Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions

Pantelimon Stănică[1*], Subhamoy Maitra[2], John A. Clark[3]

[1] Mathematics Department, Auburn University Montgomery
Montgomery, AL 36124-4023, USA
pstanica@mail.aum.edu

[2] Applied Statistics Unit, Indian Statistical Institute,
203, B T Road, Kolkata 700 108, INDIA
subho@isical.ac.in

[3] Department of Computer Science, University of York,
York YO10 3EE, England.
jac@cs.york.ac.uk

Abstract. Recent research shows that the class of Rotation Symmetric Boolean Functions (RSBFs), i.e., the class of Boolean functions that are invariant under circular translation of indices, is potentially rich in functions of cryptographic significance. Here we present new results regarding the Rotation Symmetric (rots) correlation immune (CI) and bent functions. We present important data structures for efficient search strategy of rots bent and CI functions. Further, we prove the nonexistence of homogeneous rots bent functions of degree ≥ 3 on a single cycle.

Keywords: Rotation Symmetric Boolean Function, Bent Functions, Balancedness, Nonlinearity, Autocorrelation, Correlation Immunity, Resiliency.

1 Introduction

A variety of criteria for choosing Boolean functions with cryptographic applications (for secret key cryptosystems) have been identified. These are balancedness, nonlinearity, autocorrelation, correlation immunity, algebraic degree etc. The trade-offs among these criteria have received a lot of attention in Boolean function literature for a long time (see [7] and the references in this paper). The more criteria that have to be taken into account, the more difficult the problem is to obtain a Boolean function satisfying these properties.

It has been found recently that the class of RSBFs is extremely rich in terms of cryptographically significant Boolean functions. These functions have been analyzed in [4], where the authors studied the nonlinearity of these Boolean functions up to 9 variables and found encouraging results. This study has been extended in [15, 16] and important properties (further to [4]) of these functions

---

* This author is associated with the Institute of Mathematics "Simion Stoilow" of the Romanian Academy, Bucharest - Romania.

up to 8 variables have been demonstrated. Also, the enumeration of RSBFs of specific degree has been discussed in [15, 16]. On the other hand, in [11], Pieprzyk and Qu studied these functions as components in the rounds of a hashing algorithm and research in this direction was later continued in [3].

The space of RSBFs is of size approximately $2^{\frac{2^n}{n}}$ for n-variable, which is of size n-th root of the total space 2^{2^n}. Thus any kind of search becomes comparatively easier and it has been shown in [15] that it is easy to get a 7-variable, 2-resilient RSBF with nonlinearity 56, which has earlier been considered as a function that is not easy to search for [10]. Moreover, these functions also possess the best known autocorrelation spectra. Thus it is important to present tools that can be used to efficiently search the space of RSBFs. We present important data structures, the matrices ${}_n\mathcal{A}$ and ${}_n\mathcal{B}$, that make this search and the study of bent functions more efficient.

Using these data structures, for the first time we could find 8-variable, 1-resilient, algebraic degree 6, nonlinearity 116, PC(1) functions with maximum absolute value in the autocorrelation spectra 32. Functions with such parameters have not been reported earlier. Moreover, interesting results are obtained for 9-variable correlation immune functions. The space for these functions in the Rotation Symmetric class is too large to execute exhaustive search. Hence we exploited simulated annealing technique to find these functions. The results found by simulated annealing are as follows. We could find 9-variable, 2-resilient, algebraic degree 6 and nonlinearity 240 functions and unbalanced 9-variable, 3rd order correlation immune, algebraic degree 5 and nonlinearity 240 functions. These functions have been posed as important open questions in [13, 14]. Note that the details of simulated annealing is not included in this paper and that has been published in [2].

In this paper, we also try to analyze the RSBFs class using combinatorial techniques in Section 3. We present enumerative results (based on constructive techniques) on balanced and correlation immune RSBFs. Further, we show that it is possible to transform a class of RSBFs to correlation immune functions depending on full rank of binary circulant matrices over $\mathbf{Z}_2$. In [15], it was observed that there is no homogeneous rots bent functions of degree ≥ 3 up to 10 variables. We here theoretically show the nonexistence of homogeneous rots bent functions of degree ≥ 3 on a single cycle for any (even) number of input variables ≥ 6.

2 Preliminaries

A Boolean function on n variables may be viewed as a mapping from $V_n = \{0,1\}^n$ into $\{0,1\}$. A Boolean function $f(x_1, \ldots, x_n)$ is also interpreted as the output column of its *truth table* f, i.e., a binary string of length 2^n, $f = [f(0,0,\cdots,0), f(1,0,\cdots,0), f(0,1,\cdots,0), \ldots, f(1,1,\cdots,1)]$.

The *Hamming distance* between S_1, S_2 is denoted by $d(S_1, S_2) = \#(S_1 \neq S_2)$. Also the *Hamming weight* or simply the weight of a binary string S is the number of ones in S. This is denoted by $wt(S)$. An n-variable function f is said to be *balanced* if its output column in the truth table contains equal number of 0's and 1's (i.e., $wt(f) = 2^{n-1}$).

Addition operator over $GF(2)$ is denoted by $\oplus$. An n-variable Boolean function $f(x_1, \ldots, x_n)$ can be considered to be a multivariate polynomial over $GF(2)$. This polynomial can be expressed as a sum of products representation of all distinct k-th order products $(0 \leq k \leq n)$ of the variables. More precisely, $f(x_1, \ldots, x_n)$ can be written as

$$a_0 \oplus \bigoplus_{1 \leq i \leq n} a_i x_i \oplus \bigoplus_{1 \leq i < j \leq n} a_{ij} x_i x_j \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \{0, 1\}$. This representation of f is called the *algebraic normal form* (ANF) of f. The number of variables in the highest order product term with nonzero coefficient is called the *algebraic degree*, or simply the degree of f and denoted by $deg(f)$.

Take $0 \leq b \leq n$. An n-variable function is called *nondegenerate* on b variables if its ANF contains exactly b distinct input variables. A Boolean function is said to be *homogeneous* if its ANF contains terms of the same degree only.

Functions of degree at most one are called *affine* functions. An affine function with constant term equal to zero is called a *linear* function. The set of all n-variable affine (respectively linear) functions is denoted by $A(n)$ (respectively $L(n)$). The nonlinearity of an n-variable function f is

$$nl(f) = min_{g \in A(n)}(d(f, g)),$$

i.e., the distance from the set of all n-variable affine functions.

Let $x = (x_1, \ldots, x_n)$ and $\omega = (\omega_1, \ldots, \omega_n)$ both belonging to $\{0, 1\}^n$ and $x \cdot \omega = x_1\omega_1 \oplus \ldots \oplus x_n\omega_n$. Let $f(x)$ be a Boolean function on n variables. Then the *Walsh transform* of $f(x)$ is a real valued function over $\{0, 1\}^n$ which is defined as

$$W_f(\omega) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus x \cdot \omega}.$$

In terms of Walsh spectra, the nonlinearity of f is given by

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \{0,1\}^n} |W_f(\omega)|.$$

In [5], an important characterization of correlation immune functions has been presented, which we use as the definition here. A function $f(x_1, \ldots, x_n)$ is m-th order correlation immune (respectively m-resilient) iff its Walsh transform satisfies

$$W_f(\omega) = 0, \text{ for } 1 \leq wt(\omega) \leq m \text{ (respectively } 0 \leq wt(\omega) \leq m).$$

As the notation used in [13, 14], by an (n, m, d, σ) function we denote an n-variable, m-resilient function with degree d and nonlinearity σ. Further by an $[n, m, d, \sigma]$ function we denote an unbalanced n-variable, mth order correlation immune function with degree d and nonlinearity σ.

