ISSN:0975-9646
Anand Joshi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4005 - 4009

On some classes of Z-bent functions

Anand Joshi, R. K. Sharma
Department of Mathematics,
Indian Institute of Technology Delhi
New Delhi 110016, India

***Abstract*—Construction and classification of bent functions is an open problem. There is a lack of recursive method to construct bent functions. For the first time Dobbertin and Leander have embedded the problem of construction of bent functions into a recursive framework by introducing the idea of a more general type of functions said to be Z-bent functions. The construction of Z-bent functions of special class is an important problem. In this paper we construct some special class of Z-bent functions.**

Keywords— **Booolean functions, Bent functions, Fourier transform**

I. INTRODUCTION

Boolean functions play an important role in cryptography and error correcting coding activities. Shannon [12] introduces the concept of confusion and diffusion as a fundamental technique to achieve security in cryptographic system. Confusion is reflected in nonlinearity of certain cryptographic primitives; most linear systems are easily breakable. So, it is important to have criteria which reflect nonlinearity. The best known criterion is the so-called perfect nonlinearity introduced by Meier and Staffelbach in [3]. This concept is equivalent to the bent property discovered by Rothaus in [9]. Bent functions have practical applications in cryptography, coding theory and spread spectrum communication. Classification and construction of bent functions is a very important open problem [8, 9]. Although substantial effort has been given on the study of bent functions in the last three decades even the set of all 8-variables bent functions could not be completely classified. There is only few known method to construct bent functions. Dobbertin and Leander [1] have embedded for the first time the problem of construction of bent functions into a recursive framework by introducing the idea of more general type of functions said to be Z-bent functions. By using this technique they enumerated all the bent functions on 8-variables. In this recursive method Z-bent functions are partitioned into Z-bent functions of different levels. The Z-bent functions of level r on n-variables can be
Used to construct Z-bent functions of level r-1 on n+2 variables by a 'gluing' technique introduced by Dobbertin and Leander [1]. Continuing in this way eventually Z-bent functions of level 0 on n+2r variables are obtained which are same as bent Boolean functions on n+2r variables. In the same paper they mentioned the need of finding out constructions of particular classes of Z-bent functions of arbitrary levels. In paper [2] we have given the construction of PS-type Z-bent functions of arbitrary level r for any r ≥1 and constructed all bent functions up to affine equivalence on 6-variables by using PS-type Z-bent functions of level 1 on 4-variables. In the same paper [2] we have given a new primary construction of bent functions using Z-bent functions. So the study of Z-bent functions of different level is an interesting problem. In this paper we are giving some class of Z-bent functions which are analogous to Maiorana-McFarland functions, Gold like functions and Rotational symmetric functions. We have constructed all rotational symmetric Z-bent functions of level 1on 4-variables and constructed bent functions of level zero i.e. binary bent functions on 6-variables using these Z-bent functions on level 1 on 4-variables.

II. PRELIMINARIES

Any function from F_{2^n} to F_2 is called a Boolean function on n-variables, where $F_2 = \{0,1\}$ is the prime field of characteristic 2 and F_{2^n} is an extension field of degree n over F_2 . The set of all n-variables Boolean functions is denoted by B_n. The Algebraic Normal Form (ANF) of a Boolean function is given as

$$f(x) = \oplus_{a \in F_{2^n}} \mu_a x^a$$

Where $x^a = \prod_{i=1}^{n} x_i^{a_i}$ is a monomial and $\mu_a \in F_2$.

The degree of a Boolean function is the degree of its Algebraic Normal Form. The affine functions are the Boolean functions having degree at most one. The set of all affine functions on n-variables are denoted by A_n. The Hamming distance between two Boolean functions f, g ∈ B_n is denoted by d(f,g) is the size of the set $\{x \in F_{2^n} : f \oplus g \neq 0\}$. If there are two functions f, g∈ B_n such that there exist b, λ ∈ F_2^n and ε ∈ F_2

$$f(x) = g(Ax+b) + Tr_1^n(\lambda x) + \varepsilon$$

Where A∈ GL(n, F_2) is n×n non-singular matrix.
Nonlinearity of f∈ B_n is defined as $nl(f) = \min_{l \in A_n} \{d(f,l)\}$. The Walsh transform of f ∈ B_n at any point λ ∈ F_2^n is defined as

$$W_f(\lambda) = \sum_{x \in F_{2^n}} (-1)^{f(x)+Tr_1^n(\lambda x)}$$

The set $\{W_f(\lambda) : \lambda \in F_{2^n}\}$ is set to be the Walsh spectrum of f. The Fourier transform of f ∈ B_n is defined as

$$\hat{f}(\lambda) = \frac{1}{2^k} \sum_{x \in F_{2^n}} f(x)(-1)^{\lambda \cdot x}$$

Where λ·x is the inner product on F_{2^n} when consider as vector space over F_2. There is a vector space isomprphism between F_2^n and F_{2^n}, where F_2^n is the set of all n-tuples over F_2.

