Generalized Rotation Symmetric and Dihedral Symmetric Boolean Functions – 9 variable Boolean Functions with Nonlinearity 242

Selçuk Kavut and Melek D. Yücel

Electrical & Electronics Engineering Dept. and Institute of Applied Mathematics,
Middle East Technical University,
Ankara, 06531, Turkey
{kavut, melekdy}@metu.edu.tr

Abstract. Recently, 9-variable Boolean functions having nonlinearity 241, which is strictly greater than the bent concatenation bound of 240, have been discovered in the class of Rotation Symmetric Boolean Functions (RSBFs) by Kavut, Maitra and Yücel. In this paper, we present several 9-variable Boolean functions having nonlinearity of 242, which we obtain by suitably generalizing the classes of RSBFs and Dihedral Symmetric Boolean Functions (DSBFs).

1 Introduction

Boolean functions with very high nonlinearity is one of the most challenging problems in the area of cryptography and combinatorics. The problem is also related to the covering radius of the first order Reed-Muller code. The Boolean functions attaining maximum nonlinearity of $2^{n-1}-2^{(n/2)-1}$ are called bent [22] which occur only for even number of input variables n. For odd number of variables n, the maximum nonlinearity (upper bound) can be at most $2\lfloor 2^{n-2}-2^{(n/2)-2} \rfloor$ [10]. For odd n, one can get Boolean functions having nonlinearity $2^{n-1}-2^{(n-1)/2}$ by concatenating two bent functions on $(n-1)$ variables. That is the reason why the nonlinearity value $2^{n-1}-2^{(n-1)/2}$ for odd n is known as the bent concatenation bound.

Recently, 9-variable Boolean functions having nonlinearity 241, which is greater than the bent concatenation bound, have been discovered [12] in the RSBF class. The question of whether it is possible to exceed the bent concatenation bound for n = 9, 11, 13 was open for almost three decades. It was known for odd $n \leq 7$, that the maximum nonlinearity is equal to the bent concatenation bound, $2^{n-1}-2^{(n-1)/2}$; since the maximum nonlinearity of 5-variable Boolean functions was found as 12 in 1972 [1], and that of 7-variable

Boolean functions was computed as 56 in 1980 [18]. However, in 1983 [19], 15-variable Boolean functions with nonlinearity 16276 which exceeded the bent concatenation bound were demonstrated and using this result, it became possible to get Boolean functions with nonlinearity $2^{n-1}-2^{(n-1)/2}+20\times2^{(n-15)/2}$ for odd $n\geq15$. Until 2006, there was a gap for n = 9, 11, 13 and the maximum nonlinearity known for these cases was $2^{n-1}-2^{(n-1)/2}$. In 2006, 9-variable functions, which belong to the class of Rotation Symmetric Boolean functions (RSBFs), with nonlinearity 241 ($=2^{n-1}-2^{(n-1)/2}+1$) were discovered [12]. Such functions were attained utilizing a steepest-descent based iterative heuristic that appeared in [14], which was suitably modified for a search in the class of RSBFs.

The class of RSBFs is important in terms of their cryptographic and combinatorial properties [2–7, 9, 13, 16, 17, 20, 23, 24]. The nonlinearity and correlation immunity of such functions have been studied in detail in [2, 9, 13, 16, 17, 23, 24]. It is now clear that the RSBF class is quite rich in terms of these properties and the recently found 9-variable RSBFs having nonlinearity 241 [12] support this fact. In [15], a subspace of RSBFs called Dihedral Symmetric Boolean Functions (DSBFs), which are invariant under the action of dihedral group are introduced. It has been shown that some of the 9-variable RSBFs having nonlinearity 241 also belong to this subspace, confirming the richness of DSBFs.

Since the space of the RSBF class is much smaller ($\approx 2^{2^n/n}$) than the total space of Boolean functions (2^{2^n}) on n variables, it is possible to exhaustively search the space of RSBFs up to a certain value of n. In [11], an exhaustive search is carried out for the whole space of 9-variable RSBFs exploiting some combinatorial results related to the Walsh spectra of RSBFs; and it has been shown that there is no RSBF having nonlinearity > 241. In order to find functions with higher nonlinearity, one needs to increase the search space. This motivated us to generalize the classes of RSBFs and DSBFs, and our search in the generalized DSBF and RSBF classes successfully ended up with 9-variable functions having nonlinearity 242.

