Count of rotational symmetric bent Boolean functions

Shashi Kant Pandey*and P. R. Mishra[†]

Abstract

Counting the Boolean functions having specific cryptographic features is an interesting problem in combinatorics and cryptography. Count of bent functions for more than eight variables is unexplored. In this paper, we propose an upper bound for the count of rotational symmetric bent Boolean functions and characterize its truth table representation from the necessary condition of a rotational symmetric bent Boolean function.

Keywords: Rotational Symmetric Boolean Function, Algebraic Normal Form, Bent Boolean Function, Cryptography, Hamming Weight, Symmetric Boolean Function
Mathematics Subject Classification: 06E30, 94C10 94A60, 05E05.

1 Introduction

Boolean functions having rich cryptographic characteristics are essentially required in all cryptographic systems. An efficient selection of Boolean functions is the top prior job to either break the linearity or provide the immunity to the system from various other cryptographic attacks. A Boolean function is a function from an n dimensional vector space V_n over base field $\mathbb{F}_2^n$ to $\mathbb{F}_2$. It implies that the cardinality of set of all Boolean function is 2^{2^n}. Among all Boolean functions very less number of Boolean functions show some useful cryptographic behaviours. Symmetric Boolean functions are well known Boolean functions to implement a complex combination of larger number of variables in a cryptosystem. These Boolean functions are characterized on their output which depends only on the hamming weight of the input bit streams. In [1], Wegener described various complexities for symmetric Boolean functions in different model of computational systems. Symmetric Boolean functions show so many required benefits in cryptography, such as, a compact presentation and efficiency. Therefore it is always an exiting domain to explore those symmetric Boolean functions equipped with other required cryptographic properties.In [3], it is proved that there is only two symmetric bent Boolean function on $\mathbb{F}_2^n$ for every even value of n and in [4] count of the rotational symmetric Boolean function is presented. In [2], Canteaut studied

*shashikantshvet@gmail.com
[†]prasanna.r.mishra@gmail.com

the degree of symmetric Boolean function and also addressed the propagation characteristics of symmetric Boolean function. In the same paper the characterization of all balanced symmetric Boolean functions of degree less then 7 is presented. A Boolean function having higher degree and high non-linearity always protect a cryptosystem from linear and differential attacks. However, both of these parameters of a Boolean function cannot be able to increase simultaneously [3, 5]. Bent boolean functions are those Boolean function which have highest non-linearity, but they can exist only for even number of variables and the at most degree of these Boolean functions is $\frac{n}{2}$, where n represent the number of variables. Symmetric Boolean function exists for even as well as odd values of n. There are various conjectures about the possible bounds on the degree of symmetric Boolean functions[6, 7].

Based on the rotational permutation of input bits of a Boolean function, Pieprzy and Qu studied an another symmetric Boolean function namely rotational symmetric Boolean function[8]. These Boolean functions are more desirable in the computation of efficient implementation of various Hash algorithms. Among all possible Boolean functions, it is hard to computationally search all possible symmetric and rotational symmetric Boolean functions. So their counting is a challenging problem in cryptography and combinatorics. As per our literature survey all available proposed constructions of symmetric and rotational symmetric Boolean functions having other essential cryptographic characteristics are based on iteration techniques. Therefore the count of those symmetric Boolean function which satisfy some important cryptographic requirements is a remarkable work. Results on the count of symmetric and rotational symmetric Boolean function on $\mathbb{F}_2^n$ are available in [6]. In the same paper various enumeration of bent symmetric Boolean function is proposed. It can be found in [15, 10, 14], that the trade off among various criteria of a cryptographic Boolean function is difficult to attain. Balance Boolean function is an important cryptographic requirement to protect it from correlation attack. Therefore balanced symmetric and rotational symmetric Boolean functions are favourable choice in cryptography. In [9], Shano Jing *et al.* proposed the enumeration of balanced rotational symmetric Boolean functions and first order correlation immune rotational symmetric Boolean functions for $n = p^r$ number of variables, where p is a prime number and $r > 1$ be any positive integer. In [11], some results on the non-linearity of symmetric and rotational symmetric Boolean functions was introduced. In the same paper they investigated the characteristics of the Walsh spectrum of plateaued rotational symmetric Boolean functions and derived the necessary condition for the existence of balanced plateaued rotational symmetric Boolean functions. In continuation of the enumeration of cryptographic symmetric Boolean functions Lakshmy K.V. *et al.*[4] proved the counting result of balanced rotational symmetric Boolean functions on $\mathbb{F}_2^n$ for $n = pq$, where p and q are two distinct primes. In this paper, we develop some necessary Diophantine equations for rotational symmetric bent Boolean functions. We enumerate bent rotational symmetric Boolean functions on $\mathbb{F}_2^n$. For $n = 2q$, $q > 3$ a prime number, we characterize the truth table of rotational symmetric bent Boolean functions. In the last section, we propose a much reduced upper bound for the number of rotational symmetric bent Boolean function on $\mathbb{F}_2^n$ for $n = 2q$, where $q > 3$ is a prime number. We hope that this method of counting of bent symmetric Boolean function is efficiently applicable in plateaued symmetric and rotational symmetric Boolean functions.

