Enumerating Results of Homogeneous Rotation Symmetric Boolean Functions over $GF(p)$

Guang-Pu Go, Xi-Yong Zhang, and Wen-Fen Liu
Department of Applied Mathematics,
Zhengzhou Information Science and Technology Institute,
P.O. Box 1001-745, Zhengzhou 450002, China
E-mail: gaoguangpu@yahoo.com.cn.

Abstract

In this paper, we consider the open problem of counting homogeneous rotation symmetric Boolean functions over $GF(p)$. By using inclusion–exclusion principle, we obtain a formula to exactly enumerate such class of functions. As a consequence, the known formula of [8, Theorem 9] in Boolean case is simplified.

Keywords. Rotation symmetry, Homogenous, Minimal function, Enumeration, Inclusion–exclusion principle

1 Introduction

Rotation symmetric(RotS) Boolean functions, introduced by Pieprzyk and Qu [1], have received a lot of attention from a cryptographic perspective [2–5, 8–12]. This class of functions is invariant under circular translation of indices. Such property is highly desirable in hashing, for instance in the implementation of MD4, MD5 or HAVAL, since one can reuse evaluations from previous iterations. It has been demonstrated that the class of RotS functions is extremely rich in terms of cryptographically significant Boolean functions. For nonlinearity, Kavut *et.al.* have found Boolean functions on 9-variables with nonlinearity 241, which solved an open problem for almost three decades [2, 3]. Motivated by this study, important cryptographic properties such as nonlinearity, balancedness, correlation immunity, algebraic degree and algebraic immunity of these functions have been investigated at the same time and encouraging results have been obtained. For detailed discussion see [5, 8, 9, 12] and the reference therein.

This work is supported by National Nature Science Foundation of China under Grant number 60803154.

It is important to ensure that the selected criteria for the Boolean functions, supposed to be used in some cryptosystems, do not restrict the choice of the functions too severely. Hence, the set of functions should be enumerated. In [8], Maitra and Stanica presented various counting results for RotS Boolean functions involving the number of homogenous functions. Li [6] generalized the concept of RotS function from $GF(2)$ to $GF(p)$ and obtained many enumerating results about RotS functions over $GF(p)$. In particular, he has enumerated homogeneous RotS functions with degree no more than 3. That how to count homogeneous RotS functions with degree greater than 3 is left an interesting problem. In this direction, Fu *et al.* gave a lower bound on the number of homogeneous RotS functions in [7]. Besides, they presented a formula to enumerate such class of functions when the greatest common divisor of the number of input variables and the algebraic degree of the function is a prime power. However, it remains an open problem to enumerate homogeneous RotS functions for general n.

In this paper, we will continue to focus on this problem. We first observe that there is an equivalence between the orbits of $GF^n(p)$ and their minimal functions(see Remark 2). Consequently, the exact number of minimal functions having fixed degree is obtained by using inclusion–exclusion principle. As an immediate corollary, we completely solve the enumerating problem of homogenous RotS function over $GF(p)$.

2 Preliminaries

Let p be a prime number. Denote by $GF^n(p)$ the n-dimension vector space over the finite field $GF(p)$. An n-variable function $f(x), x = (x_1, x_2, \ldots, x_n) \in GF^n(p)$ is a mapping from $GF^n(p)$ to $GF(p)$, which can be uniquely represented as multivariate polynomial over $GF(p)$, called its algebraic normal form(ANF):

$$f(x_1, x_2, \ldots, x_n) = \sum_{k_1,k_2,\ldots,k_n=0}^{p-1} a_{k_1,k_2,\ldots,k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$$

where each coefficient $a_{k_1,k_2,\ldots,k_n}$ is a constant in $GF(p)$. The number $k_1 + k_2 + \cdots + k_n$ is defined as the degree of the term $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ with nonzero coefficient. The greatest degree of all the terms of f is called the algebraic degree, denoted by $deg(f)$. If the degrees of all the terms of f are equal, then we say f is homogeneous. Let $x_i \in GF(p)$ for $1 \le i \le n$. For $1 \le k \le n$, we define

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

Then we can extend the definition of ρ_n^k on tuples and monomials as follows:

$$\rho_n^k(x_1, x_2, \ldots, x_n) = (\rho_n^k(x_1), \rho_n^k(x_2), \ldots, \rho_n^k(x_n)),$$

and

$$\rho_n^k(x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}) = (\rho_n^k(x_1))^{k_1}(\rho_n^k(x_2))^{k_2}\dots(\rho_n^k(x_n))^{k_n}.$$