Definition 1: A Boolean function on n variables, where n is even is said to bent if it at the maximum distance to the set of affine functions. Bent functions are the maximally nonlinear in the sense that their Walsh transform attain precisely the value $\pm 2^{\frac{n}{2}}$. Alternatively bent functions are the ± 1 valued functions with ± 1 Fourier transform. The notion of bent functions was defined by Rothaus [9] in 1976.

***Definition 2*:** The Maiorana McFarland class M is the set of all function on $F_2{}^n = \{(x, y) : x, y \in F_2{}^{\frac{n}{2}}\}$ of the form

$$f(x, y) = x\pi(y) \oplus g(y)$$

Where π is a permutation on $F_2{}^{\frac{n}{2}}$ and g is a Boolean function on $F_2{}^{\frac{n}{2}}$. Any such function is bent function.

Definition 3: A Boolean function is said to be Rotational symmetric if for each input $(x_1, ..., x_n) \in \{0,1\}^n$, $f(\rho_n{}^k(x_1, ..., x_n)) = f(x_1, ..., x_n)$ for $1 \leq k \leq n$.

Where $\rho_n{}^k(x_i) = \{^{x_{i+k} if i+k \leq n}_{x_{i+k-n} if i+k > n}$ and

$\rho_n{}^k(x_1, ..., x_n) = (\rho_n{}^k(x_1), ..., \rho_n{}^k(x_n))$

Let

$G_n(x_1, ..., x_n) = \{\rho_n{}^k(x_1, ..., x_n) = (\rho_n{}^k(x_1), ..., \rho_n{}^k(x_n))\}$

then $G_n(x_1, ..., x_n)$ generate a partition on the set V_n. Let g_n be the number of such partition, then the total number of rotational symmetric function on n-variables are 2^{g_n}. The space of rotational symmetric Boolean functions is much smaller than the Boolean functions on n-variables. The space of rotational symmetric Boolean functions is approximately $2^{\frac{2^n}{2}}$ for n-variables. So, any kind of search become comparatively easier.

In the next section we are defining rotational symmetric Z-bent functions and giving some computational results using 'C' programming.

Definition 4: The trace function on F_{2^n} is defined as

$$Tr_1{}^n(x) = x + x^2 + ... + 2^{n-1} \forall x \in F_{2^n}$$

The trace function satisfies the following properties [7]

1. $Tr_1{}^n(x + y) = Tr_1{}^n(x) + Tr_1{}^n(y) \forall x, y \in F_{2^n}$
2. $Tr_1{}^n(cx) = cTr_1{}^n(x) \forall x \in F_2{}^n$ and $c \in F_2$
3. $Tr_1{}^n$ is a linear function from F_{2^n} to F_2 where both are viewed as vector space on F_2
4. $Tr_1{}^n(2^{2^r}) = Tr_1{}^n(x) \forall x \in F_{2^n}$ and for any positive integer r.

Definition 5: A polynomial of the form

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$$

With the coefficient in the extended field F_{q^m} of F_q is said to be linearized polynomial over F_{q^m}.

Let us denote the set of integers by Z. A Boolean function can be viewed as integer valued function by considering $f(x) = (-1)^{F(x)} \in \{-1,1\} \subset Z$. Dobbertin and Leander generalized the notion of bent functions to Z-bent functions [1]. Consider a sequence of subset of Z as

$$W_0 = \{-1,1\}$$
$$W_r = \{w \in Z : -2^{r-1} \leq w \leq 2^{r-1}\}, r \geq 1$$

Definition 6: A function from $F_2{}^n \to W_r$ is said to Z-bent function of size k (here n=2k) and level r if and only if $\hat{f}$ is also a function into W_r. Let the set of all Z-bent functions of size k and level r is denoted by $BF_r{}^k$. Any function belonging to $\cup_{r \geq 0} BF_r{}^k$ is said to be Z-bent function.