2 Preliminaries

Let $\mathbb{F}_2^n$ denotes the $n-$dim vector space over the field $\mathbb{F}_2$ of order 2. A Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ can always written in terms of $n-$ number of variables. This representation named as Algebraic Normal Form (ANF) of a Boolean function. On the other hand the truth table of a Boolean function is treated as a column matrix of order $2^n \times 1$. Following is the column matrix of truth table of a Boolean f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$,

$$M_{TT} = [f(0,0,...,0)\, f(0,1,0,...,0) \ldots f(1,1,...,1)]^T \tag{1}$$

A more general presentation of a Boolean function in terms of multivariate polynomial is as follows,

$$f(x_1,x_2,...,x_n) = a_0 \oplus \sum_{i=1}^{n} a_i x_i \oplus \sum_{1\leq i\leq j\leq n}^{n} a_{i,j} x_i x_j \oplus ... \oplus a_{1,2,...,n} x_1 x_2 \ldots x_n, \tag{2}$$

where $a_i, a_{i,j}, ..., a_{1,2,3,...,n} \in \mathbb{F}_2$ for all $0 \leq i,j \leq n$. The hamming weight of a Boolean function is defined as the number of non zero entries in the matrix M_{TT} and it is denoted as $wt(f)$. The hamming distance between two equal size column matrix M_t and M_s is defined as $d_H(M_t, M_s) = wt(M_t \oplus M_s)$. A Boolean function is said to be balanced if frequency of 0 and 1 is equal in M_{TT} in other words $wt(f) = 2^{n-1}$. The *Algebraic degree* of f, is defined as the number of variables in the highest order term with non-zero coefficient in (2). Boolean functions of algebraic degree at most one are called *affine* Boolean functions. Here we take $\mathbb{A}_n$ as the set of all affine Boolean functions. Those affine functions in which constant term is zero are called linear functions. The term non-linearity for a Boolean function is defined as the minimum distance from all affine functions. Non-linearity of a Boolean function can be calculated from the Walsh spectrum of Boolean function. Walsh spectrum of a Boolean function is a collection of magnitudes of the Walsh coefficients. Walsh transformation W_f, of a Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is defined as

$$W_f(w) = \sum_{x\in\mathbb{F}_2^n} -1^{f(x)+w.x}, \tag{3}$$

it is a transformation from $\mathbb{F}_2^n$ to $\mathbb{Z}$ and for $w, x \in \mathbb{F}_2^n$, $w.x = w_1x_1 \oplus w_2x_2 \oplus ... \oplus w_nx_n$. Observe that the Walsh transformation can be defined as,

$$W_f(w) = \mathbf{card}\{x : f(x) + w.x = 0\} - \mathbf{card}\{x : f(x) + w.x \neq 0\}. \tag{4}$$

Walsh spectrum characterises almost all the cryptographic measures of a Boolean function. For example, $|W_f(0)| = 0$ in case of balanced Boolean function f and $|W_f(w)| = \pm 2^{n/2}$

for all $w \in \mathbb{F}_2^n$ where f is a bent Boolean function. Bent Boolean function does not exist for odd number of variables. However they are the source of Boolean functions having maximum non-linearity. Therefore those Boolean functions having three valued Walsh spectrum, that is, $\{0, \pm\lambda\}$ are significantly important in cryptographic applications. These Boolean functions are named as plateaued Boolean function[12, 13].

A symmetric Boolean function is invariant under the action of full symmetric group $\mathbb{S}_n$ on $\mathbb{F}_2^n$. Its Walsh transformation is computed as,

$$W_f(w) = \sum_{k=0}^{n} (-1)^{c_k} \sum_{wt(x)=k} (-1)^{w.x},$$

where $\{f(x) = c_k \in \mathbb{F}_2 : wt(x) = k\}$. Now to define rotational symmetric Boolean function we present the definition of cyclic rotation,

Definition 2.1 (Cyclic rotation)**.** Let $x = (x_1, x_2, ..., x_n)$ be any element in $\mathbb{F}_2^n$, where $x_i \in \mathbb{F}_2$; for any $1 \leq i \leq n$. A cyclic rotation for each x_i of x is defined as,

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

where k is any positive integer.

