# On generalized rotation symmetric bent functions

**Anand Joshi**
*Department of Mathematics and Astronomy,*
*University of Lucknow, Lucknow, India*

**Abstract**

The construction of Boolean bent functions and counting(up to affine equivalence) of Boolean bent functions is an important problem in cryptography and combinatorics. Many attempts have been made to generalized the Boolean functions. This paper define rotation symmetric $\mathbb{Z}$-bent (generalized rotation symmetric bent functions) functions. Some results related to rotation symmetric $\mathbb{Z}$-bent functions are given in this paper. Boolean bent functions on 6 variables are constructed using these generalized rotation symmetric $\mathbb{Z}$-bent functions and affine equivalence of these bent functions are checked and the number of Boolean bent functions on 6-variables up to affine equivalence are counted.

**Subject class [2010]**:22E46, 53C35, 57S20
**Keywords**: Boolean functions, bent functions, rotation symmetric bent functions, generalized bent functions, $\mathbb{Z}$-bent functions.

## 1 Introduction

Boolean functions paly an important role in cryptography. Boolean functions with high nonlinearity are used in design of S-boxs in DES block cipher. Many attempts have been made to generalized the bent functions, Kumar et al. [4] have extended the notion of classical bent Boolean functions in the generalized setup on $\mathbb{Z}_q^n$. Some results on the generalize q-array bent functions is given in [3]. There are many known properties of Boolean function to design a good cryptosystem, nonlinearity is one of them. In order to provide confusion cryptographic function should be at large Hamming distance to the set of all affine functions. The maximum nonlinearity for a function on even $n$ is $2^{n-1} - 2^{\frac{n}{2}-1}$. The functions achieving this value are called bent functions. Classification and construction of bent functions is a an important open problem [10, 5]. In last few decades many efforts have been given on the study of bent functions. Still the set of all 8 variable bent functions could not be completely classified. This is due to lack of recurrence relation. First time Dobbertin and Leander [1] have embedded the problem of construction of bent functions into a recursive framework by introducing the idea of generalized Boolean functions they called these functions $Z$-bent functions. The $\mathbb{Z}$-bent functions can be partitioned into $\mathbb{Z}$-bent functions of different levels. These $\mathbb{Z}$-bent functions of one level up are used to generate the $\mathbb{Z}$-bent functions of one level down, for example thee $\mathbb{Z}$-bent functions of level $r$ on $n$ variables can be used to construct $\mathbb{Z}$-bent functions of level $r-1$ on $n+2$ variables by a 'gluing' technique introduced by Dobbertin and Leander [1]. Continuing in this manner one can eventually get $\mathbb{Z}$-bent functions of level 0 on $n + 2r$ variables. These obtained

functions of level 0 are same as Boolean bent functions on $n + 2r$ variables. It is proved in [1] that in this way one can obtain all the bent functions although for large variables the computation may not be feasible. The construction of Boolean bent function is an important problem. $\mathbb{Z}$-bent functions of level $r \geq 1$ can be used to construct the $\mathbb{Z}$-bent function of level zero i.e. classical bent functions, therefore from this point of view the construction of some class of $\mathbb{Z}$-bent of different levels and study of these $\mathbb{Z}$-bent functions of different level is interesting problem in cryptography. A primary construction of bent functions from $PS_{ap}$ type $\mathbb{Z}$-bent functions is given in [2]. Here in this paper we define rotation symmetric $\mathbb{Z}$-bent functions and give some experimental results. We construct all the rotational symmetric $\mathbb{Z}$-bent functions on 4-variables and construct Boolean bent functions on 6-variables using the gluing technique.

