., 2007, ”On Boolean functions which are bent and negabent,” SSC, Lect. Notes Comput. Sci., Springer, 4893, pp.9- 23.

[6] Rothaus O. S., 1976, ”On bent functions,” J. Combi. Theory, Ser. A, 20, pp.300-30