Definition 7: An integer- valued function h on $F_2{}^m$, m odd is called an odd Z-bent function if the Fourier spectrum of h lies in $\sqrt{2}Z$.

Suppose $f \in BF_r{}^k$,

$U_{\varepsilon_1\varepsilon_2} = \{(\varepsilon_1, \varepsilon_2, y) : y \in F_2{}^{n-2}\}, \varepsilon_1, \varepsilon_2 \in F_2$

and $h_{\varepsilon_1\varepsilon_2}(y) = f(\varepsilon_1, \varepsilon_2, y), y \in F_2{}^{n-2}$

Construct functions $f_{\varepsilon_1\varepsilon_2}$ as follows:

Case 1: For r≥1

$$\begin{pmatrix} f_{00} & f_{10} \\ f_{10} & f_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} \quad (1)$$

Case 2: For r≥0

$$\begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} \quad (2)$$

It is proved in ([1], Proposition 2) that the functions $f_{\varepsilon_1\varepsilon 2} \in BF_{r+1}{}^{k-1}$ for all $\varepsilon_1, \varepsilon_2 \in F_2$. The functions $f_{\varepsilon_1\varepsilon 2} \in BF_{r+1}{}^{k-1}$ form the canonical decomposition of

$f \in BF_r^k$ and f can be recovered from $f_{00}, f_{10}, f_{01}, f_{11}$ by

$$\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} \quad (3)$$

In the case $r = 0$ f can be recovered from $f_{00}, f_{10}, f_{01}, f_{11}$ by

$$\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} \quad (4)$$

Reversing the decomposition is called gluing but gluing is possible under certain condition. Using this gluing technique it is possible to construct Z-bent functions of large size and lower level from Z-bent functions of smaller size and higher level. So, proceeding in this way after a finite number of steps it is possible to obtain Z-bent functions of level 0, which are same as bent functions. Due to the success of this recursive framework generating and characterizing subclasses of Z-bent functions is an important problem.

III . SOME SPECIAL TYPE OF Z-BENT FUNCTIONS

Here in this section we are defining some special class of Z-bent functions. We call them Maiorana-McFrland type Z-bent functions, Gold like Z-bent functions and Rotational symmetric Z-bent functions.

A. *Maiorana-McFarland type Z-bent functions*

Theorem 1: Let f be an n(=2k)-variables function which is constructed in such a way that $f(x,y) = c_y(-1)^{x\Box\pi(y)}$ where $x, y \in F_2^k, c_y \in W_r$ and π be a permutation on F_2^k, then $f(x,y)$ is a Z-bent function of level r.

Proof: The Fourier transform of f at any point $(a,b) \in F_2^n$ where $a,b \in F_2^{\frac{n}{2}}$ is

$$\hat{f}(a,b) = \frac{1}{2^{\frac{n}{2}}} \sum_{x,y \in F_2^{\frac{n}{2}}} f(x,y)(-1)^{a\Box x + b\Box y}$$

$$= \frac{1}{2^{\frac{n}{2}}} \sum_{x,y \in F_2^{\frac{n}{2}}} c_y(-1)^{x\Box\pi(y)}(-1)^{a\Box x + b\Box y}$$

$$= \frac{1}{2^{\frac{n}{2}}} \sum_{y \in F_2^{\frac{n}{2}}} c_y(-1)^{b\Box y} \sum_{x \in F_2^{\frac{n}{2}}} (-1)^{x\Box\pi(y) + a\Box x}$$

$$= \frac{1}{2^{\frac{n}{2}}} \sum_{y \in F_2^{\frac{n}{2}}} c_y(-1)^{b\Box y} \sum_{x \in F_2^{\frac{n}{2}}} (-1)^{x\Box(\pi(y) + a)}$$

$$= \frac{1}{2^{\frac{n}{2}}} c_{\pi^{-1}(a)} \times 2^{\frac{n}{2}}(-1)^{b\Box\pi^{-1}(a)}$$

$$= c_{\pi^{-1}(a)}(-1)^{b\Box\pi^{-1}(a)}$$

Since as by construction $f \in W_r$ and by proof $\hat{f} \in W_r$. Hence f is a Z-bent function of level r.

Corollary 1: If f is a Maiorana-McFarland type Z-bent function of level r then its dual $\hat{f}$ is also a Z-bent function of level r.

