Results on Rotation Symmetric Bent Functions

Deepak Kumar Dalai and Subhamoy Maitra
Applied Statistics Unit, Indian Statistical Institute,
203 B. T. Road, Calcutta, Pin 700 108, INDIA
E-mail: {deepak_r, subho}@isical.ac.in

Abstract

In this paper we analyze the combinatorial properties related to the Walsh spectra of rotation symmetric Boolean functions on even number of variables. These results are then applied in studying rotation symmetric bent functions.

Keywords: Boolean Functions, Balancedness, Combinatorial Cryptography, Correlation Immunity, Nonlinearity, Rotational Symmetry, Walsh Transform.

1 Introduction

Recently the class of rotation symmetric Boolean functions (RSBFs) has received a lot of attention in terms of their cryptographic properties [1, 2, 4, 5, 6, 7, 8, 11, 12, 3]. Initial study on these functions has been made in [4], where nonlinearity was the main focus. Later nonlinearity and correlation immunity of such functions have been studied in detail in [1, 5, 6, 7, 11, 12]. Applications of such functions in hashing has also been demonstrated [8]. The set of RSBFs are interesting to look into as the space is much smaller ($\approx 2^{\frac{2^n}{n}}$) than the total space of Boolean functions (2^{2^n}) and the set contains functions with very good cryptographic properties. It has been experimentally demonstrated that there are functions in this class which are good in terms of balancedness, nonlinearity, correlation immunity, algebraic degree and algebraic immunity (resistance against algebraic attack) [3] at the same time.

The combinatorial analysis of such functions is also very interesting as they possess certain nice structures. It has been demonstrated in [12] that analysis of Walsh spectra of such functions gives rise to certain matrix with interesting combinatorial properties that helps in fast calculations of different properties of the functions. Later this matrix has been studied in detail in [6, 7] for odd number of variables and new structures have been discovered. However, the problem remained open for even variable case. In this paper we identified important structural patterns in the matrix that helps in analyzing the Walsh spectra of RSBFs in a more efficient way.

It is well known that bent functions only exist on even number of variables [9]. The rotation symmetric bent functions have been studied in detail in [1, 4, 12, 11]. We apply the matrix structure discovered here in studying the rotation symmetric bent functions. Further, this structure provides efficient methods in sieving rotation symmetric bent functions.

1.1 Preliminaries

To save space we refer to [12] for basic definitions related to Boolean functions. Let $x_i \in \{0,1\}$ for $1 \leq i \leq n$. For $1 \leq k \leq n$, we define the permutation $\rho_n^k(x_i)$ as $\rho_n^k(x_i) = x_{i+k}$, if $i+k \leq n$ and $\rho_n^k(x_i) = x_{i+k-n}$, if $i+k > n$. Let $(x_1, x_2, \ldots, x_{n-1}, x_n) \in V_n$. Then we extend the definition as $\rho_n^k(x_1, x_2, \ldots, x_{n-1}, x_n) = (\rho_n^k(x_1), \rho_n^k(x_2), \ldots, \rho_n^k(x_{n-1}), \rho_n^k(x_n))$. Hence, ρ_n^k acts as k-cyclic rotation on an n-bit vector.

Definition 1 *A Boolean function f is called* rotation symmetric *if for each input*

$$(x_1, \ldots, x_n) \in \{0,1\}^n,\ f(\rho_n^k(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n) \text{ for } 1 \leq k \leq n.$$

That is, the rotation symmetric Boolean functions are invariant under cyclic rotation of inputs. The inputs of a rotation symmetric Boolean function can be divided into partitions so that each partition consists of all cyclic shifts of one input. A partition is generated by $G_n(x_1, x_2, \ldots, x_n) = \{\rho_n^k(x_1, x_2, \ldots, x_n) | 1 \leq k \leq n\}$ and the number of such partitions is denoted by g_n. Thus the number of n-variable RSBFs is 2^{g_n}. Let $\phi(k)$ be Euler's *phi*-function, then it can be shown by Burnside's lemma that (see also [11]) $g_n = \frac{1}{n}\sum_{k|n} \phi(k)\, 2^{\frac{n}{k}}$.

By $g_{n,w}$ we denote the number of partitions with weight w. For the formula of how to calculate $g_{n,w}$ for arbitrary n and w, we refer to [11, 6, 7].

A *partition*, or *group*, is completely determined by its *representative element* $\Lambda_{n,i}$, which is the lexicographically first element belonging to the group [12]. These representative elements are again arranged lexicographically. *The rotation symmetric truth table* (RSTT) is defined as the g_n-bit string $[f(\Lambda_{n,0}), f(\Lambda_{n,1}), \ldots, f(\Lambda_{n,g_{n-1}})]$. For our purpose (the reason will be clearer later) we will arrange the representative elements in a permuted way to represent the RSTT and will refer that to as RSTT$^\pi$.

In [12] it was shown that the Walsh transform takes the same value for all elements belonging to the same group, i.e., $W_f(u) = W_f(v)$ if $u \in G_n(v)$. In analyzing the Walsh spectra of RSBFs, the ${}_n\mathcal{A}$ matrix has been introduced [12]. The matrix ${}_n\mathcal{A}$ is defined as ${}_n\mathcal{A}_{i,j} = \sum_{x \in G_n(\Lambda_{n,i})} (-1)^{x \cdot \Lambda_{n,j}}$, for an n-variable RSBF. Using this $g_n \times g_n$ matrix, the Walsh spectra for an RSBF can be calculated from the RSTT as $W_f(\Lambda_{n,j}) = \sum_{i=0}^{g_n-1} (-1)^{f(\Lambda_{n,i})}\, {}_n\mathcal{A}_{i,j}$.

