COUNT AND CRYPTOGRAPHIC PROPERTIES OF GENERALIZED SYMMETRIC BOOLEAN FUNCTIONS

Shashi Kant Pandey
Department of Mathematics
University of Delhi
Delhi – 110007
India
e-mail: shashikantshvet@gmail.com

P.R. Mishra
Scientific Analysis Group
Metcalfe House Complex, DRDO
Delhi – 110054
India
e-mail: prasanna.r.mishra@gmail.com

B.K. Dass
Department of Mathematics
University of Delhi
Delhi – 110007
India
e-mail: dassbk@rediffmail.com

Abstract. Boolean functions with symmetry have been the object of interest to the researchers. With their concise representation and ease of computation, they offer themselves as cut above the rest candidates for the filtering and exploration of optimal Boolean functions. Generalized Boolean functions have been explored as a number of trade-offs in usual Boolean hinder, the process of selecting good Boolean functions required for a specific application. Therefore, it would be interesting to investigate symmetry in Boolean functions in a generalized scenario. We look into three different symmetries in generalized Boolean function according to different parameter of symmetry and present enumeration formulae. We also present an exhaustive construction of bent and balanced symmetric generalized functions (in form of ANF) on smaller domains.

Keywords: Bent function, non linearity, symmetric group.
AMS Subject Classification: 94A60, 94A50, 20B30, 11T71.

1. Introduction

Boolean functions are amply used in cryptographic designs especially in stream cipher designs where these functions play roles for combiners and filters. Not every Boolean function is a suitable candidate to be used in a cryptographic designs. A cryptograhically suited Boolean function must possess some properties

which make a design resistant to cryptanalytic attacks. The computational search for cryptographically suited Boolean functions becomes harder and harder as the number of variables increases. This is because the search space grows exponentially with the number of variables. That is why it is sometimes easier to search for good Boolean functions in a relatively smaller but wisely chosen subset of set of all Boolean functions. Examples of such subsets are the sets of symmetric and rotational symmetric Boolean function.

Another problem with Boolean functions is the presence of a number of trade-offs between various properties[1], [3], [7], [9], [11]. For example, Camion et al. [2] has shown that for a p variable Boolean function, there is a trade-off between the correlation immunity k and the degree d, i.e., $(d+k) < (p-1).k$. Such trade-offs do not let us maximize the desired properties to their maximum possible values.

Therefore, study of symmetries of Boolean functions in a generalized scenario would be an interesting direction to explore into. Not much has been reported so far in this direction. Though some work on generalization of partial symmetric Boolean functions can be found in [3]. We are presenting here generalization of three type of symmetric Boolean functions and their characterizations. The direct generalization of symmetric Boolean functions from binary field provide us a chance to generalized the result of Savicky [4] on symmetric bent function and we landed up to a conjecture which is given in the last section of this paper. In Section 2, we provide enumeration of all three generalized symmetric Boolean functions and, in Section 3, we proved some results in correspondence with bent properties and balancedness of generalized symmetric functions.

2. Generalized symmetric Boolean functions

Symmetries of Boolean functions are seen as behaviour of the function at orbits under the action of some permutation group. On similar lines, we can define symmetries for Generalized functions. Below we define a symmetric function on generalized domain.

Definition 1. Let $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ be an arbitrary function. f is said to be generalized symmetric Boolean function (GSBF) if for every $\mathbf{x} \in \mathbb{Z}_q^n$, f is constant on the orbit of $\mathbf{x}$ under the action of $\mathfrak{S}_n$ on $\mathbf{x} \in \mathbb{Z}_q^n$.

We can see that on the basis of the selection of the permutation group we can categorize the action of these group on the set of vectors. The next definition of a rotational symmetric function is just another choice of the permutations. To this end, we first define a shift operator ρ_n^k on $\mathbb{Z}_q^n$ as:

Given $\mathbf{x} = (x_1, x_2, ..., x_n) \in \mathbb{Z}_q^n$ $1 \le i \le n$ and $1 \le k \le n$ we define

$$\rho_n^k(\mathbf{x}) = (x_{t_1}, x_{t_2}, ..., x_{t_n})$$

where, $t_i = \begin{cases} t_{i+k}, & \text{if } i+k \le n, \\ t_{i+k-n}, & \text{otherwise,} \end{cases}$ for all $1 \le i \le n$.