Now for any $x \in \mathbb{F}_2^n$, this cyclic rotation can extend as $\rho_n^k(x) = (\rho_n^k(x_1), \rho_n^k(x_2), ..., \rho_n^k(x_n)) \in \mathbb{F}_2^n$. Outputs of rotational symmetric Boolean function (RSBF) are invariant under the cyclic rotation. In next definition a precise explanation of RSBF is available.

Definition 2.2 (RSBF)**.** A Boolean function $f(x_1, x_2, ..., x_n)$, from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called rotational symmetric Boolean function if $f(\rho_n^k(x_1, x_2, ..., x_n)) = f(x_1, x_2, ..., x_n)$ for each input $(x_1, x_2, ..., x_n) \in \mathbb{F}_2^n$ and any $0 \leq k \leq n-1$.

The cyclic permutation mentioned in the definition (2.1), generates partition in $\mathbb{F}_2^n$. It is proved by Stanica *et al.*[6] that $g_n = \sum_{t|n} \phi(t) 2^{n/t}$ number of partitions of $\mathbb{F}_2^n$ under the action of cyclic permutation. Let $G_n(x_1, x_2, ..., x_n)$ be partitions of $\mathbb{F}_2^n$ by ρ_n^k for some positive integer k. Therefore all the partitions in $\mathbb{F}_2^6$ can be written as,

$$\begin{aligned}
&G_6(0,0,0,0,0,0) = \{(0,0,0,0,0,0)\};\\
&G_6(1,1,1,1,1,1) = \{(1,1,1,1,1,1)\};\\
&G_6(1,0,0,0,0,0) = \{(1,0,0,0,0,0),(0,1,0,0,0,0),...,(0,0,0,0,0,1)\};\\
&G_6(1,1,0,0,0,0) = \{(1,1,0,0,0,0),(0,1,1,0,0,0),...,(1,0,0,0,0,1)\};\\
&G_6(1,0,1,0,0,0) = \{(1,0,1,0,0,0),(0,1,0,1,0,0),...,(0,1,0,0,0,1)\};\\
&G_6(1,0,0,1,0,0) = \{(1,0,0,1,0,0),(0,1,0,0,1,0),(0,0,1,0,0,1)\};\\
&G_6(1,1,1,0,0,0) = \{(1,1,1,0,0,0),(0,1,1,1,0,0),...,(1,1,0,0,0,1)\};\\
&G_6(1,1,1,1,0,0) = \{(1,1,1,1,0,0),(0,1,1,1,1,0),...,(1,1,1,0,0,1)\};\\
&G_6(1,1,1,1,1,0) = \{(1,1,1,1,1,0),(0,1,1,1,1,1),...,(1,1,1,1,0,1)\};\\
&G_6(1,0,1,0,1,0) = \{(1,0,1,0,1,0),(0,1,0,1,0,1)\};\\
&G_6(1,1,1,0,1,0) = \{(1,1,1,0,1,0),(0,1,1,1,0,1),...,(1,1,0,1,0,1)\};\\
&G_6(0,1,1,0,1,1) = \{(0,1,1,0,1,1),(1,0,1,1,0,1),(1,1,0,1,1,0)\};\\
&G_6(1,0,0,1,0,1) = \{(1,0,0,1,0,1),(1,1,0,0,1,0),...,(0,0,1,0,1,1)\};\\
&G_6(1,0,0,1,1,0) = \{(1,0,0,1,1,0),(0,1,0,0,1,1),...,(0,0,1,1,0,1)\}.
\end{aligned}$$

Here we can see that $g_6 = 14$ and all partitions with there corresponding cardinality are as follows,

$$\begin{aligned}
\mathbf{Card}G_6(0,0,0,0,0,0) = \mathbf{Card}G_6(1,1,1,1,1,1) &= 1,\\
\mathbf{Card}G_6(1,0,1,0,1,0) &= 2,\\
\mathbf{Card}G_6(1,0,0,0,0,0) = \mathbf{Card}G_6(1,1,0,0,0,0) = \mathbf{Card}G_6(1,0,1,0,0,0) &= 6,\\
\mathbf{Card}G_6(1,1,1,0,0,0) = \mathbf{Card}G_6(1,1,1,1,0,0) = \mathbf{Card}G_6(1,1,1,1,1,0) &= 6,\\
\mathbf{Card}G_6(1,1,1,0,1,0) = \mathbf{Card}G_6(1,0,0,1,0,1) = \mathbf{Card}G_6(1,0,0,1,1,0) &= 6,\\
\mathbf{Card}G_6(1,0,0,1,0,0) = \mathbf{Card}G_6(0,1,1,0,1,1) &= 3.
\end{aligned}$$

In [6], results on the counting of RSBF are available. However the set of RSBF is very small in size ($\approx 2^{\frac{2^n}{n}}$) as compared to the whole set of Boolean functions of size($\approx 2^{2^n}$). While count of symmetric Boolean functions having other cryptographic characteristics are also small in size. In the next section we present an enumeration technique of total number of rotational symmetric bent Boolean functions. Using this technique we propose an upper bound for the number of rotational symmetric bent Boolean functions. However this technique is also useful in general to find the bound for other cryptographic Boolean functions.