## 2 Preliminaries

Let $\mathbb{F}_2$ be the prime field of characteristic 2 and $\mathbb{F}_{2^n}$ be the $n$ degree extension field of $\mathbb{F}_2$. Any function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ is said to be a Boolean function on $n$ variables. The set of all Boolean functions on $n$ variables is denoted by $\mathcal{B}_n$. A way of representing an $n$-variable Boolean function is in the polynomial form over the field $\mathbb{F}_2$ with $n$ many indeterminate $x_1, x_2, ..., x_n$ is called its algebraic normal form. It can be uniquely (up to permutation of indeterminate and monomials) represented in the ring $\mathbb{F}_2[x_1, x_2, ..., x_n]/ < x_1^2 - x_1, x_2^2 - x_2, ..., x_n^2 - x_n >$ as follows:

$$f(x) = \bigoplus_{I \in P(N)} a_I (\prod_{i \in I} x_i) = \bigoplus_{I \in P(N)} a_I x^I$$

where $P(N)$ denote the power set of $N = 1, ..., n$. The degree of a Boolean function is the degree of its algebraic normal form. The affine functions are the Boolean functions having the degree at most one. Another way to represent a Boolean functions is the truth table representation and the Hamming distance between two Boolean functions is the number of places where they differ in their truth table representation. The notion of bent functions was introduced by Rothaus[5] in 1976. Bent functions are Boolean functions on $\mathbb{F}_2^n$ with $n$ even, which are maximally nonlinear in the sense that their Walsh transform attains precisely the values $\pm 2^{\frac{n}{2}}$. The walsh transform of a Boolean function $F$ at a point $a \in \mathbb{F}_{2^n}$ is defined as:

$$W_F(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{F(x)} (-1)^{<a,x>}$$

and the Fourier transform of a function $f$ at a point $a \in \mathbb{F}_{2^n}$ is defined as:

$$\hat{f}(a) = \frac{1}{2^k} \sum_{x \in \mathbb{F}_{2^n}} f(x) (-1)^{<a,x>}$$

where $n = 2k$ and $< a, x >$ is an inner product on $\mathbb{F}_{2^n}$ when considered as a vector space over $\mathbb{F}_2$.
Many attempted have been made to generalized the Boolean functions. In paper [1] boolean

functions are generalized into the set of integers, which are called $\mathbb{Z}$-bent functions. Let us denote the set of integers by $\mathbb{Z}$. A Boolean function can be viewed as an integer valued function by considering $f(x) = (-1)^{F(x)} \in \{-1, 1\} \subset \mathbb{Z}$. As bent functions are Boolean functions on $\mathbb{F}_2^n$ with $n$ even, which are maximally nonlinear in the sense that their Walsh transform attains precisely the values $\pm 2^{\frac{n}{2}}$. Alternately bent functions can be defined as $\pm 1$-valued functions on $\mathbb{F}_2^n$ with $\pm 1$ valued Fourier transform.
Dobbertin and Leander generalized the notion of bent functions to $\mathbb{Z}$-bent functions [1]. Consider a sequence of subsets of $\mathbb{Z}$ as follows:

$$\begin{aligned} W_0 &= \{-1, 1\} \\ W_r &= \{w \in \mathbb{Z} | -2^{r-1} \leq w \leq 2^{r-1}\} \text{ for } r > 0. \end{aligned}$$

**Definition 2.1.** A function $f : \mathbb{F}_{2^n} \longrightarrow W_r$ is said to be a $\mathbb{Z}$-bent function of size $k$ (equivalently on $n$ variables) level $r$ if and only if $\hat{f}$ is also a function into $W_r$. Let set of all $\mathbb{Z}$-bent functions of size $k$ and level $r$ be denoted by $\mathcal{B}F_r^k$. Any function belonging to $\cup_{r\geq 0}\mathcal{B}F_r^k$ is said to be a $\mathbb{Z}$-bent function.

Suppose $f \in \mathcal{B}F_r^k$,

$$U_{\epsilon_1\epsilon_2} = \{(\epsilon_1, \epsilon_2, y) | y \in \mathbb{F}_2^{n-2}\}, \epsilon_1, \epsilon_2 \in \mathbb{F}_2.$$

and

$$h_{\epsilon_1\epsilon_2}(y) = f(\epsilon_1, \epsilon_2, y), y \in \mathbb{F}_2^{n-2}.$$