Definition 2. Let $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ be an arbitrary function. f is said to be generalized rotational symmetric Boolean function (GRSBF) if for every $\mathbf{x} \in \mathbb{Z}_q^n$, f is constant on the orbit of $\mathbf{x}$ under the action of ρ_n^i on $\mathbf{x} \in \mathbb{Z}_q^n$. In other words, for any $(x_1, x_2, ..., x_n) \in \mathbb{Z}_q^n$, $f(\rho_n^k(x_1, x_2, ..., x_n)) = f(x_1, x_2, ..., x_n)$.

Now, we are showing the next generalization of symmetric Boolean function on the basis of direct extension of the definition of symmetric Boolean function for $q = 2$.

Definition 3. *Let $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ be an arbitrary function. f is said to be generalized super symmetric Boolean function (GSSBF) if for every $\mathbf{x} \in \mathbb{Z}_q^n$, f is constant on all $\mathbf{x}$ of same hamming weight, irrespective of its permutation.*

We can express this function as $f(\mathbf{x}) = v_{wt(\mathbf{x})} \in \mathbb{Z}_q$, where $wt(\mathbf{x})$ denotes Hamming weight of vector $\mathbf{x}$.

Definition 4. *A function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is said to be balanced if for $0 \leq k \leq q-1$, the cardinality of $S = \{x \in Z_q^n : f(x) = k\}$ is independent of k.*

3. Walsh transform of generalized symmetric and super symmetric functions

It is obvious that, for $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^n \implies \mathfrak{S}_n.\mathbf{x} = \mathfrak{S}_n.\mathbf{y}$ if and only if $\{x_1, x_2, ..., x_n\} = \{y_1, y_2, ..., y_n\}$, where $\mathbf{x} = (x_1, x_2, ..., x_n), \mathbf{y} = (y_1, y_2, ..., y_n)$. We define the set $U = \{\mathbf{u} | \mathbf{u} = (u_1, u_2, ..., u_n), u_1 \leq u_2 \leq \cdots u_n\}$. Clearly, U is the maximal subset of $\mathbb{Z}_q^n$ with the property $\mathbf{u_1}, \mathbf{u_2} \in U_k, \mathbf{u_1} \neq \mathbf{u_2} \implies \mathfrak{S}_n.\mathbf{u}_1 \neq \mathfrak{S}_n.\mathbf{u}_2$. Hence $\mathbb{Z}_q^n$ can be written as disjoint union of orbits of elements in U.

$$\mathbb{Z}_q^n = \bigcup_{\mathbf{u} \in U} \mathfrak{S}_n.\mathbf{u} \tag{1}$$

As per definition, f is constant on orbits. Therefore, we define $f(x) = v_{\mathbf{u}}$, $\forall \mathbf{x} \in \mathfrak{S}_n.\mathbf{u}$. The Walsh transform of f at $\mathbf{w} \in \mathbb{Z}_q^n$ can be given as

$$W_f(\mathbf{w}) = \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \zeta^{f(\mathbf{x}) + \mathbf{w}.\mathbf{x}} = \sum_{\mathbf{u} \in U} \sum_{\mathbf{x} \in \mathfrak{S}_n.\mathbf{u}} \zeta^{f(\mathbf{x}) + \mathbf{w}.\mathbf{x}} = \sum_{\mathbf{u} \in U} \zeta^{v_{\mathbf{u}}} \sum_{\mathbf{x} \in \mathfrak{S}_n.\mathbf{u}} \zeta^{\mathbf{w}.\mathbf{x}}. \tag{2}$$