The structure of ${}_n\mathcal{A}$ has been studied in detail for odd n in [6]. Define $\hat{\Lambda}_{n,i}$ as representative element of $G_n(x_1, x_2, \ldots, x_n)$ that contains complement of $\Lambda_{n,i}$. For odd n, there is a one-to-one correspondence between the classes of even weight $\Lambda_{n,i}$'s and the classes of odd weight $\Lambda_{n,i}$'s by $\Lambda_{n,i} \rightarrow \hat{\Lambda}_{n,i}$. Hence, the set of groups can be divided into two parts (of same cardinality) containing representative elements of even weight and odd weight, respectively. The authors of [6] permuted the rows of the matrix ${}_n\mathcal{A}$ using a permutation π such that the first $\frac{g_n}{2}$ rows correspond to the representative elements, $\Lambda_{n,i}$, of even weights (arranged in lexicographical order of representative elements and recognized as $\Lambda_{n,i}$ for $i = 0$ to $\frac{g_n}{2} - 1$) and the next $\frac{g_n}{2}$ rows correspond to the complements of them (these are of odd weights) and recognized as $\Lambda_{n,i} = \hat{\Lambda}_{n,i-\frac{g_n}{2}}$ for $i = \frac{g_n}{2}$ to $g_n - 1$. In the permutation, the corresponding rows and columns of ${}_n\mathcal{A}$ are swapped. The resulting matrix is denoted by ${}_n\mathcal{A}^\pi$, which has the form ${}_n\mathcal{A}^\pi = \left(\begin{array}{c|c} {}_n\mathcal{H} & {}_n\mathcal{H} \\ \hline {}_n\mathcal{H} & -{}_n\mathcal{H} \end{array}\right)$. Using this matrix ${}_n\mathcal{A}^\pi$, the authors of [6] showed that Walsh spectra calculation could be reduced by almost half of the amount compared to [12]. Let $\sigma_1 = ((-1)^{f(\Lambda_{n,0})}, \ldots, (-1)^{f(\Lambda_{n,\frac{g_n}{2}-1})})$ and $\sigma_2 = ((-1)^{f(\Lambda_{n,\frac{g_n}{2}})}, \ldots, (-1)^{f(\Lambda_{n,g_n-1})})$ be vectors of dimension $\frac{g_n}{2}$. Remember that these $\Lambda_{n,i}$'s are numbered after the permutation π takes

place, i.e., $\sigma_1 \parallel \sigma_2$ is basically $(-1)^{\mathrm{RSTT}^{\pi}}$. Let us now consider the values $w_1 = \sigma_1\ {}_n\mathcal{H}, w_2 = \sigma_2\ {}_n\mathcal{H}$. Then the Walsh spectra of f have $(w_1 + w_2)$ for the first $\frac{g_n}{2}$ many representative elements (which are of even weights) and $(w_1 - w_2)$ for the next $\frac{g_n}{2}$ many representative elements (which are of odd weights). Using this strategy [6], one needs $2 \cdot \left(\frac{g_n}{2}\right)^2 + g_n = \frac{g_n^2}{2} + g_n$ operations, whereas g_n^2 operations are needed using matrix ${}_n\mathcal{A}$ as in [12].

2 Walsh spectra of RSBFs on even number of variables

In this section we derive combinatorial results related to the Walsh spectra of RSBFs on even number of variables and then use the results in the analysis of rotation symmetric bent functions. For the analysis we need to concentrate on the classes where the complement (coordinate wise complement) of each vector of that class falls in the same class. Such situation does not happen when n is odd [6], and that is the reason the situation is more complicated when n is even. When n is odd, if the weight of a vector is even (respectively odd) then the weight of its complement is odd (respectively even). However, for n even, there are some classes (vectors from this class have weight $\frac{n}{2}$) where the complement of each vector falls in that same class. For example, for $n = 4$, $G_4((0,0,1,1))$ and $G_4((0,1,0,1))$ are such type of classes.

From now on we assume that n is even. Note that if the vectors of $G_n(\Lambda_{n,i})$ have even (respectively odd) weight, then the vectors of $G_n(\hat{\Lambda}_{n,i})$ have weight even (respectively odd), since n is even. Also, there are some classes of weight $\frac{n}{2}$ such that $G_n(\Lambda_{n,i}) = G_n(\hat{\Lambda}_{n,i})$. Now we partition the class representatives into 5 ordered sets M_n, U_n, $\hat{U_n}$, V_n and $\hat{V_n}$ as follows:

$M_n = \{\Lambda_{n,i} | wt(\Lambda_{n,i}) = \frac{n}{2}\ \&\ G_n(\Lambda_{n,i}) = G_n(\hat{\Lambda}_{n,i})\}$,

Divide the set $\{\Lambda_{n,i} | wt(\Lambda_{n,i}) = \frac{n}{2}\ \&\ G_n(\Lambda_{n,i}) \neq G_n(\hat{\Lambda}_{n,i})\}$ into two disjoint sets M_n^1 and M_n^2 such that $\Lambda_{n,i} \in M_n^1\ iff\ \hat{\Lambda}_{n,i} \in M_n^2$.

$U_n = \{\Lambda_{n,i} | wt(\Lambda_{n,i}) \leq \frac{n}{2}\ \&\ wt(\Lambda_{n,i})\ is\ even\} \setminus (M_n \cup M_n^2)$, $\hat{U}_n = \{\hat{\Lambda}_{n,i} | \Lambda_{n,i} \in U_n\}$,

$V_n = \{\Lambda_{n,i} | wt(\Lambda_{n,i}) \leq \frac{n}{2}\ \&\ wt(\Lambda_{n,i})\ is\ odd\} \setminus (M_n \cup M_n^2)$, $\hat{V}_n = \{\hat{\Lambda}_{n,i} | \Lambda_{n,i} \in V_n\}$.

Consider that the elements in U_n, V_n and M_n are ordered in lexicographical manner and the elements in $\hat{U}_n$ and $\hat{V}_n$ (they are basically the representatives of the groups that contain elements which are complements of U_n, V_n) are ordered according to the ordering of U_n and V_n (that is $\hat{\Lambda}_{n,i}$ of $\hat{U}_n$ or $\hat{V}_n$ comes corresponding to $\Lambda_{n,i}$ of U_n or V_n in the ordering). We permute the rows and columns of ${}_n\mathcal{A}$ using a permutation π such that the elements in any row and column will be in the order: $U_n, V_n, M_n, \hat{V}_n, \hat{U}_n$. In the permutation we swap rows and the corresponding columns of ${}_n\mathcal{A}$. We denote the resulting matrix by ${}_n\mathcal{A}^{\pi}$, which will give a useful submatrix structure presented in Theorem 1. For this we first need the following technical result.

