Construction of Rotation Symmetric Boolean Functions with optimal Algebraic Immunity*

Construcción de Funciones Booleanas de Rotación Simétrica con Inmunidad Algebraica Óptima

Sumanta Sarkar[1] **and Subhamoy Maitra**[2]

[1] SECRET
INRIA Rocquencourt, B.P. 105
78153 Le Chesnay Cedex, FRANCE
sumanta.sarkar@inria.fr
[2] Applied Statistics Unit, Indian Statistical Institute,
203, B T Road, Calcutta 700 108, INDIA
subho@isical.ac.in

Article received on March 1, 2008, accepted on June 14, 2008

Abstract
In this paper, we present theoretical constructions of Rotation Symmetric Boolean Functions (RSBFs) on odd number of variables with the maximum possible algebraic immunity. To get high nonlinearity, we generalize our construction to a search technique in the RSBF class. We present RSBFs with the maximum algebraic immunity and high nonlinearity for odd number of variables. We also study the RSBFs on even number of variables for maximum algebraic immunity.
Keywords: Algebraic Immunity, Boolean Function, Nonlinearity, Nonsingular Matrix, Rotational Symmetry, Walsh Spectrum.

Resumen
En este artículo, presentamos construcciones teóricas de funciones Booleanas de rotación simétrica (RSBFs por sus siglas en inglés) con un número impar de variables y con máxima inmunidad algebraica. Con el objeto de obtener funciones Booleanas de muy alta no linealidad, generalizamos nuestra construcción a una técnica de búsqueda en la clase RSBF. Presentamos así RSBFs con inmunidad algebraica máxima y alta no linealidad para un número impar de variables, y también RSBFs con un número par de variables que exhiben inmunidad algebraica máxima.
Palabras Claves: Inmunidad algebraica, funciones Booleanas, no-linealidad, matrices no singulares, simetría rotacional, Espectro de Walsh.

1 Introduction

Algebraic attack has received a lot of attention recently in studying the security of stream ciphers as well as block ciphers (Armknecht 2004; Batten 2004; Braeken and Preneel 2005; Canteaut 2005; Cheon and Lee 2004; Cho and Pieprzyk 2004; Courtois and Pieprzyk 2002; Courtois and Meier 2003; Courtois 2003; Armknecht, Carlet, Gaborit, Künzli, Meier, and Ruatta 2006; Didier and Tillich 2006; Courtois, Debraize, and Garrido 2006). One necessary condition to resist this attack is that the function used in the cipher should have high Algebraic Immunity (AI). It is known (Courtois and Meier 2003) that for any n-variable function, the maximum possible AI is $\lceil \frac{n}{2} \rceil$.

So far, a few theoretical constructions of functions with optimal AI have been presented in the literature. In (Dalai, Gupta, and Maitra 2005), the first ever construction of functions with the maximum AI was proposed. Later, the construction of symmetric functions with the maximum AI was given in (Dalai, Maitra, and Sarkar 2006). For odd

*This is an extended and revised version of the paper (Sarkar and Maitra 2007).

number of input variables, majority functions are the examples of symmetric functions with the maximum AI. Recently in (Li and Qi 2006a), the idea of modifying symmetric functions to get other functions with the maximum AI has been proposed using the technique of (Dalai and Maitra 2006).

It is known that the class of n-variable symmetric functions forms a subclass of n-variable rotation symmetric functions. Therefore, all the symmetric functions with the maximum AI are also examples of RSBFs with the maximum AI. However, so far there has been no known construction method available which gives n-variable RSBFs having maximum AI which are not symmetric. It has been proved in (Li and Qi 2006b; Qu, Li, and Feng 2007), that the majority function (up to complementation) is the only possible symmetric function on odd number of variables which has the maximum AI. Hence, there is a need to get a theoretical construction method which provides new class of RSBFs with the maximum AI, which are not symmetric.

We present a construction (Construction 1) that provides RSBFs on odd number of variables (≥ 5) with the maximum AI, which are not symmetric. Note that up to 3 variables, RSBFs are all symmetric, and that is the reason we concentrate on $n \geq 5$. In this construction, the complement of n-variable majority function is considered and its outputs are toggled at the inputs of the orbits of size $\lfloor \frac{n}{2} \rfloor$ and $\lceil \frac{n}{2} \rceil$ respectively. These orbits are chosen in such a manner that a sub matrix associated to these points is nonsingular. This idea follows the work of (Dalai and Maitra 2006), where the sub matrix was introduced to reduce the complexity for determining AI of a function. We also show that the functions of this class have nonlinearity $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor} + 2$ which is better than $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$, the lower bound (Lobanov 2005) on nonlinearity of any n (odd) variable function with the maximum AI. Prior to this work (Sarkar and Maitra 2007), the general theoretical constructions (Dalai, Gupta, and Maitra 2005; Dalai, Maitra, and Sarkar 2006) could achieve this lower bound only. Later to the work (Sarkar and Maitra 2007), very recently in (Carlet, Zeng, Li, and Hu 2007), construction of n-variable functions with the maximum AI has been provided for odd n with good nonlinearity too.

Further, Construction 1 is generalized in Construction 2 which is further generalized in Construction 3. In each of the generalizations we release the restrictions on choosing orbits and achieve better nonlinearity of the constructed RSBFs with the maximum AI. We find RSBFs having nonlinearities equal to or slightly less than $2^{n-1} - 2^{\frac{n-1}{2}}$ for odd n, $7 \leq n \leq 11$.

Contributions discussed above cover up to Section 5 of the paper which were the main contributions of the paper (Sarkar and Maitra 2007). Section 6 is the new addition to the contributions provided in (Sarkar and Maitra 2007). In this section, we show how one can get a construction (Construction 4) of RSBFs (which are not symmetric) on even number of variables with the maximum AI from the construction given in (Dalai, Maitra, and Sarkar 2006, Construction 2). We also show that the nonlinearity of these functions is equal to $2^{n-1} - \binom{n-1}{\frac{n}{2}}$. This nonlinearity is equal to the nonlinearity of the functions constructed in Construction 2 of (Dalai, Maitra, and Sarkar 2006). We discuss the recent work (Carlet, Zeng, Li, and Hu 2007), where construction of functions with the maximum AI has been given for even number of variables. We show how RSBFs on even number variables with the maximum AI can be obtained from this construction. For $n \geq 8$, the nonlinearity of this class of RSBFs is equal to $2^{n-1} - \binom{n-1}{\frac{n}{2}} + 4$. We also present some generalizations of this construction.

2 Basics of Boolean functions

Let us denote $V_n = \{0,1\}^n$. An n-variable Boolean function f can be seen as a mapping $f : V_n \rightarrow V_1$. By truth table of a Boolean function on n input variables $(x_1, \ldots, x_n)$, we mean the 2^n length binary string

$$f = [f(0,0,\cdots,0), f(1,0,\cdots,0), f(0,1,\cdots,0), \ldots, f(1,1,\cdots,1)].$$

We denote the set of all n-variable Boolean functions as $\mathcal{B}_n$. Obviously $|\mathcal{B}_n| = 2^{2^n}$. The *Hamming weight* of a binary string T is the number of 1's in T, denoted by $wt(T)$. An n-variable function f is said to be *balanced* if its truth table contains an equal number of 0's and 1's, i.e., $wt(f) = 2^{n-1}$. Also, the *Hamming distance* between two

equidimensional binary strings T_1 and T_2 is defined by $d(T_1, T_2) = wt(T_1 \oplus T_2)$, where $\oplus$ denotes the addition over $GF(2)$. Support of f denoted by $supp(f)$ is the set of inputs $x \in V_n$ such that $f(x) = 1$.

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 $a_0, a_i, a_{ij}, \ldots, a_{12\ldots n} \in \{0, 1\}$. 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 $deg(f)$.

Let $x = (x_1, \ldots, x_n)$ and $\omega = (\omega_1, \ldots, \omega_n)$ both belonging to V_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 an integer valued function over V_n which is defined as

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

The Walsh spectrum of f is the multiset $\{W_f(\omega) | \omega \in V_n\}$. In terms of Walsh spectrum, the nonlinearity of f is given by

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

An n-variable Symmetric Boolean functions are the ones which are invariant under the action of the Symmetric group S_n on V_n, i.e., for $\mu, \nu \in V_n$, if $wt(\mu) = wt(\nu)$ then $f(\mu) = f(\nu)$. In (Dalai, Maitra, and Sarkar 2006), analysis of the Walsh spectra of the Symmetric functions has been done in terms of Krawtchouk polynomial. Krawtchouk polynomial (MacWilliams and Sloane 1977, Page 151, Part I) of degree i is given by $K_i(x, n) = \sum_{j=0}^{i} (-1)^j \binom{x}{j} \binom{n-x}{i-j}$, $i = 0, 1, \ldots, n$. It is known that for a fixed $\omega \in V_n$, such that $wt(\omega) = k$, $\sum_{wt(x)=i} (-1)^{\omega \cdot x} = K_i(k, n)$. Thus it can be checked that if f is an n-variable Symmetric function, then for $wt(\omega) = k$, $W_f(\omega) = \sum_{i=0}^{n} (-1)^{re_f(i)} K_i(k, n)$, where $re_f(i)$ is the value of f at an input of weight i. It is also known that for a symmetric function f on n variables and $\mu, \nu \in \{0, 1\}^n$, $W_f(\mu) = W_f(\nu)$, if $wt(\mu) = wt(\nu)$. Note that $K_i(k, n)$ is the (i, k)-th element of the Krawtchouk matrix (KR_M) of order $(n + 1) \times (n + 1)$. Thus Walsh spectrum of f can be determined as $(ref[0], \ldots, ref[n]) \times (KR_M[0], \ldots, KR_M[n])$, where each $KR_M[i]$, $(0 \leq i \leq n)$ is a column vector of KR_M.

A nonzero n-variable Boolean function g is called an annihilator of a n-variable Boolean function f if $f * g = 0$. We denote the set of all annihilators of f by $AN(f)$. Then algebraic immunity of f, denoted by $\mathcal{AI}_n(f)$, is defined (Meier, Pasalic, and Carlet 2004) as the degree of the minimum degree annihilator among all the annihilators of f or $1 \oplus f$, i.e., $\mathcal{AI}_n(f) = \min\{\deg(g) : g \neq 0,\ g \in AN(f) \cup AN(1 \oplus f)\}$. We repeat that the maximum possible algebraic immunity of f is $\lceil \frac{n}{2} \rceil$.