We can see that the rightmost summation in (2) is independent of the choice of f and to calculate the internal sum we use Bernside's lemma [12]. So the order of U can be given by

$$|U| = |\mathbb{Z}_q^n / \mathfrak{S}_n| = \frac{1}{n!} \sum_{s \in \mathfrak{S}_n} \mathbb{Z}_q^{n^s}, \tag{3}$$

where $\mathbb{Z}_q^{n^s} = \{\mathbf{x} \in \mathbb{Z}_q^n | s.\mathbf{x} = \mathbf{x}\}$. Also, from the orbit stabilizer theorem,

$$|\mathfrak{S}_n.\mathbf{x}| = \frac{n!}{Stab(\mathbf{x})},$$

where $Stab(\mathbf{x}) = \{s \in \mathfrak{S}_n | s.\mathbf{x} = \mathbf{x}\}$. So to enumerate U we need $|Stab(\mathbf{x})|$ under the action of s.

The Walsh transformation of GSBF is defined as

$$W_f(w) = \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \zeta^{f(\mathbf{x})+w.\mathbf{x}} = \sum_{k=0}^{n} \zeta^{v_k} \sum_{wt(\mathbf{x})=k} \zeta^{w.\mathbf{x}}$$

3.1. Enumeration of generalized symmetric and rotational symmetric Boolean function

Theorem 3.1. *Total number of GSBF $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is $q^{\binom{n+q-1}{q-1}}$.*

Proof. By the definition of GSBF the number of GSBF is given as,

$$\#GSBF = q^{|U|} \tag{4}$$

We have shown in (3) that how $|U|$ can be calculated. We here proceed in a different manner to estimate $|U|$. From the definition of U, it is clear that U has one to one correspondence with the set of all combinations of n objects each can be repeated q times. This set has cardinality $\binom{n+q-1}{q-1}$. Therefore,

$$|U| = \binom{k+q-1}{q-1} \tag{5}$$

(4) and (5) together give

$$\#GSBF = q^{\binom{n+q-1}{q-1}}. \tag{6}$$

∎

The next theorem deals with the enumeration of GRSBF.

Theorem 3.2. *The number of GRSBF on $\mathbb{Z}_q^n$ is q^{s_n} where $s_n = (1/n)\sum_{m|n} \phi(m) q^{n/m}$.*

Proof. The set of all rotations (denote it by S_n) is a subgroup of $\mathfrak{S}_n$. The orbit of $\mathbf{x} = (x_1, ..., x_n)$ under the action of S_n is given as

$$S_n \cdot \mathbf{x} = \{\rho_n^k(\mathbf{x}) | 1 \le k \le n\}.$$

Let s_n is the number of orbits formed by this action. Clearly, the number of rotational symmetric $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is q^{s_n}.

We derive the expression for s_n using Burnside's lemma. The disjoint cyclic decomposition of ρ_n^i can be written as

$$\rho_n^i = C_1 C_2 \dots C_k,$$

where $k = \gcd(n, i)$ and each C_i is of length $n/\gcd(n, i)$.

To apply Burnside's lemma we need the number of fixed points of ρ_n^i, $i = 1, 2, ..., n$. It is easy to observe that any $x \in \mathbb{Z}_q^n$ is fixed by ρ_n^i for $i = 1, 2, ..., n$ if and only if it is fixed by each of $C_i, 1 \le i \le k$. Further, if a cycle C_i permutes $x_{j_1}, x_{j_2}, ..., x_{j_{n/k}}$, then it fixes $\mathbf{x}$ if and only if $x_{j_1} = x_{j_2} = \cdots = x_{j_{n/k}}$. Clearly,

there are q choices for each $C_i, 1 \leq i \leq k$. Hence there are q^k number of fixed points of ρ_n^i. Now, the Burnside's lemma implies

$$\begin{aligned} s_n &= (1/n)\sum_{i=1}^{n} q^{\gcd(n,i)} = (1/n)\sum_{m|n}\sum_{\gcd(n,i)=m}^{n} q^m \\ &= (1/n)\sum_{m|n} q^m \sum_{j,\gcd(n/m,j)=1} 1 = (1/n)\sum_{m|n}\phi(m)q^{n/m}. \end{aligned}$$ ∎

The enumeration of GSSBF is based on the classification of $\mathbb{Z}_q^n$ under the constraints discussed earlier in definition 3. Since the number of class of $\mathbb{Z}_q^n$ depends on the number of the possible choices of the weight of the vectors in $\mathbb{Z}_q^n$ so in next theorem we are showing the count of GSSBF.