Considering a Boolean function f as a mapping from $GF(2^n)\rightarrow GF(2)$, the functions for which $f(\alpha^2) = f(\alpha)$ for any $\alpha\in GF(2^n)$, are referred to as idempotents [6, 7]. In [19], 15-variable Patterson-Wiedemann functions having nonlinearity $16276=2^{n-1}-2^{(n-1)/2}+20$ are identified in the idempotent class. As pointed out in [6, 7], the idempotents can be seen as RSBFs with proper choice of basis. In the following section, we will define the generalized k-RSBFs, as functions which satisfy $f(\alpha^{2^k}) = f(\alpha)$, where $1< k \mid n$ and $\gcd(n, k) \neq 1$. Note that if $\gcd(n, k) = 1$, the resulting functions are the same as idempotents. We then impose the condition of invariance under the action of dihedral group to obtain the class of generalized k-DSBFs as a subset of k-RSBFs.

2 Generalized Rotation and Dihedral Symmetric Boolean Functions

After briefly summarizing RSBFs, we propose the generalized classes of k-RSBFs and k-DSBFs in Definition 2 and Definition 3 respectively. Letting $(x_0, x_1, ..., x_{n-1}) \in V_n$, the (left) k-cyclic shift operator ρ^k_n on n-tuples is defined as $\rho^k_n(x_0, x_1, ..., x_{n-1}) = (x_{(0+k)\bmod n}, ... , x_{(n-1+k)\bmod n})$, for $1 \le k \le n$.

Definition 1. A Boolean function f is called *Rotation Symmetric* if for each input $(x_0, ..., x_{n-1}) \in \{0, 1\}^n$, $f(\rho^1_n(x_0, ..., x_{n-1})) = f(x_0, ..., x_{n-1})$.

That is, RSBFs are invariant under all cyclic rotations of the 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 generated by $(x_0, x_1, ..., x_{n-1})$ is $G_n(x_0, x_1, ..., x_{n-1}) = \{\rho^k_n(x_0, x_1, ..., x_{n-1}) \mid 1 \le k \le n\}$ and the number of such orbits is denoted by g_n ($\approx 2^{2^n/n}$). More specifically, g_n is equal to $(1/n)\sum_{t|n}\phi(t)2^{n/t}$ is the number of rotation symmetric classes [23], where $\phi(t)$ is the Euler's phi-function. The total number of n-variable RSBFs is 2^{g_n}.

In the following, we define the generalized RSBFs as k-rotation symmetric Boolean functions (k-RSBFs).

Definition 2. Let $1 < m < n$ such that $\gcd(n, m) = k \neq 1$. An n-variable Boolean function f is called *k-rotation symmetric* if for each input $(x_0, ..., x_{n-1}) \in \{0, 1\}^n$, $f(\rho^k_n(x_0, ..., x_{n-1})) = f(x_0, ..., x_{n-1})$.

As can be seen, the k-rotation symmetric Boolean functions are invariant under k-cyclic rotations of inputs. Therefore, an orbit of a k-RSBF generated by $(x_1, x_2, ..., x_n)$ is $G^k_n(x_1, x_2, ..., x_n) = \{\rho^i_n(x_1, x_2, ..., x_n) \mid i = k, 2k, 3k, ..., n\}$. For example, $G^3_9(001, 001, 111) = \{(001, 001, 111), (001, 111, 001), (111, 001, 001)\}$.

If $g_{n,k}$ is the number of distinct orbits in the class of k-RSBFs of n variables, one can show that $g_{n,k} = (k/n) \sum_{t \mid (n/k)} \phi(t)2^{n/t}$, where $\phi(t)$ is the Euler's phi function.

In [15], a subspace of RSBFs called Dihedral Symmetric Boolean Functions (DSBFs), which are invariant under the action of dihedral group D_n are introduced. In addition to the (left) k-cyclic shift operator ρ^k_n on n-tuples, which is defined as $\rho^k_n(x_0, x_1, ..., x_{n-1}) = (x_{(0+k)\bmod n}, ... , x_{(n-1+k)\bmod n})$, the dihedral group D_n also includes the reflection operator $\tau_n(x_0, x_1, \ldots, x_{n-1}) = (x_{n-1}, \ldots, x_1, x_0)$. So, $2n$ permutations of D_n are $\{\rho^1{}_n, \rho^2{}_n, \ldots, \rho^{n-1}{}_n, \rho^n{}_n, \tau_n\rho^1{}_n, \tau_n\rho^2{}_n, \ldots, \tau_n\rho^{n-1}{}_n, \tau_n\rho^n{}_n\}$. The dihedral group D_n generates equivalence classes in the set V_n [21]. Let d_n be the number of such partitions. The following proposition gives the exact value of d_n [8, page 184], [15].