3 Necessary condition for symmetric and rotational symmetric bent Boolean function

In this section, we show the necessary condition on the truth table for bent function and symmetric bent Boolean function.

Theorem 3.1. Let f be a bent Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Then $\mathbf{Card}\{x : f(x) = 0\} = 2^{n-1} \pm 2^{\frac{n}{2}-1}$ and $\mathbf{Card}\{x : f(x) = 1\} = 2^n - 2^{n-1} \pm 2^{\frac{n}{2}-1}$.

Proof. We know that the Walsh transformation of f, denoted as W_f is a function from $\mathbb{F}_2^n$ to $\mathbb{Z}$. Now let $a = \mathbf{Card}\{x : f(x) + w.x = 0\}$ and $b = \mathbf{Card}\{x : f(x) + w.x = 1\}$ for all $w, x \in \mathbb{F}_2^n$ and a Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Therefore combining the necessary condition on bent Boolean function f, that is $|W_f(w)| = 2^{n/2}$ for all $w \in \mathbb{F}_2^n$ and (4),

$$a - b = \pm 2^{n/2}. \tag{5}$$

Now observe that

$$a + b = 2^n. \tag{6}$$

Solving (5) and (6),

$$a = 2^{n-1} \pm 2^{\frac{n}{2}-1} \ \textit{and} \ b = 2^n - 2^{n-1} \pm 2^{\frac{n}{2}-1}$$

Hence the theorem is proved. □

Remark: It is interesting to find those $w \in \mathbb{F}_2^n$ for a Boolean function f, such that $\mathbf{Card}\{w : f(x) \oplus w.x = 0\} = 2^{n-1} \pm 2^{\frac{n}{2}-1}$, for all $x \in \mathbb{F}_2^n$.

In the next theorem we present the necessary condition for a symmetric bent Boolean function on its truth table matrix. Before that we recall some result of enumeration on number of orbits of various lengths under the action of cyclic rotation on $\mathbb{F}_2^n$, discussed in [11]. Number of orbit of length l, which is $\mathbf{Card}G_n$, for some $G_n \subset \mathbb{F}_2^n$ can be calculated as

$$\mathbf{Card}\{G_n : \mathbf{Card}G_n = l\} = d_{n,l} = \frac{1}{l} \sum_{k/l} \mu(\frac{l}{k}) 2^{gcd(n,k)}. \tag{7}$$

We'll use this result in proof of forthcoming theorems.

Theorem 3.2. The necessary condition for a rotational symmetric bent Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is

$$\sum_{i=1, d_i|n}^{k} z_i d_i = a \, or \, b,$$

where a, b are as mentioned in Theorem 3.1 and $z_i \in \mathbb{Z}^+ \cup \{0\}$.

Proof. Let f be a bent Boolean function on $\mathbb{F}_2^n$. Then from Theorem 3.1 we can write

$$\mathbb{F}_2^n = A \cup B,$$

where $A = \{x \in \mathbb{F}_2^n : f(x) = 0\}$ and $B = \mathbb{F}_2^n \ \{x \in \mathbb{F}_2^n : f(x) = 1\}$ having cardinality a and b respectively. From the constrained of RSBF there are g_n number of classes for $\mathbb{F}_2^n$ and for each class G_n^i of $\mathbb{F}_2^n$ for $1 \leq i \leq g_n$, $G_n^i \subset A$ or $G_n^i \subset B$. In particular for some $1 \leq k \leq g_n$,

$$\cup_{1 \leq i \leq k} G_n^i = A \, or \, B$$

or

$$\sum_{1 \leq i \leq k} \mathbf{Card} G_n^i = \mathbf{Card}\{x \in \mathbb{F}_2^n : f(x) = 1\}. \tag{8}$$

Observe that for any particular $x \in \mathbb{F}_2^n$, $\mathbf{Card} G_n(x)$ is a factor of n and let set of all possible divisors of n is $\{1, d_1, d_2, ..., d_k\} = D$. From (7), equation (8) can be rewritten as,

$$\sum_{i=1, d_i | n}^{k} z_i d_i = a \, or \, b, \tag{9}$$

where $z_i, 1 \leq i \leq k$ are any positive integer lying between 0 to $\max_{l \in D}\{d_{n,l}\}$. □

Solution of equation (9) presents more clear picture of distribution in the truth table matrix of a rotation symmetric bent Boolean function. In the next section, we use this condition and present the upper bound of count of rotational symmetric bent Boolean functions.