Theorem 3.3. *Total number of GSSBF $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is q^{n+1}.*

Proof. We can do the classification of Z_q^n on the basis of hamming weight of all $x \in Z_q^n$. Let $S_k = \{x \in Z_q^n : wt(x) = k\}$, so we can write

$$Z_q^n = \bigcup_{k=0}^{n} S_k.$$

Therefore, $n+1$ total number of classes are there for Z_q^n. Now by definition of super symmetric function $f : Z_q^n \to Z_q$ maps on maximum possibly $n+1$ distinct values from Z_q for all $x \in Z_q^n$. Hence total number of GSSBF are q^{n+1}. ∎

4. Bent functions

A function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is said to Bent function if function having $\{\pm q^{n/2}\}$ valued Walsh spectrum. This spectrum furnished it an optimal non-linearity among all boolean functions. From cryptographic point of view a Boolean functions having good non-linearity profile are useful in designing linear attack immune cryptosystems. A rich Boolean function required to satisfy another criteria simultaneously viz. high algebraic degree and balancedness. For $q = 2$ it is proved that a bent function never be a balanced function. In the next theorem, we are presenting the proof for any prime q.

Proposition 1. *$f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is balanced if and only if $\sum_{x \in Z_q^n, f(x)=k} 1 = q^{n-1}$ for all $0 \leq k < q$.*

Proof. The proof directly follows the definition of balancedness. ∎

Theorem 4.4. *$f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is balanced if and only if $W_f(\boldsymbol{0}) = 0$ where $\boldsymbol{0} \in \mathbb{Z}_q^n$ and q is any prime number.*

Proof. Let f be a balanced function. The Walsh transform at $\mathbf{0}$ can be calculated by

$$W_f(\mathbf{0}) = \sum_{x \in Z_q^n} \zeta^{f(x)} = \sum_{k=0}^{p-1} \sum_{x \in z_q^n, f(x)=k} \zeta^k = \sum_{k=0}^{q-1} \zeta^k \sum_{x \in z_q^n, f(x)=k} 1$$

Since f is balanced so

$$W_f(\mathbf{0}) = q^{n-1} \sum_{k=0}^{q-1} \zeta^k = 0 \quad \text{as} \quad \sum_{k=0}^{q-1} \zeta^k = 0.$$

Now, conversely, if $W_f(\mathbf{0}) = 0$, then

$$\sum_{k=0}^{q-1} \zeta^k \sum_{x \in z_q^n, f(x)=k} 1 = 0. \tag{7}$$

Let $\sum_{x \in Z_q^n, f(x)=k} 1 = a_k$ for $0 \leq k < q$. Then equation (7) implies

$$\sum_{k=0}^{q-1} a_k = q^n \tag{8}$$

$$\sum_{k=0}^{q-1} a_k \zeta^k = 0. \tag{9}$$

But $x^{q-1} + x^{q-2} + ... + x + 1$ is the minimal polynomial of ζ. Hence we have

$$\frac{a_0}{1} = \frac{a_1}{1} = ... = \frac{a_{q-1}}{1} = a(say).$$

From equation (8) we have,

$$qa = q^n \Rightarrow a = q^{n-1} \Longrightarrow \sum_{x \in Z_q^n, f(x)=k} 1 = q^{n-1} \text{ for all } 0 \leq k < q.$$

Hence f is balanced. ∎

Now, the above theorem is obviously implying the proof of next corollary.