Proposition 1. Let d_n be the total number of orbits induced by the dihedral group D_n acting on V_n. Then $d_n = g_n/2 + l$, where, $g_n = 1/n \sum_{t|n} \phi(t)2^{n/t}$ is the number of rotation symmetric classes [23], $\phi(t)$ is the Euler's phi-function and

$$l = \begin{cases} (3/4)2^{n/2} & \text{if } n \text{ is even,} \\ 2^{(n-1)/2} & \text{if } n \text{ is odd.} \end{cases}$$

Since there are 2^{d_n} number of n-variable DSBFs, a reduction in the size of the search space over the size of RSBFs is provided.

Definition 3. Let $1 < m < n$ such that $\gcd(n, m) = k \neq 1$. An n-variable Boolean function f is called *k-dihedral symmetric* if f is invariant under the group action $D^k{}_n = \{\rho^i{}_n, \tau_n\rho^i{}_n \mid i = k, 2k, 3k, \ldots, n\}$.

As the class of DSBFs is a subspace of k-DSBFs, we call k-DSBFs generalized dihedral symmetric Boolean functions. One should observe that k-DSBFs is a subspace of k-RSBFs.

When Proposition 1 is applied to k-dihedral symmetric functions, we obtain the following corollary.

Corollary 1. Let $d_{n,k}$ be the number of distinct orbits, in the class of k-DSBFs of n variables. Then, $d_{n,k} = g_{n,k}/2 + l$, where, $g_{n,k} = k/n \sum_{t \mid n/k} \phi(t)2^{n/t}$ is the number of k-rotation symmetric classes, $\phi(t)$ is the Euler's phi-function and

$$l = \begin{cases} 2^{(n/2)-1} & \text{if } n \text{ is even, } k \text{ is even,} \\ 3\cdot 2^{(n/2)-2} & \text{if } n \text{ is even, } k \text{ is odd,} \\ 2^{(n-1)/2} & \text{if } n \text{ is odd.} \end{cases}$$

Table 1 compares the orbit counts of k-rotational classes, k-dihedral classes, RSBFs, and DSBFs.

Table 1. Comparison of the orbit counts g_n, d_n, $g_{n,k}$ and $d_{n,k}$ for n = 4, 6, ..., 15, and all integers k, which divide n.

n		k	2	3	4	5	6	7
4	$g_4 = 6$	$g_{4,k}$	10	–	–	–	–	–
	$d_4 = 6$	$d_{4,k}$	7	–	–	–	–	–
6	$g_6 = 14$	$g_{6,k}$	24	36	–	–	–	–
	$d_6 = 13$	$d_{6,k}$	16	24	–	–	–	–
8	$g_8 = 36$	$g_{8,k}$	70	–	136	–	–	–
	$d_8 = 30$	$d_{8,k}$	43	–	76	–	–	–
9	$g_9 = 60$	$g_{9,k}$	–	176	–	–	–	–
	$d_9 = 46$	$d_{9,k}$	–	104	–	–	–	–
10	$g_{10} = 108$	$g_{10,k}$	208	–	–	528	–	–
	$d_{10} = 78$	$d_{10,k}$	120	–	–	288	–	–
12	$g_{12} = 352$	$g_{12,k}$	700	1044	1376	–	2080	–
	$d_{12} = 224$	$d_{12,k}$	382	570	720	–	1072	–
14	$g_{14} = 1182$	$g_{14,k}$	2344	–	–	–	–	8256
	$d_{14} = 687$	$d_{14,k}$	1236	–	–	–	–	4224
15	$g_{15} = 2192$	$g_{15,k}$	–	6560	–	10944	–	–
	$d_{15} = 1224$	$d_{15,k}$	–	3408	–	5600	–	–

3 Search Strategy

We present the basic description of our search strategy and for details we refer the reader to [12-14]. The search strategy uses a steepest-descent like iterative algorithm in the pre-chosen set of n-variable Boolean functions, where each iteration accepts the function f and outputs the function f_{min}. At each iteration step, a cost function is calculated within a pre-defined neighborhood of f and the function having the smallest cost is chosen as the iteration output f_{min}. In some rare cases, the cost of f_{min} may be larger than or equal to the cost of f. This is the crucial part of the search strategy, which provides the ability to escape from local minima and its distinction from the steepest-descent algorithm. Our steepest-descent based search technique minimizes the cost until a local minimum is attained, but then it takes a step in the direction of non-decreasing cost. That is, whenever possible, the cost is minimized; otherwise, a step in the reverse direction is taken. The deterministic step in the reverse direction corresponds to the smallest possible cost increase within the pre-defined neighborhood of the preceding Boolean function, which also makes it possible to escape from the local minima.

