# Enumeration of 9-variable Rotation Symmetric Boolean Functions having Nonlinearity > 240

Selçuk Kavut*, Subhamoy Maitra†, Sumanta Sarkar† and Melek D. Yücel*

**Abstract**

The existence of 9-variable Boolean functions having nonlinearity strictly greater than 240 has been shown very recently (May 2006) by Kavut, Maitra and Yücel. The functions with nonlinearity 241 have been identified by a heuristic search in the class of Rotation Symmetric Boolean Functions (RSBFs). In this paper we efficiently perform the exhaustive search to enumerate the 9-variable RSBFs having nonlinearity $> 240$ and found that there are such functions with nonlinearity 241 only and there is no RSBF having nonlinearity $> 241$. Our search enumerates $8 \times 189$ many 9-variable RSBFs having nonlinearity 241. We further show that there are only two functions which are different up to the affine equivalence. Towards the end we explain the coding theoretic significance of these functions.

**Keywords:** Boolean Functions, Covering Radius, Reed-Muller Code, Nonlinearity, Rotational Symmetry, Walsh Transform.

## 1 Introduction

The class of Rotation Symmetric Boolean functions has received a lot of attention in terms of their cryptographic and combinatorial properties [4–10, 13, 17, 18, 21, 24, 25]. The nonlinearity and correlation immunity of such functions have been studied in detail in [4, 10, 13, 17, 18, 24, 25]. It is now clear that the RSBF class is extremely rich in terms of these properties. As an important support of that very recently 9-variable Boolean functions having nonlinearity 241 have been discovered [14] in the RSBF class, which has been open for almost three decades. One should note that the space of the RSBF class is much smaller ($\approx 2^{\frac{2^n}{n}}$) than the total space of Boolean functions ($2^{2^n}$) on $n$ variables.

The Boolean functions attaining maximum nonlinearity are called bent [23] which occurs only for even number of input variables $n$ and the nonlinearity is $2^{n-1} - 2^{\frac{n}{2}-1}$. For

*Department of Electrical Engineering and Institute of Applied Mathematics, Middle East Technical University (METU – ODTÜ), 06531 Ankara, Türkiye. Email: selcukkavut@gmail.com, yucel@eee.metu.edu.tr

†Applied Statistics Unit, Indian Statistical Institute, 203 B T Road, Kolkata 700 108, India. Email: {subho, sumanta_r}@isical.ac.in

odd number of variables $n$, the maximum nonlinearity (upper bound) can be at most $2\lfloor 2^{n-2} - 2^{\frac{n}{2}-2} \rfloor$ [12]. Before [14], the following results related to maximum nonlinearity (actually attained) of Boolean functions have been known. In 1972 [1], it was shown that the maximum nonlinearity of 5-variable Boolean functions is 12 and in 1980 [19] it was proved that the maximum nonlinearity of 7-variable Boolean functions is 56. Thus for odd $n \leq 7$, the maximum nonlinearity of $n$-variable functions is $2^{n-1} - 2^{\frac{n-1}{2}}$. In 1983 [20], Boolean functions on 15 variables having nonlinearity 16276 were demonstrated and using this result one can show that for odd $n \geq 15$, it is possible to get Boolean functions having nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 20 \cdot 2^{\frac{n-15}{2}}$. There was a gap for $n = 9, 11, 13$ and the maximum nonlinearity known for these cases prior to [14] was $2^{n-1} - 2^{\frac{n-1}{2}}$. Very recently [14] Boolean functions having nonlinearity 241 have been discovered which belong to the class of Rotation Symmetric Boolean functions. The technique used to find such functions is a suitably modified steepest-descent based iterative heuristic [13, 14].

As the functions could be found by heuristic search only [14], there is a serious need to study the complete RSBF class of 9-variables for nonlinearity $> 240$. Given the nice combinatorial structure of the Walsh spectra for RSBFs on odd number of variables [17], such a search becomes feasible with considerable computational effort. The complete details of the exhaustive search strategy is explained in Section 2 of this paper. The search shows that the maximum nonlinearity of 9-variable RSBFs is 241. We exploit certain results related to binary nonsingular circulant matrices and their variations to show that there are actually two different 9-variable nonlinearity 241 functions in the 9-variable RSBF class up to the affine equivalence. This is described in Section 3. As the maximum nonlinearity issue of Boolean functions is related to the covering radius of first order Reed-Muller code, we briefly outline the coding theoretic implications of our results in Section 4.

## 1.1 Preliminaries

A Boolean function on $n$ variables may be viewed as a mapping from $V_n = \{0,1\}^n$ into $\{0,1\}$. The *truth table* of a Boolean function $f(x_1, \ldots, x_n)$ is 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 weight* of a binary string $S$ is the number of 1's in $S$ denoted by $wt(S)$. 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 equidimensional binary strings $S_1$ and $S_2$ is defined by $d(S_1, S_2) = wt(S_1 \oplus S_2)$, where $\oplus$ denotes the addition over $GF(2)$, i.e., XOR.

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 $deg(f)$.

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 minimum 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 spectrum, the nonlinearity of $f$ is given by

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

The autocorrelation spectrum [22, 26] of a Boolean function is also important to study its usefulness in a cryptosystem.