Construct functions $f_{\epsilon_1\epsilon_2}$ as follows:
**Case 1** For $r \geq 1$:

$$\begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix}. \tag{2.1}$$

**Case 2** For $r = 0$:

$$\begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix}. \tag{2.2}$$

It is proved in ([1], Proposition 2) that the functions $f_{\epsilon_1\epsilon_2} \in \mathcal{B}F_{r+1}^{k-1}$, for all $\epsilon_1, \epsilon_2 \in \mathbb{F}_2$. The functions $f_{\epsilon_1\epsilon_2} \in \mathcal{B}F_{r+1}^{k-1}$, for all $\epsilon_1, \epsilon_2 \in \mathbb{F}_2$ form the canonical decomposition of $f \in \mathcal{B}F_r^k$ and $f$ can be recovered from $f_{00}, f_{10}, f_{01}$, and $f_{11}$ by

$$\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix}. \tag{2.3}$$

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

$$\begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix}. \tag{2.4}$$

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

## 3 Rotation symmetric $\mathbb{Z}$-bent functions

The class of Boolean functions that are invariant under circular translation of indices, is potentially rich in functions of cryptographic significance. Several cryptographically good functions gave been obtained by searching over rotational symmetric functions. Kavut, Maitra and Yucel obtained Boolean functions on 9 variables with nonlinearity 241 by searching over rotational symmetric functions [7, 6]. The rotation symmetric Boolean functions are defined as follows
For $1 \leq k \leq n$ the function $\rho_n^k$ defined as

$$\rho_n^k(x_i) = \begin{cases} x_{i+k}, & \text{if } i+k \leq n, \\ x_{i+k-n}, & \text{if } i+k > n. \end{cases}$$

Then a Boolean function $f$ is rotation symmetric if and only if for any $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$, $f(\rho_n^k(x_1, x_2, \ldots, x_n)) = f(x_1, x_2 ..., x_n)$ for any $1 \leq k \leq n$. We let

$$G_n(x_1, \ldots, x_n) = \{\rho_n^k(x_1, \ldots, x_n), \text{ for } 1 \leq k \leq n\},$$

that is, orbit of $(x_1, \ldots, x_n)$ under the action of $\rho_n^k$, $1 \leq k \leq n$. Then $G_n(x_1, \ldots, x_n)$ generate a partition of cardinality $g_n$, of the set $\mathbb{F}_2^n$. For $(x_1, \ldots, x_n)$, a function is rotation symmetric if it takes the same value for all the elements in $G_n(x_1, \ldots, x_n)$. The Walsh spectrum of a rotational symmetric Boolean function is at most $g_n$ valued. Pieprzyk and Qu studied these functions as components in the rounds of a hashing algorithm [8]. The size of space of rotation symmetric Boolean functions is approximately $2^{\frac{2^n}{n}}$ for $n$ variables, which is of size $n$-th root of the total space $2^{2^n}$. Thus any kind of search becomes comparatively easier.

Here we are generalizing rotation symmetric Boolean bent functions into the the rotation symmetric generalized bent functions. We define the rotation symmetric $\mathbb{Z}$-bent functions in a similar fashion as rotation symmetric Boolean bent functions.

For $1 \leq k \leq n$ the function $\rho_n^k$ defined as

$$\rho_n^k(x_i) = \begin{cases} x_{i+k}, & \text{if } i+k \leq n, \\ x_{i+k-n}, & \text{if } i+k > n. \end{cases}$$

A function $f$ from $\mathbb{F}_2^n$ into $W_r$ is called $W_r$-rotation symmetric function if and only if for any $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$, $f(\rho_n^k(x_1, x_2, \ldots, x_n)) = f(x_1, x_2 ..., x_n)$ for any $1 \leq k \leq n$. We let

$$G_n(x_1, \ldots, x_n) = \{\rho_n^k(x_1, \ldots, x_n), \text{ for } 1 \leq k \leq n\},$$

that is, orbit of $(x_1, \ldots, x_n)$ under the action of $\rho_n^k$, $1 \leq k \leq n$. Then $G_n(x_1, \ldots, x_n)$ generate a partition of cardinality $g_n$, of the set $\mathbb{F}_2^n$. For $(x_1, \ldots, x_n)$, a function is rotation symmetric if it takes the same value for all the elements in $G_n(x_1, \ldots, x_n)$.