4 Enumeration of rotational symmetric bent Boolean function

In the next Theorem we present a technique to find a necessary condition for rotational symmetric bent Boolean function.

Theorem 4.1. Necessary conditions for a rotational symmetric bent Boolean function f from $\mathbb{F}_2^{2q}$ to $\mathbb{F}_2$ are

$$\begin{aligned}
q(z_3 + 2z_4) &= 2^{2q-1} \pm 2^{q-1}, \\
1 + q(z_3 + 2z_4) &= 2^{2q-1} \pm 2^{q-1}, \\
2 + q(z_3 + 2z_4) &= 2^{2q-1} \pm 2^{q-1}, \\
3 + q(z_3 + 2z_4) &= 2^{2q-1} \pm 2^{q-1}, \\
4 + q(z_3 + 2z_4) &= 2^{2q-1} \pm 2^{q-1}.
\end{aligned}$$

where $z_3, z_4 \in \mathbb{Z}^+ \cup \{0\}$ and q is an odd prime.

Proof. All possible divisors of $n = 2q$ are $1, 2, q$ and $n = 2q$ itself. Now from theorem 3.2, the necessary equation for $n = 2q$ can be written as

$$z_1 + 2z_2 + qz_3 + 2qz_4 = 2^{2q-1} \pm 2^{q-1}, \tag{10}$$

where all $z_i, 1 \leq i \leq 4$ are some integers lies between 1 and $2q$.

Note that from (7), in (10), range of all $z_i, 1 \leq i \leq 4$ are $0 \leq z_1 \leq d_{n,1}, 0 \leq z_2 \leq d_{n,2}, 0 \leq z_3 \leq d_{n,q}$ and $0 \leq z_4 \leq d_{n,n}$. Further simplifying $d_{n,l}$ for all $l \in \{1, 2, q, 2q\}$, $z_1 + 2z_2 \in \{0, 1, 2, 3, 4\}, z_3 \in \{0, 1, ..., \frac{2^q-2}{q}\} and z_4 \in \{0, 1, 2, ..., \frac{2^n-2^q-2}{2q}\}$. Therefore in case of $n = 2q$, only four possibility of (10),

$$\begin{aligned} q(z_3 + 2z_4) &= 2^{2q-1} \pm 2^{q-1}, \\ 1 + q(z_3 + 2z_4) &= 2^{2q-1} \pm 2^{q-1}, \\ 2 + q(z_3 + 2z_4) &= 2^{2q-1} \pm 2^{q-1}, \\ 3 + q(z_3 + 2z_4) &= 2^{2q-1} \pm 2^{q-1}, \\ 4 + q(z_3 + 2z_4) &= 2^{2q-1} \pm 2^{q-1}. \end{aligned} \tag{11}$$

Hence the theorem is proved. □

From Theorem 3.1, the distribution of zeros in truth table of a rotational symmetric bent Boolean function are of two types, either it has $2^{2q-1} - 2^{q-1}$ number of zero or $2^{2q-1} + 2^{q-1}$ number of zeros. Let f be a rotational symmetric bent Boolean function of type I if f takes zero value $2^{2q-1} - 2^{q-1}$ number of times and it is a rotational symmetric bent Boolean function of type II if f takes zero value $2^{2q-1} + 2^{q-1}$ number of times. Let $\mathfrak{B}_\mathfrak{n}^\mathfrak{o}$ and $\mathfrak{B}_\mathfrak{n}$ be the set of rotational symmetric bent Boolean functions of type I and II respectively. The existence of solutions of (11), ensures the existence of rotational symmetric bent Boolean functions for a particular value of q. Using these equations in following theorems we demonstrate some interesting properties of both of types of rotational symmetric bent Boolean functions.

Theorem 4.2. Let $f : \mathbb{F}_2^{2q} \to \mathbb{F}_2$, $q > 3$ a prime number, be a rotational symmetric bent Boolean functions of type I. Then f satisfies the following

(i) $f(x) \neq 0$ for all partitions of $\mathbb{F}_2^{2q}$ for which $\mathbf{Card}G_n(x) = 2$.

(ii) $f(x) = 0$ for one partition of $\mathbb{F}_2^{2q}$ such that $\mathbf{Card}G_n(x) = 1$.