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

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

and the absolute indicator is

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

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

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

## 1.2 Rotation Symmetric Boolean Functions

To save space we refer to [25] for basic definitions related to Boolean functions. Let $x_i \in \{0,1\}$ for $1 \leq i \leq n$. For some integer $k \geq 0$ we define $\rho_n^k(x_i)$ as $\rho_n^k(x_i) = x_{i+k \bmod n}$, with the exception that when $i+k \equiv 0 \bmod n$, then we will assign $i+k \bmod n$ by $n$ instead of 0. This is to cope up with the input variable indices $1, \ldots, n$ for $x_1, \ldots, x_n$.

Let $(x_1, x_2, \ldots, x_{n-1}, x_n) \in V_n$. Then we extend the definition as

$$\rho_n^k(x_1, x_2, \ldots, x_{n-1}, x_n) = (\rho_n^k(x_1), \rho_n^k(x_2), \ldots, \rho_n^k(x_{n-1}), \rho_n^k(x_n)).$$

Hence, $\rho_n^k$ acts as $k$-cyclic rotation on an $n$-bit vector. A Boolean function $f$ is called *rotation symmetric (RSBF)* if for each input $(x_1, \ldots, x_n) \in \{0,1\}^n$,

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

That is, the rotation symmetric Boolean functions are invariant under cyclic rotation of inputs. The inputs of a rotation symmetric Boolean function can be divided into orbits so that each orbit consists of all cyclic shifts of one input. An orbit is generated by

$$G_n(x_1, x_2, \ldots, x_n) = \{\rho_n^k(x_1, x_2, \ldots, x_n) | 1 \leq k \leq n\}$$

and the number of such orbits is denoted by $g_n$. Thus the number of $n$-variable RSBFs is $2^{g_n}$. Let $\phi(k)$ be Euler's *phi*-function, then it can be shown by Burnside's lemma that (see also [24]) $g_n = \frac{1}{n}\sum_{k|n} \phi(k)\, 2^{\frac{n}{k}}$.

An *orbit* is completely determined by its *representative element* $\Lambda_{n,i}$, which is the lexicographically first element belonging to the orbit [25]. These representative elements are again arranged lexicographically as $\Lambda_{n,0}, \ldots, \Lambda_{n,g_n-1}$. In [25] it was shown that the Walsh transform takes the same value for all elements belonging to the same orbit, i.e., $W_f(u) = W_f(v)$ if $u \in G_n(v)$. In analyzing the Walsh spectra of RSBFs, the ${}_n\mathcal{A}$ matrix has been introduced [25]. The matrix ${}_n\mathcal{A}$ is defined as ${}_n\mathcal{A}_{i,j} = \sum_{x \in G_n(\Lambda_{n,i})} (-1)^{x \cdot \Lambda_{n,j}}$, for an $n$-variable RSBF. Using this $g_n \times g_n$ matrix, the Walsh spectra for an RSBF can be calculated as $W_f(\Lambda_{n,j}) = \sum_{i=0}^{g_n-1} (-1)^{f(\Lambda_{n,i})}\, {}_n\mathcal{A}_{i,j}$.

# 2 Search Algorithm

In this section we present the search algorithm that exhausts the 9-variable RSBFs having nonlinearity $> 240$. To understand the search method, we first need to study the structure of ${}_n\mathcal{A}$ under some permutation of the orbit leaders as explained in [17].

## 2.1 Structure of ${}_n\mathcal{A}$ [17] for $n$ odd

The structure of ${}_n\mathcal{A}$ has been studied in detail for odd $n$ in [17]. Instead of ordering the representative elements in lexicographical manner, the ordering was considered in a different way to get better combinatorial structures. Define $\hat{\Lambda}_{n,i}$ as the representative element of $G_n(x_1, x_2, \ldots, x_n)$ that contains complement of $\Lambda_{n,i}$. For odd $n$, there is a one-to-one correspondence between the classes of even weight $\Lambda_{n,i}$'s and the classes of odd weight $\Lambda_{n,i}$'s by $\Lambda_{n,i} \rightarrow \hat{\Lambda}_{n,i}$. Hence, the set of orbits can be divided into two parts (of same cardinality) containing representative elements of even weights and odd weights respectively.

Let us consider the ordering of the representative elements in the following way. First the representative elements of even weights are arranged in lexicographical order and they are termed as $\Lambda_{n,i}$, for $i = 0$ to $\frac{g_n}{2}-1$). Then the next $\frac{g_n}{2}$ representative elements correspond to the complements of the even weight ones, i.e., these are of odd weights. These are recognized as $\Lambda_{n,i} = \hat{\Lambda}_{n,i-\frac{g_n}{2}}$ for $i = \frac{g_n}{2}$ to $g_n - 1$. Thus following [17], the matrix ${}_n\mathcal{A}$ needs to be reorganized. The resulting matrix is denoted by ${}_n\mathcal{A}^\pi$, which has the form [17]

$$ {}_n\mathcal{A}^\pi = \left( \begin{array}{c|c} {}_n\mathcal{H} & {}_n\mathcal{H} \\ \hline {}_n\mathcal{H} & -{}_n\mathcal{H} \end{array} \right), $$

where ${}_n\mathcal{H}$ is a sub matrix of ${}_n\mathcal{A}^\pi$. Using this matrix ${}_n\mathcal{A}^\pi$, the authors of [17] showed that Walsh spectra calculation could be reduced by almost half of the amount compared to [25].