**Proposition 3.1.** *The number of $W_r$-rotation symmetric functions are $(2^r + 1)^{g_n}$, where $g_n$ is the cardinality of the partition set $G_n(x_, \ldots, x_n)$ and $r > 0$.*

*Proof.* Since $W_r = \{w \in \mathbb{Z} | -2^{r-1} \leq w \leq 2^{r-1}\}$ for $r > 0$. The cardinality of the set $W_r$ is $2^r + 1$, so it is obvious by the definition of $W_r$ valued function the number of such functions are $(2^r + 1)^{g_n}$, hence proved. □

For example the number of $W_1$ rotation symmetric functions on $\mathbb{F}_2^4$ are $3^6$. Here the partition of $G_n(x_1, x_2, x_3, x_4)$ is given as

$$
\begin{aligned}
&G_4(0,0,0,0) = (0,0,0,0),\\
&G_4(0,0,0,1) = (0,0,0,1),(0,0,1,0),(0,1,0,0),(1,0,0,0),\\
&G_4(0,0,1,1) = (0,0,1,1),(0,1,1,0),(1,0,0,1),(1,1,0,0),\\
&G_4(0,1,0,1) = (0,1,0,1),(1,0,1,0),\\
&G_4(0,1,1,1) = (0,1,1,1),(1,0,1,1),(1,1,0,1),(1,1,1,0),\\
&G_4(1,1,1,1) = (1,1,1,1).
\end{aligned}
$$

Here the cardinality of partition is $g_n = 6$. Hence the number of $W_1$-rotation symmetric functions are $(2^r + 1)^{g_n} = (2^1 + 1)^6 = 3^6$, here $r = 1$.

Let the lexicographically first element is each partition is considered as the representative element. Let the representative element is denoted by $\bigwedge_{n,i}$, where $i$ varies from 0 to $g_n - 1$. In the above example $\bigwedge_{4,0} = (0,0,0,0), \bigwedge_{4,1} = (0,0,0,1), \bigwedge_{4,2} = (0,0,1,1), \bigwedge_{4,3} = (0,1,0,1), \bigwedge_{4,4} = (0,1,1,1), \bigwedge_{4,0} = (1,1,1,1)$.

**Proposition 3.2.** *Let $u, v \in \mathbb{F}_2^n$ and $u \neq v$ with $u \in G_n(v)$. Let $f$ be an $n$-variable rotational symmetric $\mathbb{Z}$-bent function of level $r$, i.e., $f \in \mathcal{B}F_r^k, k = \frac{n}{2}$, then $\hat{f}(u) = \hat{f}(v)$.*

*Proof.* Since $u \in G_n(v)$, therefore $u = \rho_n^k(v)$ for some $k$.

$$\hat{f}(u) = \frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{<u,x>} \tag{3.1}$$

$$= \frac{1}{2^{n/2}} \sum_{i=0}^{g_n - 1} \sum_{x \in G_n(\bigwedge_{n,i})} f(x)(-1)^{<u,x>} \tag{3.2}$$

Since $\sum_{x \in G_n(\bigwedge_{n,i})} f(x)(-1)^{<u,x>} = \sum_{x \in G_n(\bigwedge_{n,i})} f(\rho_n^k(x)(-1)^{\rho_n^k(u), \rho_n^k(x)}$, take $y = \rho_n^k(x)$,

therefore

$$\hat{f}(u) = \frac{1}{2^{n/2}} \sum_{i=0}^{g_n-1} \sum_{y \in G_n(\bigwedge_{n,i})} f(y)(-1)^{<y,v>} \tag{3.3}$$

$$= \frac{1}{2^{n/2}} \sum_{i=0}^{g_n-1} \sum_{x \in G_n(\bigwedge_{n,i})} f(x)(-1)^{<x,v>} \tag{3.4}$$

$$= \frac{1}{2^{n/2}} \sum_{i=0}^{g_n-1} \sum_{x \in G_n(\bigwedge_{n,i})} f(x)(-1)^{<x,v>} \tag{3.5}$$

$$= \frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{<v,x>} \tag{3.6}$$

$$= \hat{f}(v) \tag{3.7}$$

□

**Proposition 3.3.** *Let $u, v \in \mathbb{F}_2^n$ and $u \neq v$ with $u \in G_n(v)$. Let $f$ be an $n$-variable rotational symmetric $\mathbb{Z}$-bent function of level $r$, i.e., $f \in \mathcal{BF}_r^k, k = \frac{n}{2}$. The fourier transform of $f \in \mathcal{BF}_r^k$ can be at most $g_n$ valued.*