Propagation Characteristics (PC) and Strict Avalanche Criteria (SAC) [12] are important properties of Boolean functions to be used in S-boxes. Further, Zhang and Zheng [18] identified related cryptographic measures called Global Avalanche Characteristics (GAC).

Let $\alpha \in \{0,1\}^n$ and f be an n-variable Boolean function. Let us denote the autocorrelation value of the Boolean function f with respect to the vector α as

$$\Delta_f(\alpha) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus f(x \oplus \alpha)},$$

and the absolute indicator

$$\Delta_f = \max_{\alpha \in \{0,1\}^n, \alpha \neq \bar{0}} |\Delta_f(\alpha)|.$$

A function is said to satisfy PC(k), if

$$\Delta_f(\alpha) = 0 \ for\ 1 \leq wt(\alpha) \leq k.$$

2.1 Rotation Symmetric Boolean Functions

Let $x_i \in \{0,1\}$ for $1 \leq i \leq n$. For $1 \leq k \leq n$, we define

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

Let $(x_1, x_2, \ldots, x_{n-1}, x_n) \in V_n$. We can extend the definition of ρ_n^k on tuples and monomials as $\rho_n^k(x_1, x_2, \ldots, x_n) = (\rho_n^k(x_1), \rho_n^k(x_2), \ldots, \rho_n^k(x_n))$ and $\rho_n^k(x_{i_1} x_{i_2} \cdots) = \rho_n^k(x_{i_1}) \rho_n^k(x_{i_2}) \cdots$.

Definition 1. *A Boolean function f is called* Rotation Symmetric *if for each input $(x_1, \ldots, x_n) \in \{0,1\}^n$, $f(\rho_n^k(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n)$ for $1 \leq k \leq n$.*

Following [15], let us denote

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

Note that $G_n(x_1, \ldots, x_n)$ generates a partition in the set V_n. Let g_n be the number of such partitions. Using Burnside's lemma, it can be shown (see also [15]) that the number of n-variable RSBFs is

$$2^{g_n}, \text{ where } g_n = \frac{1}{n} \sum_{k|n} \phi(k)\, 2^{\frac{n}{k}},$$

ϕ being Euler's *phi*−function. Further the following result has been proved regarding n-variable RSBFs of some specific degree. The number of

(i) degree w homogeneous functions is $2^{g_{n,w}} - 1$,
(ii) the number of degree w functions is $(2^{g_{n,w}} - 1) 2^{\sum_{i=0}^{w-1} g_{n,i}}$ and

(iii) the number of functions with degree at most w is $2^{\sum_{i=0}^{w} g_{n,i}}$, where $g_{n,w}$ is defined as follows (see also [15]).

Consider $G_n(x_1, \ldots, x_n)$, where $wt(x_1, \ldots, x_n)$ is exactly w, and define $g_{n,w}$ as the number of partitions over the n bit binary strings of weight w (total number $\binom{n}{w}$), determined by G_n. Further, denote by $h_{n,w}$ the number of distinct sets $G_n(x_1, \ldots, x_n)$, where $wt(x_1, \ldots, x_n) = w$ and $|G_n(x_1, \ldots, x_n)| = n$, that is, the number of long cycles of weight w. It is easy to see that $h_{n,w} < g_{n,w}$. Write $k|m$, if k $(1 < k \leq m)$ is a proper divisor of m. The following results were obtained in [15].

(i) $g_{n,w} = \frac{1}{n}\binom{n}{w}$, if $gcd(n, w) = 1$. Also, $g_{n,0} = g_{n,n} = 1$.

(ii) $g_{n,w} = \frac{1}{n}\left(\binom{n}{w} - \sum_{k|gcd(n,w)} \frac{n}{k} \cdot h_{\frac{n}{k},\frac{w}{k}}\right) + \sum_{k|gcd(n,w)} h_{\frac{n}{k},\frac{w}{k}}$, if $w < n$.

Filiol and Fontaine [4] discussed the set of idempotent Boolean functions in an experimental setting. Let $\mathcal{B} = (b_1, \ldots, b_n)$ be a basis of F_2^n (which is identified with F_{2^n}). An *idempotent* f is a Boolean function on F_{2^n} that satisfies $f^2 = f$. Define the *Mattson-Solomon (MS) polynomial* by

$$MS_f(Z) = \sum_{j=0}^{2^n-2} A_j Z^{2^n-j-1}, \text{ where } A_j = \sum_{i=0}^{2^n-1} f(\alpha^i)\alpha^{ij},$$

where α is a primitive element of F_{2^n}. Using the representation

$$f = \sum_{g \in F_{2^n}^*} f(g)(g)$$

(in the multiplicative algebra $F_2[F_{2^n}, \times]$), one gets that f is an idempotent iff $f(g) = f(g^2)$, $\forall\, g$; the coefficients of the MS polynomial belong to F_2; $A_j = A_k$ for all k in the 2-cyclotomic class of j $(\{j, 2j, \ldots, 2^{n-1}j\})$; the ANF of f (using a normal basis $(\gamma, \gamma^2, \ldots, \gamma^{2^{n-1}})$ remains invariant under circular shift. This gives that the corpus of idempotents is the same as the class of Rotation Symmetric Boolean functions. For $n = 5, 7$, they found idempotents of highest nonlinearity (12, respectively 56) of degrees 2, 3 (for $n = 5$), and degrees $2, 3, 4, 5, 6$ (for $n = 7$). For $n = 6, 8$ they found all idempotents of highest nonlinearity (28, respectively 120), of degrees $2, 3$, respectively, $2, 3, 4$. They were not able to find all idempotent functions for $n = 8$, though. Finally, for $n = 9$, they found 1142395 functions (up to equivalence) with nonlinearity 240, some of which are balanced, of degrees $2, 3, 4, 5, 6, 7$.

3 Study on RSBFs

Motivated by [4, 15], in this section we will investigate the richness of the RSBFs class in terms of cryptographic properties and present some important data structures. The data structures will help in running the search algorithms very fast. In this direction we start with a few technical results. In the preliminaries, we have defined $G_n(x_1,\ldots,x_n) = \{\rho_n^k(x_1,\ldots,x_n),\ \text{for } 1 \le k \le n\}$. As example, for $n = 4$ we get the following partition of $\{0,1\}^n$:

$$\begin{gathered}
G_4(0,0,0,0) = \{(0,0,0,0)\};\\
G_4(0,0,0,1) = \{(0,0,0,1),(0,0,1,0),(0,1,0,0),\ (1,0,0,0)\};\\
G_4(0,0,1,1) = \{(0,0,1,1),(0,1,1,0),(1,0,0,1),(1,1,0,0)\};\\
G_4(0,1,0,1) = \{(0,1,0,1),\ (1,0,1,0)\};\\
G_4(0,1,1,1) = \{(0,1,1,1),(1,0,1,1),(1,1,0,1),(1,1,1,0)\};\\
G_4(1,1,1,1) = \{(1,1,1,1)\}.
\end{gathered}$$

Note that there are g_n such partitions, and the lexicographically first element of each part is considered as the representative element. We denote these representative elements by $\Lambda_{n,i}$ where i varies from 0 to $g_n - 1$ and representative elements are again arranged lexicographically. That is, in the above example, $\Lambda_{4,0} = (0,0,0,0), \Lambda_{4,1} = (1,0,0,0), \Lambda_{4,2} = (1,1,0,0), \Lambda_{4,3} = (1,0,1,0), \Lambda_{4,4} = (1,1,1,0), \Lambda_{4,5} = (1,1,1,1)$.