Given the new ordering of $\Lambda_{n,i}$'s, we represent two strings

$$ \mu_f = ((-1)^{f(\Lambda_{n,0})}, \ldots, (-1)^{f(\Lambda_{n,\frac{g_n}{2}-1})}) \text{ and } \nu_f = ((-1)^{f(\Lambda_{n,\frac{g_n}{2}})}, \ldots, (-1)^{f(\Lambda_{n,g_n-1})}) $$

corresponding to an $n$-variable RSBF $f$. Note that $\mu_f, \nu_f$ are vectors of dimension $\frac{g_n}{2}$.

Let us now consider the vectors $u_f = \mu_f \ {}_n\mathcal{H}, v_f = \nu_f \ {}_n\mathcal{H}$. Then the Walsh spectra values of $f$ will be $(u_f[i] + v_f[i])$ for the first $\frac{g_n}{2}$ many representative elements (which are of even weights) and $(u_f[i] - v_f[i])$ for the next $\frac{g_n}{2}$ many representative elements (which are of odd weights).

## 2.2 Walsh Spectra of 9-variable RSBFs having nonlinearity $> 240$

Let us start with a technical result which is easy to prove.

**Proposition 1** *Let $a, b$ and $M$ be three integers with $M > 0$. Then $|a+b| \leq M$, $|a-b| \leq M$ iff $|a| + |b| \leq M$.*

The matrix ${}_9\mathcal{A}^\pi$ for 9-variable RSBFs is a $60 \times 60$ matrix, as the number of distinct orbits is 60. The matrix ${}_9\mathcal{H}$ is a $30 \times 30$ matrix.

For an RSBF $f$ on 9 variables, which has nonlinearity strictly greater than 240, the values in the Walsh spectrum are in the range $[-30, 30]$. Thus for a pattern $\mu_f||\nu_f$, one must get $|u_f[i] + v_f[i]| \leq 30$ and $|u_f[i] - v_f[i]| \leq 30$; using Proposition 1, these two conditions are equivalent to $|u_f[i]| + |v_f[i]| \leq 30$ for $0 \leq i \leq \frac{g_9}{2} - 1 = 29$.

Thus one needs to find a 9-variable RSBF $f$ (represented by a 60-bit vector $\mu_f||\nu_f$) such that $|u_f[i]| + |v_f[i]| \leq 30$ for $0 \leq i \leq 29$. By a naive method this requires to exhaust the search space of $2^{60}$, i.e., generating all the $\mu_f||\nu_f$ patterns and then checking whether the condition $|u_f[i]| + |v_f[i]| \leq 30$ is satisfied for $0 \leq i \leq 29$ for each of such patterns.

Next we present an efficient method for this. Note that if we look at the patterns $\mu_f$ and $\nu_f$ separately, then each of these patterns must satisfy the necessary conditions $|u_f[i]| \leq 30$ and $|v_f[i]| \leq 30$ respectively for $0 \leq i \leq 29$. Thus we first search for all the patterns $\mu_f$'s such that $|u_f[i]| \leq 30$ for $0 \leq i \leq 29$. Let us denote the set of such patterns by $S$. This search requires checking for $2^{29}$ such patterns by fixing $\mu_f[0] = (-1)^0 = 1$. The reason why

we fix $u_f[0]$ is presented in Proposition 2 and the discussion after it. In a computer with the specification 3.6 Ghz Intel Xeon and 4 GB RAM, it took little less than half an hour to generate the file containing all these patterns and it contains 24037027 many records, i.e., $|S| = 24037027$. Note that $2^{24} < 24037027 < 2^{25}$.

Clearly the search for all the patterns $\nu_f$'s such that $|v_f[i]| \leq 30$ for $0 \leq i \leq 29$ will produce the same set $S$. Hence the search for $\mu_f||\nu_f$ with the property $|u_f[i]| + |v_f[i]| \leq 30$ for $0 \leq i \leq 29$ requires choosing any two patterns $\mu_f, \nu_f$ from $S$ and checking them. To explain how we select two patterns, we first need to present the following technical result.