Proposition 1 *Let $x = (x_1, x_2, \cdots, x_n), y = (y_1, y_2, \cdots, y_n) \in \{0,1\}^n$, where n is even. Then, the following hold:*

1. If $wt(x)$ and $wt(y)$ are both even,

$\bigoplus_{i=1}^n (x_i \wedge y_i) = \bigoplus_{i=1}^n (\overline{x}_i \wedge y_i) = \bigoplus_{i=1}^n (x_i \wedge \overline{y}_i) = \bigoplus_{i=1}^n (\overline{x_i} \wedge \overline{y_i})$.

2. If $wt(x)$ is even and $wt(y)$ is odd,

$\bigoplus_{i=1}^n (x_i \wedge y_i) = 1 \oplus \bigoplus_{i=1}^n (\overline{x_i} \wedge y_i) = \bigoplus_{i=1}^n (x_i \wedge \overline{y_i}) = 1 \oplus \bigoplus_{i=1}^n (\overline{x_i} \wedge \overline{y_i})$.

3. If $wt(x)$ and $wt(y)$ are both odd,

$\bigoplus_{i=1}^n (x_i \wedge y_i) = 1 \oplus \bigoplus_{i=1}^n (\overline{x_i} \wedge y_i) = 1 \oplus \bigoplus_{i=1}^n (x_i \wedge \overline{y_i}) = \bigoplus_{i=1}^n (\overline{x_i} \wedge \overline{y_i})$

Proof : The proof of above claims follows directly from the following observations: (i) $\bigoplus_{i=1}^{n}((a_i \wedge b_i) \bigoplus (\overline{a_i} \wedge b_i)) = \bigoplus_{i=1}^{n} b_i$, (ii) $\bigoplus_{i=1}^{n}((a_i \wedge b_i) \bigoplus (a_i \wedge \overline{b_i})) = \bigoplus_{i=1}^{n} a_i$, (iii) $\bigoplus_{i=1}^{n}((a_i \wedge \overline{b_i}) \bigoplus (\overline{a_i} \wedge \overline{b_i})) = \bigoplus_{i=1}^{n} \overline{b}_i$. ■

Theorem 1 *When n is even, the matrix ${}_n\mathcal{A}^{\pi}$ is of the form*

$$
{}_n\mathcal{A}^{\pi} = \begin{array}{c} \\ U_n \\ V_n \\ M_n \\ \hat{V}_n \\ \hat{U}_n \end{array}
\begin{array}{c}
\begin{array}{cccccc} U_n & V_n & & M_n & \hat{V}_n & \hat{U}_n \end{array} \\
\left(\begin{array}{c|c|c|c|c}
{}_nG^1 & {}_nG^2 & {}_nG^3 & {}_nG^2 & {}_nG^1 \\ \hline
{}_nG^4 & {}_nG^5 & {}_nG^6 = 0 & -{}_nG^5 & -{}_nG^4 \\ \hline
{}_nG^7 & {}_nG^8 = 0 & {}_nG^9 & (-1)^{n/2}\ {}_nG^8 = 0 & (-1)^{n/2}\ {}_nG^7 \\ \hline
{}_nG^4 & -{}_nG^5 & (-1)^{n/2}\ {}_nG^6 = 0 & {}_nG^5 & -{}_nG^4 \\ \hline
{}_nG^1 & -{}_nG^2 & (-1)^{n/2}\ {}_nG^3 & -{}_nG^2 & {}_nG^1
\end{array}\right)
\end{array}
$$

where ${}_nG^1$, ${}_nG^2$, ${}_nG^3$, ${}_nG^4$, ${}_nG^5$, ${}_nG^6$, ${}_nG^7$, ${}_nG^8$ and ${}_nG^9$ are matrices of size $|U_n| \times |U_n|$, $|U_n| \times |V_n|$, $|U_n| \times |M_n|$, $|V_n| \times |U_n|$, $|V_n| \times |V_n|$, $|V_n| \times |M_n|$, $|M_n| \times |U_n|$, $|M_n| \times |V_n|$ and $|M_n| \times |M_n|$. Further ${}_nG^9$ is a zero matrix if $n \equiv 2 \pmod 4$ is odd.

Proof : Consider the element ${}_n\mathcal{A}^{\pi}_{r,c}$ in matrix ${}_n\mathcal{A}^{\pi}$ as the element corresponding to the row representer element $\Lambda_{n,r}$ and column representer element $\Lambda_{n,c}$. Similarly, the element ${}_n\mathcal{A}^{\pi}_{\overline{r},c}$ in matrix ${}_n\mathcal{A}^{\pi}$ is the element corresponding to the row representer element $\hat{\Lambda}_{n,r}$ and column representer element $\Lambda_{n,c}$. Similarly, we define ${}_n\mathcal{A}^{\pi}_{r,\overline{c}}$ and ${}_n\mathcal{A}^{\pi}_{\overline{r},\overline{c}}$. Now,

$${}_n\mathcal{A}^{\pi}_{r,c} = \sum_{x \in G_n(\Lambda_{n,r})}(-1)^{x.\Lambda_{n,c}} = \sum_{x \in G_n(\Lambda_{n,r})}(-1)^{\oplus_{i=1}^{n}(x_i \wedge \Lambda_{(n,c)_i})},$$
$${}_n\mathcal{A}^{\pi}_{r,\overline{c}} = \sum_{x \in G_n(\Lambda_{n,r})}(-1)^{x.\Lambda_{n,\overline{c}}} = \sum_{x \in G_n(\Lambda_{n,r})}(-1)^{\oplus_{i=1}^{n}(x_i \wedge \hat{\Lambda}_{(n,c)_i})},$$
$${}_n\mathcal{A}^{\pi}_{\overline{r},c} = \sum_{x \in G_n(\Lambda_{n,\overline{r}})}(-1)^{x.\Lambda_{n,c}} = \sum_{x \in G_n(\Lambda_{n,r})}(-1)^{\oplus_{i=1}^{n}(\overline{x}_i \wedge \Lambda_{(n,c)_i})},$$
$${}_n\mathcal{A}^{\pi}_{\overline{r},\overline{c}} = \sum_{x \in G_n(\Lambda_{n,\overline{r}})}(-1)^{x.\Lambda_{n,\overline{c}}} = \sum_{x \in G_n(\Lambda_{n,r})}(-1)^{\oplus_{i=1}^{n}(\overline{x}_i \wedge \hat{\Lambda}_{(n,c)_i})}.$$