Proof. Let $f \in \mathfrak{B}_\mathfrak{n}^\mathfrak{o}$. Then the necessary equations from 11 can be rewritten as

$$\begin{aligned} q(z_3 + 2z_4) = &\quad 2^{2q-1} - 2^{q-1}, \\ q(z_3 + 2z_4) = &\ 2^{2q-1} - 2^{q-1} - 1, \\ q(z_3 + 2z_4) = &\ 2^{2q-1} - 2^{q-1} - 2, \\ q(z_3 + 2z_4) = &\ 2^{2q-1} - 2^{q-1} - 3, \\ q(z_3 + 2z_4) = &\ 2^{2q-1} - 2^{q-1} - 4. \end{aligned} \tag{12}$$

Integer solutions of (12), exist if and only if q is a common factor of each of the elements from following set

$$\{2^{2q-1}-2^{q-1}, 2^{2q-1}-2^{q-1}-1, 2^{2q-1}-2^{q-1}-2, 2^{2q-1}-2^{q-1}-3, 2^{2q-1}-2^{q-1}-4\}.$$

Now since $q > 3$ is a prime number therefore $gcd(2, q) = 1$ and

$$2^{q-1} = 1 \mod q. \tag{13}$$

Using (12) and (13) we can write the necessary equation for a bet RSBF f,

$$q(z_3 + 2z_4) = 2^{2q-1} - 2^{q-1} - 1. \tag{14}$$

Equation (10) and (14) implies that,

$$z_1 + 2z_2 = 1 \tag{15}$$

it is clear from (9) that $0 \leq z_1 \leq 2$ and $0 \leq z_2 \leq 1$. Hence the only solution of (15) is $z_1 = 1$ and $z_2 = 0$. Therefore z_2 does not participate in necessary equation (10) for type I rotational symmetric bent Boolean functions. This implies that

$$f(x) \neq 0 \,\text{for all x such that }\, \mathbf{Card}G_n(x) = 2$$

hence (i) is proved.
Now $z_1 = 1$ implies that $f(x) = 0$, at most one for one $x \in \mathbb{F}_2^{2q}$ such that $\mathbf{Card}G_n(x) = 1$. It is clear that

$$\{x \in \mathbb{F}_2^{2q} : \mathbf{Card}G_n(x) = 1\} = \{(0, 0, ..., 0), (1, 1, ..., 1)\}.$$

Therefore $f(x) \neq 0$ on both of $x \in \{(0, 0, ..., 0), (1, 1, ..., 1)\}$. Hence (ii) is proved. □

Theorem 4.3. Let $f : \mathbb{F}_2^{2q} \to \mathbb{F}_2$, $q > 3$ a prime number, be a rotational symmetric bent Boolean function of type II. Then f satisfies the following

(i) $f(x) = 0$ for only one partition of $\mathbb{F}_2^{2q}$ such that $\mathbf{Card}G_n(x) = 1$.

(ii) $f(x) = 0$ for only one partition of $\mathbb{F}_2^{2q}$ such that $\mathbf{Card}G_n(x) = 2$.

Proof. Let $f \in \mathfrak{B}_\mathfrak{n}$. Then the necessary equations (11) for f, can be rewritten as

$$\begin{array}{rl} q(z_3 + 2z_4) = & 2^{2q-1} + 2^{q-1}, \\ q(z_3 + 2z_4) = & 2^{2q-1} + 2^{q-1} - 1, \\ q(z_3 + 2z_4) = & 2^{2q-1} + 2^{q-1} - 2, \\ q(z_3 + 2z_4) = & 2^{2q-1} + 2^{q-1} - 3, \\ q(z_3 + 2z_4) = & 2^{2q-1} + 2^{q-1} - 4. \end{array} \tag{16}$$

Now for the existence of rotational symmetric bent Boolean function, solution of the equation (16) should exist in terms of (z_0, z_1, z_2, z_3). We know that $gcd(2, q) = 1$ and $2^{q-1} = 1$ mod q, therefore solution exist only if

$$q(z_3 + 2z_4) = 2^{2q-1} + 2^{q-1} - 3. \tag{17}$$

This implies that $z_1 + 2z_2 = 3$ and $q(z_3 + 2z_4) = 2^{2q-1} + 2^{q-1}$. It is earlier discussed in Theorem 4.1 that $z_1 \in \{0, 1, 2\}$ and $z_2 \in \{0, 1\}$, therefore set of solutions of (17) is $\{(1, 1, z_3, z_4) : q(z_2 + 2z_2) = 2^{2q-1} + 2^{q-1}\}$. Hence $z_1 = 1$ implies (i) and $z_2 = 1$ implies (ii). □

Solution of necessary equation (12) represents all possible distributions of zeros and ones in the truth table of a rotational symmetric bent Boolean function. Therefore in the counting of all rotational symmetric bent Boolean function this equation plays an important role. In next section, we show the upper bound for the number of rotational symmetric bent Boolean functions.