**Proposition 2** *Consider a 9-variable RSBF $f$ which is represented as $\mu_f||\nu_f$ such that $|u_f[i]| + |v_f[i]| \leq 30$ for $0 \leq i \leq 29$. Consider the functions $g$ such that any of the following holds:*

1. $\mu_g = \mu_f$, $\nu_g = \nu_f^c$, *i.e.*, $g(x_1 \dots x_9) = f(x_1, \dots, x_9) \oplus l_9$,
2. $\mu_g = \mu_f^c$, $\nu_g = \nu_f$, *i.e.*, $g(x_1 \dots x_9) = f(x_1, \dots, x_9) \oplus l_9 \oplus 1$,
3. $\mu_g = \mu_f^c$, $\nu_g = \nu_f^c$, *i.e.*, $g(x_1 \dots x_9) = f(x_1, \dots, x_9) \oplus 1$,
4. $\mu_g = \nu_f$, $\nu_g = \mu_f$, *i.e.*, $g(x_1 \dots x_9) = f(1 \oplus x_1, \dots, 1 \oplus x_9)$,
5. $\mu_g = \nu_f$, $\nu_g = \mu_f^c$, *i.e.*, $g(x_1 \dots x_9) = f(1 \oplus x_1, \dots, 1 \oplus x_9) \oplus l_9$,
6. $\mu_g = \nu_f^c$, $\nu_g = \mu_f$, *i.e.*, $g(x_1 \dots x_9) = f(1 \oplus x_1, \dots, 1 \oplus x_9) \oplus l_9 \oplus 1$,
7. $\mu_g = \nu_f^c$, $\nu_g = \mu_f^c$, *i.e.*, $g(x_1 \dots x_9) = f(1 \oplus x_1, \dots, 1 \oplus x_9) \oplus 1$,

*where $l_9 = x_1 \oplus x_2 \dots \oplus x_8 \oplus x_9$, the rotation symmetric linear function containing all the variables. Then $|u_g[i]| + |v_g[i]| \leq 30$ for $0 \leq i \leq 29$.*

Thus from a single 9-variable RSBF $f$ one can get 8 many (including $f$) RSBFs having the same nonlinearity. This is the reason we fix $\mu_f[0] = 1$. We initially check that repeating a pattern from $S$ twice (i.e., $\mu_f||\nu_f$, when $\nu_f = \mu_f$) one can not satisfy the condition $|u_f[i]| + |v_f[i]| \leq 30$ for $0 \leq i \leq 29$. Thus one requires $\binom{24037027}{2} = 288889321480851$ many pairs to check. Note that $2^{48} < 288889321480851 < 2^{49}$.

We first apply a sieving method to reduce the size of $S$. The idea is to fix some $t$, $0 \leq t \leq 29$ and list all the $\mu_f$ patterns from $S$ such that $|u_f[t]| = 30$ and store them in the set $S_{30,t}$. Similarly, we form the set $S_{0,t}$ consisting of $\nu_f$ patterns from the same set $S$ such that $|v_f[t]| = 0$. Then we choose each of the $\mu_f$ patterns from $S_{30,t}$ and each of the $\nu_f$ patterns from $S_{0,t}$. If for some $\mu_f$ and $\nu_f$, the condition $|u_f[i]| + |v_f[i]| \leq 30$ for all $i$ such that $0 \leq i \leq 29$ holds, then $\mu_f||\nu_f$ is a 9-variable RSBF having nonlinearity 241. We store these RSBFs with nonlinearity 241 and update $S$ by $S \setminus S_{30,t}$ as the elements of $S_{30,t}$ when considered as $\mu_f$, can not be attached with any $\nu_f$ of $S$ except the elements of $S_{0,t}$ to generate an RSBF having nonlinearity $> 240$.

We do this by fixing $t$ taking all integers in [0, 29]. The result found is presented in the following table. Before running the algorithm we like to note the following two observations.

1. For $t = 28$, in the set $S$, there is no $\mu_f$ such that $|u_f[28]| \leq 2$. Thus we initially remove all the $\mu_f$ patterns such that $28 \leq |u_f[28]| \leq 30$. This reduces the number of patterns in $S$ from 24037027 to 18999780.

2. For $t = 0$, in the set $S$, there is no $\mu_f$ such that $|u_f[0]| = 30$. Thus we do not consider this.

| $t$ | $\lvert S_{30,t}\rvert$ | $\lvert S_{0,t}\rvert$ | # of $\mu_f \lvert\rvert \nu_f$ such that $nl(f) = 241$ |
|---|---|---|---|
| 29 | 747073 | 37584 | 0 |
| 15 | 552651 | 77328 | 27 |
| 1 | 687215 | 37584 | 0 |
| 27 | 613686 | 37584 | 0 |
| 26 | 542078 | 37584 | 0 |
| 24 | 597941 | 37584 | 0 |
| 16 | 531456 | 37584 | 0 |
| 4 | 545152 | 37584 | 0 |
| 2 | 514474 | 37584 | 0 |
| 19 | 495350 | 37584 | 0 |
| 12 | 464475 | 37584 | 0 |
| 5 | 408014 | 37584 | 0 |
| 14 | 385125 | 37584 | 0 |
| 13 | 364029 | 37584 | 0 |
| 8 | 338321 | 37584 | 0 |
| 23 | 320685 | 37584 | 0 |
| 20 | 272767 | 37584 | 0 |
| 6 | 255915 | 37584 | 0 |
| 10 | 237525 | 37584 | 0 |
| 17 | 222237 | 37584 | 0 |
| 9 | 206952 | 37584 | 0 |
| 21 | 192113 | 37584 | 0 |
| 3 | 132406 | 77328 | 27 |
| 7 | 126821 | 77328 | 27 |
| 11 | 121290 | 77328 | 27 |
| 18 | 115705 | 77328 | 27 |
| 25 | 110174 | 77328 | 27 |
| 22 | 104643 | 77328 | 27 |

Table 1: Initial search result for 9-variable RSBFs having nonlinearity $> 241$.