Since $wt(\Lambda_{n,i})$ and $wt(\hat{\Lambda}_{n,i})$ are even for $\Lambda_{n,i} \in U_n$, it follows from Proposition 1 that ${}_n\mathcal{A}^{\pi}_{r,c} = {}_n\mathcal{A}^{\pi}_{r,\overline{c}} = {}_n\mathcal{A}^{\pi}_{\overline{r},c} = {}_n\mathcal{A}^{\pi}_{\overline{r},\overline{c}}$ for $\Lambda_{n,r}, \Lambda_{n,c} \in U_n$. Similarly from Proposition 1 we get, for $\Lambda_{n,r} \in U_n$ and $\Lambda_{n,c} \in V_n$, ${}_n\mathcal{A}^{\pi}_{r,c} = {}_n\mathcal{A}^{\pi}_{r,\overline{c}} = -\ {}_n\mathcal{A}^{\pi}_{\overline{r},c} = -\ {}_n\mathcal{A}^{\pi}_{\overline{r},\overline{c}}$. Further, considering other possibilities we will get the matrix ${}_n\mathcal{A}^{\pi}$ in required structure.

Note that, $\Lambda_{n,i} \in M_n$ implies $\Lambda_{n,i} = \hat{\Lambda}_{n,i}$. Now for any odd weight $v \in \{0,1\}^n$ and any $w \in M_n$,

(1) ${}_n\mathcal{A}^{\pi}_{v,w} = \sum_{x \in G_n(v)}(-1)^{x.w} = \sum_{x \in G_n(v)}(-1)^{x.\overline{w}} = -{}_n\mathcal{A}^{\pi}_{v,w} \Rightarrow {}_n\mathcal{A}^{\pi}_{v,w} = 0.$

(2) ${}_n\mathcal{A}^{\pi}_{w,v} = \sum_{x \in G_n(w)}(-1)^{x.v} = \sum_{x \in G_n(w)}(-1)^{\overline{x}.v} = -{}_n\mathcal{A}^{\pi}_{w,v} \Rightarrow {}_n\mathcal{A}^{\pi}_{w,v} = 0.$

Further, using these two results we get ${}_nG^6 = {}_nG^8 = 0$ and ${}_nG^9 = 0$ if $n \equiv 2 \pmod 4$. ■

We will present an example for 6-variables. Note that the matrix structure presented here extracts the regularity from the basic structure presented in [12, Section 3].

Example 1 $U_6 = \{(0,0,0,0,0,0), (0,0,0,0,1,1), (0,0,0,1,0,1), (0,0,1,0,0,1)\}$,
$V_6 = \{(0,0,0,0,0,1), (0,0,1,0,1,1)\}$, $M_6 = \{(0,0,0,1,1,1), (0,1,0,1,0,1)\}$,
$\hat{U}_6 = \{(1,1,1,1,1,1), (0,0,1,1,1,1), (0,1,0,1,1,1), (0,1,1,0,1,1)\}$
and $\hat{V}_6 = \{(0,1,1,1,1,1), (0,0,1,1,0,1)\}$.

$$
{}_6\mathcal{A}^{\pi} = \begin{array}{c} \\ U_6 \\ V_6 \\ M_6 \\ \hat{V}_6 \\ \hat{U}_6 \end{array}
\begin{array}{c}
\begin{array}{cccccccccccccc} U_6 & & & & V_6 & & M_6 & & \hat{V}_6 & & & & & \hat{U}_6 \end{array} \\
\left(\begin{array}{cccc|cc|cc|cc|cccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
6 & 2 & -2 & -2 & 2 & -2 & 2 & -6 & 2 & -2 & 6 & 2 & -2 & -2 \\
6 & -2 & 2 & -2 & 2 & -2 & -2 & 6 & 2 & -2 & 6 & -2 & 2 & -2 \\
3 & -1 & -1 & 3 & 1 & 1 & -3 & -3 & 1 & 1 & 3 & -1 & -1 & 3 \\ \hline
6 & 2 & 2 & 2 & 4 & 0 & 0 & 0 & -4 & 0 & -6 & -2 & -2 & -2 \\
6 & -2 & -2 & 2 & 0 & -4 & 0 & 0 & 0 & 4 & -6 & 2 & 2 & -2 \\ \hline
6 & 2 & -2 & -6 & 0 & 0 & 0 & 0 & 0 & 0 & -6 & -2 & 2 & 6 \\
2 & -2 & 2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 2 & -2 & 2 \\ \hline
6 & 2 & 2 & 2 & -4 & 0 & 0 & 0 & 4 & 0 & -6 & -2 & -2 & -2 \\
6 & -2 & -2 & 2 & 0 & 4 & 0 & 0 & 0 & -4 & -6 & 2 & 2 & -2 \\ \hline
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\
6 & 2 & -2 & -2 & -2 & 2 & -2 & 6 & -2 & 2 & 6 & 2 & -2 & -2 \\
6 & -2 & 2 & -2 & -2 & 2 & 2 & -6 & -2 & 2 & 6 & -2 & 2 & -2 \\
3 & -1 & -1 & 3 & -1 & -1 & 3 & 3 & -1 & -1 & 3 & -1 & -1 & 3
\end{array}\right)
\end{array}
$$