2.1 Rotation Symmetric Boolean Functions

We consider the action of the Cyclic group C_n on the set V_n. Let $x = (x_1, x_2, \ldots, x_{n-1}, x_n) \in V_n$ and $\rho_n^i \in C_n$, where $i \geq 0$. Then C_n acts on V_n as follows,

$$\rho_n^i(x_1, x_2, \ldots, x_{n-1}, x_n) = (x_{1+i}, x_{2+i}, \ldots, x_{n-1+i}, x_{n+i}),$$

where $k+i$ $(1 \leq k \leq n)$ takes the value $k+i \bmod n$ with the only exception that when $k+i \equiv 0 \bmod n$, then we will assign $k + i \bmod n$ by n instead of 0. This is to cope up with the input variable indices $1, \ldots, n$ for $x_1, \ldots, x_n$. An n-variable Boolean function f is called *Rotation Symmetric Boolean function (RSBF)* if it is invariant under the action of C_n, i.e., for each input $(x_1, \ldots, x_n) \in V_n$, $f(\rho_n^i(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n)$ for $1 \leq i \leq n - 1$. We denote the

orbit generated by $x = (x_1, \ldots, x_n)$ under this action as G_x, therefore, $G_x = \{\rho_n^i(x_1, \ldots, x_n) | 1 \leq i \leq n\}$ and the number of such orbits is denoted by g_n. Thus the number of n-variable RSBFs is 2^{g_n}. Let ϕ be Euler's *phi*-function, then it can be shown by Burnside's lemma that (see also (Stănică and Maitra 2008)) $g_n = \frac{1}{n}\sum_{k|n} \phi(k)\, 2^{\frac{n}{k}}$.

An *orbit* is completely determined by its *representative element* $\Lambda_{n,i}$, which is the lexicographically first element belonging to the orbit (Stănică, Maitra, and Clark 2004) and we define the weight of the orbit is exactly the same as weight of the representative element. These representative elements are again arranged lexicographically as $\Lambda_{n,0}, \ldots, \Lambda_{n,g_n-1}$. Note that for any n, $\Lambda_{n,0} = (0, 0, \ldots, 0)$ (the all zero input), $\Lambda_{n,1} = (0, 0, \ldots, 1)$ (the input of weight 1) and $\Lambda_{n,g_n-1} = (1, 1, \ldots, 1)$ (the all 1 input). Thus an n-variable RSBF f can be represented by the g_n length string $f(\Lambda_{n,0}), \ldots, f(\Lambda_{n,g_n-1})$ which we call RSTT of f and denote it by $RSTT_f$.

In (Stănică, Maitra, and Clark 2004) it was shown that the Walsh spectrum of an RSBF f takes the same value for all elements belonging to the same orbit, i.e., $W_f(u) = W_f(v)$ if $u \in G_v$. Therefore the Walsh spectrum of f can be represented by the g_n length vector $(wa_f[0], \ldots, wa_f[g_n])$ where $wa_f[j] = W_f(\Lambda_{n,j})$. In analyzing the Walsh spectrum of an RSBF, the ${}_n\mathcal{A}$ matrix has been introduced (Stănică, Maitra, and Clark 2004). The matrix ${}_n\mathcal{A} = ({}_n\mathcal{A}_{i,j})_{g_n \times g_n}$ is defined as

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

for an n-variable RSBF. Using this $g_n \times g_n$ matrix, the Walsh spectrum for an RSBF can be calculated as

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

3 Existing results related to annihilators

Let $V_n = \{0,1\}^n$. We take the degree graded lexicographic order "$<^{dgl}$" on the set of all monomials on n-variables $\{x_{m_1} \ldots x_{m_k} : 1 \leq k \leq n, 1 \leq m_1, \ldots, m_k \leq n\}$, i.e., $x_{m_1} x_{m_2} \ldots x_{m_k} < x_{r_1} x_{r_2} \ldots x_{r_l}$ if either $k < l$ or $k = l$ and there is $1 \leq p \leq k$ such that $m_k = r_k, m_{k-1} = r_{k-1}, \ldots, m_{p+1} = r_{p+1}$ and $m_p < r_p$. For example, for $n = 7$, $x_1x_3x_6 <^{dgl} x_1x_2x_4x_5$ and $x_1x_3x_7 <^{dgl} x_1x_4x_7$.

Let $v_{n,d}(x) = (m_1(x), m_2(x), \ldots, m_{\sum_{i=0}^{d}\binom{n}{i}}(x))$, where $m_i(x)$ is the i-th monomial as in the order ($<^{dgl}$) evaluated at the point $x = (x_1, x_2, \ldots, x_n)$.

Definition 1. *Given a function f on n-variables, let $M_{n,d}(f)$ be the $wt(f) \times \sum_{i=0}^{d}\binom{n}{i}$ matrix defined as*

$$ M_{n,d}(f) = \begin{bmatrix} v_{n,d}(P_1) \\ v_{n,d}(P_2) \\ \vdots \\ v_{n,d}(P_{wt(f)}) \end{bmatrix}, $$

where $0 \leq d \leq n$, $P_i \in supp(f)$, $1 \leq i \leq wt(f)$ and $P_1 <^{dgl} P_2 <^{dgl} \cdots <^{dgl} P_{wt(f)}$.

Let $f(x_1, \ldots, x_n)$ be an n-variable function and the n-variable function $g(x_1, \ldots, x_n)$ be an annihilator of f, i.e., $fg = 0$ for all $(x_1, \ldots, x_n) \in V_n$. That means,

$$ g(x_1, \ldots, x_n) = 0 \text{ if } f(x_1, \ldots, x_n) = 1. \tag{1} $$

If the degree of the function g is less than or equal to d, then the ANF of g is of the form

$$ g(x_1, \ldots, x_n) = a_0 + \sum_{i=0}^{n} a_i x_i + \cdots + \sum_{1 \leq i_1 < i_2 \cdots < i_d \leq n} a_{i_1 \ldots i_d} x_{i_1} \cdots x_{i_d}, $$

where $a_0, a_1, \ldots, a_{12}, \ldots a_{n-d+1,\ldots,n}$ are from $\{0,1\}$ not all zero. Then the relation 1 gives a homogeneous linear equation

$$a_0 + \sum_{i=0}^{n} a_i x_i + \cdots + \sum_{1 \le i_1 < i_2 \cdots < i_d \le n} a_{i_1 \ldots i_d} x_{i_1} \cdots x_{i_d} = 0, \tag{2}$$

with $a_0, a_1, \ldots, a_{12}, \ldots a_{n-d+1\ldots n}$ as variables for each input $(x_1, \ldots, x_n) \in supp(f)$ and thus, $wt(f)$ homogeneous linear equations in total. If this system of equations has a nonzero solution, then g having the coefficients in its ANF which is the solution of this system of equations is an annihilator of f of degree less than or equal to d. Note that in this system of equations $M_{n,d}(f)$ is the coefficient matrix. Then it is clear that if the rank of $M_{n,d}(f)$ is equal to $\sum_{i=0}^{d} \binom{n}{i}$, i.e., the number of variables, f does not posses any annihilator of degree d. If for $d = \lfloor \frac{n}{2} \rfloor$, both of f and $1 \oplus f$ do not have any annihilator of degree less than or equal to d, then f has the maximum algebraic immunity, $\lceil \frac{n}{2} \rceil$.

Theorem 1. *(Dalai and Maitra 2006) Let g be an n-variable function defined as $g(x) = 1$ if and only if $wt(x) \le d$ for $0 \le d \le n$. Then $M_{n,d}(g)^{-1} = M_{n,d}(g)$, i.e., $M_{n,d}(g)$ is a self inverse matrix.*

3.1 Existence of functions with the maximum AI on odd number of variables

We start this section with a few available results on n-variable functions with the maximum AI. Henceforth, we will consider the $<^{dgl}$ ordering of the inputs of V_n unless stated for odd n.

Proposition 1. *(Dalai, Gupta, and Maitra 2004) An odd variable function with the maximum* AI *must be balanced.*

Then we have the following result.

Proposition 2. *Let f be an n (odd) variable function. Then* AI *of f is $\lceil \frac{n}{2} \rceil$ if and only if f is balanced and $M_{n,\lfloor \frac{n}{2} \rfloor}(f)$ has full rank.*

We define the n (odd) variable function Q_n as follows

$$Q_n(x) \quad = \quad \begin{cases} 1 \text{ if } wt(x) \le \lfloor \frac{n}{2} \rfloor, \\ 0 \text{ if } wt(x) \ge \lceil \frac{n}{2} \rceil. \end{cases}$$

The function Q_n is a balanced symmetric function and it has been proved in (Dalai, Maitra, and Sarkar 2006) that this function has the maximum algebraic immunity, i.e., $\lceil \frac{n}{2} \rceil$. Then both of the matrices $M_{n,\lfloor \frac{n}{2} \rfloor}(Q_n)$ and $M_{n,\lfloor \frac{n}{2} \rfloor}(1 \oplus Q_n)$ are of the order $2^{n-1} \times 2^{n-1}$ and nonsingular. Now we take a look at a construction of an n-variable function having the maximum AI by modifying some outputs of Q_n.

Let $\{X_1, \ldots, X_{2^{n-1}}\}$ and $\{Y_1, \ldots, Y_{2^{n-1}}\}$ be the support of Q_n and $1 \oplus Q_n$ respectively. Suppose $X^j = \{X_{j_1}, \ldots, X_{j_k}\} \subset \{X_1, \ldots, X_{2^{n-1}}\}$ and $Y^i = \{Y_{i_1}, \ldots, Y_{i_k}\} \subset \{Y_1, \ldots, Y_{2^{n-1}}\}$ are two k-subsets. Construct the function F_n as

$$F_n(x) \quad = \quad \begin{cases} 1 \oplus Q_n(x), \text{ if } x \subset X^j \cup Y^i, \\ Q_n(x), \text{ otherwise.} \end{cases}$$

The next result follows from Proposition 2.