Proof: By the above theorem the dual of $f(x,y) = c_y(-1)^{x\Box\pi(y)}$ is $\hat{f}(a,b) = c_{\pi^{-1}(a)}(-1)^{b\Box\pi^{-1}(a)}$.

This show that dual of Maiorana-McFarland type Z-bent function is again Maiorana-McFarland type Z-bent function.

B. *Gold like Z-bent function*

Here we define Gold like Z-bent function on odd dimension and this type of function are called odd Z-bent functions [1].

Theorem 2: Let $f(x) = \alpha(-1)^{g(x)}$ where $g(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr_1^n(x^{2^i+1}), c_{i\in}\{0,1\}$ and n is odd then $f(x)$ is odd Z-bent function of level 1 if and only if the dimension of the kernel of the cyclic matrix

$$L = \begin{pmatrix} c_0 & \cdots & c_{n-1} \\ \vdots & \ddots & \vdots \\ c_1 & \cdots & c_0 \end{pmatrix}$$

over F_2 is 1, where we define $c_0 = 0$ and $c_{n-i} = c_i$ for $i = 0,\ldots,\frac{n-1}{2}$.

Proof: Since $f(x) = \alpha(-1)^{g(x)}$, therefore $f(x) \in W_1$. The Fourier transform of f at any point λ is given as

$$\hat{f}(\lambda) = \frac{1}{2^{\frac{n}{2}}} \sum_{x \in F_{2^n}} f(x)(-1)^{Tr_1^n(\lambda x)}.$$

$$\hat{f}^2(\lambda) = \frac{1}{2^n} \sum_{x,y \in F_{2^n}} \alpha^2(-1)^{g(x)+Tr_1^n(\lambda x)}(-1)^{g(y)+Tr_1^n(\lambda y)}$$

$$= \frac{1}{2^n} \sum_{x,y \in F_{2^n}} \alpha^2(-1)^{g(x)+Tr_1^n(\lambda x)+g(y)+Tr_1^n(\lambda y)}$$

$$= \frac{1}{2^n} \sum_{x,y \in F_{2^n}} \alpha^2(-1)^{g(x)+Tr_1^n(\lambda\omega)+g(x+\omega)}$$

taking $y = x + \omega$

$$= \frac{1}{2^n} \sum_{\omega \in F_{2^n}} \alpha^2(-1)^{g(\omega)+Tr_1^n(\lambda\omega)} \sum_{x \in F_{2^n}} (-1)^{g(x)+g(\omega)+g(x+\omega)}$$

$$= \frac{1}{2^n} \sum_{\omega \in F_{2^n}} \alpha^2 (-1)^{g(\omega)+Tr_1^n(\lambda\omega)} \sum_{x \in F_{2^n}} (-1)^{\phi(x,\omega)}$$

Where $\phi(x,\omega) = g(\omega) + g(x) + g(x+\omega)$

$$\phi(x,\omega) = \sum_{i=1}^{\frac{n-1}{2}} c_i [Tr_1^n(x^{2^i+1}) + Tr_1^n(\omega^{2^i+1}) + Tr_1^n((x+\omega)^{2^i+1})]$$

$$\phi(x,\omega) = \sum_{i=1}^{\frac{n-1}{2}} c_i [Tr_1^n(x^{2^i+1}) + Tr_1^n(\omega^{2^i+1}) + Tr_1^n((x^{2^i}+\omega^{2^i})(x+\omega))]$$

$$= \sum_{i=1}^{\frac{n-1}{2}} c_i [Tr_1^n(x\omega^{2^i} + x\omega^{2^{n-i}})]$$

Since $Tr_1^n(x^{2^i}\omega) = Tr_1^n(x^{2^i}\omega)^{2^{n-i}} = Tr_1^n(x\omega^{2^{n-i}})$

$$= \sum_{i=1}^{\frac{n-1}{2}} c_i [Tr_1^n(x(\omega^{2^{n-i}} + \omega^{2^i}))]$$

$$= Tr_1^n(x(L(\omega)))$$

Where $L(\omega) = \sum_{i=1}^{\frac{n-1}{2}} c_i(\omega^{2^{n-i}} + \omega^{2^i})$. Since L is a linear function under the normal basis $\{\alpha, \alpha^2, \alpha^{2^2}, ..., \alpha^{2^{n-1}}\}$ of F_{2^n}, the matrix representation of L is given as

$$L = \begin{pmatrix} c_0 & \cdots & c_{n-1} \\ \vdots & \ddots & \vdots \\ c_1 & \cdots & c_0 \end{pmatrix}$$