The structure of the matrix ${}_n\mathcal{A}^\pi$ helps in analyzing the Walsh spectra for RSBFs on even number of variables. For notational purposes, divide the $(-1)^{\mathrm{RSTT}^\pi}$ into five partitions represented as vectors $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5$ by: $\sigma_1 = \{(-1)^{f(\Lambda_{n,0})}, \ldots, (-1)^{f(\Lambda_{n,|U_n|-1})}\}$,
$\sigma_2 = \{(-1)^{f(\Lambda_{n,|U_n|})}\}, \ldots, (-1)^{f(\Lambda_{n,|U_n|+|V_n|-1})}\}$,
$\sigma_3 = \{(-1)^{f(\Lambda_{n,|U_n|+|V_n|})}, \ldots, (-1)^{f(\Lambda_{n,|U_n|+|V_n|+|M_n|-1})}\}$,
$\sigma_4 = \{(-1)^{f(\Lambda_{n,|U_n|+|V_n|+|M_n|})}, \ldots, (-1)^{f(\Lambda_{n,g_n-|U_n|-1})}\}$, and
$\sigma_5 = \{(-1)^{f(\Lambda_{n,g_n-|U_n|})}, \ldots, (-1)^{f(\Lambda_{n,g_n-1})}\}$.
Then we define, $w_1 = \sigma_1\ {}_nG^1$, $w_2 = \sigma_1\ {}_nG^2$, $w_3 = \sigma_1\ {}_nG^3$,
$w_4 = \sigma_2\ {}_nG^4$, $w_5 = \sigma_2\ {}_nG^5$, $w_6 = \sigma_2\ {}_nG^6 = 0$,
$w_7 = \sigma_3\ {}_nG^7$, $w_8 = \sigma_3\ {}_nG^8 = 0$, $w_9 = \sigma_3\ {}_nG^9$,
$\hat{w}_4 = \sigma_4\ {}_nG^4$, $\hat{w}_5 = \sigma_4\ {}_nG^5$, $\hat{w}_6 = \sigma_4\ {}_nG^6 = 0$,
$\hat{w}_1 = \sigma_5\ {}_nG^1$, $\hat{w}_2 = \sigma_5\ {}_nG^2$, $\hat{w}_3 = \sigma_5\ {}_nG^3$.
The Walsh spectra of the function can be seen as: $((w_1 + w_4 + w_7 + \hat{w}_4 + \hat{w}_1) \parallel (w_2 + w_5 - \hat{w}_5 - \hat{w}_2) \parallel (w_3 + w_9 + (-1)^{n/2}\hat{w}_3) \parallel (w_2 - w_5 + \hat{w}_5 - \hat{w}_2) \parallel (w_1 - w_4 + (-1)^{n/2}\hat{w}_7 - \hat{w}_4 + \hat{w}_1))$.

To compute the Walsh spectra using the structure of ${}_n\mathcal{A}^\pi$, one needs a little more than half of the total computation than using ${}_n\mathcal{A}$ as described in [12]. Here, using the submatrices of ${}_n\mathcal{A}^\pi$, we need $2|U_n|(|U_n| + |V_n| + |M_n|) + 2|V_n|(|U_n| + |V_n|) + |M_n|(|U_n| + |M_n|) + g_n = |U_n|(2|U_n| + 2|V_n| + |M_n|) + |V_n|(2|U_n| + 2|V_n|) + |M_n|(2|U_n| + |M_n|) + g_n = |U_n|g_n + |V_n|(g_n - |M_n|) + |M_n|(g_n - 2|V_n|) + g_n = g_n(|U_n| + |V_n| + \frac{|M_n|}{2}) + (\frac{g_n}{2} - 3|V_n|)|M_n| + g_n \leq \frac{g_n^2}{2} + g_n$ many operations. Now we study the cardinality of U_n, V_n, M_n.

Lemma 1 *When n is even, the number of classes $G_n(\Lambda_{n,i})$ such that $G_n(\Lambda_{n,i}) = G_n(\hat{\Lambda}_{n,i})$ is $\sum_{k|\frac{n}{2}} \frac{1}{2k} d_k$ where $d_k = 2^k - \sum_{\frac{k}{k_1}=odd>1} d_{k_1}$.*

Proof : Let $x = \Lambda_{n,i}$ be the leader of one of such classes where $G_n(\Lambda_{n,i}) = G_n(\hat{\Lambda}_{n,i})$. So, for $x = (x_1, x_2, \cdots, x_n)$, $\overline{x} = (\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n)$, there exists a k, $0 < k < n$, such that $\rho_n^k(\overline{x}) = x$, i.e., $(x_1, x_2, \cdots, x_n) = \rho_n^k(\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n)$. This implies, $(x_1, \cdots, x_n) = (\overline{x}_{k+1}, \cdots, \overline{x}_n, \overline{x}_1, \cdots, \overline{x}_k)$ and hence,

$$(x_1, \cdots, x_{n-k}) = (\overline{x}_{k+1}, \cdots, \overline{x}_n), \tag{1}$$

$$(x_1, \cdots, x_k) = (\overline{x}_{n-k+1}, \cdots, \overline{x}_n). \tag{2}$$

Now, we will get from (1) that

$$(x_1, \cdots, x_k) = (\overline{x}_{k+1}, \cdots, \overline{x}_{2k}) = (x_{2k+1}, \cdots, x_{3k}) = \cdots \tag{3}$$

$$(\overline{x}_{n-k+1}, \cdots, \overline{x}_n) = (x_{n-2k+1}, \cdots, x_{n-k}) = (\overline{x}_{n-3k+1}, \ldots, \overline{x}_{n-2k}) = \cdots \tag{4}$$

Then, from (1), (2) and (3), we deduce $x = b\overline{b}b\overline{b}\cdots b\overline{b}$, where b is a block of length k. Thus, k must divide $\frac{n}{2}$. Now, we need to count the strings of above form where b is the smallest block. There could be 2^k different patterns and hence the number of strings of form $b\overline{b}b\overline{b}\cdots b\overline{b}$ is also 2^k. Next, we need to take care of the double counting when b is of the form $c\overline{c}c\overline{c}\cdots\overline{c}c$ where c is of length k_1 and $\frac{k}{k_1}$ is odd. Thus, the count of such strings for a fixed k is $d_k = 2^k - \sum_{\frac{k}{k_1}=odd>1} d_{k_1}$. The string $b\overline{b}b\overline{b}\cdots b\overline{b}$ has cycle length $2k$. So, each class contains $2k$ many elements. So, we have $\frac{1}{2k}(2^k - \sum_{\frac{k}{k_1}=odd>1} d_{k_1})$ many classes where length of b is k. Since we need to count for every k such that $k|\frac{n}{2}$. ∎

The next result follows from the count $g_{n,w}$ in [12, 7] and the count in Lemma 1.