Proposition 3. *The function F_n has the maximum* AI *if and only if the two k-sets X^j and Y^i be such that $M_{n,\lfloor \frac{n}{2} \rfloor}(F_n)$ is nonsingular.*

This idea was first proposed in (Dalai and Maitra 2006) and using this idea, a few examples of functions on odd number of variables with the maximum AI have been demonstrated in (Li and Qi 2006a). However, this has not been studied in the domain of RSBFs.

Let's have a quick look at a result from linear algebra which is a consequence of the Steinitz Exchange Lemma (Kurosh 1955).

Theorem 2. *Let V be a vector space over the field F of dimension τ and $\{\alpha_1, \ldots, \alpha_\tau\}$ and $\{\beta_1, \ldots, \beta_\tau\}$ are two bases of V. Then for any k $(1 \leq k \leq \tau)$, there will be a pair of k-sets $\{\beta_{a_1}, \ldots, \beta_{a_k}\}$ and $\{\alpha_{b_1}, \ldots, \alpha_{b_k}\}$ such that the set $\{\alpha_1, \ldots, \alpha_\tau\} \cup \{\beta_{a_1}, \ldots, \beta_{a_k}\} \setminus \{\alpha_{b_1}, \ldots, \alpha_{b_k}\}$ will be a basis of V.*

The row vectors $v_{n,\lfloor \frac{n}{2} \rfloor}(X_1), \ldots, v_{n,\lfloor \frac{n}{2} \rfloor}(X_{2^{n-1}})$ of $M_{n,\lfloor \frac{n}{2} \rfloor}(Q_n)$ form a basis of the vector space $V_{2^{n-1}}$. Similarly the row vectors $v_{n,\lfloor \frac{n}{2} \rfloor}(Y_1), \ldots, v_{n,\lfloor \frac{n}{2} \rfloor}(Y_{2^{n-1}})$ of $M_{n,\lfloor \frac{n}{2} \rfloor}(1 \oplus Q_n)$ also form a basis of the vector space $V_{2^{n-1}}$. By finding two k-sets $\{v_{n,\lfloor \frac{n}{2} \rfloor}(X_{j_1}), \ldots, v_{n,\lfloor \frac{n}{2} \rfloor}(X_{j_k})\}$ and $\{v_{n,\lfloor \frac{n}{2} \rfloor}(Y_{i_1}), \ldots, v_{n,\lfloor \frac{n}{2} \rfloor}(Y_{i_k})\}$ (which always exist by Theorem 2), one can construct an n-variable function F_n with the maximum algebraic immunity if and only if the corresponding matrix $M_{n,\lfloor \frac{n}{2} \rfloor}(F_n)$ is nonsingular. Complexity of checking the nonsingularity of the matrix $M_{n,\lfloor \frac{n}{2} \rfloor}(F_n)$ is $O((\sum_{t=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{t})^3)$. However, this task can be done with lesser effort by forming a matrix, $W = M_{n,\lfloor \frac{n}{2} \rfloor}(1 \oplus Q_n) \times (M_{n,\lfloor \frac{n}{2} \rfloor}(Q_n))^{-1}$ and checking a sub matrix of it. Since $(M_{n,\lfloor \frac{n}{2} \rfloor}(Q_n))^{-1} = M_{n,\lfloor \frac{n}{2} \rfloor}(Q_n)$, then $W = M_{n,\lfloor \frac{n}{2} \rfloor}(1 \oplus Q_n) \times M_{n,\lfloor \frac{n}{2} \rfloor}(Q_n)$. We have the following proposition.

Proposition 4. *(Dalai and Maitra 2006) Let A be a nonsingular $m \times m$ binary matrix where the row vectors are denoted as $a_1, \ldots, a_m$. Let B be a $k \times m$ matrix, $k \leq m$, where the vectors are denoted as $b_1, \ldots, b_k$. Let $Z = BA^{-1}$, be a $k \times m$ binary matrix. Consider that a matrix A' is formed from A by replacing the rows $a_{i_1}, \ldots, a_{i_k}$ of A by the vectors $b_1, \ldots, b_k$. Further consider the $k \times k$ matrix Z' is formed by taking the j_1-th, j_2-th, …, j_k-th columns of Z. Then A' is nonsingular if and only if Z' is nonsingular.*

From the construction of F_n, it is clear that it is balanced. Now construct the matrix $W = M_{n,\lfloor \frac{n}{2} \rfloor}(1 \oplus Q_n) \times M_{n,\lfloor \frac{n}{2} \rfloor}(Q_n)$. Consider A to be the matrix $M_{n,\lfloor \frac{n}{2} \rfloor}(Q_n)$ and let B be the matrix formed by i_1-th, …, i_k-th rows of $M_{n,\lfloor \frac{n}{2} \rfloor}(1 \oplus Q_n)$ which are the row vectors $v_{n,\lfloor \frac{n}{2} \rfloor}(Y_{i_1}), \ldots, v_{n,\lfloor \frac{n}{2} \rfloor}(Y_{i_k})$ respectively. Replace the j_1-th, …, j_k-th rows of $M_{n,\lfloor \frac{n}{2} \rfloor}(Q_n)$ which are respectively the row vectors $v_{n,\lfloor \frac{n}{2} \rfloor}(X_{j_1}), \ldots, v_{n,\lfloor \frac{n}{2} \rfloor}(X_{j_k})$ by the rows of B and form the new matrix A'. Note that A' is exactly the $M_{n,\lfloor \frac{n}{2} \rfloor}(F_n)$ matrix. Let $W_{|Y^i| \times |X^j|}$ be the matrix formed by taking i_1-th, …, i_k-th rows and j_1-th, …, j_k-th columns of W. Then $M_{n,\lfloor \frac{n}{2} \rfloor}(F_n)$ is nonsingular if and only if $W_{|Y^i| \times |X^j|}$ is nonsingular. Thus, we have the following result.

Proposition 5. *The function F_n has the maximum algebraic immunity if and only if the sub matrix $W_{|Y^i| \times |X^j|}$ is nonsingular.*

The next proposition characterizes W.

Proposition 6. *(Dalai and Maitra 2006) The (q, p)-th element of the matrix W is given by*

$$W_{(q,p)} = \begin{cases} 0, \text{ if } WS(X_p) \not\subseteq WS(Y_q), \\ \sum_{t=0}^{\lfloor \frac{n}{2} \rfloor - wt(X_p)} \binom{wt(Y_q) - wt(X_p)}{t} \bmod 2, \text{ else}; \end{cases}$$

where $WS((x_1, \ldots, x_n)) = \{i : x_i = 1\} \subseteq \{1, \ldots, n\}$.

4 New class of RSBFs with the maximum AI for odd n

Proposition 7. *Given odd n, all the orbits G_μ generated by $\mu = (\mu_1, \ldots, \mu_n) \in V_n$ of weight $\lfloor \frac{n}{2} \rfloor$ or $\lceil \frac{n}{2} \rceil$ have n elements.*

Proof : From (Stănică and Maitra 2008), it is known that if $gcd(n, wt(\mu)) = 1$, then the orbit G_μ contains n elements. Since $gcd(n, \lfloor \frac{n}{2} \rfloor) = gcd(n, \lceil \frac{n}{2} \rceil) = 1$, the result follows.

Construction 1.

1. *Take odd $n \geq 5$.*
2. *Take an element $\mu \in V_n$ of weight $\lfloor \frac{n}{2} \rfloor$ and generate the orbit G_μ.*
3. *Choose an orbit G_ν by an element $\nu \in V_n$ of weight $\lceil \frac{n}{2} \rceil$ such that*

$$\textit{for each } x' \in G_\mu \textit{ there is a unique } y' \in G_\nu \textit{ where } WS(x') \subset WS(y').$$

4. *Construct*

$$R_n(x) = \begin{cases} Q_n(x) \oplus 1, \textit{ if } x \in G_\mu \cup G_\nu, \\ Q_n(x), \textit{ otherwise.} \end{cases}$$

We have the following theorem.

Theorem 3. *The function R_n is an n-variable RSBF with the maximum* AI.

Proof : R_n is obtained by toggling all outputs of Q_n corresponding to the inputs belonging to the two orbits G_μ and G_ν. Therefore, R_n is an RSBF on n variables. By Proposition 7, we have $|G_\mu| = |G_\nu|$. It is also clear that $Q_n(x) = 1$ for all $x \in G_\mu$ and $Q_n(x) = 0$ for all $x \in G_\nu$. So $wt(R_n) = 2^{n-1} - |G_\mu| + |G_\nu| = 2^{n-1}$. Thus, R_n is a balanced RSBF on n-variables.

Let us now investigate the matrix $W_{|G_\nu| \times |G_\mu|}$. We reorder the elements in G_μ and G_ν as $x^{(1)}, \ldots, x^{(|G_\mu|)}$ and $y^{(1)}, \ldots, y^{(|G_\nu|)}$ respectively where $WS(x^{(p)}) \subset WS(y^{(p)})$, for all $1 \leq p \leq |G_\mu| = |G_\nu|$. As $WS(x^{(p)}) \not\subseteq WS(y^{(q)})$ for all $q \in \{1, \ldots, |G_\nu|\} \setminus \{p\}$, then by Proposition 6, the value of $W_{(q,p)} = 0$, for all $q \in \{1, \ldots, |G_\nu|\} \setminus \{p\}$. Again by Proposition 6, the value of $W_{(p,p)}$ can be determined as

$$W_{(p,p)} = \sum_{t=0}^{\lfloor \frac{n}{2} \rfloor - wt(x^{(p)})} \binom{wt(y^{(p)}) - wt(x^{(p)})}{t} = \sum_{t=0}^{\lfloor \frac{n}{2} \rfloor - \lfloor \frac{n}{2} \rfloor} \binom{\lceil \frac{n}{2} \rceil - \lfloor \frac{n}{2} \rfloor}{t} = 1.$$

Thus, the matrix $W_{|G_\nu| \times |G_\mu|}$ is a diagonal matrix where all the diagonal elements are all equal to 1. Hence, $W_{|G_\nu| \times |G_\mu|}$ is nonsingular. Therefore, Theorem 5 implies that R_n has the maximum AI.