By RSTT (rotation symmetric truth table) we mean the g_n-bit long binary string

$$[f(\Lambda_{n,0}), f(\Lambda_{n,1}), \ldots, f(\Lambda_{n,g_n-1})],$$

which gives the complete information of the function f when it is rots.

Lemma 1. *Let $u, v \in \{0,1\}^n$ and $u \neq v$ with $u \in G_n(v)$. Let f be an n-variable RSBF. Then $W_f(u) = W_f(v)$, which implies that the Walsh spectra of f can be at most g_n valued.*

Proof. First we show that for $a \in \{0,1\}$,

$$\sum_{x \in G_n(\Lambda_{n,i})} (-1)^{a \oplus x\cdot u} = \sum_{x \in G_n(\Lambda_{n,i})} (-1)^{a \oplus x \cdot v}.$$

Since $u \in G_n(v)$, $u = \rho_n^k(v)$ for some k. Now $\sum_{x \in G_n(\Lambda_{n,i})} (-1)^{a\oplus x\cdot u}$ $= \sum_{x\in G_n(\Lambda_{n,i})} (-1)^{a \oplus \rho_n^k(x)\cdot \rho_n^k(u)} = \sum_{y \in G_n(\Lambda_{n,i})} (-1)^{a\oplus y\cdot v}$ (take $y = \rho_n^k(x)$) $=$ $\sum_{x\in G_n(\Lambda_{n,i})} (-1)^{a\oplus x\cdot v}$.

$W_f(u) = \sum_{x\in\{0,1\}^n} (-1)^{f(x)\oplus x\cdot u} = \sum_{i=0}^{g_n-1} \sum_{x\in G_n(\Lambda_{n,i})} (-1)^{f(x)\oplus x\cdot u}$ $=$ (using the above result) $\sum_{i=0}^{g_n-1} \sum_{x\in G_n(\Lambda_{n,i})} (-1)^{f(x)\oplus x\cdot v} = W_f(v)$. □

Note that, Lemma 1 helps to run any heuristic in a much smaller space. Now we define an important matrix called ${}_n\mathcal{A}$ with respect to the set of n-variable RSBFs as:

$${}_n\mathcal{A}_{i,j} = \sum_{x\in G_n(\Lambda_{n,i})} (-1)^{x\cdot \Lambda_{n,j}}.$$

See the following example corresponding to 6-variable case.

i	0	1	2	3	4	5	6
$\Lambda_{6,i}$	000000	000001	000011	000101	000111	001001	001011

i	7	8	9	10	11	12	13
$\Lambda_{6,i}$	001101	001111	010101	010111	011011	011111	111111

$$
{}_6\mathcal{A} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
6 & 4 & 2 & 2 & 0 & 2 & 0 & 0 & -2 & 0 & -2 & -2 & -4 & -6 \\
6 & 2 & 2 & -2 & 2 & -2 & -2 & -2 & 2 & -6 & -2 & -2 & 2 & 6 \\
6 & 2 & -2 & 2 & -2 & -2 & -2 & -2 & -2 & 6 & 2 & -2 & 2 & 6 \\
6 & 0 & 2 & -2 & 0 & -6 & 0 & 0 & -2 & 0 & 2 & 6 & 0 & -6 \\
3 & 1 & -1 & -1 & -3 & 3 & 1 & 1 & -1 & -3 & -1 & 3 & 1 & 3 \\
6 & 0 & -2 & -2 & 0 & 2 & -4 & 4 & 2 & 0 & 2 & -2 & 0 & -6 \\
6 & 0 & -2 & -2 & 0 & 2 & 4 & -4 & 2 & 0 & 2 & -2 & 0 & -6 \\
6 & -2 & 2 & -2 & -2 & -2 & 2 & 2 & 2 & 6 & -2 & -2 & -2 & 6 \\
2 & 0 & -2 & 2 & 0 & -2 & 0 & 0 & 2 & 0 & -2 & 2 & 0 & -2 \\
6 & -2 & -2 & 2 & 2 & -2 & 2 & 2 & -2 & -6 & 2 & -2 & -2 & 6 \\
3 & -1 & -1 & -1 & 3 & 3 & -1 & -1 & -1 & 3 & -1 & 3 & -1 & 3 \\
6 & -4 & 2 & 2 & 0 & 2 & 0 & 0 & -2 & 0 & -2 & -2 & 4 & -6 \\
1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1
\end{bmatrix}
$$

This matrix is of size $g_n \times g_n$. Now for an n-variable RSBF f, we have $W_f(\omega) = \sum_{x\in\{0,1\}^n}(-1)^{f(x)\oplus x\cdot\omega} = \sum_{i=0}^{g_n-1}\sum_{x\in G_n(\Lambda_{n,i})}(-1)^{f(x)\oplus x\cdot\omega}$ $= \sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}\sum_{x\in G_n(\Lambda_{n,i})}(-1)^{x\cdot\Lambda_{n,j}}$, if $\omega \in G_n(\Lambda_{n,j})$. Thus, $W_f(\Lambda_{n,j}) = \sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}\,{}_n\mathcal{A}_{i,j}$. To summarize, we have the following result.

Proposition 1. $W_f(\Lambda_{n,j}) = \sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}\,{}_n\mathcal{A}_{i,j}$.

In terms of Proposition 1, we can list the following.

Lemma 2. *Let f be an n-variable RSBF.*

1. $nl(f) = 2^{n-1} - \frac{1}{2}\max_{\Lambda_{n,j},0\le j<g_n}|\sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}\,{}_n\mathcal{A}_{i,j}|$.
2. *f is balanced iff*
$$\sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}\,{}_n\mathcal{A}_{i,0} = 0.$$
3. *f is m-th order CI (respectively m-resilient) iff*
$$\sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}\,{}_n\mathcal{A}_{i,j} = 0,\ \textit{for } 1 \textit{ (respectively } 0) \le wt(\Lambda_{n,j}) \le m.$$
4. *f is bent iff*
$$\sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}\,{}_n\mathcal{A}_{i,j} = \pm 2^{\frac{n}{2}} \textit{ for } 0 \le j \le g_n - 1.$$

Theorem 1. *The number of balanced RSBFs is exactly $2\pi_n$, where π_n is the number of partitions of the space V_n as $V_n = A_n \cup B_n$, where A_n and B_n have the same cardinal, and both include complete cycles of any length. Further, if $n = p$ is an odd prime, then the number of balanced RSBFs is $2 \cdot \binom{(2^p-2)/p}{(2^{p-1}-1)/p}$; if $n = p^a$ $(a > 1)$ and p is an odd prime, then the number of balanced RSBFs is $2 \cdot \pi_n$, with $\pi_n \geq \binom{x}{x/2} \cdot \prod_{i=1}^{a} \binom{x_i}{x_i/2}$, where $x_i = \dfrac{2^{p^i} - 2^{p^{i-1}}}{p^i}$, and*

$$x = p^{-a}\left(2^{p^a} + \sum_{j=1}^{a} \phi(p^j) \cdot 2^{p^{a-j}}\right) - \sum_{i=1}^{a} x_i - 2.$$

Proof. Using item 2 of Lemma 2, to determine balanced RSBFs, it suffices to find the RSBFs satisfying $\sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}{}_n\mathcal{A}_{i,0} = 0$. According to the definition ${}_n\mathcal{A}_{i,0} = \sum_{i=0}^{g_n-1}(-1)^{x\cdot\Lambda_{n,0}} = \#G_n(\Lambda_{n,i})$. Since the values of $(-1)^{f(\Lambda_{n,i})}$ are either ± 1, and f is constant on $G_n(v)$ for any v, we get the first claim.