4.1 Bound on number of rotational symmetric bent Boolean function

Count of bent Boolean function is still an open problem in cryptography. Up to eight variable, total number of bent Boolean functions are enumerated moreover the gap is very large between upper and lower bound of the enumeration result of bent boolean function of n number of variables($2^{2^{\frac{n}{2}+\log_2^{n-2}-1}} \leq \textbf{card}\{\text{Bent Boolean functions}\} \leq 2^{2^{n-1}+\frac{\binom{n}{n/2}}{2}}$). Here we refine this upper bound in the case of rotational symmetric bent Boolean functions. In case of a Boolean function $f \in \mathfrak{B}_6$, we found only three solutions for their necessary equations discussed in Theorem 4.3 for $n = 6$. Solutions are as follows,

$$(z_1, z_2, z_3, z_4) \in \{(0, 0, 0, 6), (0, 0, 2, 5), (1, 1, 1, 5)\}.$$

Above values of (z_1, z_2, z_3, z_4) provide us a shorter upper bound of number of rotational symmetric bent Boolean function on $\mathbb{F}_2^6$ and this is, $2(\binom{9}{6} + \binom{9}{5}\binom{2}{2} + \binom{9}{5}\binom{2}{1}\binom{2}{1}\binom{1}{1}) = 1428$. It is very less with respect to total number of bent Boolean functions for 6 number of variables, that is , 2^{42}. It is interesting to see that in this way total number of rotational symmetric bent Boolean function of type I are just half of the number of type II functions, that is 714. In the next theorem we present more general result on this bound for $n = 2q$, where $q > 3$ is prime number.

Theorem 4.4. Let $n = 2q$ and $q > 3$ be any prime number. Then

$$\textbf{Card}\mathfrak{B}_{\mathfrak{n}}^{\circ} \leq \sum_{i=1, r=2i-1}^{m} \binom{d_{n,1}}{1}\binom{d_{n,q}}{r}\binom{d_{n,n}}{k}$$

and

$$\mathbf{Card}\mathfrak{B}_{\mathfrak{n}} \leq \sum_{i=1, r=2i-1}^{m} \binom{d_{n,1}}{1} \binom{d_{n,q}}{r} \binom{d_{n,n}}{k},$$

where $m = \frac{2^q-2}{2q}$ and $k = \frac{2^{q-1}(2^q-1)-1-rq}{2}$.

Proof. Let $f : \mathbb{F}_2^{2q} \to \mathbb{F}_2$ be a Boolean function taken from $\mathfrak{B}_n^0$. Then (14) implies that

$$z_3 + 2z_4 = \frac{2^{2q-1} - 2^{q-1} - 1}{q}. \tag{18}$$

Similarly if $f \in \mathfrak{B}_n$ then (17) implies that

$$z_3 + 2z_4 = \frac{2^{2q-1} + 2^{q-1} - 3}{q}. \tag{19}$$

It is clear from (18) and (19) that z_3 must be an odd integer and (9) implies that values of z_3 must be in arithmetic progression with first term 1 and last term $\frac{2^q-2-q}{q}$. There are $m = \frac{2^q-2}{2q}$ number of integer values of z_3 and using them we calculate equal number of integral values of z_4. Following are the solutions of (18)

$$(z_3, z_4) = \begin{cases} (1, \frac{2^{q-1}(2^q-1)-1-q}{2q}), \\ (3, \frac{2^{q-1}(2^q-1)-1-3q}{2q}), \\ (...), \\ (\frac{2^q-2-q}{q}, \frac{2^{q-1}(2^q-1)+1+q}{2q}). \end{cases} \tag{20}$$

Similarly solutions of (19) are as follows

$$(z_3', z_4') = \begin{cases} (1, \frac{2^{q-1}(2^q+11)-3-q}{2q}), \\ (3, \frac{2^{q-1}(2^q+1)-3-3q}{2q}), \\ (...), \\ (\frac{2^q-2-q}{q}, \frac{2^{q-1}(2^q+1)-3-q(\frac{2^q-2-q}{q})}{2q}). \end{cases} \tag{21}$$

Now from (7) and Theorem 3.2, count of all possible matrix of type M_{TT} such that $f \in \mathfrak{B}_n^0$ is

$$\sum_{p(z_3+2z_4)=2^{2q-1}-2^{q-1}-1} \binom{d_{n,1}}{1} \binom{d_{n,q}}{z_3} \binom{d_{n,n}}{z_4}.$$