Example 1. *Take $n = 5$. Consider $\mu = (1,0,0,1,0)$ and $\nu = (1,0,0,1,1)$ and generate the orbits*

$$\begin{aligned} G_\mu &= \{(1,0,0,1,0), (0,1,0,0,1), (1,0,1,0,0), (0,1,0,1,0), (0,0,1,0,1)\} \textit{ and} \\ G_\nu &= \{(1,0,0,1,1), (1,1,0,0,1), (1,1,1,0,0), (0,1,1,1,0), (0,0,1,1,1)\}. \end{aligned}$$

Here, for each $x' \in G_\mu$, there is a unique $y' \in G_\nu$ such that $WS(x') \subset WS(y')$. Therefore, by Theorem 3, the function

$$R_n(x) = \begin{cases} Q_n(x) \oplus 1, \textit{ if } x \in G_\mu \cup G_\nu, \\ Q_n(x), \textit{ otherwise,} \end{cases}$$

is a 5-variable RSBF with the maximum AI 3.

It is known (Lobanov 2005) that for an n (odd) variable function f with the maximum AI, we have $nl(f) \geq 2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$. Therefore, nonlinearity of the function R_n will be at least $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$. Let us now examine the exact nonlinearity of R_n. In the rest of the paper, we denote an orbit representative for an n-variable RSBF by Λ^n for both odd and even n. We also consider the weight of an orbit as the weight of the elements it contains.

Theorem 4. *The nonlinearity of the function R_n is $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor} + 2$.*

Proof : As per the assumptions of Construction 1, $n \geq 5$ and it is odd; and weights of the orbits G_μ and G_ν are respectively $\lfloor \frac{n}{2} \rfloor$ and $\lceil \frac{n}{2} \rceil$. Now Q_n being a symmetric function, it is also an RSBF. So R_n can be viewed as a function, which is obtained by toggling the outputs of the RSBF Q_n corresponding to the orbit G_μ and G_ν. From (Dalai, Maitra, and Sarkar 2006), we know that $nl(Q_n) = 2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$. It is also known that the maximum absolute Walsh spectrum value of Q_n, i.e., $2\binom{n-1}{\lfloor \frac{n}{2} \rfloor}$ occurs at the inputs corresponding to the orbits of weight 1 and n. Note that when, $wt(\Lambda^n) = n$, the value of $W_{Q_n}(\Lambda^n)$ is $-2\binom{n-1}{\lfloor \frac{n}{2} \rfloor}$ or $2\binom{n-1}{\lfloor \frac{n}{2} \rfloor}$ according as $\lfloor \frac{n}{2} \rfloor$ is even or odd, and for $wt(\Lambda^n) = 1$, $W_{Q_n}(\Lambda^n) = -2\binom{n-1}{\lfloor \frac{n}{2} \rfloor}$.

Let us first find the relation between the values of $W_{R_n}(\Lambda^n)$ and $W_{Q_n}(\Lambda^n)$. We have

$$\begin{aligned}
W_{R_n}(\Lambda^n) &= \sum_{\zeta \in V_n \setminus \{G_\mu \cup G_\nu\}} (-1)^{R_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} + \sum_{\zeta \in G_\mu} (-1)^{R_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&\quad + \sum_{\zeta \in G_\nu} (-1)^{R_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&= \sum_{\zeta \in V_n \setminus \{G_\mu \cup G_\nu\}} (-1)^{Q_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} + \sum_{\zeta \in G_\mu} (-1)^{1 \oplus Q_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&\quad + \sum_{\zeta \in G_\nu} (-1)^{1 \oplus Q_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&= \sum_{\zeta \in V_n \setminus \{G_\mu \cup G_\nu\}} (-1)^{Q_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} - \sum_{\zeta \in G_\mu} (-1)^{Q_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&\quad - \sum_{\zeta \in G_\nu} (-1)^{Q_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&= \sum_{\zeta \in V_n} (-1)^{Q_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} - 2 \sum_{\zeta \in G_\mu} (-1)^1 (-1)^{\zeta \cdot \Lambda^n} - 2 \sum_{\zeta \in G_\nu} (-1)^0 (-1)^{\zeta \cdot \Lambda^n} \\
&= W_{Q_n}(\Lambda^n) + 2 \sum_{\zeta \in G_\mu} (-1)^{\zeta \cdot \Lambda^n} - 2 \sum_{\zeta \in G_\nu} (-1)^{\zeta \cdot \Lambda^n} \qquad (3)
\end{aligned}$$

Consider that $wt(\Lambda^n) = 1$. It can be proved that for any two orbits G_γ and G_δ of weight $\lfloor \frac{n}{2} \rfloor$ and $\lceil \frac{n}{2} \rceil$ respectively, $\sum_{\zeta \in G_\gamma} (-1)^{\zeta \cdot \Lambda} = 1$ and $\sum_{\zeta \in G_\delta} (-1)^{\zeta \cdot \Lambda} = -1$. Thus, $\sum_{\zeta \in G_\mu} (-1)^{\zeta \cdot \Lambda} = 1$ and $\sum_{\zeta \in G_\nu} (-1)^{\zeta \cdot \Lambda} = -1$. Therefore, from Equation 3 we get, $W_{R_n}(\Lambda^n) = -2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} + 4$.

Let us now check the Walsh spectrum value $W_{R_n}(\Lambda^n)$ for $wt(\Lambda^n) = n$. We do it in the following two cases.

CASE I: $\lfloor \frac{n}{2} \rfloor$ is even.

We have, $\sum_{\zeta \in G_\mu} (-1)^{\zeta \cdot \Lambda^n} = |G_\mu| = n$, since $\zeta \cdot \Lambda^n$ is $\lfloor \frac{n}{2} \rfloor$ which is even. Again for $\zeta \in G_\nu$, we have, $\zeta \cdot \Lambda^n = \lceil \frac{n}{2} \rceil$ which is odd, so $\sum_{\zeta \in G_\nu} (-1)^{\zeta \cdot \Lambda^n} = |G_\nu| = -n$. Therefore, from Equation 3, we get $W_{R_n}(\Lambda^n) = -2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} + 2n + 2n = -2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} + 4n$.

CASE II: $\lfloor \frac{n}{2} \rfloor$ is odd.

Using the similar argument as we have applied in the previous case, we can show that $\sum_{\zeta \in G_\mu} (-1)^{\zeta \cdot \Lambda^n} = -n$ and $\sum_{\zeta \in G_\nu} (-1)^{\zeta \cdot \Lambda^n} = n$. Then from Equation 3, we get $W_{R_n}(\Lambda^n) = 2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 2n - 2n = 2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 4n$.

Note that $2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} > 4n$, except for the case $n = 5$. Therefore, for both of the cases and for $n \geq 7$, $|W_{R_n}(\Lambda^n)| = 2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 4n$. Moreover, $2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 4n < 2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 4$, for $n \geq 7$. This implies that $|W_{R_n}(\Lambda^n)| \leq |W_{R_n}(\Delta^n)|$ for $n \geq 7$, where $\Delta^n \in V_n$ is an input of weight 1. For $n = 5$, $2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} = 12$ and thus, $W_{R_n}(\Lambda^n) = -8 = W_{R_n}(\Delta^n)$. Therefore, $|W_{R_n}(\Lambda^n)| \leq |W_{R_n}(\Delta^n)|$ for all $n \geq 5$.

Let us check the Walsh spectrum values of R_n at the other inputs, i.e., except inputs of weight 1 and n. For $n \geq 7$, the second maximum absolute value in the Walsh spectrum of Q_n occurs at the inputs of weight 3 and $n-2$. The exact value at weight 3 input is $\mathcal{C} = [\binom{n-3}{\frac{n-1}{2}} - 2\binom{n-3}{\frac{n-1}{2}-1} + \binom{n-3}{\frac{n-1}{2}-2}]$, whereas at the input of weight $n-2$, the exact value is $\mathcal{C}$ when $\lfloor \frac{n}{2} \rfloor$ is even and it is $-\mathcal{C}$ when $\lfloor \frac{n}{2} \rfloor$ is odd. Equation 3 implies that when $wt(\Lambda^n) = 3$ or $n-2$, $|W_{R_n}(\Lambda^n)|$ can attain value maximum up to $|W_{Q_n}(\Lambda^n)| + 4n$, i.e., $\binom{n-3}{\frac{n-1}{2}} - 2\binom{n-3}{\frac{n-1}{2}-1} + \binom{n-3}{\frac{n-1}{2}-2} + 4n$. But it is clear that, $\binom{n-3}{\frac{n-1}{2}} - 2\binom{n-3}{\frac{n-1}{2}-1} + \binom{n-3}{\frac{n-1}{2}-2} + 4n \leq 2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 4 = |W_{R_n}(\Delta^n)|$. Therefore, for all $n \geq 7$, the maximum absolute Walsh Spectrum value of R_n is $2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 4$.

For $n = 5$, it can be verified that for any choice of a pair of orbits G_μ and G_ν assumed in Construction 1, the absolute Walsh spectrum value of R_n, for all the inputs Λ^n of weight 3 is 8 which is equal to $|W_{R_n}(\Delta^n)|$.

Hence, $nl(R_n) = 2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor} + 2$.

5 Generalization of Construction 1

Construction 2. *Take orbits $G_{z_1}, \ldots, G_{z_k}$ with $Q_n(z_i) = 1$, for $z_i \in V_n, 1 \leq i \leq k$ and $G_{w_1}, \ldots, G_{w_l}$ with $Q_n(w_i) = 0$ for $w_i \in V_n, 1 \leq i \leq l$. Assume that,*

1. $\sum_{t=0}^{k} |G_{z_t}| = \sum_{t=0}^{l} |G_{w_t}|$.
2. *For each $x' \in \cup_{t=0}^{k} G_{z_t}$ there is a unique $y' \in \cup_{t=0}^{l} G_{w_t}$ s.t. $WS(x') \subset WS(y')$.*
3. $\sum_{t=0}^{\lfloor \frac{n}{2} \rfloor - wt(x')} \binom{wt(y')-wt(x')}{t}$ *is odd, for any $x' \in \cup_{t=0}^{k} G_{z_t}$ and corresponding $y' \cup_{t=0}^{l} G_{w_t}$ such that $WS(x') \subset WS(y')$. Then construct,*

$$R'_n(x) = \begin{cases} Q_n(x) \oplus 1, \text{ if } x \in \{\cup_{t=0}^{k} G_{z_t}\} \bigcup \{\cup_{t=0}^{l} G_{w_t}\} \\ Q_n(x), \text{ otherwise.} \end{cases}$$

Theorem 5. *The function R'_n is an n-variable RSBF with the maximum* AI.