If $n = p$ is prime, the number of long cycles is $h_p = \frac{2^p-2}{p}$ and the number of short cycles is 2 (the trivial ones) (see Subsection 2.1). Therefore, to partition $V_n = A_n \cup B_n$ (with A_n, B_n having the same number of elements), we need to place a short cycle in each of A_n, B_n, and the rest of $p \cdot h_p$ elements must be placed half in A_n and half in B_n (keeping together cycles). That can be done in $\binom{(2^p-2)/p}{(2^{p-1}-1)/p}$ ways. The second claim is proved.

If $n = p^a$ $(a > 1)$, the number of short cycles of length p^i (for any $i = 1, \ldots, a-1$) is $x_i = (2^{p^i} - 2^{p^{i-1}})/p^i$ (see Subsection 2.1). For each i, we can put half of the cycles in A_n, and half in B_n. The same can be done with the long cycles. Since the number of long cycles is x, the result is proved. $\square$

For example, consider the case for 4-variable balanced RSBFs. We have

$$V_4 = G_4(\Lambda_{4,0}) \cup G_4(\Lambda_{4,1}) \cup G_4(\Lambda_{4,2}) \cup G_4(\Lambda_{4,3}) \cup G_4(\Lambda_{4,4}) \cup G_4(\Lambda_{4,5}).$$

Now consider

$$W_4 = G_4(\Lambda_{4,0}) \cup G_4(\Lambda_{4,3}) \cup G_4(\Lambda_{4,5}).$$

Hence

$$V_4 = W_4 \cup G_4(\Lambda_{4,1}) \cup G_4(\Lambda_{4,2}) \cup G_4(\Lambda_{4,4}).$$

Therefore, a balanced RSBF must be 1 at the output corresponding to any two of $W_4, G_4(\Lambda_{4,1}), G_4(\Lambda_{4,2}), G_4(\Lambda_{4,4})$. Hence $\pi_4 = 3$ and there are 6 balanced RSBFs on 4-variables. The reason we do not exhaust all possibilities in the second part of the previous theorem is because we can get a different partition of V_n, satisfying the requirements, by placing more short cycles in A_n (or B_n) as long as one ends up with the same number of elements in A_n, B_n.

Note that we have defined $\rho_n^k(x_{i_1}x_{i_2}\cdots) = \rho_n^k(x_{i_1})\rho_n^k(x_{i_2})\cdots$ in Subsection 2.1. By abuse of notation let us denote

$$G_n(x_{i_1}x_{i_2}\ldots x_{i_l}) = \{\rho_n^k(x_{i_1}x_{i_2}\ldots x_{i_l}), \text{ for } 1 \leq k \leq n\}.$$

We select the representative element of $G_n(x_{i_1}x_{i_2}\ldots x_{i_l})$ as the lexicographically first element. As example, the representative element of $\{x_1x_2x_3,\ x_2x_3x_4,\ x_3x_4x_1,\ x_4x_1x_2\}$ is $x_1x_2x_3$. Note that it is also clear that the term x_1 will always exist in the lexicographically first element (the representative element).

We now define the *short algebraic normal form* (SANF) of an RSBF. An RSBF $f(x_1,\ldots,x_n)$ can be written as

$$a_0 + a_1x_1 + \sum a_{1j}x_1x_j + \ldots + a_{12\ldots n}x_1x_2\ldots x_n,$$

where the coefficients $a_0, a_1, a_{1j}, \ldots, a_{12\ldots n} \in \{0,1\}$, and the existence of a representative term $x_1x_{i_2}\ldots x_{i_l}$ implies the existence of all the terms from the set $G_n(x_1x_{i_2}\ldots x_{i_l})$ in the ANF. This representation of f is called the *short algebraic normal form* (SANF) of f. Note that the number of terms in each summation ($\sum$) corresponding to same degree terms depends on the number of short and long cycles.

As example consider the ANF of a 4-variable RSBF $x_1 + x_2 + x_3 + x_4 + x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2$. Its SANF is $x_1 + x_1x_2x_3$.

We can easily identify a monomial $x_{i_1}x_{i_2}\cdots x_{i_k}$ as a binary string of length n where the positions $i_1, i_2, \cdots, i_k$ contain '1' and the rest of the positions contain '0'. By abuse of notation we associate the n-bit patterns with monomials. It is clear that all the monomials in $G_n(\Lambda_{n,i})$ will either be present in the ANF or all of them will be absent if the Boolean function is rotation symmetric. Let us define another matrix ${}_n\mathcal{B}$ as

$${}_n\mathcal{B}_{i,j} = \bigoplus_{e \in G_n(\Lambda_{n,j})} e|_{\Lambda_{n,i}}.$$

That is, we take an RSBF (say h) with all the monomials coming from a single Rotation Symmetric group (say represented by $\Lambda_{n,j}$). Then we check what is the value of h at the representative input points $\Lambda_{n,i}$ and put that in the location ${}_n\mathcal{B}_{i,j}$ which contains either 0 or 1. Given ${}_n\mathcal{B}_{i,j}$ and the SANF of an RSBF, one can directly get the RSTT of the RSBF. The example for ${}_6\mathcal{B}$ is as follows.

$${}_6\mathcal{B} = \begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&1&0&0&0&0&0&0&0&0&0&0\\
1&1&0&1&1&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&1&0&0&0&0&0&0&0&0\\
1&1&1&1&0&1&1&0&0&0&0&0&0&0\\
1&1&1&1&0&1&0&1&0&0&0&0&0&0\\
1&0&1&0&0&1&1&1&1&0&0&0&0&0\\
1&1&0&1&0&0&0&0&0&1&0&0&0&0\\
1&0&0&1&1&1&1&1&0&1&1&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&1&0&0\\
1&1&0&0&1&0&1&1&0&1&0&1&1&0\\
1&0&0&0&0&1&0&0&0&0&0&1&0&1
\end{bmatrix}$$

Note that the matrices ${}_n\mathcal{A}$, ${}_n\mathcal{B}$ help to perform the search much faster than the naive Boolean function implementation.

3.1 Correlation Immune (CI) and Resilient RSBFs

We start our discussion with construction of 1st order CI RSBFs. Note that the second column of the matrix ${}_n\mathcal{A}$ is instrumental in the analysis of first order CI functions. From item 3 of Lemma 2 we get that f is 1st order CI if $\sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}\, {}_n\mathcal{A}_{i,j} = 0$ for $wt(\Lambda_{n,j}) = 1$, i.e., when $j = 1$, i.e., $\Lambda_{n,j} = \Lambda_{n,1}$. Note that ${}_n\mathcal{A}_{i,1} = \frac{(n-2wt(\Lambda_{n,i}))}{k}$ for cycles of length $\frac{n}{k}$, where $k\,(1 \leq k \leq n)$ is a divisor of n. See the second column of ${}_6\mathcal{A}$ as example. Thus we have the following result.