*Proof.* From the proposition 3.2, $\hat{f}(u) = \hat{f}(v)$ for $u, v \in \mathbb{F}_2^n$ and $u \neq v$ with $u \in G_n(v)$ which imply that fourier spectrum of a rotational symmetric $\mathbb{Z}$ bent function $f$ can be at most $g_n$ valued. □

Now here we are defining the rotation symmetric structure on a function $f$ on $\mathbb{F}_2^n$ into $W_1$, where $W_1 = \{-1, 0, 1\}$, for $n = 4$. The total number of such $W_1$-valued functions on $n$ variable are $3^{2^n}$ and the total number of rotation symmetric $W_1$-valued functions on $n$ variables are $3^{g_n}$ by proposition 3.1. For $n = 4$ we get the following partition on $\mathbb{F}_2^n$

$$\begin{aligned}
&G_4(0,0,0,0) = (0,0,0,0),\\
&G_4(0,0,0,1) = (0,0,0,1), (0,0,1,0), (0,1,0,0), (1,0,0,0),\\
&G_4(0,0,1,1) = (0,0,1,1), (0,1,1,0), (1,0,0,1), (1,1,0,0),\\
&G_4(0,1,0,1) = (0,1,0,1), (1,0,1,0),\\
&G_4(0,1,1,1) = (0,1,1,1), (1,0,1,1), (1,1,0,1), (1,1,1,0),\\
&G_4(1,1,1,1) = (1,1,1,1).
\end{aligned}$$

Therefore the total number of $W_1$-valued functions on 4 variables are $3^{2^4}$ i.e. $3^{16}$ and the total number of rotation symmetric $W_1$-valued functions are $3^{g_n}$ i.e. $3^6$ since $g_n = 6$ in this case. The rotation symmetric $\mathbb{Z}$-bent functions of level are the those $W_r$-rotation symmetric functions whose fourier transform also lie in the set $W_r$. Using MATLAB program by exhaustive search method we count all the rotation symmetric $\mathbb{Z}$-bent functions of level 1.

Out of these $3^6$ $W_1$-rotation symmetric functions, only 41 functions are $\mathbb{Z}$-bent functions of level 1 on 4 variables. We are giving the list of all rotation symmetric $\mathbb{Z}$-bent functions of level 1 on 4 variables in the table 1.

| | | |
|---|---|---|
| 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 | 1-1-1-1-1-1-1-11-1-1-11-1111 |
| -11101-10-110-1-10-1-1-1 | -1000000-1000-10-1-11 | |

Tab. 1: Rotation symmetric $\mathbb{Z}$-bent functions of level 1 on 4 variable

## 4 Construction of Boolean bent functions from the generalized rotation symmetric $\mathbb{Z}$-bent functions

In this section we construct classical(Boolean) bent functions on 6 variables from the rotation symmetric $\mathbb{Z}$-bent functions of level 1 as described in section3. We get all rotation symmetric $\mathbb{Z}$-bent functions on 4 variables and then we use the technique of gluing describe in [1] to get the Boolean bent functions on $n = 6$ variables. After gluing these Rotation Symmetric $\mathbb{Z}$-bent functions of level 1 on 4 variables we get $\mathbb{Z}$-bent functions of level 0(classical bent functions) on 6 variables. We get 512 $\mathbb{Z}$-bent function of level 0 on 6 variables i.e. **5**12 classical bent functions on 6 variables. In the next section we check the affine equivalence of these Boolean bent functions.