Theorem 2 $|M_n| = \sum_{k|\frac{n}{2}} \frac{1}{2k} d_k$ *where* $d_k = 2^k - \sum_{\frac{k}{k_1}=odd>1} d_{k_1}$.

If $\frac{n}{2}$ *is even,* $|U_n| = |\hat{U}_n| = \sum_{w\leq\frac{n}{2}\ \&even} g_{n,w} - |M_n|$, $|V_n| = |\hat{V}_n| = \sum_{w<\frac{n}{2}\ \&odd} g_{n,w}$.

If $\frac{n}{2}$ *is odd,* $|U_n| = |\hat{U}_n| = \sum_{w<\frac{n}{2}\ \&even} g_{n,w}$, $|V_n| = |\hat{V}_n| = \sum_{w\leq\frac{n}{2}\ \&odd} g_{n,w} - |M_n|$.

Now we look for further symmetry in the ${}_n\mathcal{A}$ and ${}_n\mathcal{A}^\pi$. Note that this result works for both even and odd n.

Theorem 3 ${}_n\mathcal{A}_{i,j} = \frac{{}_n\mathcal{A}_{i,0}}{{}_n\mathcal{A}_{j,0}}\ {}_n\mathcal{A}_{j,i}$ *and* ${}_n\mathcal{A}^\pi_{i,j} = \frac{{}_n\mathcal{A}^\pi_{i,0}}{{}_n\mathcal{A}^\pi_{j,0}}\ {}_n\mathcal{A}^\pi_{j,i}$ *for any positive integer* n.

Proof : Let $k_i = |G_n(\Lambda_{n,i})| = {}_n\mathcal{A}_{i,0}$ and $n_i = \frac{n}{k_i}$ for $0 \leq i < n$. Note that ${}_n\mathcal{A}_{i,j} = \sum_{x\in G_n(\Lambda_{n,i})}(-1)^{x.\Lambda_{n,j}} = (-1)^{\rho_n^0(\Lambda_{n,i}).\Lambda_{n,j}} + \cdots + (-1)^{\rho_n^{k_i-1}(\Lambda_{n,i}).\Lambda_{n,j}} = (-1)^{\rho_n^{k_i}(\Lambda_{n,i}).\Lambda_{n,j}} + \cdots + (-1)^{\rho_n^{2k_i-1}(\Lambda_{n,i}).\Lambda_{n,j}} = \ldots = (-1)^{\rho_n^{(n_i-1)k_i}(\Lambda_{n,i}).\Lambda_{n,j}} + \cdots + (-1)^{\rho_n^{n_ik_i-1}(\Lambda_{n,i}).\Lambda_{n,j}}$. As $n_ik_i = n$, $n_i\ {}_n\mathcal{A}_{i,j} = \sum_{x\in G_n(\Lambda_{n,i})}(-1)^{x.\Lambda_{n,j}} + \cdots + \sum_{x\in G_n(\Lambda_{n,i})}(-1)^{x.\Lambda_{n,j}} = (-1)^{\rho_n^0(\Lambda_{n,i}).\Lambda_{n,j}} + \cdots + (-1)^{\rho_n^{n-1}(\Lambda_{n,i}).\Lambda_{n,j}}$. Since $(-1)^{\rho_n^t(\Lambda_{n,i}).\Lambda_{n,j}} = (-1)^{\Lambda_{n,i}.\rho_n^{n-t}\Lambda_{n,j}}$, we can write, $(-1)^{\rho_n^0(\Lambda_{n,i}).\Lambda_{n,j}} + \cdots + (-1)^{\rho_n^{n-1}(\Lambda_{n,i}).\Lambda_{n,j}} = (-1)^{\Lambda_{n,i}.\rho_n^n(\Lambda_{n,j})} + \cdots + (-1)^{\Lambda_{n,i}.\rho_n^1(\Lambda_{n,j})} = (-1)^{\Lambda_{n,i}.\rho_n^0(\Lambda_{n,j})} + \cdots + (-1)^{\Lambda_{n,i}.\rho_n^{k_j-1}(\Lambda_{n,j})} + (-1)^{\Lambda_{n,i}.\rho_n^{k_j}(\Lambda_{n,j})} + \cdots + (-1)^{\Lambda_{n,i}.\rho_n^{2k_j-1}(\Lambda_{n,j})} + \cdots + (-1)^{\Lambda_{n,i}.\rho_n^{(n_j-1)k_j}(\Lambda_{n,j})} + \cdots + (-1)^{\Lambda_{n,i}.\rho_n^{n_jk_j-1}(\Lambda_{n,j})} = n_j\left((-1)^{\Lambda_{n,i}.\rho_n^0(\Lambda_{n,j})} + \cdots + (-1)^{\Lambda_{n,i}.\rho_n^{k_j-1}(\Lambda_{n,j})}\right) = n_j\ {}_n\mathcal{A}_{j,i}$.

Thus, ${}_n\mathcal{A}_{i,j} = \frac{n_j}{n_i}\ {}_n\mathcal{A}_{j,i} = \frac{k_i}{k_j}\ {}_n\mathcal{A}_{j,i} = \frac{{}_n\mathcal{A}_{i,0}}{{}_n\mathcal{A}_{j,0}}\ {}_n\mathcal{A}_{j,i}$. Since ${}_n\mathcal{A}^\pi$ is generated by permuting rows and columns of ${}_n\mathcal{A}$ simultaneously using the permutation π, ${}_n\mathcal{A}^\pi$ also preserves the symmetry. ■

So by this way we can reduce the computation time by around half to compute ${}_n\mathcal{A}$ and ${}_n\mathcal{A}^\pi$ for any n. The computation time to construct the submatrices of ${}_n\mathcal{A}^\pi$ is reduced. Since this result works for both even and odd n, this gives further insight to the matrix structure for odd n over the results presented in [6].