Since $\sum_{x \in F_{2^n}} (-1)^{\phi(x,\omega)} = \sum_{x \in F_{2^n}} (-1)^{Tr(xL(\omega))} = 2^n$ if and only if $L(\omega) = 0$, otherwise the sum is zero. Therefore $\hat{f}^2(\lambda) = \sum_{\omega \in Ker(L)} \alpha^2 (-1)^{g(\omega)+Tr_1^n(\lambda\omega)}$

Since $\alpha \in W_1 = \{-1, 0, 1\}$ therefore $\hat{f}^2(\lambda) = \sum_{\omega \in Ker(L)} (-1)^{g(\omega)+Tr_1^n(\lambda\omega)}$ or 0. By definition of ϕ, $Tr_1^n(\lambda\omega) + g(\omega)$ is a linear function on Ker(L) and assuming dim(Ker(L))= τ. Therefore

$$\sum_{\omega \in Ker(L)} (-1)^{g(\omega)+Tr_1^n(\lambda\omega)} \in \{2^\tau, 0\}$$

This imply that $\hat{f}(\lambda) \in \{0, \pm 2^{\frac{\tau}{2}}\}$. If dim(Ker(L))=1 then $\hat{f}(\lambda) \in \{0, \pm\sqrt{2}\} = \sqrt{2}W_1$. This imply that $f(x)$ is an odd Z-bent function of level 1.

A way to get Z-bent function of higher level on n-variables is the extension of suitable mapping f on F_2^{n-1} by doubling, i.e, setting $h = [f \mid f]$. Now we have $\hat{h} = \sqrt{2}\left[\hat{f} \mid 0\right]$ because we know that if we set $h = [f_0 \mid f_1]$ and $\hat{h} = [H_0 \mid H_1]$ then

$$\begin{pmatrix} H_0 \\ H_1 \end{pmatrix} = M \begin{pmatrix} \hat{f}_0 \\ \hat{f}_1 \end{pmatrix}$$

Where $M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the self inverse unitery matrix.

Thus the function $h = [f \mid f]$ is of level 2 with Fourier spectrum $\sqrt{2}\{\pm\sqrt{2}, 0\} = \{\pm 2, 0\}$ .Thus we can construct the Z-bent functions of level 2 using the odd Z-bent functions of level 1.

C. **Rotation Symmetric Z-bent functions**

Now in this subsection we are defining the rotational symmetric structure on a function f into W_1, where $W_1 = \{-1, 0, 1\}$ for n= 4. Then we get all rotational symmetric Z-bent function of level 1 on 4-variables and then we use the technique of gluing describe in [1] to get the bent functions of 6-variables. The total number of such functions on n-variables are 3^{2^n} and the total number of rotational symmetric functions are 3^{g_n}. For n=4 we get the following partition

$$G_4(0,0,0,0) = (0,0,0,0);$$
$$G_4(0,0,0,1) = \{(0,0,0,1),(0,0,1,0),(0,1,0,0),(1,0,0,0)\};$$
$$G_4(0,0,1,1) = \{(0,0,1,1),(0,1,1,0),(1,0,0,1),(1,1,0,0)\};$$
$$G_4(0,1,0,1) = \{(0,1,0,1),(1,0,1,0)\};$$
$$G_4(0,1,1,1) = \{(0,1,1,1),(1,0,1,1),(1,1,0,1),(1,1,1,0)\};$$
$$G_4(1,1,1,1) = \{(1,1,1,1)\}$$

Therefore the total number of such function on 4-variables are 3^{2^4} i.e., 3^{16} and the total number of rotational symmetric functions are 3^{g_n} i.e, 3^6 since $g_n = 6$ in this case. Out of these 3^6 rotational symmetric functions only 41 functions are Z-bent functions of level 1. Below is the list of 41 rotational symmetric Z-bent functions on 4-variables.