Proof : Following the same argument as used in Theorem 3, we can show that the matrix $W_{|\cup_{t=0}^{k} G_{z_t}| \times |\cup_{t=0}^{l} G_{w_t}|}$ is diagonal whose diagonal elements are all equal to 1, i.e., it is nonsingular. This proves the theorem.

Example 2. *Let $n = 7$. Take $z_1 = (0,0,0,1,1,0,1), z_2 = (0,0,1,0,1,0,1)$ and $w_1 = (0,0,0,1,1,1,1), w_2 = (0,0,1,0,1,1,1)$ and generate the orbits*

$$\begin{aligned} G_{z_1} = \; & \{(0,0,0,1,1,0,1),(0,0,1,1,0,1,0),(0,1,1,0,1,0,0),(1,1,0,1,0,0,0), \\ & (1,0,1,0,0,0,1),(0,1,0,0,0,1,1),(1,0,0,0,1,1,0)\}; \end{aligned}$$

$$\begin{aligned} G_{z_2} = \; & \{(0,0,1,0,1,0,1),(0,1,0,1,0,1,0),(1,0,1,0,1,0,0),(0,1,0,1,0,0,1), \\ & (1,0,1,0,0,1,0),(0,1,0,0,1,0,1),(1,0,0,1,0,1,0)\}; \end{aligned}$$

$$\begin{aligned} G_{w_1} = \; & \{(0,0,0,1,1,1,1),(0,0,1,1,1,1,0),(0,1,1,1,1,0,0),(1,1,1,1,0,0,0), \\ & (1,1,1,0,0,0,1),(1,1,0,0,0,1,1),(1,0,0,0,1,1,1)\}; \end{aligned}$$

$$\begin{aligned} G_{w_2} = \; & \{(0,0,1,0,1,1,1),(0,1,0,1,1,1,0),(1,0,1,1,1,0,0),(0,1,1,1,0,0,1), \\ & (1,1,1,0,0,1,0),(1,1,0,0,1,0,1),(1,0,0,1,0,1,1)\}. \end{aligned}$$

Here for each $x' \in G_{z_1} \cup G_{z_2}$, there exists a unique $y' \in G_{w_1} \cup G_{w_2}$ such that $WS(x') \subset WS(y')$ and $\sum_{t=0}^{\lfloor \frac{n}{2} \rfloor - wt(x')} \binom{wt(y')-wt(x')}{t}$ is odd. Then construct,

$$R'_n(x) = \begin{cases} Q_n(x) \oplus 1, \text{ if } x \in \{G_{z_1} \cup G_{z_2}\} \bigcup \{G_{w_1} \cup G_{w_2}\} \\ Q_n(x), \text{ otherwise.} \end{cases}$$

Then by Theorem 5, R'_n is an 7-variable RSBF with the maximum AI 4.

As in Construction 2, outputs of Q_n are toggled at more inputs, one can expect better nonlinearity than the Construction 1.

For 7-variable functions with the maximum AI, the lower bound on nonlinearity is 44 (Lobanov 2005) and that is exactly achieved in the existing theoretical construction (Dalai, Gupta, and Maitra 2005; Dalai, Maitra, and Sarkar 2006). Our Construction 1 provides the nonlinearity 46. Further we used Construction 2 to get all possible functions R'_n and they provide the nonlinearity 48.

5.1 Further generalization

Construction 3. *Take $n \geq 5$ and odd. Consider the orbits $G_{z_1}, \ldots, G_{z_k}$ and $G_{w_1}, \ldots, G_{w_k}$ such that the sub matrix $W_{|\cup_{t=0}^{k} G_{z_t}| \times |\cup_{t=0}^{l} G_{w_t}|}$ is nonsingular. Then construct,*

$$R''_n(x) = \begin{cases} Q_n(x) \oplus 1, \text{ if } x \in \{\cup_{t=0}^{k} G_{z_t}\} \bigcup \{\cup_{t=0}^{l} G_{w_t}\} \\ Q_n(x), \text{ otherwise.} \end{cases}$$

Clearly, the function R''_n is an n-variable RSBF with the maximum AI. Construction 3 will provide all the RSBFs with the maximum AI. In this case we need a heuristic to search through the space of RSBFs with the maximum AI as the exhaustive search may not be possible as the number of input variables n increases. One may note that it is possible to use these techniques to search through the space of general functions, but that space is much larger (2^{2^n}) in comparison with the space of RSBFs $(\approx 2^{\frac{2^n}{n}})$ and getting high nonlinearity after a small amount of search using a heuristic is not expected. We present a simple form of heuristic as follows that we run for several iterations.

1. Start with an RSBF having the maximum AI using Construction 1.

2. Choose two orbits of the same sizes having different output values and toggle the outputs corresponding to both the orbits (this is to keep the function balanced).

3. If the modified function has the maximum AI and having better nonlinearity than the previous ones, then we store that as the best function.

By this heuristic, we achieved 7, 9, 11 variable RSBFs with the maximum possible AI having nonlinearities 56, 240, 984 respectively with very small amount of search. Note that these nonlinearities are either equal or close to $2^{n-1} - 2^{\frac{n-1}{2}}$.

Later to the work (Sarkar and Maitra 2007), a construction has been shown in (Carlet, Zeng, Li, and Hu 2007) for Boolean functions (in general, i.e., not in RSBF class) on odd number of variables with good nonlinearity and the construction works for higher number of variables, i.e., for odd $n \geq 15$. The nonlinearity is given as (Carlet, Zeng, Li, and Hu 2007, Theorem 4.4) $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor} + \Theta(n)$, where the value of $\Theta(n)$ is as follows. $\Theta(n) = 2\lfloor \sum_{i=0}^{k-1} \binom{3k-2}{k+i-1} \frac{k-i}{k} \rfloor$ for $n = 4k+1, k \geq 4$ and $2\lfloor \sum_{i=0}^{k+1} \binom{3k-1}{k+i} \frac{k+2-i}{k+2} \rfloor$ for $n = 4k+3, k \geq 5$. Further, $\Theta(15) = 268$ and $\Theta(19) = 2436$. One should note that the nonlinearity of 15-variable function with the maximum AI is $16384 - 3432 + 268 = 13220$ in (Carlet, Zeng, Li, and Hu 2007), but a much sharper search result is available which gives nonlinearity 16272 (Sarkar and Maitra 2008).

6 RSBFs with the maximum AI on even number of variables

Let us start with an existing construction of functions with the maximum AI for even number of variables n provided in (Dalai, Maitra, and Sarkar 2006, Construction 2).

$$\begin{aligned} P_n(x) &= 1 \text{ for } wt(x) < \frac{n}{2}, \\ &= 0 \text{ for } wt(x) > \frac{n}{2}, \\ &= c_x \in \{0,1\} \text{ for } wt(x) = \frac{n}{2}. \end{aligned}$$

This construction directly gives a construction of an n-variable symmetric function (Dalai, Maitra, and Sarkar 2006) with the maximum AI for even n as follows.

$$\begin{aligned} S_n(x) &= 1 \text{ for } wt(x) \leq \frac{n}{2}, \\ &= 0 \text{ for } wt(x) > \frac{n}{2}. \end{aligned}$$

From P_n, we can also get a construction of n-variable RSBFs (which are not symmetric) with the maximum AI for even n. Since all the n-variable RSBFs are also symmetric for $n \leq 3$, we consider even $n \geq 4$.

Construction 4.

1. *Take $n \geq 4$ and even.*
2. *Let G_λ be any orbit generated by $\lambda \in V_n$ such that $wt(\lambda) = \frac{n}{2}$.*
3. *Construct*

$$H_n(x) = \begin{cases} S_n(x) \oplus 1, \text{ if } x \in G_\lambda, \\ S_n(x), \text{ otherwise.} \end{cases}$$

It is clear that H_n is RSBF and not symmetric.

Theorem 6. *The function H_n is an n-variable RSBF with the maximum* AI.

Proof : Since P_n can have any output corresponding to all the inputs of weight $\frac{n}{2}$, the proof follows.

In Theorem 7, we analyze the nonlinearity of the function H_n. First we need the following lemma.

Lemma 1. *Let n be even and G_x be the orbit generated by $x \in V_n$ such that $wt(x) = \frac{n}{2}$. Then the number of occurrence of 1's and 0's at any coordinate position among all the elements of G_x are the same.*

Proof : The orbits generated by the elements of weight $\frac{n}{2}$ can be divided into two classes, say, C_1 and C_2. Let C_1 contains orbits such that the complement of each of the elements in an orbit situates in the same orbit, otherwise the orbits are in C_2. The proof is clear if $G_x \in C_1$.

Next we consider that G_x belongs to C_2 and contains n number of elements. Since x has n different cyclic permutations in G_x, then each bit of x appears exactly once at any fixed coordinate position among all the elements of G_x. Since, $wt(x) = \frac{n}{2}$, the proof follows.

Finally we consider that G_x belongs to C_2 and contains $k < n$ elements. One may note that $k|n$ and k is even. Now in x, all the adjacent $\frac{n}{k}$-blocks (each of length k) will be the same. Since $wt(x) = \frac{n}{2}$, the proof follows.

Therefore, according to this lemma, for an orbit of weight $\frac{n}{2}$, the number of occurrence of $1'$s and $0'$s in any coordinate position among all the elements are equal to $\frac{n}{2}$. For example, for $n = 4$, we take the following orbit $\{(0,0,1,1),(0,1,1,0),(1,1,0,0),(1,0,0,1)\}$. Consider the last coordinate position. The number of occurrence of 1's in the last coordinate position is 2. It is clear that for this orbit, this happens for any coordinate position.

Theorem 7. *The nonlinearity of the function H_n is $2^{n-1} - \binom{n-1}{\frac{n}{2}}$.*

Proof : It is known from (Dalai, Maitra, and Sarkar 2006) that $nl(S_n) = 2^{n-1} - \binom{n-1}{\frac{n}{2}}$. Moreover, the maximum absolute Walsh spectrum value occurs at the inputs of weight zero, one and n and the value is $\binom{n}{\frac{n}{2}}$.