4 Results

We apply our search strategy to 9-variable 3-DSBFs, where the size of search space is 2^{104}(see Table 1). We have found several unbalanced Boolean functions having nonlinearity 242. Among them there are two different absolute indicator values, which are 32, 40.

The following is the truth table of a 9-variable, 3-dihedral symmetric Boolean function having nonlinearity 242, absolute indicator value 40, and algebraic degree 7:

```
68B7EF2DA03B0D3EA00DB6A96DD99AEAFDB9C842B6D5DC8C4526CE0DD29020DB
B75FE3314568344E73688FF0CB2482E065231869E1AA4583765CC491F8A8DB12
```

And, the function below is another 9-variable 3-DSBF having nonlinearity 242, absolute indicator value 32, and algebraic degree 7:

```
125425D30A398F36508C06817BEE122E250D973314F976AED58A3EA9120DA4FE
0E4D4575C42DD0426365EBA7FC5F45BE9B2F336981B5E1863618F49474F6FE00
```

Using a computer system with Pentium IV 2.8 GHz processor and 256 MB RAM, and setting the iteration number to 60, 000, a typical run of the search algorithm takes 1 minute and 34 seconds. We have carried out 100 runs each with the iteration number N = 60,000. Out of 6 million 3-DSBFs, 152 functions have the nonlinearity 241, and 36 many 3-DSBFs have the nonlinearity 242.

Additionally, we have applied the search strategy to 9-variable 3-RSBFs (the size of the search space is now 2^{176} as can be seen from Table 1), for which we initiate the search algorithm with a 9-variable 3-DSBF having nonlinearity 242. Then we have obtained some 9-variable 3-RSBFs having nonlinearity 242, absolute indicator 56, and algebraic degree 7. The following is the truth table of such a function:

```
3740B6A118A1E19642A85E2B7E2F3C3CB65FA0D95EC9DB1EA92BDB3666185AE0
087F5FE6E0757106A12FC918754C40E8A1BCCB7A714032A8961456E066E8A801
```

It is clear that using one of the above 9-variable functions (say f) and a 2-variable bent function (say g), the 11-variable function $g(y_1, y_2) \oplus f(x_1, ..., x_9)$ with highest -till date- nonlinearity of $2^{11-1} - 2^{(11-1)/2} + 4 = 996$, can be obtained. Similarly $h(y_1, y_2, y_3, y_4) \oplus f(x_1, ..., x_9)$ is the most nonlinear 13-variable function known to date, with nonlinearity $2^{13-1} - 2^{(13-1)/2} + 8 = 4040$ where h is a 4-variable bent function and f is one of the above 9-variable functions with nonlinearity 242. We think this is a significant improvement on the results of [12].

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*, Volume IT-18(1), 203–207, January 1972.

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

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

[4] 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.

[5] 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.

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

[7] 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.

[8] F. Harary. Graph Theory. *Addison-Wesley Publishing Company*, 1972.

[9] 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.

[10] 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.

[11] S. Kavut, S. Maitra S. Sarkar and M. D. Yücel. Enumeration of 9-variable Rotation Symmetric Boolean Functions having Nonlinearity > 240. *INDOCRYPT 2006*, Lecture Notes in Computer Science, Springer-Verlag, Volume 4329, 266–279, 2006.

[12] S. Kavut, S. Maitra and M. D. Yücel. Search for Boolean Functions with Excellent Profiles in the Rotation Symmetric Class. *IEEE Transactions on Information Theory*, Volume IT-53(5), 1743-1751, May 2007. An earlier version of this paper is available under the title "There exist Boolean functions on n (odd) variables having nonlinearity $> 2^{n-1} - 2^{(n-1)/2}$ if and only if $n > 7$" at IACR eprint server, http://eprint.iacr.org/2006/181, 28 May, 2006.

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

[14] S. Kavut and M. D. Yücel. A new algorithm for the design of strong Boolean functions. In *First National Cryptology Symposium*, pages 95–105, METU, Ankara, Turkey, November 18-20, 2005.

[15] S. Maitra, S. Sarkar and D. K. Dalai. On Dihedral Group Invariant Boolean Functions. In *Third International Workshop on Boolean Functions: Cryptography and Applications (BFCA, 2007)*, Univeristy of Rouen, France, 2007.

[16] 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.

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

[19] 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*, Volume IT-36(2), 443, 1990.

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

[21] F. S. Roberts. *Applied Combinatorics*. Prentice-Hall, Inc, Englewood Cliffs, New Jersey.

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

[23] P. Stanica 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.

[24] P. Stanica, 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.