3 Rotation Symmetric Bent Functions

Construction and enumeration of bent RSBFs have been studied in [4, 11, 12, 1]. It is easy to see that [9, 12] an RSBF f is bent iff $W_f(\Lambda_j) = \sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}{}_n\mathcal{A}^\pi_{i,j} = \pm 2^{\frac{n}{2}}$ for $0 \leq j \leq g_n - 1$. As we find interesting regular structure in ${}_n\mathcal{A}^\pi_{i,j}$, we may apply that in studying rotation symmetric bent functions (RSBNFs). Once again we recall remind that the order of representative elements are according to the order: $U_n, V_n, M_n, \hat{V}_n, \hat{U}_n$. Let us define the following five elements which are basically partial values of the Walsh spectra:

$Q_{1,j} = \sum_{i=0}^{|U_n|-1}(-1)^{f(\Lambda_{n,i})}{}_n\mathcal{A}^\pi_{i,j}$, $Q_{2,j} = \sum_{i=|U_n|}^{|U_n|+|V_n|-1}(-1)^{f(\Lambda_{n,i})}{}_n\mathcal{A}^\pi_{i,j}$,

$Q_{3,j} = \sum_{i=|U_n|+|V_n|}^{|U_n|+|V_n|+|M_n|-1}(-1)^{f(\Lambda_{n,i})}{}_n\mathcal{A}^\pi_{i,j}$, $Q_{4,j} = \sum_{i=|U_n|+|V_n|+|M_n|}^{|U_n|+2|V_n|+|M_n|-1}(-1)^{f(\Lambda_{n,i})}{}_n\mathcal{A}^\pi_{i,j}$,

$Q_{5,j} = \sum_{i=|U_n|+2|V_n|+|M_n|}^{2|U_n|+2|V_n|+|M_n|-1}(-1)^{f(\Lambda_{n,i})}{}_n\mathcal{A}^\pi_{i,j}$. Note that $W_f(\Lambda_{n,j}) = \sum_{k=1}^5 Q_{k,j}$. Based on these notations, we get the following results:

1. Let $\Lambda_{n,j} \in M_n$ then $\sum_{\Lambda_{n,i}\in U_n\bigcup M_n\bigcup\hat{U}_n}(-1)^{f(\Lambda_{n,i})}{}_n\mathcal{A}^\pi_{i,j} = \pm 2^{\frac{n}{2}}$ as ${}_nG^6 = {}_nG^8 = 0$. Further if $\frac{n}{2}$ is odd, since, ${}_nG^9 = 0$, we have $\sum_{\Lambda_{n,i}\in U_n\bigcup\hat{U}_n}(-1)^{f(\Lambda_{n,i})}{}_n\mathcal{A}^\pi_{i,j} = \pm 2^{\frac{n}{2}}$. That is, if $\Lambda_{n,j} \in M_n$ then for $\frac{n}{2}$ even, $Q_{1,j} + Q_{3,j} + Q_{5,j} = \pm 2^{\frac{n}{2}}$ and for $\frac{n}{2}$ odd, $Q_{1,j} + Q_{5,j} = \pm 2^{\frac{n}{2}}$.

2. Let $\Lambda_{n,j} \in V_n$ then $Q_{1,j} + Q_{2,j} + Q_{4,j} + Q_{5,j} = \pm 2^{\frac{n}{2}}$. Also, $\hat{\Lambda}_{n,j} = \Lambda_{n,k} \in \hat{V}_n$. Then $Q_{1,k} + Q_{2,k} + Q_{4,k} + Q_{5,k} = Q_{1,j} - Q_{2,j} - Q_{4,j} + Q_{5,j} = \pm 2^{\frac{n}{2}}$. From these two equations we will get either $Q_{1,j} + Q_{5,j} = 0$ and $Q_{2,j} + Q_{4,j} = \pm 2^{\frac{n}{2}}$ or $Q_{1,j} + Q_{5,j} = \pm 2^{\frac{n}{2}}$ and $Q_{2,j} + Q_{4,j} = 0$

3. Let $\Lambda_{n,j} \in U_n$, i.e., $\hat{\Lambda}_{n,j} \in \hat{U}_n$. Then one can check that if $\frac{n}{2}$ is odd, either $Q_{1,j} + Q_{5,j} = \pm 2^{\frac{n}{2}}$ and $Q_{2,j} + Q_{3,j} + Q_{4,j} = 0$ or, $Q_{1,j} + Q_{5,j} = 0$ and $Q_{2,j} + Q_{3,j} + Q_{4,j} = \pm 2^{\frac{n}{2}}$.

   If $\frac{n}{2}$ is even, then either $Q_{1,j} + Q_{3,j} + Q_{5,j} = \pm 2^{\frac{n}{2}}$ and $Q_{2,j} + Q_{4,j} = 0$ or, $Q_{1,j} + Q_{3,j} + Q_{5,j} = 0$ and $Q_{2,j} + Q_{4,j} = \pm 2^{\frac{n}{2}}$.

The above results are necessary conditions on partial Walsh spectra for a function to be RSBNF. Consequently, this gives a sieving strategy for RSBNFs. We have already divided $(-1)^{\mathrm{RSTT}^{\pi}}$ into five parts as $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5$. Let us describe the case when $\frac{n}{2}$ is even with a continuing example $n = 8$.

We first choose the string patterns for $\sigma_1, \sigma_3, \sigma_5$ and select the patterns that satisfy $Q_{1,j} + Q_{3,j} + Q_{5,j} = \pm 2^{\frac{n}{2}}$ when $\Lambda_{n,j} \in M_n$. The size of this string is $2|U_n| + |M_n|$. As example for 8-variables this is $2 \cdot 8 + 4 = 20$. We can also fix $f(x) = 0$ for $wt(x) = 0$ for the search of bent functions. Thus basically we need to search all the 19-bit patterns. Out of these 2^{19} patterns we found only 4954 many that satisfy the property.

Then we concentrate on $\Lambda_{n,j} \in V_n$. The conditions to be satisfied here are $Q_{1,j} + Q_{5,j}$ must be $\pm 2^{\frac{n}{2}}$ or 0. In this case we need to consider only σ_1, σ_5 (but not σ_3). Thus we search 15 bit subpattern out of the 19 bits and found that out of 4954, only 602 satisfy this condition.