First we find the relation between the Walsh spectrum values of H_n and S_n. We have,

$$\begin{aligned}
W_{H_n}(\Lambda^n) &= \sum_{\zeta \in V_n \setminus G_\lambda} (-1)^{H_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} + \sum_{\zeta \in G_\lambda} (-1)^{H_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&= \sum_{\zeta \in V_n \setminus G_\lambda} (-1)^{S_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} + \sum_{\zeta \in G_\lambda} (-1)^{1 \oplus S_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&= \sum_{\zeta \in V_n \setminus G_\lambda} (-1)^{S_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} - \sum_{\zeta \in G_\lambda} (-1)^{S_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&= \sum_{\zeta \in V_n} (-1)^{S_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} - 2 \sum_{\zeta \in G_\lambda} (-1)^1 (-1)^{\zeta \cdot \Lambda^n} \\
&= W_{S_n}(\Lambda^n) + 2 \sum_{\zeta \in G_\lambda} (-1)^{\zeta \cdot \Lambda^n} \qquad (4)
\end{aligned}$$

Now we investigate the values of $W_{H_n}(\Lambda^n)$ for different weights of Λ^n.

CASE I: $wt(\Lambda^n) = 0$.

From (Dalai, Maitra, and Sarkar 2006), we have, $W_{S_n}(\Lambda^n) = -\binom{n}{\frac{n}{2}}$. Since, $|G_\lambda| \leq n$, the maximum value that can be attained by $\sum_{\zeta \in G_\lambda} (-1)^{\zeta \cdot \Lambda^n}$ is n. Therefore, $|W_{H_n}(\Lambda^n)| \leq -\binom{n}{\frac{n}{2}} + 2n$, if $\binom{n}{\frac{n}{2}} \leq 2n$ and $|W_{H_n}(\Lambda^n)| \leq \binom{n}{\frac{n}{2}} - 2n$, otherwise.

CASE II: $wt(\Lambda^n) = n$.

From (Dalai, Maitra, and Sarkar 2006), it is known that $W_{H_n}(\Lambda^n) = \mp\binom{n}{\frac{n}{2}}$ according as $\frac{n}{2}$ is even or odd. If $\frac{n}{2}$ is even, the scaler product $\zeta \cdot \Lambda^n$ will be even for all $\zeta \in G_\lambda$ and hence, the maximum value that $\sum_{\zeta \in G_\lambda} (-1)^{\zeta \cdot \Lambda^n}$ can attain is n. Therefore, $|W_{H_n}(\Lambda^n)| \leq -\binom{n}{\frac{n}{2}} + 2n$, if $\binom{n}{\frac{n}{2}} \leq 2n$ and $|W_{H_n}(\Lambda^n)| \leq \binom{n}{\frac{n}{2}} - 2n$, otherwise.

If $\frac{n}{2}$ is odd, the scaler product $\zeta \cdot \Lambda^n$ will be odd for all $\zeta \in G_\lambda$ and hence, the minimum value that $\sum_{\zeta \in G_\lambda} (-1)^{\zeta \cdot \Lambda^n}$ can attain is $-n$. Therefore, $|W_{H_n}(\Lambda^n)| \leq \binom{n}{\frac{n}{2}} - 2n$, if $\binom{n}{\frac{n}{2}} \geq 2n$ and $|W_{H_n}(\Lambda^n)| \leq -\binom{n}{\frac{n}{2}} + 2n$, otherwise.

CASE III: $wt(\Lambda^n) = 1$.

From Lemma 1, we have $\sum_{\zeta \in G_\lambda} (-1)^{\zeta \cdot \Lambda^n} = -\frac{n}{2} + \frac{n}{2} = 0$. Therefore, $W_{H_n}(\Lambda^n) = \binom{n}{\frac{n}{2}}$.

CASE IV: $2 \leq wt(\Lambda^n) \leq n - 1$.

From (Dalai, Maitra, and Sarkar 2006), it is known that, the second maximum value of W_{S_n} is attained at the inputs of weights $2, 3, n-2$ and $n-1$ respectively and that value is equal to $\frac{1}{n-1} \cdot \binom{n}{\frac{n}{2}}$. Since, $|G_\lambda| \leq n$, toggling outputs of S_n at the orbit G_λ can increase the absolute value at most by $2n$. However, it can be checked that $\frac{1}{n-1} \cdot \binom{n}{\frac{n}{2}} + 2n \leq \binom{n}{\frac{n}{2}}$ for $n \geq 6$.

Therefore, for $n \geq 6$, the maximum absolute value of W_{H_n} is $\binom{n}{\frac{n}{2}}$.

For $n = 4$, it can be checked from the corresponding Walsh spectrum matrix is that the maximum absolute value of W_{H_n} is also $\binom{n}{\frac{n}{2}}$.

Hence, for $n \geq 4$, the maximum absolute value of W_{H_n} is $\binom{n}{\frac{n}{2}}$ and $nl(H_n) = 2^{n-1} - \frac{1}{2}\binom{n}{\frac{n}{2}} = 2^{n-1} - \binom{n-1}{\frac{n}{2}}$.

Note that the nonlinearity of H_n is equal to that of S_n.

As per the construction of P_n, for toggling outputs of S_n at any number of orbits of weight $\frac{n}{2}$, AI will not drop. Moreover, for each modified functions, nonlinearity would be the same, which follows from the proof of Theorem 7.

Very recently in (Carlet, Zeng, Li, and Hu 2007), construction of functions with the maximum AI has been given for even number of variables n. Let W^d be the set of all elements of $\{0,1\}^n$ with weight d and $W^{<d} = W^0 \cup W^1 \cup \ldots \cup W^{d-1}$ and $W^{>d} = W^{d+1} \cup W^{d+2} \cup \ldots \cup W^n$. Let $T = \{\alpha_1, \ldots, \alpha_l\} \subseteq W^{<\frac{n}{2}}, S = \{\beta_1, \ldots, \beta_s\} \subseteq W^{>\frac{n}{2}}, U = \{u_1, \ldots, u_l\} \subseteq W^{\frac{n}{2}}$ and $V = \{v_1, \ldots, v_s\} \subseteq W^{\frac{n}{2}}$. Then the construction is as follows.

Construction 5.

1. *Choose T, S, U, V such that*

$$\begin{array}{l} U \cap V = \emptyset, \\ \forall\, 1 \le i \le l, WS(\alpha_i) \subset WS(u_i) \quad and \quad \forall\, 1 \le j < i \le l, WS(\alpha_i) \not\subset WS(u_j), \\ \forall\, 1 \le i \le s, WS(v_i) \subset WS(\beta_i) \quad and \quad \forall\, 1 \le j < i \le s, WS(v_i) \not\subset WS(\beta_j). \end{array}$$

2. *Construct*

$$I_n(x) \quad = \quad \begin{cases} 0, \text{ if } x \in W^{<\frac{n}{2}} \cup S \cup U \setminus T, \\ c_x, \text{ if } x \in W^{\frac{n}{2}} \setminus U \cup V, \\ 1, \text{ if } x \in W^{>\frac{n}{2}} \cup T \cup V \setminus S, \end{cases}$$

where $c_x \in \{0,1\}$.

In the following construction, we show how n-variable RSBFs with the maximum AI for even n can be obtained using Construction 5. Let $\overline{A} = \{\overline{x} | x \in A\}$, then $\overline{G_\alpha} = \{\overline{x} | x \in G_\alpha\} = G_{\overline{\alpha}}$.

Construction 6.

1. *Choose $\alpha_1 \in W^{\frac{n}{2}-1}$.*
2. *Choose $u_1 \in W^{\frac{n}{2}}$ such that*
   - *(a) $|G_{\alpha_1}| = |G_{u_1}|$,*
   - *(b) $\overline{u_1} \notin G_{u_1}$ and*
   - *(c) $WS(\alpha_1) \subset WS(u_1)$.*
3. *Construct*

$$I'_n(x) \quad = \quad \begin{cases} 0, \text{ if } x \in W^{<\frac{n}{2}} \cup \overline{G_{\alpha_1}} \cup G_{u_1} \setminus G_{\alpha_1}, \\ 0 \text{ if } x \in W^{\frac{n}{2}} \setminus G_{u_1} \cup \overline{G_{u_1}}, \\ 1, \text{ if } x \in W^{>\frac{n}{2}} \cup G_{\alpha_1} \cup \overline{G_{u_1}} \setminus \overline{G_{\alpha_1}}. \end{cases}$$

For $n = 4$, it is not possible to get such pair of orbits G_{α_1} and G_{u_1} which satisfy all the conditions of Construction 6. So we have the following preposition.

Proposition 8. *The function I'_n is an n-variable function with the maximum* AI *for $n \ge 6$.*

Proof : Since, $wt(\alpha_1) = \frac{n}{2} - 1$, $wt(u_1) = \frac{n}{2}$ and $WS(\alpha_1) \subset WS(u_1)$, the sets $G_{\alpha_1}, G_{u_1}, \overline{G_{u_1}}$ and $\overline{G_{\alpha_1}}$ have the property as required by for the sets T, U, V, S in Construction 6. This proves the result.

Example 3. *Let $n = 8$. Take $\alpha_1 = (0,0,0,1,0,0,1,1)$ and $u_1 = (0,0,0,1,0,1,1,1)$. Form the orbits $G_{\alpha_1}, G_{u_1}, \overline{G_{\alpha_1}}$ and $\overline{G_{u_1}}$. Then construct I'_n as in Construction 6. I'_n will have the maximum* AI.

Though the proposition works for $n \geq 6$, the following theorem is valid for $n \geq 8$ only. For $n = 6$, nonlinearity obtained for the RSBFs from Construction 6 are 18 and 22 respectively.