In Table 1, we try to fix $t$ such that more number of rows can be removed by lesser search, however this is done only by observation and no specific strategy is involved here. That is the reason the indices in the table are not in order. We find $7 \times 27 = 189$ many RSBFs by this method and hence following Proposition 2, we get $8 \times 189$ many 9-variable RSBFs having nonlinearity 241. Thus after this experiment the set $S$ is reduced to 9540580 elements which is less than half of its initial size 24037027. The experiment requires little more than a day in a PC having 3.6 Ghz Intel Xeon and 4 GB RAM.

Then we go for exhaustive search by taking any two patterns in $\binom{9540580}{2}$ ways. Note that $2^{45} < \binom{9540580}{2} < 2^{46}$. We use 20 computers in parallel that work for 30 hours to check this and we do not find any other function having nonlinearity $> 240$. The specification of computers are 2.8 GHz Pentium IV with 256 MB RAM.

Thus we have the following result.

**Theorem 1** *There are* $8 \times 189$ *many* 9*-variable RSBFs having nonlinearity* 241 *and this is the highest nonlinearity for the 9-variable RSBF class.*

Now let us present the Walsh spectra of the 189 functions available from Table 1 and interestingly all of them are same.

| $W_f(\omega)$ | -30 | -22 | -14 | -6 | 2 | 10 | 18 | 26 |
|---|---|---|---|---|---|---|---|---|
| # of $\omega$'s | 127 | 27 | 36 | 18 | 55 | 39 | 54 | 156 |

Table 2: Walsh spectra of the functions found in Table 1.

We found two classes of functions out of them (63 functions in one class and rest in another class) having different autocorrelation spectra as follows.

| $\Delta_f(\omega)$ | -52 | -44 | -36 | -20 | -12 | -4 | 4 | 12 | 28 |
|---|---|---|---|---|---|---|---|---|---|
| # of nonzero $\omega$'s | 9 | 9 | 9 | 18 | 81 | 85 | 198 | 81 | 21 |

| $\Delta_f(\omega)$ | -76 | -36 | -28 | -20 | -12 | -4 | 4 | 12 | 20 | 28 |
|---|---|---|---|---|---|---|---|---|---|---|
| # of nonzero $\omega$'s | 1 | 9 | 18 | 36 | 81 | 135 | 108 | 54 | 48 | 21 |

Table 3: Autocorrelation spectra of the functions found in Table 1.

Thus it is expected that the 189 functions found in Table 1 are linear transformations of two different functions up to affine equivalence and we justify this in the next section.

# 3 Affine equivalence of RSBFs having nonlinearity 241

Given two Boolean functions $f, g$ on $n$ variables, we call them affinely equivalent if there exist a binary nonsingular $n \times n$ matrix $A$, two $n$-bit binary vectors $b, d$ and a binary constant $c$ such that $g(x) = f(xA \oplus b) \oplus d \cdot x \oplus c$. Thus it is clear that given the function $f$ in Proposition 2, all the other seven functions are affinely equivalent to $f$. In this section we will try to find out affine equivalence among the 189 functions available from Table 1.

Given $(a_1, \ldots, a_n) \in \{0,1\}^n$, the $n \times n$ circulant matrix generated by $(a_1, \ldots, a_n)$ is given by

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

The determinant of the matrix $C(a_1, a_2, \ldots, a_n)$ is given by

$$det[C(a_1, a_2, \ldots, a_n)] = \prod_{i=0}^{n-1} (a_1 + a_2\omega_i + a_3\omega_i^2 + \ldots + a_n\omega_i^{n-1}),$$

where $\omega_i$'s $(0 \leq i \leq n-1)$ are the $n$-th roots of unity. In particular we denote $\omega_0 = 1$. We are interested in the binary circulant matrices which are nonsingular.

**Proposition 3** *Let $\alpha, \beta \in \{0,1\}^n$ such that $\alpha \in G_n(\beta)$ and $A$ be an $n \times n$ nonsingular binary circulant matrix. Then $\alpha A \in G_n(\beta A)$.*

**Proof:** As $\alpha \in G(\beta)$, we have $\alpha = \rho^k(\beta)$, for some $k$ such that $0 \leq k < n$. It is also clear that the columns $A_1, A_2, \ldots, A_n$ of the matrix $A = C(a_1, a_2, \ldots, a_n)$ are cyclic shift of each other, precisely, $A_j = \rho^{j-1}(A_1)$. Now,

$$\begin{aligned} \beta A &= (\beta A_1, \quad \beta A_2, \quad \beta A_3, \quad \ldots, \quad \beta A_n) \\ &= (\beta A_1, \quad \beta\rho^1(A_1), \quad \beta\rho^2(A_1), \quad \ldots, \quad \beta\rho^{n-1}(A_1)) \\ &= (\beta A_1, \quad \rho^{n-1}(\beta)A_1, \quad \rho^{n-2}(\beta)A_1, \quad \ldots, \quad \rho^1(\beta)A_1) \end{aligned}$$