## 5 Inequivalence of constructed Boolean functions

In this section we check the affine equivalence of Boolean functions constructed in the above section by the second derivative spectrum algorithm developed by S.Gangopadhyay et al. [9]. Affine equivalence paly an important role of construct a new class of Boolean functions. Two Boolean functions $F, G \in \mathcal{B}_n$ are said to be equivalent if there exist $A \in GL(n, \mathbb{F}_2)$, the general linear group acting on $\mathbb{F}_2^n$, $b, \lambda \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$ such that $G(x) = F(Ax + b) + \langle \lambda, x \rangle + \epsilon$ for all $x \in \mathbb{F}_2^n$. If $\lambda = 0$ and $\epsilon = 0$ then $F$ and $G$ are said to be affine equivalent. The important fact is that equivalence preserves the bent property. That is to say, given two equivalent functions $F$ and $G$, it holds that $F$ is bent if and only if $G$ is bent. This allows to someone to construct many bent functions from a single one in

a trivial way. Rothaus [5] obtained all the inequivalent bent functions on 6 variables by using computational techniques. Rothaus [5] proved that there are only 4 bent functions on 6 variables up to affine equivalence. These 4 functions are shown in Table 2. For two

| Sr.No. | Function(f) |
|---|---|
| 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 | $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6x_1x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6$ |

Tab. 2: All bent functions in dimension 6

given functions, the task of deciding whether those functions are (affine) equivalent or not might be difficult. One way out of this problem is to come up with suitable invariants such as the weight distribution of the Fourier spectra, the autocorrelation spectra, the algebraic degrees of the functions under consideration. However, in case of bent functions with the same algebraic degree this method fails since any two bent functions have the same weight distribution of Fourier spectra up to complementation, and identical autocorrelation spectra. Dillon [10] considered this problem and proved the following results.

**Theorem 5.1** ([10], Theorem 2.1)**.** *For any function $f \in \mathcal{B}_n$, let $\mathcal{D}_k(f)$ denote the multiset of all kth-derivatives (k-dimensional derivatives) of $f$. If $f, g \in \mathcal{B}_n$ are affine equivalent, then so are $\mathcal{D}_k(f)$ and $\mathcal{D}_k(g)$. If the nonsingular affine transformation $A$ (operating on $\mathcal{B}_n$) maps $f$ onto $g$, then it also maps $\mathcal{D}_k(f)$ onto $\mathcal{D}_k(g)$.*

Furthermore, Dillon proved the following corollary to Theorem 5.1.

**Corollary 5.1.** *If $\mathcal{P}$ is any affine invariant for $\mathcal{B}_n$, then*

$$f \to \mathcal{P}\{\mathcal{D}_k(f)\} \tag{5.1}$$

*is also an affine invariant for $\mathcal{B}_n$.*

As a special case of the above result due to Dillon, for bent functions in dimension 6 a particular suitable invariant is the **P** value introduced in [9] and we recall its definition and properties here. Suppose $\mathcal{T}_2^n$ is the set of all distinct two-dimensional subspaces of $\mathbb{F}_2^n$. For any $V \in \mathcal{T}_2^n$, the second derivative of $F$ at $V$ is defined as

$$D_V F(x) = F(x) + F(x+a) + F(x+b) + F(x+a+b), \text{ for all } x \in \mathbb{F}_2^n,$$

where $\{a, b\}$ is a basis of $V$. It is to be noted that the second derivative of $F$ at $V$ is independent of the choice of the basis. Suppose

$$S(F:V) = \sum_{x \in \mathbb{F}_2^n} D_V F(x).$$

Let $\mathbf{P}(F) = (P_1(F), P_2(F), P_3(F)) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ be such that $P_1(F)$ is the number of elements $V \in \mathcal{T}_2^n$ where $D_V(F) = 0$, $P_2(F)$ is the number of elements $V \in \mathcal{T}_2^n$ where

| Sr. No. | Function $(F)$ | $(P_1(F), P_2(F), P_3(F))$ |
|---|---|---|
| 1 | $x_1x_2 \oplus x_3x_4 \oplus x_5x_6$ | $(315, 336, 0)$ |
| 2 | $x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$ | $(91, 112, 448)$ |
| 3 | $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5$ | $(35, 56, 560)$ |
| 4 | $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4$ $\oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6$ | $(7, 28, 616)$ |

Tab. 3: All bent functions in dimension 6 along with their **P** value.