Theorem 2. *An n-variable Rotation Symmetric Boolean function f is 1st order CI iff $\sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}\frac{(n-2wt(\Lambda_{n,i}))}{k_i} = 0$, where $|G_n(\Lambda_{n,i})| = \frac{n}{k_i}$.*

Based on this we present the following enumerative result when n is prime.

Corollary 1. *There are at least $2\prod_{w=1}^{\frac{n-1}{2}}\sum_{k=0}^{g_{n,w}}\binom{g_{n,w}}{k}^2$ many 1st order CI RSBFs on n variables, where n is an odd prime. In this case, $g_{n,w} = \frac{\binom{n}{w}}{n}$.*

Proof. For n prime we know that $g_n = \frac{2^n-2}{n} + 2$. There are $\frac{2^n-2}{n}$ full cycles and two trivial short cycles (all zero and all one). Thus it is clear that ${}_n\mathcal{A}_{i,1} = n - 2wt(\Lambda_{n,i})$ for $1 \leq i \leq g_n - 2$ and ${}_n\mathcal{A}_{0,1} = 1$, ${}_n\mathcal{A}_{g_n-1,1} = -1$. Note that, ${}_n\mathcal{A}_{i_1,1} = -{}_n\mathcal{A}_{i_2,1}$, when $wt(\Lambda_{n,i_1}) = n - wt(\Lambda_{n,i_2})$. Now consider an assignment of 0 or 1 value at output corresponding to the $g_{n,w}$ classes where $wt(\Lambda_{n,i_1}) = w$. We have to put the same number of 0's and 1's corresponding to the $g_{n,n-w}$ classes where $wt(\Lambda_{n,i_2}) = n - w$. The two trivial cycles should also have the same value at the output, either both zero or both 1. This satisfies the condition that $\sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}\, {}_n\mathcal{A}_{i,1} = 0$, i.e., $W_f(\Lambda_{n,1}) = 0$, i.e., f is 1st order CI. Hence the number of possible options is $2 \times \prod_{w=1}^{\frac{n-1}{2}}(\sum_{k=0}^{g_{n,w}}\binom{g_{n,w}}{k}\cdot\binom{g_{n,w}}{k})$. □

Note that similar strategy can be exploited for higher order correlation immune or resilient RSBFs. However, in those cases, the analysis will be more involved.

3.2 A large subclass of RSBFs that are transformable to 1st order CI functions

We first investigate the independence of the vectors of a full cycle, i.e., the vectors in $G_n(\Lambda_{n,i})$ when $|G_n(\Lambda_{n,i})| = n$.

Lemma 3. *Consider the elements of $G_n(\Lambda_{n,i})$ for some i, where $|G_n(\Lambda_{n,i})| = n$. Let $\Lambda_{n,i} = (a_1, a_2, \ldots, a_n)$ of weight w and the positions of 1's in $\Lambda_{n,i}$ be $s_1 = 1, s_2, \ldots, s_w$. The vectors in $G_n(\Lambda_{n,i})$ are linearly dependent (over $\mathbf{Z}_2$) iff there is an n-th root of unity μ such that $1 + \mu^{s_2}\cdots + \mu^{s_w} = 0$, over $\mathbf{Z}_2$.*

Proof. The set $\{(a_1, a_2, \ldots, a_n), (a_n, a_1, \ldots, a_{n-1}), \ldots\}$ is linear dependent over $\mathbf{Z}_2$ if and only if the matrix

$$\mathrm{circ}(a_1, a_2, \ldots, a_n) = \begin{bmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ a_n & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \ldots & a_{n-2} \\ \vdots & & & & \vdots \\ a_2 & a_3 & a_4 & \ldots & a_1 \end{bmatrix}$$

has zero determinant over $\mathbf{Z}_2$. We observe that the matrix is circular and it is known that the determinant of a circular matrix is given by

$$\det(\mathrm{circ}(a_1, a_2, \ldots, a_n)) = \prod_{\mu} \left(a_1 + a_2\mu + a_3\mu^2 + \cdots + a_n\mu^{n-1}\right),$$

where the product runs over all the n number of n-th roots of unity. Since a_i's are 1 in the positions described by s_j's and 0 elsewhere, we get that

$$\det(\mathrm{circ}(a_1, a_2, \ldots, a_n)) = \prod_{\mu} \left(1 + \mu^{s_2} + \cdots + \mu^{s_w}\right),$$

which is zero if and only if one of the factors is zero, that is, iff there exists an n-th root of unity such that $1 + \mu^{s_2} \cdots + \mu^{s_w} = 0$ (over $\mathbf{Z}_2$). □

Corollary 2. *Take n arbitrary. If $wt(\Lambda_{n,i})$ is even, then the full cycle generated by $\Lambda_{n,i}$ is dependent.*

Proof. We have $\det(\mathrm{circ}(\Lambda_{n,i})) = \prod_{\mu} (1 + \mu^{s_2} + \cdots + \mu^{s_w}) = 0$, since $1 + \mu^{s_2} + \cdots + \mu^{s_w} = 0$ (in $\mathbf{Z}_2$), for $\mu = 1$ (which is an n-th root of unity, for any n). □

Now we present some examples. Take the cycle generated by $(1, 1, 0, 0)$ in V_4. The circular determinant is $\det(\mathrm{circ}(1, 1, 0, 0)) = \prod_{\mu} (1 + \mu) = 0$, since $\mu = -1$ is one of the 4-roots of unity. Another example is the cycle generated over V_6 by $(1, 1, 1, 0, 1, 0)$. We have $\det(\mathrm{circ}(1, 1, 1, 0, 1, 0)) = \prod_{\mu} \left(1 + \mu + \mu^2 + \mu^4\right) = 0$, since $\mu = 1$ (a 6-root of unity) satisfies $1 + \mu + \mu^2 + \mu^4 = 0$ over $\mathbf{Z}_2$. On the other hand, the full cycle generated in V_6 by $(1, 1, 0, 0, 1, 0)$ is linearly independent.

Corollary 3. *Let n be a positive integer, and p be the least odd prime occurring in the factorization of n. Take $\Lambda_{n,i}$ (a generator of a full cycle), of odd weight w and $s_w \leq p - 2$. Then the full cycle generated by $\Lambda_{n,i}$ is independent.*

Proof. As before, under the above conditions, if we have dependence, then there is an n-th root of unity μ, such that $P(\mu) = 0$, where $P(x) = x^{s_w} + \cdots + x^{s_2} + 1$. Since w is odd, $\mu \neq \pm 1$. There exists $k \,|\, n$ such that μ is a primitive k-th root of unity. Therefore, the cyclotomic polynomial $\Phi_k(x)$ divides $P(x)$ over $\mathbf{Z}_2$ (see [6], Ch. 2 & 3). If $k < p$, then it must be that k is a power of 2, say 2^l (since k is a divisor of n, and p is the least odd prime dividing n). But that is impossible, since then $\Phi_k(x)$ will divide $x^{2^l} - 1$, so (over $\mathbf{Z}_2$) $1 = \mu^{2^l} = \mu$. Therefore, $k \geq p$.

