Enumeration of 9-Variable Rotation Symmetric Boolean Functions Having Nonlinearity > 240

Selçuk Kavut[1], Subhamoy Maitra[2], Sumanta Sarkar[2], and Melek D. Yücel[1]

[1] Department of Electrical Engineering and Institute of Applied Mathematics, Middle East Technical University(METU – ODTÜ), 06531 Ankara, Türkiye
selcukkavut@gmail.com, yucel@eee.metu.edu.tr
[2] Applied Statistics Unit, Indian Statistical Institute, 203, B.T. Road, Kolkata 700 108, India
{subho, sumanta_r}@isical.ac.in

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; a few functions with nonlinearity 241 have been identified by a heuristic search in the class of Rotation Symmetric Boolean Functions (RSBFs). In this paper, using combinatorial results related to the Walsh spectra of RSBFs, we efficiently perform the exhaustive search to enumerate the 9-variable RSBFs having nonlinearity > 240 and found that there are 8×189 many functions with nonlinearity 241 and there is no RSBF having nonlinearity > 241. We further prove that among these functions, there are only two which are different up to the affine equivalence. This is found by utilizing the binary nonsingular circulant matrices and their variants. Finally we explain the coding theoretic significance of these functions. This is the first time orphan cosets of $R(1, n)$ having minimum weight 241 are demonstrated for $n = 9$. Further they provide odd weight orphans for $n = 9$; earlier these were known for certain $n \geq 11$.

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

1 Introduction

Nonlinearity is one of the most important cryptographic properties of a Boolean function to be used as a primitive in any crypto system. High nonlinearity resists Best Affine Approximation (BAA) attacks [8] in case of stream ciphers and Linear cryptanalysis [18] in case of block ciphers. One may like to access the references in this paper and the references there in to study the extremely rich literature on Boolean functions having high nonlinearity with other cryptographic properties. Nonlinearity is important in coding theoretic aspects too.

The class of Rotation Symmetric Boolean functions has received a lot of attention in terms of their cryptographic and combinatorial properties [4, 5, 9, 10, 11, 19, 20, 23, 26, 27, 6, 14, 7]. The nonlinearity and correlation immunity of such functions have been studied in detail in [4,11,19,20,26,27,14]. It is now clear that

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 266–279, 2006.

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 [15] in the RSBF class, which had 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 [25] which occurs only for even number of input variables n and the nonlinearity is $2^{n-1} - 2^{\frac{n}{2}-1}$. For odd number of variables n, the maximum nonlinearity (upper bound) can be at most $2\lfloor 2^{n-2} - 2^{\frac{n}{2}-2} \rfloor$ [13]. Before [15], 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 [21] 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 [22], 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 [15] was $2^{n-1} - 2^{\frac{n-1}{2}}$. Very recently [15] 9-variable 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 [14, 15].

As the functions could be found by heuristic search only [15], there is a theoretical 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 [19], 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 variants 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.

Let us consider any Boolean function as a mapping from $GF(2^n) \rightarrow GF(2)$. Then the functions for which $f(\alpha^2) = f(\alpha)$, for any $\alpha \in GF(2^n)$ are referred as idempotents [9, 10] as it follows from $f^2 = f$ in multiplicative algebra. In [9, 10] the idempotents were studied for $n = 9$ with the motivation that the Patterson-Wiedemann functions [22] for $n = 15$ were idempotents. However, in [9, 10] the search was not exhaustive and that is why the functions with nonlinearity 241 could not be discovered. In fact, the idempotents can be seen as RSBFs [9, 10]. Interestingly if one looks at an RSBF, the nice structure [19] in the Walsh spectrum can be exploited to execute an efficient search which is not immediate if one looks at the functions as idempotents.