$D_V(F) = 2^n$, and $P_3(F)$ is the number of elements $V \in \mathcal{T}_2^n$ where $0 < D_V(F) < 2^n$. Clearly $P_3(F) = |\mathcal{T}_n| - P_1(F) - P_2(F)$.
In Table 3 we give the **P** values corresponding to each of the 4 inequivalent classes of bent functions in dimension 6 ([9]). In particular it is obvious from this table that two bent functions in dimension 6 are equivalent if and only if they have the same **P** value. We compare the **P** value of the bent functions obtained from the gluing of rotational symmetric functions in section 4 with the table 3 and find that these functions are affine equivalence to only two bent function $x_1x_2 \oplus x_3x_4 \oplus x_5x_6$ and $x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$. In section 4 we got 512 Boolean functions out of which 128 functions are affine equivalence to the $x_1x_2 \oplus x_3x_4 \oplus x_5x_6$ bent function and 384 functions are affine equivalence to the $x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$ bent function. These functions are affine equivalence to only two bent functions on 6 variables. So, we use this list and the **P** values to show that it is possible to generate the bent functions on 6 variables, up to affine equivalence, starting from rotation symmetric $\mathbb{Z}$-bent functions of level 1 on 4 variables.

## 6 Conclusion

A class of generalized rotation symmetric functions which are called rotation symmetric $\mathbb{Z}$ functions is given in this paper. Few results are given related to these rotation symmetric $\mathbb{Z}$-bent functions. Classical bent functions on 6 variables have been constructed using these rotation symmetric $\mathbb{Z}$ functions of level 1 on 4 variables by gluing these functions. Affine equivalence have been checked by using the second derivative test and Boolean bent functions on 6 variables have been counted up to affine equivalence.

## References

[1] H.Dobbertin and G.Leander "Bent functions embedded into the recursive framework of $\mathbb{Z}$-bent functions", *Design Codes and Cryptography, 49 (2008), 3–22, 2008.*

[2] S.Gangopadhyay and Anand Joshi and Gregor Leander and R.K. Sharma , "A new construction of bent functions based on $\mathbb{Z}$-bent functions", *Design Codes and Cryptography, 66, 243–256, 2013",.*

[3] Deep Singh, Maheshanand Bhaintwal, Brajesh Kumar Singh "Some results on q-ary bent functions", *International Journal of Computer Mathematics, 90(9): 1761-1773 (2013).*

[4] P.V. Kumar, R.A. Scholtz, and L.R.Welch, "Generalized bent functions and their properties", *J. Comb. Theory Ser.A 40 , pp. 90-107 (1985).*

[5] O.S. Rothaus, "On bent functions,", *Journal of Combinatorial Theory, volume(20), 300–305, 1976.*

[6] S. Kavut and S. Maitra and M. D. Yücel, "Search for Boolean Functions With Excellent Profiles in the Rotation Symmetric Class", *IEEE Transactions on Information Theory, volume(53), 1743–1751, 2007.*

[7] S. Kavut and S. Maitra and M. D. Yücel , "Enumeration of 9-variable Rotation Symmetric Boolean Functions having Nonlinearity $> 240$",*INDOCRYPT, 266–279, 2006*

[8] J. Pieprzyk and C.X. Qu , "Fast Hashing and Rotation-Symmetric Functions", *Journal of Universal Computer Science, (5),20–31, 1999.*

[9] S.Gangopadhyay and D.Sharma and S.Sarkar and S.Maitra , "On affine (non)equivalence of Boolean functions", *Computing", (85), 37–55, 2009.*

[10] J.F. Dillon , "Elementary Hadamard Difference Sets", *In the proceeding of* 6*th S. E. Conferrence of Combinatorics, Graph Theory, and Computing, Utility Mathemtics, Winnipeg, 237–249, 1975.*