Assume $k = 2^l p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. If $r \geq 1$, then $p_i \geq p$, so $\phi(k) \geq \phi(p_i) = p_i - 1 \geq p - 1$. But the degree of $P(x)$ is at most $p-2$ and that of $\Phi_k(x)$ is greater than or equal to $p-1$. That is a contradiction. If $r = 0$, then $k = 2^l > p$, and the previous case's argument applies. □

Corollary 3 is the best we can get in that direction, as we see taking the cycles in V_{14} generated by $(1, 1, 1, 1, 1, 0, 0, 0, \ldots)$ and $(1, 1, 1, 1, 1, 1, 1, 0, \ldots)$. Now, the prime 7 is the least odd prime dividing $n = 14$. The weight w and s_w of the first generator is 5 and the cycle is independent; the weight w and s_w of the second generator is 7 and the cycle is dependent.

With the background of Lemma 3, Corollary 2 and Corollary 3 we present the following result.

Theorem 3. *Let f be an n-variable RSBF with $W_f(\Lambda_{n,j}) = 0$ for some j such that $G_n(\Lambda_{n,j})$ contains n independent vectors. Then the function f can be transformed to a 1st order correlation immune function g which may or may not be RSBF. Further if f is balanced, i.e., $W_f(\overline{0}) = 0$, then g is 1-resilient.*

Proof. Given the set of n independent vectors, at which the values of the Walsh spectra are 0, it is possible to apply linear transformation on the function f to get a function g which is 1st order correlation immune (using the methods of [8]). Note that, after the linear transformation, the Rotation Symmetric property of g is not guaranteed. □

Theorem 3 presents a simple method to get 1st order CI or 1-resilient functions easily from RSBFs satisfying some conditions. Moreover, the combinatorially interesting point is that the conditions are related to full rank of binary circulant matrices over $\mathbf{Z_2}$ and n-th roots of unity as described in Lemma 3.

3.3 Search for important functions

Recall the notation $g_{n,w}$ in Subsection 2.1. It is clear that for an RSBF, the $\binom{n}{w}$ many monomials of degree w are partitioned into $g_{n,w}$ many groups and the monomials of each group are either present or absent together. Now the search technique works as follows.

1. Choose a candidate RSBF (say f) represented by its SANF.
2. Use ${}_n\mathcal{B}$ to get the RSTT of f from the SANF.
3. Use ${}_n\mathcal{A}$ and the RSTT of f to analyze the Walsh Spectra of f.

Let us now consider the (8, 1, 6, 116) functions. These functions are of lot of interest as evident from [7, 1, 9]. Note that so far there was no evidence of $(8, 1, 6, 116)$ functions with PC(1) property. We here show that there are such functions in the RSBFs class. We consider $f(\overline{0}) = 0$, and there can not be any term of degree 7, 8 in the ANF. Thus we need to take any combination from $\sum_{i=1}^{5} g_{8,i}$ groups and at least one group from $g_{8,6}$ groups. This search space is of size $2^{\sum_{i=1}^{5} g_{8,i}}(2^{g_{8,6}} - 1)$. Note that $g_{8,1} = 1$, $g_{8,2} = g_{8,6} = 4$, $g_{8,3} = g_{8,5} =$

$7, g_{8,4} = 10$. Thus we need to search a space of size $2^{29}(2^4 - 1) \approx 2^{33}$ and the search needed little more than a day on a Pentium 1.6 GHz computer with 256 MB RAM using Linux 7.2 operating system. We searched the complete space and found 10272 such functions. The Δ_f (autocorrelation values) of the functions are 32 (2176 many), 40 (1024 many), 48 (128 many), 64 (6688 many) and 128 (256 many). Next we searched the set of these 10272 functions for the propagation property. There are 2672 such functions. The Δ_f (autocorrelation values) of the functions are 32 (384 many), 40 (256 many), 64 (1936 many) and 128 (96 many). Thus we have the following theorem.

Theorem 4. *There are* 10272 *many* $(8, 1, 6, 116)$ *RSBFs* f *with* $f(\overline{0}) = 0$. *Among them we have* 2672 *many* $(8, 1, 6, 116)$ *RSBFs which are also PC*(1) *and out of them* 384 *many functions have* Δ_f *value as low as* 32.

The following one is the truth table (in Hex) of an $(8, 1, 6, 116)$, PC(1) RSBF with $\Delta_f = 32$.

```
0055 6267 7d59 2d7a 3be6 32c3 4da2 3bcc
0f8b fd3c 5a49 b05a 31f6 c94c 5e9a e4a0
```

Next we concentrate on 9-variable functions. As we discuss, it will be clear that even if the search space is reduced, it is not possible to go for an exhaustive search. Thus we attempted heuristic search using simulated annealing. Note that the details of simulated annealing is not included in this paper and that has been published in [2].

Let us consider the (9, 2, 6, 240) functions with $f(\overline{0}) = 0$. There can not be any term of degree 7, 8, 9. Thus we need to take any combination from $\sum_{i=1}^{5} g_{9,i}$ groups and at least one group from $g_{9,6}$ groups. Now $g_{9,1} = 1$, $g_{9,2} = 4$, $g_{9,3} = g_{9,6} = 10$, $g_{9,4} = g_{9,5} = 14$. Thus the search space is of size $2^{\sum_{i=1}^{5} g_{9,i}}(2^{g_{9,6}} - 1) = 2^{43}(2^{10} - 1) \approx 2^{53}$. With the current computational facility this search would be extremely time consuming. Hence we attempted heuristic search in this case and succeeded to get such functions. Note that this function was posed as an important open question in [13, 14]. The best possible functions that have been achieved earlier [13] are $(9, 2, 6, 232)$ and $(9, 2, 5, 240)$, i.e., the first one has smaller nonlinearity (than the upper bound 240) when the algebraic degree was maximum and the second one has smaller algebraic degree (maximum upper bound 6) when the nonlinearity was maximum.

Next we consider the (9, 3, 5, 240) functions with $f(\overline{0}) = 0$. There can not be any term of degree 6, 7, 8, 9. Thus we need to take any combination from $\sum_{i=1}^{4} g_{9,i}$ groups and at least one group from $g_{9,5}$ groups. Thus the search space is of size $2^{\sum_{i=1}^{4} g_{9,i}}(2^{g_{9,5}} - 1) = 2^{29}(2^{14} - 1) \approx 2^{43}$. Though this search space is not extremely large, with our current implementation it is expected to take almost 3 years to complete the search on a single Pentium 1.6 GHz computer with 256 MB RAM using Linux 7.2 operating system. Hence we attempted heuristic search, but could not succeed. Instead we could achieve unbalanced $[9, 3, 5, 240]$ functions, which were also not known earlier.

4 Rotation Symmetric Bent Functions

Let us now discuss a sieving strategy for rots bent functions. Given the matrix ${}_n\mathcal{A}$, a rots bent function needs to satisfy item 5 of Lemma 2. Thus the idea is to get the RSTT of the function which can be seen as a column of g_n elements. Now one needs to calculate $\sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}\,{}_n\mathcal{A}_{i,j}$ and check whether this is equal to $\pm 2^{\frac{n}{2}}$ for $0 \leq j \leq g_n - 1$. The first time it fails for some j, we terminate checking that function and go for the next. This gives a very good performance for search strategies.