Theorem 8. *For $n \geq 8$, the nonlinearity of I'_n is $2^{n-1} - \binom{n-1}{\frac{n}{2}} + 4$.*

Proof : The function I'_n is the function obtained from $1 \oplus S_n$ by complementing its outputs corresponding to the inputs which belong to the orbits $G_{\alpha_1}, \overline{G_{\alpha_1}}$ and $G_{\overline{u_1}}$ respectively. We have,

$$\begin{aligned}
W_{I'_n}(\Lambda^n) &= \sum_{\zeta \in V_n \setminus G_{\alpha_1} \cup \overline{G_{u_1}} \cup \overline{G_{\alpha_1}}} (-1)^{I'_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} + \sum_{\zeta \in G_{\alpha_1}} (-1)^{I'_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&= \sum_{\zeta \in V_n} (-1)^{1 \oplus S_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} + \sum_{\zeta \in G_{\alpha_1}} (-1)^{I'_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&\quad + \sum_{\zeta \in \overline{G_{u_1}}} (-1)^{I'_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} + \sum_{\zeta \in \overline{G_{\alpha_1}}} (-1)^{I'_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&\quad - \sum_{\zeta \in G_{\alpha_1}} (-1)^{1 \oplus S_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&\quad - \sum_{\zeta \in \overline{G_{u_1}}} (-1)^{1 \oplus S_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} - \sum_{\zeta \in \overline{G_{\alpha_1}}} (-1)^{1 \oplus S_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&= \sum_{\zeta \in V_n} (-1)^{1 \oplus S_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} + 2[\sum_{\zeta \in G_{\alpha_1}} (-1)^{I'_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} \\
&\quad + \sum_{\zeta \in \overline{G_{u_1}}} (-1)^{I'_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n} + \sum_{\zeta \in \overline{G_{\alpha_1}}} (-1)^{I'_n(\zeta)} (-1)^{\zeta \cdot \Lambda^n}] \\
&\quad (\text{ since } I'_n(\zeta) = 1 \oplus S_n(\zeta) \text{ for } \zeta \in G_{\alpha_1} \cup \overline{G_{\alpha_1}} \cup \overline{G_{u_1}}) \\
&= W_{1 \oplus S_n}(\Lambda^n) + 2[\sum_{\zeta \in \overline{G_{\alpha_1}}} (-1)^{\zeta \cdot \Lambda^n} - \sum_{\zeta \in G_{\alpha_1}} (-1)^{\zeta \cdot \Lambda^n} - \sum_{\zeta \in \overline{G_{u_1}}} (-1)^{\zeta \cdot \Lambda^n}]
\end{aligned} \tag{5}$$

From (Dalai, Maitra, and Sarkar 2006), we know that $nl(1 \oplus S_n) = 2^{n-1} - \binom{n-1}{\frac{n}{2}}$. Moreover, the maximum absolute Walsh spectrum value occurs at the inputs of weight zero, one and n and the value is $\binom{n}{\frac{n}{2}}$.

Following results are required for the analysis of the Walsh spectrum of I'_n. Since, $wt(\alpha_1) = \frac{n}{2} - 1$, $wt(u_1) = \frac{n}{2}$ and $WS(\alpha_1) \subset WS(u_1)$, we can easily conclude that $|G_{\alpha_1}| = n$ which implies that $|\overline{G_{\alpha_1}}| = n$. Moreover, as the number of 1's at any coordinate position among all the elements of G_{u_1} is $n/2$ (by Lemma 1), we can say that the number of 1's at any coordinate position among all the elements of G_{α_1} and $\overline{G_{\alpha_1}}$ are $\frac{n}{2} - 1$ and $\frac{n}{2} + 1$ respectively. In the following cases, we analyze the Walsh spectrum of I'_n.

CASE I: $wt(\Lambda^n) = 0$.
Since $|G_{\alpha_1}| = |\overline{G_{\alpha_1}}| = |G_{u_1}| = n$, from Equation 5, we get $W_{I'_n}(\Lambda^n) = \binom{n}{\frac{n}{2}} + 2[n - n - n] = \binom{n}{\frac{n}{2}} - 2n$.

CASE II: $wt(\Lambda^n) = n$.
From (Dalai, Maitra, and Sarkar 2006), it is known that $W_{I'_n}(\Lambda^n) = \pm\binom{n}{\frac{n}{2}}$ according as $\frac{n}{2}$ is even or odd. For $\frac{n}{2}$ even, weight of both G_{α_1} and $\overline{G_{\alpha_1}}$ is odd. Then for both the cases, $\zeta \in G_{\alpha_1}$ and $\zeta \in \overline{G_{\alpha_1}}$, the scalar product $\zeta \cdot \Lambda^n$ will be odd. Obviously, for $\zeta \in \overline{G_{u_1}}$, the scalar product $\zeta \cdot \Lambda^n$ will be even. Therefore, from Equation 5, we get

$W_{I'_n}(\Lambda^n) = \binom{n}{\frac{n}{2}} + 2[-n+n-n] = \binom{n}{\frac{n}{2}} - 2n$. On the other hand, for $\frac{n}{2}$ is odd, using similar argument we get from Equation 5, $W_{I'_n}(\Lambda^n) = -\binom{n}{\frac{n}{2}} + 2[n-n+n] = -\binom{n}{\frac{n}{2}} + 2n$.

CASE III: $wt(\Lambda^n) = 1$.

Since the number of 1's at any coordinate position among all the elements of G_{α_1} and $\overline{G_{\alpha_1}}$ are $\frac{n}{2} - 1$ and $\frac{n}{2} + 1$ respectively, then $\sum_{\zeta \in \overline{G_{\alpha_1}}} (-1)^{\zeta \cdot \Lambda^n} = -(\frac{n}{2}+1)+(\frac{n}{2}-1) = -2$ Similarly, $\sum_{\zeta \in G_{\alpha_1}} (-1)^{\zeta \cdot \Lambda^n} = -(\frac{n}{2}-1)+(\frac{n}{2}+1) = 2$. Since, the number of 1's and the number of 0's are the same at any coordinate position among all the elements of $\overline{G_{u_1}}$, then $\sum_{\zeta \in \overline{G_{u_1}}} (-1)^{\zeta \cdot \Lambda^n} = -\frac{n}{2} + \frac{n}{2} = 0$. Therefore, from Equation 5, we get $W_{I'_n}(\Lambda^n) = \binom{n}{\frac{n}{2}} + 2[-2-2-0] = \binom{n}{\frac{n}{2}} - 8$.

CASE IV: $2 \leq wt(\Lambda^n) \leq n-1$.

From (Dalai, Maitra, and Sarkar 2006), it is known that, the second maximum absolute value of $W_{1 \oplus S_n}$ is attained at the inputs of weights $2, 3, n-2$ and $n-1$ respectively and that value is equal to $\frac{1}{n-1} \cdot \binom{n}{\frac{n}{2}}$. Toggling outputs of $1 \oplus S_n$ at three orbits can increase the absolute value at most by $6n$. However, it is easy to check that for $n \geq 8$, $\frac{1}{n-1} \cdot \binom{n}{\frac{n}{2}} + 6n \leq \binom{n}{\frac{n}{2}} - 8$.

As $n \geq 8$, the maximum absolute Walsh spectrum value of I'_n is $\binom{n}{\frac{n}{2}} - 8$. Therefore, $nl(I'_n) = 2^{n-1} - \frac{1}{2}(\binom{n}{\frac{n}{2}} - 8) = 2^{n-1} - \binom{n-1}{\frac{n}{2}} + 4$.

For example, nonlinearities of this class of RSBFs for $n = 8, 10, 12$ are respectively $97, 390, 1590$. For $n = 6$, the maximum and the second maximum absolute Walsh spectrum values of $1 \oplus S_n$ are 20 and 4 respectively. From Theorem 8, we know that the values of $W_{I'}(\Lambda^n)$ will be $8, 12, -12$ for $wt(\Lambda^n) = 0, 1, n$ respectively. Since I'_n is constructed by toggling outputs of S_n at three orbits, the second maximum Walsh spectrum value of I'_n can reach maximum up to $4 + 36$, i.e., 40. Therefore, the function I'_n may not have 12 as the maximum absolute value in its Walsh spectrum. Hence, the nonlinearity may not be equal to $2^{n-1} - \binom{n-1}{\frac{n}{2}} + 4$. We constructed all the 6-variable RSBFs using Construction 6 and found the nonlinearities obtained in this class are 18 and 22 respectively.

Construction 6 can be generalized as follows.

Construction 7.

1. *Choose* $\alpha_1 \in W^{<\frac{n}{2}-1}$.
2. *Choose* $u_1 \in W^{\frac{n}{2}}$ *such that*
   - *(a)* $|G_{\alpha_1}| = |G_{u_1}|$,
   - *(b)* $\overline{u_1} \notin G_{u_1}$ *and*
   - *(c)* $WS(\alpha_1) \subset WS(u_1)$.
   - *(d)* G_{α_1} *and* G_{u_1} *have the property that* T *and* U *respectively have in Construction 5 have.*
3. *Construct*

$$I''_n(x) = \begin{cases} 0, \text{ if } x \in W^{<\frac{n}{2}} \cup \overline{G_{\alpha_1}} \cup G_{u_1} \setminus G_{\alpha_1}, \\ 0 \text{ if } x \in W^{\frac{n}{2}} \setminus G_{u_1} \cup \overline{G_{u_1}}, \\ 1, \text{ if } x \in W^{>\frac{n}{2}} \cup G_{\alpha_1} \cup \overline{G_{u_1}} \setminus \overline{G_{\alpha_1}}. \end{cases}$$

This is clear that such pair of orbits G_{α_1} and G_{u_1} can not be available for $n = 4$. It follows from Construction 7 that the orbits $G_{\alpha_1}, G_{u_1}, \overline{G_{u_1}}, \overline{G_{\alpha_1}}$ follow the same property as required by the sets T, U, V, S respectively in Construction 6. Therefore, we have the following result.

Proposition 9. *For $n \geq 6$, the function I''_n is an n-variable function with the maximum* AI.

Example 4. *Let $n = 8$. Take $\alpha_1 = (0,0,0,0,0,0,1,1)$ and $u_1 = (0,0,1,0,1,0,1,1)$. Form the orbits $G_{\alpha_1}, G_{u_1}, \overline{G_{\alpha_1}}$ and $\overline{G_{u_1}}$. Then construct I''_n as in Construction 7. I''_n will have the maximum* AI.