Corollary 1. *Bent functions $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ are not balanced.*

4.1. Generalized symmetric bent functions

The number of generalized symmetric, rotational symmetric and super symmetric boolean functions on $\mathbb{Z}_q^n$ are very less with respect to the total number of Boolean functions on $\mathbb{Z}_q^n$ i.e. q^{q^n}. Search of these all possible functions having bent as well as various symmetric properties can be achievable from some tricky approach. Table 1 shows a comparative results of enumeration of symmetric functions and total number of Boolean functions based on some chosen parameters.

Table 1: Distribution of GSBF, GRSBF and GSSBF

n	q	$\#SBF$	$\#SSBF$	$\#RSBF$	$\#BF$
1	3	27	9	27	27
2	3	729	27	729	19683
3	3	59049	81	177147	7625597484987

Table 2: Truth table of SBF on $\mathbb{Z}_3^2$

x_1	x_2	$f(x_1, x_2)$	$W_f(x)$
0	0	v_0	$\zeta^{v_0} + 2\zeta^{v_1} + 2\zeta^{v_2} + \zeta^{v_4} + 2\zeta^{v_3} + \zeta^{v_5}$
0 1	1 0	v_1	$\zeta^{v_0} - \zeta^{2+v_1} - \zeta^{1+v_2} + \zeta^{1+v_4} - \zeta^{v_3} + \zeta^{2+v_5}$
0 2	2 0	v_2	$\zeta^{v_0} - \zeta^{1+v_1} - \zeta^{2+v_2} + \zeta^{2+v_4} - \zeta^{v_3} + \zeta^{1+v_5}$
1 2	2 1	v_3	$\zeta^{v_0} - \zeta^{v_1} - \zeta^{v_2} + \zeta^{v_4} - \zeta^{v_3} + \zeta^{v_5}$
1	1	v_4	$\zeta^{v_0} + 2\zeta^{1+v_1} + 2\zeta^{2+v_2} + \zeta^{2+v_4} + 2\zeta^{v_3} + \zeta^{1+v_5}$
2	2	v_5	$\zeta^{v_0} + 2\zeta^{2+v_1} + 2\zeta^{1+v_2} + \zeta^{1+v_4} + 2\zeta^{v_3} + \zeta^{2+v_5}$

Table 3: Truth table of SSBF on $\mathbb{Z}_3^2$

x_1	x_2	$f(x_1, x_2)$	$W_f(x)$
0	0	v_0	$\zeta^{v_0} + 4\zeta^{v_1} + 4\zeta^{v_2}$
0 1 0 2	1 0 2 0	v_1	$\zeta^{v_0} + \zeta^{v_1} - 2\zeta^{v_2}$
1 1 2 2	1 2 1 2	v_2	$\zeta^{v_0} - 2\zeta^{v_1} + \zeta^{v_2}$

Since the classification under the constraints of symmetric and rotational symmetric permutation of Z_q^n for $n = 2$ are same, so Table 2 also represents the Walsh spectrum of rotational symmetric Boolean function for $q = 3$. The next theorem provides us major clues about the existence and construction of both functions.

Theorem 4.5. *There are only* 6 *balanced symmetric or rotational symmetric function from* $\mathbb{Z}_3^2$ *to* $\mathbb{Z}_3$

Proof. We can classify all $x \in Z_3^2$ on the basis of its hamming weight$(0 \leq j \leq 2)$ and rotational symmetry in the following manner

$$A_j = \{x \in Z_3^2 : wt(x) = j, x_1 = x_2\}$$
$$B_j = \{x \in Z_3^2 : wt(x) = j, x_1 \neq x_2\}$$

We can see that $|A_0| = 0$, $|A_j| = 1$ and $|B_j| = 2$ for all $0 \leq j \leq 2$. Now by definition to the balancedness of 3−ary boolean functions the possibility of one combination of set of $x \in Z_3^2$ viz. A_j and B_j are

$$\{A_0, B_1\}, \{A_2, B_1\}, \{A_2, B_2\}$$

Similarly we can see that there are only 6 possible combination of these class under the balancedness condition. Hence we can say that there are only 6 balanced symmetric Boolean functions. ∎