At the time of the search we can consider that $b(\overline{0}) = 0$ and the function is free from linear terms. Moreover, for a bent function, the maximum possible algebraic degree is $\frac{n}{2}$. Here the matrix ${}_n\mathcal{B}$ comes into play. We need to consider only those columns of ${}_n\mathcal{B}$ where $2 \leq wt(\Lambda_{n,j}) \leq \frac{n}{2}$. Then we choose all the linear combinations of those columns and then search for the bent functions. Thus the algorithm needs to check $2^{\sum_{i=2}^{\frac{n}{2}} g_{n,i}} - 1$ combinations as we ignore the all zero combination. Note that in this case once we get any $\sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}\,{}_n\mathcal{A}_{i,j}$ not equal to $\pm 2^{\frac{n}{2}}$ for $0 \leq j \leq g_n - 1$, then we need not check the function further for bentness and check the next function. Thus the process of sieving is much faster.

Filiol and Fontaine [4] counted all the bent functions b on 8-variables where $b(\overline{0}) = 0$ and b is free from linear terms. There are 3776 such functions and in total $3776 \times 4 = 15104$ many. With the matrices ${}_6\mathcal{A}$,${}_6\,\mathcal{B}$, and using our sieving method we need just one minute on a Pentium 1.6 GHz computer with 256 MB RAM using Linux 7.2 operating system. The number of functions to be checked is $2^{\sum_{i=2}^{4} g_{n,i}} - 1 = 2^{21} - 1$ for $n = 8$.

Note that, $g_{10} = 108$ and $g_{n,2} = 5$, $g_{n,3} = 12$, $g_{n,4} = 22$, $g_{n,5} = 26$. Thus the search required is $2^{65} - 1$ and with the current computational facility, it is not possible to exhaust this set easily. That is the reason some kind of heuristic search is required in this case and we found enough number of bent functions in each attempt using simulated annealing. We can also increase the speed of the algorithm by noting that there can not be any single cycle rots bent function of degree ≥ 3. In [15] it has been observed that up to 10-variables, there is no rotation symmetric homogeneous bent function with degree > 2 and it has been conjectured that it is true for any even n. Our result on single cycle rots bent functions provides a partial answer to that.

We have already denoted $V_n = \{0,1\}^n$. For a Boolean function $f : V_{2n} \to V_1$, let k_i $(i = 1, \ldots, 4)$ be the number of input bits 1 (i.e., x with $f(x) = 1$) in each of the quarters of f. If S is a bit string, by $(S)_u$ or S_u we shall mean the string obtained by concatenation of u copies of S. The concatenation of two strings u, v will be denoted by uv or $u|v$. Further, $\bar{h}$ is the complement of h, and for fixed integer d, $\hat{h}$ is equal to h (bit string in V_s) with the last 2^{s-d} bits of its truth table complemented. Let $A = 0,0,1,1;\ B = 0,1,0,1;\ C = 0,1,1,0;\ D = 0,0,0,0;\ U = 1,0,0,0;\ V = 0,0,0,1;\ X = 0,1,0,0;\ Y = 0,0,1,0$. The following result was a central proposition in [17].

Proposition 2. *Let $f : V_{2n} \to V_1$ be a bent Boolean function (not necessarily homogeneous) and the corresponding k_i $(i = 1, 2, 3, 4)$. Then (i) three of k_i's are equal and one is different, and (ii) $\min(k_1, k_2, k_3, k_4) \geq 2^{2n-3} - 2^{n-1}$.*

The following lemma (Lemma 11 of [3]) turns out to be quite useful. It gives the truth table of every monomial of arbitrary degree.

Lemma 4 ([3]). *The truth table of any monomial $x_{i_1} \cdots x_{i_s}$ of degree s is*

$$\begin{array}{ll}
\left(D_{2^{n-i_1-2}} \cdots \left(D_{2^{n-i_s-2}} \bar{D}_{2^{n-i_s-2}}\right)_{2^{i_s-i_{s-1}-1}}\right)_{2^{i_1-1}}, & \\
\textit{if } 1 \leq i_1 < \cdots < i_s \leq n-2, & \\
\left(D_{2^{n-i_1-2}} \cdots \left(D_{2^{n-i_{s-1}-2}} M_{2^{n-i_{s-1}-2}}\right)_{2^{i_{s-1}-i_{s-2}-1}}\right)_{2^{i_1-1}}, & (1) \\
\textit{where } M = A \textit{ or } B \textit{ if } i_s = n-1, \textit{ respectively } i_{s-1} < n-1 \textit{ and } i_s = n, & \\
\left(D_{2^{n-i_1-2}} \cdots \left(D_{2^{n-i_{s-2}-2}} V_{2^{n-i_{s-2}-2}}\right)_{2^{i_{s-2}-i_{s-3}-1}}\right)_{2^{i_1-1}}, & \\
\textit{if } i_{s-1} = n-1 \textit{ and } i_s = n. &
\end{array}$$

Theorem 5. *There are no homogeneous RSBFs with a single full cycle of degree $d \geq 3$ on V_n ($n \geq 6$ even) that are bent.*

Proof. Any full one-cycle RSBF is affinely equivalent to an RSBF f generated by $x_1 x_2 \ldots x_d$. We show now that the first quarter in the truth table of f has weight strictly less than $2^{2n-3} - 2^{n-1}$, thus contradicting Proposition 2. Therefore, f it is not bent.

An immediate application of Lemma 4 gives that, for $i \leq n-d-2$, the truth table of $x_i x_{i+1} \ldots x_{i+d} = \left(D_{2^{n-i-2}} \cdots (D_{2^{n-i-d-2}} \bar{D}_{2^{n-i-d-2}})\right)_{2^{i-1}}$, $x_{n-d} \cdots x_{n-2} x_{n-1} = (D_{2^{d-2}} \cdots (DA))_{2^{n-d-1}}$, and $x_{n-d+1} \cdots x_{n-1} x_n = (D_{2^{d-3}} \cdots (DV))_{2^{n-d}}$, therefore the first quarter of the truth table of f is given by the first quarter of

$$\begin{aligned}
& \sum_{i=1}^{n-d-2} \left(D_{2^{n-i-2}} \cdots (D_{2^{n-i-d-2}} \bar{D}_{2^{n-i-d-2}})\right)_{2^{i-1}} + (D_{2^{d-1}-1} A)_{2^{n-d-1}} \\
& + (D_{2^{d-2}-1} V)_{2^{n-d}} \\
& = \sum_{i=1}^{n-d-2} \left(D_{2^{n-i-1}-2^{n-i-d-2}} \bar{D}_{2^{n-i-d-2}}\right)_{2^{i-1}} + (D_{2^{d-2}-1} V D_{2^{d-2}-1} Y)_{2^{n-d-1}} \quad (2)
\end{aligned}$$

To see that it is so, observe that the only terms missing are $x_1 x_{n-d+2} \cdots x_{n-1} x_n + \cdots$. But all these contain $x_1 \cdots x_{n-1} x_n$. Therefore, in all the missing terms, $i_1 = 1, i_{s-1} = n-1, i_s = n$, so the last case of Lemma 4 implies that they all have 0 in the first quarter of their truth table, so all these terms do not contribute anything to the weight of the first quarter of f.