Again,

$$\begin{aligned} \alpha A &= (\alpha A_1, \alpha A_2, \alpha A_3, \ldots, \alpha A_{k+1}, \alpha A_{k+2}, \ldots, \alpha A_n) \\ &= (\alpha A_1, \rho^{n-1}(\alpha)A_1, \rho^{n-2}(\alpha)A_1, \ldots, \rho^{n-k}(\alpha)A_1, \rho^{n-k-1}(\alpha)A_1, \ldots, \rho^1(\alpha)A_1) \\ &= (\rho^k(\beta)A_1, \rho^{n-1}(\rho^k(\beta))A_1, \rho^{n-2}(\rho^k(\beta))A_1, \ldots, \rho^{n-k}(\rho^k(\beta))A_1, \\ &\quad \rho^{n-k-1}(\rho^k(\beta))A_1, \ldots, \rho^1(\rho^k(\beta))A_1) \\ &= (\rho^k(\beta)A_1, \rho^{n-1+k}(\beta)A_1, \rho^{n-2+k}(\beta)A_1, \ldots, \rho^{n-k+k}(\beta)A_1, \\ &\quad \rho^{n-k-1+k}(\beta)A_1, \ldots, \rho^{1+k}(\beta)A_1) \\ &= (\rho^k(\beta)A_1, \rho^{k-1}(\beta)A_1, \rho^{k-2}(\beta)A_1, \ldots, \beta A_1, \rho^{n-1}(\beta)A_1, \ldots, \rho^{k+1}(\beta)A_1) \end{aligned}$$

This shows $\alpha A \in G_n(\beta A)$. ∎

**Proposition 4** *Let $f(x)$ be an $n$-variable RSBF and $A$ be an $n \times n$ nonsingular binary circulant matrix. Then $f(xA)$ is also an RSBF.*

**Proof:** Let $g(x) = f(xA)$. Consider $x_1, x_2 \in G_n(\Lambda)$. Now $g(x_1) = f(x_1A)$ and $g(x_2) = f(x_2A)$. As $x_1A, x_2A \in G_n(\Lambda A)$ (from Proposition 3) and $f$ is an RSBF, $g(x_1) = f(x_1A) = f(x_2A) = g(x_2)$. Thus $g$ is also an RSBF. ∎

We have enumerated all the 21 distinct nonsingular binary circulant $9 \times 9$ matrices up to equivalence corresponding to the row permutations. Based on Proposition 4 we first try to identify whether one of the 189 functions found in Table 1 are affinely equivalent to another function using any of these 21 matrices. We find that this is indeed true and the 189 functions can be divided into 9 classes each containing 21 functions. One example matrix used for this purpose is as follows:

$$A = C(0,0,0,1,0,1,1,1,1) = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Given one function $f(x)$, the other functions are generated as $f(xA), f(xA^2), \ldots, f(xA^{20})$ (in each class containing 21 functions). There are 9 such classes containing 21 functions each and the functions in each class are affinely equivalent. Now let us take one function from each of the 9 classes. Out of these nine functions, three functions follow the autocorrelation spectra presented in the top one of Table 3 and six functions follow the autocorrelation spectra presented in the bottom one of Table 3. However, using these 21 matrices no further affine equivalence could be achieved.

Thus we need to concentrate on some larger class of nonsingular matrices than the binary circulant matrices. We study the matrices whose rows are certain kinds of permutation of the rows of binary circulant matrices. Note that if a circulant matrix is nonsingular, then by making the permutation of rows the nonsingularity will not be disturbed. In a circulant matrix we start with a row and then rotate the row one place (we use the right rotation in this paper) to generate the next row. Instead, given the first row, we may go for $i$-rotation where $i, n$ are coprime.

Let us define $C^i(a_1, a_2, \ldots, a_n)$ as the matrix obtained by taking $(a_1, a_2, \ldots, a_n)$ as the first row and other rows are the $i$-rotations of $(a_1, a_2, \ldots, a_n)$, i.e., $C^i(a_1, a_2, \ldots, a_n) =$

$$\begin{bmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ a_{n+1-i} & a_{n+2-i} & a_{n+3-i} & \ldots & a_{n+n-i} \\ a_{2n+1-2i} & a_{2n+2-2i} & a_{2n+3-2i} & \ldots & a_{2n+n-2i} \\ \vdots & & & & \vdots \\ a_{(n-1)n+1-(n-1)i} & a_{(n-1)n+2-(n-1)i} & a_{(n-1)n+1-(n-1)i} & \ldots & a_{(n-1)n+1-(n-1)i} \end{bmatrix}.$$

**Proposition 5** *Let $\alpha, \beta \in \{0,1\}^n$ such that $\alpha \in G_n(\beta)$. Let $B$ be a nonsingular matrix, $B = C^i(a_1, a_2, \ldots, a_n)$, where $n$ and $i$ are coprime and $(a_1, a_2, \ldots, a_n) \in \{0,1\}^n$. Then $\alpha B \in G_n(\beta B)$.*