Out of these 602, we again filter the patterns corresponding to $\sigma_1, \sigma_3, \sigma_5$ using the condition $Q_{1,j} + Q_{3,j} + Q_{5,j}$ must be $\pm 2^{\frac{n}{2}}$ or 0 for $\Lambda_{n,j} \in U_n$. Then we get only 400 patterns. We put them in DATABASE 1.

Then we concentrate on $\Lambda_{n,j} \in U_n \cup V_n$. The conditions to be satisfied here are $Q_{2,j} + Q_{4,j}$ must be $\pm 2^{\frac{n}{2}}$ or 0. In this case we need to consider σ_2, σ_4 for calculating the Walsh spectra. This size is $2|V_n|$. For 8-variables we find this $2 \cdot 8 = 16$. We can also fix $f(x) = 0$ for $wt(x) = 1$ for the search of bent functions. Thus we need to search strings of length 15 only. Among the 2^{15} patterns, we find that there are only 420 patterns that satisfy the condition. We put them in DATABASE 2.

Now we create the $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5$ pattern by concatenating the elements of DATABASE 1 and 2, i.e., we need to check for $400 \cdot 420$ elements which is $< 2^{16}$. Then we check whether $W_f(\Lambda_{n,j}) = \sum_{k=1}^{5} Q_{k,j} = \pm 2^{\frac{n}{2}}$ for $\Lambda_{n,j} \in U_n \cup V_n$ and find 3776 many patterns. So there are 3776 many RSBFs with the constraint $f(x) = 0$ for $wt(x) = 0$ and $f(x) = 0$ for $wt(x) = 1$. Thus there are 4×3776 many RSBNFs as we can take $f(x) = 0$ or 1 for $wt(x) = 0$ and $f(x) = 0$ or 1 for $wt(x) = 1$.

The sieving strategy presented here is much more efficient than that of [12, Page 14]. Due to space constraint we cannot explain the complete details of improvement. Just to make a comparison we refer to the example for 8-variable case, where the computation needs only 2 seconds compared to 1 minute in [12] under the exactly same hardware, operating system and programming strategy. We are currently working to enumerate 10-variable RSBNFs (this is an open question till date) which looks feasible using this sieving strategy. Only a few 10-variable RSBNFs have been reported by heuristic search (simulated annealing) till date [1].

3.1 Modifying Symmetric Bent to RSBNF

A small subclass of Boolean functions is the set of symmetric Boolean functions where the output of the function depends only on the weight of the input vector. It is known that for any even n there are exactly 4 symmetric bent functions and these are quadratic [10]. As they are symmetric, by definition, they are rotation symmetric too. It is possible to modify these functions such that the symmetry of the functions will be disturbed, but the rotational symmetry property will be maintained and at the same time the bentness property will be preserved. For $\mu \in M_n$, weight of all elements in $G_n(\mu)$ is $\frac{n}{2}$. Also there exists $\nu \in U_n$ for $n \equiv 0 \bmod 4$ (respectively $\nu \in V_n$ for $n \equiv 2 \bmod 4$) such that weight of elements in $G_n(\nu)$ is $\frac{n}{2}$. We change the function by modifying the outputs corresponding to the inputs in $G_n(\mu)$. This breaks the symmetry property as there are now different outputs at the inputs of weight $\frac{n}{2}$. However, by this technique the function stays at least rotation symmetric. Due to space constraint, it is not possible to explain the complete details here, but we present an example corresponding to 6-variable functions. Note that if we take a symmetric bent function on 6-variables and complement the outputs corresponding to the inputs $G_6(\mu)$, where $\mu \in M_6$, the functions becomes RSBNF, but not symmetric.

References

[1] J. Clark, J. Jacob, S. Maitra and P. Stănică. Almost Boolean Functions: The Design of Boolean Functions by Spectral Inversion. *Computational Intelligence*, Pages 450–462, Volume 20, Number 3, 2004.

[2] T. W. Cusick and P. Stănică. Fast Evaluation, Weights and Nonlinearity of Rotation-Symmetric Functions. *Discrete Mathematics* **258**, 289–301, 2002.

[3] D. K. Dalai, K. C. Gupta and S. Maitra. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. In *Progress in Cryptology - INDOCRYPT 2004*, to be published in Lecture Notes in Computer Science, Springer-Verlag.

[4] E. Filiol and C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation-immunity. In *Advances in Cryptology - EUROCRYPT'98*, Springer-Verlag, 1998.

[5] M. Hell, A. Maximov and S. Maitra. On efficient implementation of search strategy for rotation symmetric Boolean functions. In *Ninth International Workshop on Algebraic and Combinatoral Coding Theory, ACCT 2004*, June 19–25, 2004, Black Sea Coast, Bulgaria.

[6] A. Maximov, M. Hell and S. Maitra. Plateaued Rotation Symmetric Boolean Functions on Odd Number of Variables. IACR eprint server, eprint.iacr.org, no. 2004/144, 2004.

[7] A. Maximov. Classes of Plateaued Rotation Symmetric Boolean functions under Transformation of Walsh Spectra. IACR eprint server, no. 2004/354.

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

[9] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, pages 300–305, vol 20, 1976.

[10] P. Savicky. On the bent Boolean functions that are symmetric. *European Journal of Combinatorics*, 15:407–410, 1994.

[11] P. Stănică and S. Maitra. Rotation Symmetric Boolean Functions – Count and Cryptographic Properties. In *R. C. Bose Centenary Symposium on Discrete Mathematics and Applications*, December 2002. Electronic Notes in Discrete Mathematics, Elsevier, Vol 15.

[12] P. Stănică, S. Maitra and J. Clark. Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions. *Fast Software Encryption Workshop (FSE 2004)*, New Delhi, INDIA, LNCS **3017**, Springer Verlag, 161–177, 2004.

[13] Y. Zheng, X-M. Zhang and H. Imai. Restriction, terms and nonlinearity of Boolean functions. *Theoretical Computer Science*, 226:207–223, 1999.