0000000000000000	1110110-1101-10-1-11
0001001001001000	11101-10-110-1-10-1-11
000-100-100-100-1000	11111-11-111-1-11-1-11
0-1-10-1001-10010110	111-11-1-1-11-1-1-1-1-1-11
0-1-11-1011-11011110	111010001000000-1
0-1-1-1-10-11-1-101-1110	1-1-10-1000-1000000-1
0110100-1100-10-1-10	-100001000010000-1
0111101-1110-11-1-10	-100101100110100-1
011-110-1-11-10-1-1-1-10	-100-101-100-110-100-1
-1110100010000001	-10000-10000-10000-1
-1-110-1000-10000001	100000010001011-1
1000010000100001	-1-1-10-1101-1011011-1
10000-10000-100001	-1-1-11-1111-1111111-1
10010-11001-101001	-1-1-1-1-11-11-1-111-111-1
100-10-1-100-1-10-1001	-1-1-10-1-101-10-11011-1
-1000000100010111	1000000-1000-10-1-1-1
1-1-10-1101-10110111	-1110110-1101-10-1-1-1
1-1-10-1-101-10-110111	-1111111-1111-11-1-1-1
1-1-11-1-111-11-111111	-111-111-1-11-11-1-1-1-1-1
1-1-1-1-1-1-11-1-1-11-1111	-11101-10-110-1-10-1-1-1
-1000000-1000-10-1-11	

Table : Rotational symmetric Z-bent functions of level 1 on 4-variables

After gluing these rotational symmetric Z-bent functions on 4-variables we get 512 Z-bent functions of level 0 on 6-variables i.e., 512 bent functions on 6-variables. These functions are affine equivalent to only two bent functions. It is proved by Rothaus in [9] that there are only 4 functions up to affine equivalent on 6-variables. These four functions are given in the following table.

Sr. No.	functions
1	$x_1x_2 \oplus x_3x_4 \oplus x_5x_6$
2	$x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$
3	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5$
4	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6x_1x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6$

We checked the affine equivalence of those bent functions which we got after gluing the rotational symmetric Z-bent functions of level 1 by using the second derivative spectrum algorithm developed by S. Gangopadhyay in [6] and we found that these
functions are affine equivalent to only two bent functions $x_1x_2 \oplus x_3x_4 \oplus x_5x_6$ and $x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$. Out of these 512 bent functions 128 are affine equivalent to $x_1x_2 \oplus x_3x_4 \oplus x_5x_6$ and 384 are affine equivalent to $x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$.

CONCLUSION

In this paper we have defined Maiorana-McFarland type of Z-bent functions, Gold like Z-bent functions and Rotational symmetric Z-bent functions. We have constructed all rotational symmetric Z-bent functions of level 1 on 4-variables and constructed 6-variables bent functions from these Z-bent functions of level 1 using the recursive technique of paper [1].

REFERENCES

[1] H. Dobbertin, G. Leander, "Bent functions embedded into the recursive framework of Z-bent functions `` Des. Codes Cryptogr. 49(2008), 3-22.

[2] S. Gangopadhyay, Anand Joshi, Gregor Leander, R.K.Sharma, "A new construction of bent functions based on Z-bent functions, Proceeding of seventh international workshop on coding and cryptography, Paris, France (2011), 153-162.

[3] W. Meier, O.Staffelbach, "Nonlinearity criteria for cryptographic functions", In Adv. eurocrypt 88 vol. 434, Berlin srringer, 1990, 54962.

[4] S. Boztas, P. V. Kumar, " Binary sequences with Gold like correlation but larger linear span" IEEE Transactions on Information Theory 40(1994), 532-537.

[5] R. Gold, "Maximal recursive sequences with 3-valued cross correlation " , IEEE Transactions on Information Theory 14(1968) , 154-156.

[6] S. Gangopadhyay, D. Sharma, S. Sarkar, S. Maitra, "On (Non) Affine Equivalence of Bent Functions", Computing 85 (2009) 27-55.

[7] R. Lidl, H. Niederreiter, "Introduction to finite fields and their applications", Cambridge University press, Cambridge (1983).

[8] J. F. Dillon, "Elementary Hadamard difference set ", Proceeding of six S. E. Conference of Combinatorics, Graph theory , and Computing, Utility Mathematics, Winnipeg (1975), 237-249.

[9] O. S. Rothaus, "On bent functions", J. Combin, Theory, Ser. A 20 (1975), 300-305.

[10] F. J. MacWilliams, N. J. Sloane, "The theory of error correcting codes", North Holland, Amsterdam, New York, Oxford 1977.

[11] Pantelimon Stanica, S. Maitra, John A. Clark, "Results on Rotational Symmetric bent and correlation immune Boolean functions" FSE 2004, LNCS, 3017, 161-177, 2004.

[12] C. Shannon, "Communication theory of secrecy systems", Bell systrm technical journal 28, 656-715, 1949.