**Proof:** As $\alpha \in G(\beta)$, then $\alpha = \rho^k(\beta)$, for some $k$ such that $1 \leq k < n$. It is also clear that the columns $B_1, B_2, \ldots, B_n$ of the matrix $B = C^i(a_1, a_2, \ldots, a_n)$ are $i$-cyclic shift of each other, precisely, $B_j = \rho^{(j-1)i} B_1$. Now,

$$\begin{aligned} \beta B &= (\beta B_1, \quad \beta B_2, \quad \beta B_3, \quad \ldots, \quad \beta B_n) \\ &= (\beta B_1, \quad \beta\rho^i(B_1), \quad \beta\rho^2 i(B_1), \quad \ldots, \quad \beta\rho^{(n-1)i}(B_1)) \\ &= (\beta B_1, \quad \rho^{n-i}(\beta)B_1, \quad \rho^{n-2i}(\beta)B_1, \quad \ldots, \quad \rho^i(\beta)B_1) \end{aligned}$$

Again,

$\alpha B = (\alpha B_1, \alpha B_2, \alpha B_3, \ldots, \alpha B_n)$
$= (\alpha B_1, \rho^{n-i}(\alpha)B_1, \rho^{n-2i}(\alpha)B_1, \ldots, \rho^i(\alpha)B_1)$
$= (\rho^k(\beta)B_1, \rho^{n-i}(\rho^k(\beta))B_1, \rho^{n-2i}(\rho^k(\beta))B_1, \ldots, \rho^i(\rho^k(\beta))B_1)$
$= (\rho^k(\beta)B_1, \rho^{n-i+k}(\beta)B_1, \rho^{n-2i+k}(\beta)B_1, \ldots, \rho^{i+k}(\beta)B_1)$.

Since $i$ and $n$ are coprime, for some integer $\gamma$ we have, $\gamma i \equiv 1 \bmod n$, i.e., $\gamma k i \equiv k \bmod n$, i.e., $ri \equiv k \bmod n$, as $\gamma k \equiv r \bmod n$, for some $r$, $0 \leq r < n$. Therefore, in the expression of $\alpha B$, we have, $\rho^{(n-ri+k)}(\beta)B_1 = \beta B_1$, $\rho^{(n-(r+1)i+k)}(\beta)B_1 = \rho^{(n-i)}(\beta)B_1$ and this continues. Therefore $\alpha B \in G_n(\beta B)$. Hence the proof. ∎

Similar to the Proposition 4, using Proposition 5 we get the following.

**Proposition 6** *Let $f(x)$ be an $n$-variable RSBF and $B$ be an $n \times n$ nonsingular binary matrix as explained in Proposition 5. Then $f(xB)$ is also an RSBF.*

In our case, $n = 9$ and we choose $i = 2$. As for example, one may consider the matrix

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

Using this matrix we find that the nine RSBFs can be represented by two distinct functions up to affine equivalence. Note that these two functions are not affinely equivalent as there autocorrelation spectra are different as given in Table 3. Below we present these two functions, the first one with maximum absolute value in the autocorrelation spectra 52 and the second one with 76. The two functions are as follows.

```
05777A7A6ED82E887CFCE3C549E994947AE4FBA5B91FE46674C3AC8386609671
3FCCAC20EE9B9966CAD357AAE921286D7A20A55A8DF0910BC03C3C51866D2B16

04757A727ED96F087EFCE2C768EB04947AECFBA5B91DE42E7CC1AC8B1060D671
2FCCEDB0EE8B8926CAD357A2E92148ED3AB4A1128DF0918B46143C51A66D2B16
```

# 4 Coding Theoretic Implications

Since the maximum nonlinearity question of Boolean functions is related to the covering radius of First order Reed-Muller code $R(1, n)$, we explain the coding theoretic implications of the 9-variable functions having nonlinearity 241. We like to refer to the papers [2, 3, 9, 11, 12, 15] for relevant coding theoretic discussions.

We present the basic definitions following [15][1]. Let us consider a binary code $C$ of length $N$. Here we consider $R(1, n)$, i.e., $C$ consists of the $2^{n+1}$ many truth tables (of length $N = 2^n$) of the affine functions on $n$ variables. Now consider any coset $D$ of the code $C$, i.e., the elements of the coset $D$ are $f \oplus l$, where $l \in R(1, n)$ and $f$ is a nonlinear Boolean function. The weight of the minimum weight vector in $D$ is considered as the weight of $D$. Let the minimum weight be $w$. Then all the vectors having weight $w$ constitute the set of the leaders in $D$, denoted as $L(D)$. One can define a partial ordering on $F_2^N$ by $S \leq T$ between two binary vectors $S, T$ of length $N$ if $S_i \leq T_i$ for $0 \leq i \leq N-1$. A partial

[1]We like to acknowledge Prof. Philippe Langevin for pointing out the coding theoretic issues presented in this section.

ordering on the space of cosets of $C$ can be defined as follows. Given two cosets $D, D'$ of $C$, $D \leq D'$ means there exist $S \in L(D)$ and $S' \in L(D')$ such that $S \leq S'$. We define a coset $D$ as an orphan or urcoset of $C$ if $D$ is a maximal coset in this partial ordering. This concept was first presented in [11] as urcoset and then in [2, 3] as orphan coset. One can check [15] that a coset $D$ is an orphan or urcoset when $\cup_{g \in L(D)} supp(g) = \{0,1\}^N$.