Theorem 4.6. *There are only* 8 *symmetric and rotational symmetric bent functions* f *from* $\mathbb{Z}_3^2$ *to* $\mathbb{Z}_3$ *and all of them are not balanced.*

Proof. By the definition of Walsh transformation and table 2. for all $w \in \mathbb{Z}_3^2$, $W_f(w) \in \{\zeta^{v_0} + 2\zeta^{v_1} + 2\zeta^{v_2} + \zeta^{v_4} + 2\zeta^{v_3} + \zeta^{v_5}, \zeta^{v_0} - \zeta^{2+v_1} - \zeta^{1+v_2} + \zeta^{1+v_4} - \zeta^{v_3} + \zeta^{2+v_5}, \zeta^{v_0} + 2\zeta^{1+v_1} + 2\zeta^{2+v_2} + \zeta^{2+v_4} + 2\zeta^{v_3} + \zeta^{1+v_5}, \zeta^{v_0} - \zeta^{v_1} - \zeta^{v_2} + \zeta^{v_4} - \zeta^{v_3} + \zeta^{v_5}, \zeta^{v_0} + 2\zeta^{1+v_1} + 2\zeta^{2+v_2} + \zeta^{2+v_4} + 2\zeta^{v_3} + \zeta^{1+v_5}, \zeta^{v_0} + 2\zeta^{2+v_1} + 2\zeta^{1+v_2} + \zeta^{1+v_4} + 2\zeta^{v_3} + \zeta^{2+v_5}\}$. Now, if f is bent, then $|W_f(w)|^2 = 9$ for all $w \in \mathbb{Z}_3^2$ which obviously imply the unbalanced property of all possible f by theorem 3.1, so we can get six different equations for all $W_f(w)$. Computationally we search the solution of these equations and found only eight set of solutions. In Table 4, we are showing these solutions.

Table 4: Bent GSBF and GRSBF on $\mathbb{Z}_3^2$

	f^1	f^2	f^3	f^4	f^5	f^6	f^7	f^8
v_0	0	0	0	0	1	1	2	2
v_1	0	1	1	2	1	2	0	2
v_2	2	0	1	2	1	0	1	2
v_3	2	1	2	1	2	0	0	1
v_4	0	2	2	1	0	1	0	0
v_5	1	0	2	1	0	0	2	0

In [5], Hou has shown the uniqueness of representation of generalized Boolean function as a multivariate polynomial. Corresponding to each solution in the above table, below we are giving multivariate representations.

Bent Symmetric and Rotational symmetric Boolean functions from $\mathbb{Z}_3^2$ to $\mathbb{Z}_3$

$$
\begin{aligned}
f^1(x_1,x_2) &= 2x_2 + 2x_1 + x_2^2 + x_1^2\\
f^2(x_1,x_2) &= 2x_2 + 2x_1 + 2x_2^2 + 2x_1^2\\
f^3(x_1,x_2) &= x_1^2 + x_2^2\\
f^4(x_1,x_2) &= 2x_2^2 + 2x_1^2\\
f^5(x_1,x_2) &= 1 + 2x_1x_2\\
f^6(x_1,x_2) &= 1 + x_2 + x_1 + x_1x_2\\
f^7(x_1,x_2) &= 2 + x_2 + x_1 + 2x_1x_2\\
f^8(x_1,x_2) &= 2 + x_1x_2
\end{aligned}
$$

Hence the proof is completed. ∎

Theorem 4.7. *There is no any super symmetric bent function for $q = 3$ and $n = 2$.*

Proof. By the definition of SSBF and the bent property of a Boolean function, we know that $|W_f(w)|^2 = 9$. We can write three equations from the Walsh spectrum values given in the table 3.