In this class we obtained better nonlinearity than I'_n. For example, the maximum nonlinearity we obtained for $n = 8, 10, 12$ are respectively $101, 394, 1598$. The 8-variable function described in Example 4 has nonlinearity 101.

Construction 6 can be generalized further as follows. Instead of choosing T, S, U, V arbitrarily but only satisfying the conditions of Construction 5, if we choose such four orbits in $\{0,1\}^n$, then Construction 5 will directly give us the construction of an RSBF with the maximum AI.

In (Carlet, Zeng, Li, and Hu 2007), nonlinearity analysis of functions constructed for some particular cases of Construction 5 has been given. It has been shown that for particular parameters, I_n can achieve nonlinearity higher than H_n. The sets T, U, V, S were chosen as follows. Take $T = \{x | wt(x) = \frac{n}{2} - wt(u), WS(x) \cap WS(u) = \emptyset\}$ and $U = \{x \oplus u | x \in T\}$, where u is any fixed element in $W^{<\frac{n}{2}}$. Then take $S = \overline{T}$ and $V = \overline{U}$. For this, I_n can achieve nonlinearity $\Gamma_k = 2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + \frac{k\binom{n-k}{\frac{n}{2}-k}}{n-k}$ for $3 \leq wt(u) = k \leq \frac{n}{2} - 1$. Taking an element $u \in W^{<\frac{n}{2}} \setminus W^0$, one cannot generate an orbit $U \subset W^{\frac{n}{2}}$ by XORing u with each element of another orbit T such that $T = \{x | wt(x) = \frac{n}{2} - wt(u), WS(x) \cap WS(u) = \emptyset\}$. Thus, this construction cannot directly give any RSBF with the maximum AI and nonlinearity equal to Γ_k. Further, constructions of balanced functions with the maximum AI and nonlinearity Γ_k for $2 \leq k \leq \frac{n}{2} - 1$, have also been presented by a little modification of the sets T and U. For example, they have shown that it is possible to get balanced functions on n-variables, ($n \geq 8$) with the maximum AI and nonlinearity Γ_2, i.e., $2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + \frac{2\binom{n-2}{\frac{n}{2}-2}}{n-2}$.

7 Conclusions

We have given theoretical constructions of RSBFs which do not belong to the class of symmetric functions and have the maximum algebraic immunity for odd number of variables. We further generalize our construction idea to an efficient search technique in the RSBF class to find functions with the maximum possible algebraic immunity and very high nonlinearity. We have studied the case for even number of variables too. We would like to point out that random functions have very high nonlinearity (Olejar and Stanek 1998) and also possess optimal AI (Meier, Pasalic, and Carlet 2004). Therefore, theoretical constructions of Boolean functions with very high nonlinearity and maximum AI will be a great interest of research.

Acknowledgments: The authors would like to thank the anonymous reviewer for his comments and suggestions on this paper.

References

Armknecht, F. (2004). Improving fast algebraic attacks. In B. K. Roy and W. Meier (Eds.), *FSE*, Volume 3017 of *Lecture Notes in Computer Science*, pp. 65–82. Springer.

Armknecht, F., C. Carlet, P. Gaborit, S. Künzli, W. Meier, and O. Ruatta (2006). Efficient computation of algebraic immunity for algebraic and fast algebraic attacks. In S. Vaudenay (Ed.), *EUROCRYPT*, Volume 4004 of *Lecture Notes in Computer Science*, pp. 147–164. Springer.

Batten, L. M. (2004). Algebraic attacks over GF(q). In A. Canteaut and K. Viswanathan (Eds.), *INDOCRYPT*, Volume 3348 of *Lecture Notes in Computer Science*, pp. 84–91. Springer.

Braeken, A. and B. Preneel (2005). Probabilistic algebraic attacks. In N. P. Smart (Ed.), *IMA International Conference*, Volume 3796 of *Lecture Notes in Computer Science*, pp. 290–303. Springer.

Canteaut, A. (2005). Open problems related to algebraic attacks on stream ciphers. In *International Workshop on Coding and Cryptography, WCC 2005*, pp. 1–10. Invited talk.

Carlet, C., X. Zeng, C. Li, and L. Hu (2007). Further properties of several classes of Boolean functions with optimum algebraic immunity. Cryptology ePrint Archive, Report 2007/370. `http://eprint.iacr.org/`.

Cheon, J. H. and D. H. Lee (2004). Resistance of S-Boxes against algebraic attacks. In B. K. Roy and W. Meier (Eds.), *FSE*, Volume 3017 of *Lecture Notes in Computer Science*, pp. 83–94. Springer.

Cho, J. Y. and J. Pieprzyk (2004). Algebraic attacks on SOBER-t32 and SOBER-t16 without Stuttering. In B. K. Roy and W. Meier (Eds.), *FSE*, Volume 3017 of *Lecture Notes in Computer Science*, pp. 49–64. Springer.

Courtois, N. (2003). Fast algebraic attacks on stream ciphers with linear feedback. In D. Boneh (Ed.), *CRYPTO*, Volume 2729 of *Lecture Notes in Computer Science*, pp. 176–194. Springer.

Courtois, N., B. Debraize, and E. Garrido (2006). On exact algebraic [non-]immunity of S-Boxes based on power functions. In L. M. Batten and R. Safavi-Naini (Eds.), *ACISP*, Volume 4058 of *Lecture Notes in Computer Science*, pp. 76–86. Springer.

Courtois, N. and W. Meier (2003). Algebraic attacks on stream ciphers with linear feedback. In E. Biham (Ed.), *EUROCRYPT*, Volume 2656 of *Lecture Notes in Computer Science*, pp. 345–359. Springer.

Courtois, N. and J. Pieprzyk (2002). Cryptanalysis of block ciphers with overdefined systems of equations. In Y. Zheng (Ed.), *ASIACRYPT*, Volume 2501 of *Lecture Notes in Computer Science*, pp. 267–287. Springer.

Dalai, D. K., K. C. Gupta, and S. Maitra (2004). Results on algebraic immunity for cryptographically significant Boolean functions. In A. Canteaut and K. Viswanathan (Eds.), *INDOCRYPT*, Volume 3348 of *Lecture Notes in Computer Science*, pp. 92–106. Springer.

Dalai, D. K., K. C. Gupta, and S. Maitra (2005). Cryptographically significant Boolean functions: Construction and analysis in terms of algebraic immunity. In H. Gilbert and H. Handschuh (Eds.), *FSE*, Volume 3557 of *Lecture Notes in Computer Science*, pp. 98–111. Springer.

Dalai, D. K. and S. Maitra (2006). Reducing the number of homogeneous linear equations in finding annihilators. In G. Gong, T. Helleseth, H. Song, and K. Yang (Eds.), *SETA*, Volume 4086 of *Lecture Notes in Computer Science*, pp. 376–390. Springer.

Dalai, D. K., S. Maitra, and S. Sarkar (2006). Basic theory in construction of Boolean functions with maximum possible annihilator immunity. *Design Codes and Cryptography 40*(1), 41–58.

Didier, F. and J. Tillich (2006). Computing the algebraic immunity efficiently. In M. J. B. Robshaw (Ed.), *FSE*, Volume 4047 of *Lecture Notes in Computer Science*, pp. 359–374. Springer.

Kurosh, A. G. (1955). *Theory of Groups*, Volume 1. Chelsea Publishing Co., New York.

Li, N. and W. Qi (2006a). Construction and analysis of Boolean functions of 2t+1 variables with maximum algebraic immunity. In X. Lai and K. Chen (Eds.), *ASIACRYPT*, Volume 4284 of *Lecture Notes in Computer Science*, pp. 84–98. Springer.

Li, N. and W. Qi (2006b). Symmetric Boolean functions depending on an odd number of variables with maximum algebraic immunity. *IEEE Transactions on Information Theory 52*(5), 2271–2273.

Lobanov, M. (2005). Tight bound between nonlinearity and algebraic immunity. Available at Cryptology ePrint Archive, eprint.iacr.org, No. 2005/441.

MacWilliams, F. J. and N. J. A. Sloane (1977). *The Theory of Error Correcting Codes*. North Holland.

Stănică, P. and S. Maitra (2008). Rotation symmetric Boolean functions-Count and cryptographic properties. *Discrete Applied Mathematics 156*(10), 1567–1580.

Meier, W., E. Pasalic, and C. Carlet (2004). Algebraic attacks and decomposition of Boolean functions. In C. Cachin and J. Camenisch (Eds.), *EUROCRYPT*, Volume 3027 of *Lecture Notes in Computer Science*, pp. 474–491. Springer.

Olejar, D. and M. Stanek (1998). On cryptographic properties of random Boolean functions. *Journal of Universal Computer Science 4*(8), 705–717.

Qu, L., C. Li, and K. Feng (2007). A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables. *IEEE Transactions on Information Theory 53*(8), 2908–2910.

Sarkar, S. and S. Maitra (2008). Idempotents in the neighbourhood of Patterson-Wiedemann functions having Walsh spectra zeros. *Design Codes and Cryptography*, 49(1-3), 95–103.

Sarkar, S. and S. Maitra (2007). Construction of rotation symmetric Boolean functions on odd number of variables with maximum algebraic immunity. In S. Boztas and H. F. Lu (Eds.), *AAECC*, Volume 4851 of *Lecture Notes in Computer Science*, pp. 271–280. Springer.

Stănică, P., S. Maitra, and J. A. Clark (2004). Results on rotation symmetric bent and correlation immune Boolean functions. In B. K. Roy and W. Meier (Eds.), *FSE*, Volume 3017 of *Lecture Notes in Computer Science*, pp. 161–177. Springer.

Sumanta Sarkar *Sumanta Sarkar received his master degree in Mathematics from the University of North Bengal in 2002. He received Ph. D. from the Jadavpur University in 2008. Currently he is a post-doctoral fellow at INRIA Rocquencourt, FRANCE.*

Subhamoy Maitra *received his Bachelor of Electronics and Telecommunication Engineering degree in the year 1992 from Jadavpur University, Kolkata and Master of Technology in Computer Science in the year 1996 from Indian Statistical Institute, Kolkata. He has completed Ph.D. from Indian Statistical Institute in 2001. Currently he is an Associate Professor at Indian Statistical Institute. His research interest is in Cryptology.*