We have checked by running computer program that given any of the two functions described in the previous function (say $f, g$), each of the cosets $f \oplus R(1,n)$ and $g \oplus R(1,n)$ is an orphan or urcoset. It is clear from Table 2 that the weight of each of the leaders is 241 and there are 127 leaders in each coset. Since each coset is an odd weight orphan, according to [15, Proposition 7], one coordinate position (out of the 512 positions numbered as 0 to 511) must be covered by all the 127 leaders (i.e., the leaders will have the value 1 at that position). In both of the cosets, the 0th position, the output of the 9-variable function corresponding to input $(0, 0, \ldots, 0, 0)$, is covered by all the leaders.

In [9], orphan cosets having minimum weight of 240 have been reported. This is the first time orphan cosets having minimum weight 241 are demonstrated. Further it is reported in [2, Page 401] that X.-D. Hou has constructed odd weight orphans of $R(1,n)$ for $n \geq 11$. Our result shows that this is true for $n = 9$ also.

Let $\rho(C)$ be the covering radius [16,20] of $C$, the weight of the coset of $C$ having largest weight. We like to point out a conjecture in this direction presented in [3]. The conjecture says that the covering radius of $R(1,n)$ is even. For $n = 9$ we found that the covering radius is at least 241, and searching the space of 9-variable RSBFs we could not get higher nonlinearity. In fact some heuristic attempts to increase the nonlinearity did not work yet. It will be an interesting open question to settle the covering radius of $R(1,9)$. The bound presented in [12] for $R(1,9)$ gives the value 244.

# References


[1] E. R. Berlekamp and L. R. Welch. Weight distributions of the cosets of the $(32, 6)$ Reed-Muller code. *IEEE Transactions on Information Theory*, IT-18(1):203–207, January 1972.

[2] R. A. Brualdi and V. S. Pless. Orphans of the first order Reed-Muller codes. *IEEE Transactions on Information Theory*, 36(2):399–401, 1990.

[3] R. A. Brualdi, N. Cai and V. Pless. Orphan structure of the first order Reed-Muller codes. *Discrete Mathematics*, No. 102, pages 239–247, 1992.

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

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

[6] D. K. Dalai, K. C. Gupta and S. Maitra. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. In *INDOCRYPT 2004*, number 3348 in Lecture Notes in Computer Science, Page 92–106, Springer Verlag, December 2004.

[7] D. K. Dalai, S. Maitra and S. Sarkar. Results on rotation symmetric Bent functions. In *Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA'06*, March 2006.

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

[9] C. Fontaine. On some cosets of the First-Order Reed-Muller code with high minimum weight. *IEEE Transactions on Information Theory*, 45(4):1237–1243, 1999.

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

[11] T. Helleseth, T. Kløve and J. Mykkeltveit. On the covering radius of binary codes. *IEEE Transactions on Information Theory*, volume IT-24, pages 627–628, September 1978.

[12] X. -d. Hou. On the norm and covering radius of the first order Reed-Muller codes. *IEEE Transactions on Information Theory*, 43(3):1025–1027, 1997.

[13] S. Kavut, S. Maitra, M. D. Yucel. Autocorrelation spectra of balanced boolean functions on odd number input variables with maximum absolute value $< 2^{\frac{n+1}{2}}$. In *Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA 06*, March 13–15, 2006, LIFAR, University of Rouen, France.

[14] S. Kavut, S. Maitra and M. D. Yücel. There exist Boolean functions on $n$ (odd) variables having nonlinearity $> 2^{n-1} - 2^{\frac{n-1}{2}}$ if and only if $n > 7$. http://eprint.iacr.org/2006/181.

[15] P. Langevin. On the orphans and covering radius of the Reed-Muller codes. In *9th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC 1991*, LNCS 539, Springer Verlag, 234–240, 1991.

[16] F. J. MacWillams and N. J. A. Sloane. *The Theory of Error Correcting Codes*. North Holland, 1977.

[17] A. Maximov, M. Hell and S. Maitra. Plateaued Rotation Symmetric Boolean Functions on Odd Number of Variables. In *First Workshop on Boolean Functions: Cryptography and Applications, BFCA 05*, March 7–9, 2005, LIFAR, University of Rouen, France.

[18] A. Maximov. Classes of Plateaued Rotation Symmetric Boolean functions under Transformation of Walsh Spectra. In WCC 2005, Pages 325–334. See also IACR eprint server, no. 2004/354.

[19] J. J. Mykkeltveit. The covering radius of the $(128, 8)$ Reed-Muller code is 56. *IEEE Transactions on Information Theory*, IT-26(3):359–362, 1980.

[20] N. J. Patterson and D. H. Wiedemann. The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, IT-29(3):354–356, 1983. See also the correction in *IEEE Transactions on Information Theory*, IT-36(2):443, 1990.

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

[22] 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.

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

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

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

[26] 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.