$$
\begin{aligned}
|\zeta^{v_0} + 4\zeta^{v_1} + 4\zeta^{v_2}| &= 3\\
|\zeta^{v_0} + \zeta^{v_1} - 2\zeta^{v_2}| &= 3\\
|\zeta^{v_0} - 2\zeta^{v_1} + \zeta^{v_2}| &= 3
\end{aligned}
$$

Let $\zeta = \exp^{i\theta}$, where $\theta = 2n\pi/3$. Above relation can be reduced in the real coefficients as follows

$$\cos(v_0 - v_1)\theta + 4\cos(v_1 - v_2)\theta + \cos(v_1 - v_2)\theta = -7 \tag{10}$$

$$2\cos(v_0 - v_1)\theta - 4\cos(v_1 - v_2)\theta - 4\cos(v_2 - v_0)\theta = 3 \tag{11}$$

$$-4\cos(v_0 - v_1)\theta - 4\cos(v_1 - v_2)\theta + 2\cos(v_2 - v_0)\theta = 3 \tag{12}$$

Now, let $\cos(v_0 - v_1)\theta = x$, $y = \cos(v_1 - v_2)\theta$ and $\cos(v_2 - v_0)\theta = z$ then $7, 8$ and 9 can be written as

$$x + 4y + z = -7 \tag{13}$$

$$2x - 4y - 4z = 3 \tag{14}$$

$$-4x - 4y + 2z = 3 \tag{15}$$

Inconsistency of above three equations implies the non existence of super symmetric bent function on $\mathbb{Z}_3^2$. ∎

Based on our analysis we present two conjectures related to the generalized super symmetric bent functions and symmetric bent functions.

Conjecture 1. *For any prime q there is no any generalized super symmetric bent function from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$.*

Conjecture 2. *For any prime q there is no any generalized homogeneous symmetric bent function from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ of degree greater then 2.*

References

[1] Canteaut, A., Videau, M., *Symmetric Boolean functions*, IEEE Transactions on Information Theory, 51 (8) (2005), 2791-2811.

[2] Camion, P., Canteaut, A., *Construction of t-resilient functions over a finite alphabet*, Advances in Cryptology-Eurocrypt 96, Springer, Berlin, 1996, 283-293.

[3] Kravets, V.N., *Generalized symmetries in Boolean functions*, Computer Aided Design, ICCAD-2000. IEEE/ACM International Conference, Nov. 2000, 526-532.

[4] Savicky, P., *On the bent Boolean functions that are symmetric*, Europian J. Combin., 15 (1994), 407-410.

[5] Hou, X.-D., *p-ary and q-ary versions of certain results about bent functions and resilient functions*, Finite Fields and Their Applications, 10 (2004), 566-582.

[6] Stanica, P., Subhamoy Maitra, S., *Rotation symmetric Boolean functions-Count and cryptographic properties*, Discrete Applied Mathematics, 156 (2008), 1567-1580.

[7] Maitra, S., Sarkar, P., *Maximum nonlinearity of symmetric Boolean functions on odd number of variables*, IEEE Trans. Inf. Theory, 48 (9) (2002), 2626-2630.

[8] Gopalakrishnan, K., Hoffman, D., Stinson, D., *A note on a conjecture concerning symmetric resilient functions*, Inform. Process. Lett., 47 (3) (1993), 139-143.

[9] Sarkar, P., Maitra, S., *Balancedness and correlation immunity of symmetric Boolean functions*, Proc. R.C. Bose Centenary Symp., 15(2003), 178-183.

[10] Cunkle, C.H., *Symmetric Boolean Functions*, The American Mathematical Monthly, 70 (8) (1963), 833-836.

[11] Paturi, R., *On the degree of polynomials that approximate symmetric Boolean functions*, STOC '92 Proceedings of the twenty-fourth annual ACM symposium on Theory of computing, 1992, 468-474.

[12] Lidl, R., Pilz, G., *Applied Abstract Algebra*, Second edition, Springer, 1998.

Accepted: 05.04.2016