Using (20) this can be written as

$$\mathbf{Card}\mathfrak{B}_{\mathfrak{n}}^{\mathfrak{o}} \leq \sum_{i=1, r=2i-1}^{m} \binom{d_{n,1}}{1} \binom{d_{n,q}}{r} \binom{d_{n,n}}{k}.$$

Now in (20) and (21) , $d_{n,n}$ and $d_{n,q}$ satisfy

$$\binom{d_{n,q}}{z_3}\binom{d_{n,n}}{z_4} = \binom{d_{n,q}}{z'_3}\binom{d_{n,n}}{z'_4} \tag{22}$$

where z_3, z_4, z'_3 and z'_4 taken from the following order, that is, $1 \leq z_3 \leq \frac{2^q-2-q}{q}$, $\frac{2^{q-1}(2^q-1)-1-q}{2q} \leq z_4 \leq \frac{2^{q-1}(2^q-1)+1+q}{2q}, \frac{2^q-2-q}{q} \geq z'_3 \geq 1$ and $\frac{2^{q-1}(2^q+1)-3-q(\frac{2^q-2-q}{q})}{2q} \geq z'_4 \geq \frac{2^{q-1}(2^q+11)-3-q}{2q}$. Therefore using (21) and (22) we can write

$$\mathbf{Card}\mathfrak{B}_{\mathfrak{n}} \leq \sum_{i=1,r=2i-1}^{m} \binom{d_{n,1}}{1}\binom{d_{n,q}}{r}\binom{d_{n,n}}{k}$$

where $m = \frac{2^q-2}{2q}$ and $k = \frac{2^{q-1}(2^q-1)-3-rq}{2}$. Hence the theorem is proved. □

References

[1] Wegener, Ingo. The complexity of symmetric Boolean functions. Computation theory and logic, 433–442, Lecture Notes in Comput. Sci., 270, Springer, Berlin, 1987.

[2] Canteaut, Anne; Videau, Marion. Symmetric Boolean functions. IEEE Trans. Inform. Theory 51 (2005), no. 8, 2791–2811.

[3] Savick, Petr. On the bent Boolean functions that are symmetric. European J. Combin. 15 (1994), no. 4, 407–410.

[4] Lakshmy, K. V.; Sethumadhavan, M.; Cusick, Thomas W. Counting rotation symmetric functions using Polya's theorem. Discrete Appl. Math. 169 (2014), 162–167.

[5] Maitra, Subhamoy; Sarkar, Palash. Maximum nonlinearity of symmetric Boolean functions on odd number of variables. IEEE Trans. Inform. Theory 48 (2002), no. 9, 2626–2630.

[6] Stanica, Pantelimon; Maitra, Subhamoy. Rotation symmetric Boolean functionscount and cryptographic properties. Discrete Appl. Math. 156 (2008), no. 10, 1567–1580.

[7] Xia, Tianbing; Seberry, Jennifer; Pieprzyk, Josef; Charnes, Chris. Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$. Discrete Appl. Math. 142 (2004), no. 1-3, 127–132.

[8] Pieprzyk, Josef; Qu, Cheng Xin. Fast hashing and rotation-symmetric functions. J.UCS 5 (1999), no. 1, 20–31.

[9] Fu, ShaoJing; Li, Chao; Qu, LongJiang. On the number of rotation symmetric Boolean functions. Sci. China Inf. Sci. 53 (2010), no. 3, 537–545.

[10] Maitra, Subhamoy; Pasalic, Enes. Further constructions of resilient Boolean functions with very high nonlinearity. IEEE Trans. Inform. Theory 48 (2002), no. 7, 1825–1834.

[11] Maximov, A; Hell, M; Maitra S, Plateaued rotational symmetric Boolean function on odd number of variable, First workshop on Boolean function, cryptography and application, BFCA05, Rouen, France, 2005, 83-104.

[12] Carlet, C;Prouff. E; On plateaued functions and their constructions. In Fast Software Encryption 2003, number 2887 in Lecture Notes in Computer Science, pages 5473. Springer Verlag, 2003.

[13] Zheng, Y; and Zhang, X.M; Plateaued Functions. In ICICS99, pages 284-300, volume 1726 in Lecture notes in Computer Science, Springer Verlag.

[14] Clark J; Jacob J; Matra S; Almost Boolean function, The design of Boolean function in spectral inversion, 2003, CEC 2003, Vol3, Newport Beach, california, USA 2003.

[15] Clark J; Jacob J; Stepney S; Evolving Boolean functions stidfying multiple criteria. INDOCRYPT 2002, LNCS, vol 2551, Berlin, SPringer, 2002, 246-259