For easy writing, denote the first quarter in the truth table of f (on V_n) by h_d^{n-2}. Let $n = d+2$ and consider h_d^d. Since the first quarter of the truth table of f (on V_n), that is h_d^d, is obtained by taking the last two variables $x_{d+1} = x_{d+2} = 0$, and since the degree is d, it follows easily that h_d^d is nonzero only for $x_1 = x_2 = \cdots = x_d = 1$, that is, $h_d^d = D_{2^{d-2}-1} V$. Inductively on s, by using the displayed relation (2), we obtain the recurrence $h_d^s = h_d^{s-1}\hat{h}_d^{s-1}$ (write the displayed relation (2) for $s-1$ and s, and look at how the first quarter of that expression for s changes from the expression for $s-1$; this is why we needed the definition for $\hat{h}$, to explain that change). As example, let $d=3$, and f be the RSBF generated by $x_1x_2x_3$. Write $fq(f)$ for the first quarter of f. If $n=5$, then the RSTT of $fq(f) = 00000001 = DV$; if $n=6$, then $fq(f) = DV(\widehat{DV}) = DVDY$; if $n=7$, then $fq(f) = DVDY(\widehat{DVDY}) = DVDY\ DVD\overline{Y}$.

When d is fixed we shall write h_d^s as h^s. Using the recurrence and Maple (a trademark of *Waterloo Maple*) we obtained easily that the sequence of weights of h^n for the first few values of n, say $d \le n \le d+10$ is

n	d	$d+1$	$d+2$	$d+3$	$d+4$	$d+5$	$d+6$	$d+7$	$d+8$	$d+9$	$d+10$
$wt(h_d^n)$	1	2	6	14	32	72	156	336	712	1496	3120

(3)

Fixing d, and using the recurrence $h^s = h^{s-1}\hat{h}^{s-1}$, we get

$$h^s = h^{s-1}h^{s-2}h^{s-3}\bar{h}^{s-4}\hat{\bar{h}}^{s-4} \text{ and } \hat{h}^s = h^{s-1}h^{s-2}\bar{h}^{s-3}h^{s-4}\hat{h}^{s-4}.$$

Therefore, denoting by w^s the weight of h^s, and by $\hat{w}^s$ the weight of $\hat{h}^s$, we arrive at the identities $\hat{w}^s = 2w^{s-1} + 2w^{s-2} - w^s + 2^{s-2}$, and $w^s = w^{s-1} + \hat{w}^{s-1}$. We deduce ($s \ge 6$)

$$wt(h^s) = 2\left(wt(h^{s-2}) + wt(h^{s-3})\right) + 2^{s-3}. \tag{4}$$

Next we want to prove that $wt(h_d^s) < wt(h_3^s) < 2^{s-1} - 2^{\lfloor \frac{s+2}{2} \rfloor}$, $s \ge 5, d > 3$. From these inequalities we derive the theorem. The first inequality on weights follows easily from the recursive definition of h_d^s. The second inequality will be proved by induction. If $s=5$, then $wt(h_d^5) = 6 < 2^4 - 2^3 = 8$; if $s=6$, then $wt(h_d^6) = 14 < 2^5 - 2^4 = 16$; if $s=7$, then $wt(h_d^7) = 32 < 2^6 - 2^4 = 48$. They are certainly true. Assume the inequality true for all values from 5 to $n-1$. Now, for dimension n, $wt(h_d^{n-2}) = 2\left(wt(h^{n-4}) + wt(h^{n-5})\right) + 2^{n-5} \le 2\left(2^{n-5} - 2^{\lfloor \frac{n-2}{2} \rfloor} + 2^{n-6} - 2^{\lfloor \frac{n-3}{2} \rfloor}\right) + 2^{n-5} = 2^{n-3} - 2^{\lfloor \frac{n-2}{2} \rfloor + 1} - 2^{\lfloor \frac{n-3}{2} \rfloor + 1} < 2^{n-3} - 2^{\lfloor \frac{n}{2} \rfloor}$, since $2^{\lfloor \frac{n-2}{2} \rfloor + 1} + 2^{\lfloor \frac{n-3}{2} \rfloor + 1} > 2^{\lfloor \frac{n}{2} \rfloor}$. □

References

1. J. Clark, J. Jacob, S. Stepney, S. Maitra and W. Millan. Evolving Boolean Functions Satisfying Multiple Criteria. In *INDOCRYPT 2002*, Volume 2551 in Lecture Notes in Computer Science, pages 246–259, Springer Verlag, 2002.
2. J. Clark, J. Jacob, S. Maitra and P. Stanica. Almost Boolean Functions: The Design of Boolean Functions by Spectral Inversion. In *CEC 2003, the 2003 Congress on Evolutionary Computation*, Volume 3 in the proceedings, page 2173–2180, IEEE Press, December 8–12, 2003, Canberra, Australia.
3. T. W. Cusick and P. Stănică. Fast Evaluation, Weights and Nonlinearity of Rotation-Symmetric Functions. *Discrete Mathematics*, pages 289-301, vol 258, no 1-3, 2002.

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. X. Guo-Zhen and J. Massey. A spectral characterization of correlation immune combining functions. *IEEE Transactions on Information Theory*, 34(3):569–571, May 1988.
6. R. Lidl and H. Niederreiter. Introduction to finite fields and their applications. Cambridge University Press, 1994.
7. S. Maitra and E. Pasalic. Further constructions of resilient Boolean functions with very high nonlinearity. *IEEE Transactions on Information Theory*, 48(7):1825–1834, July 2002.
8. S. Maitra and P. Sarkar. Cryptographically significant Boolean functions with five-valued walsh spectra. *Theoretical Computer Science*, Volume 276, Number 1–2, pages 133-146, 2002.
9. S. Maity and T. Johansson. Construction of Cryptographically Important Boolean Functions. In *INDOCRYPT 2002*, Volume 2551 in Lecture Notes in Computer Science, pages 234–245, Springer Verlag, 2002.
10. E. Pasalic, S. Maitra, T. Johansson and P. Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bound on nonlinearity. In *Workshop on Coding and Cryptography - WCC 2001*, Paris, January 8–12, 2001. Electronic Notes in Discrete Mathematics, Volume 6, Elsevier Science, 2001.
11. J. Pieprzyk and C. X. Qu. Fast Hashing and Rotation-Symmetric Functions. *Journal of Universal Computer Science*, pages 20-31, vol 5, no 1 (1999).
12. B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of Boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, Lecture Notes in Computer Science, pages 161–173. Springer-Verlag, 1991.
13. P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology - EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pages 485–506. Springer Verlag, May 2000.
14. P. Sarkar and S. Maitra. Nonlinearity bounds and constuction of resilient Boolean functions. In Mihir Bellare, editor, *Advances in Cryptology - Crypto 2000*, pages 515–532, Berlin, 2000. Springer-Verlag. Lecture Notes in Computer Science Volume 1880.
15. 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, Volume 15.
16. P. Stănică and S. Maitra. A constructive count of Rotation Symmetric functions. *Information Processing Letters*, 88:299–304, 2003.
17. T. Xia, J. Seberry, J. Pieprzyk, C. Charnes. Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$. *Discrete Mathematics*, (to appear).
18. X-M. Zhang and Y. Zheng. GAC – the criterion for global avalanche characteristics of cryptographic functions. *Journal of Universal Computer Science*, 1(5):316–333, 1995.