Definition 1 *A function $f : GF^n(p) \to GF(p)$ is called rotation symmetric if for each input $(x_1, x_2, \dots, x_n) \in GF^n(p)$,*

$$f(\rho_n^k(x_1, x_2, \dots, x_n)) = f(x_1, x_2, \dots, x_n) \quad \text{for } 0 \le k \le n-1.$$

Denote

$$G_n(x_1, x_2, \dots, x_n) = \{\rho_n^k(x_1, x_2, \dots x_n), \text{ for } 0 \le k \le n-1)\}$$

by the orbit of $(x_1, x_2, \dots, x_n)$ under the action of $\rho_n^k, 0 \le k \le n-1$. It is obvious that $G_n(x_1, x_2, \dots, x_n)$ generates a partition of the vector space $GF^n(p)$.

Remark 1 *For any given $x = (x_1, x_2, \dots, x_n) \in GF^n(p)$, where $x_1 + x_2 + \dots + x_n = d$, we can rewrite x by concatenating r copies of b, where $b = [x_1, \dots, x_{n/r}]$ is a minimal block of x. Then we have $\#G_n(x_1, x_2, \dots, x_n) = n/r$ and $x_1 + \dots + x_{n/r} = d/r$.*

3 Enumeration of Homogenous RotS functions

The remainder of this paper will devote to count the number of homogenous RotS functions over $GF(p)$. We begin with some definitions and technical discussion. By abuse of notation we use G_n further on the monomials defining

$$G_n(x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}) = \{\rho_n^k(x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}), \text{ for } 0 \le k \le n-1)\}.$$

Then we have the following definition.

Definition 2 *A function over $GF(p)$ is called minimal function if f has the form*

$$f(x_1, x_2, \dots, x_n) = \sum_{k=0}^{N-1} \rho_n^k(x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}),$$

where $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ is a monomial of f and $N = \#G_n(x_1^{k_1}x_2^{k_2}\dots x_n^{k_n})$.

Remark 2 *Note that*

$$\begin{aligned}\rho_n^k(x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}) &= (\rho_n^k(x_1))^{k_1}(\rho_n^k(x_2))^{k_2}\dots(\rho_n^k(x_n))^{k_n} \\ &= x_1^{\rho_n^{n-k}(k_1)}x_2^{\rho_n^{n-k}(k_2)}\dots x_n^{\rho_n^{n-k}(k_n)},\end{aligned}$$

then we have $\#G_n(x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}) = \#G_n(k_1, k_2, \dots, k_n)$. Therefore there is an equivalence between the orbits of $GF^n(p)$ and their corresponding minimal functions.

Denote by $\Theta(n/r, d/r, p)$ the set of all solutions of the following equation system:

$$\begin{cases} y_1 + y_2 + \cdots + y_{n/r} = d/r \\ y_i \in GF(p), \text{ for } 1 \le i \le n/r \\ r | gcd(n, d) \end{cases} \tag{1}$$

Let $\theta(n/r, d/r, p)$ be the cardinality of the set $\Theta(n/r, d/r, p)$, then it can be deduced by the following lemma.

Lemma 1 *For any positive integer $r|gcd(n, d)$, we have*

$$\theta(n/r, d/r, p) = \sum_{ip+j=d/r} (-1)^i \binom{n/r}{i} \binom{n/r + j - 1}{j}.$$

Proof. *Let $h(x) = (\sum_{i=0}^{p-1} x^i)^{n/r}$. Then we have $\theta(n/r, d/r, p)$ is equal to the coefficient of $x^{d/r}$ in the expansion of $h(x)$. Note that*

$$\begin{aligned} h(x) &= (\sum\nolimits_{i=0}^{p-1} x^i)^{n/r} \\ &= (\frac{1 - x^p}{1 - x})^{n/r} \\ &= (1 - x^p)^{n/r} (1 + x + \cdots)^{n/r}. \end{aligned}$$

By a straightforward computation, we deduce that

$$\theta(n/r, d/r, p) = \sum_{ip+j=d/r} (-1)^i \binom{n/r}{i} \binom{n/r + j - 1}{j}.$$

□

For a given vector $(x_1, x_2, \ldots, x_n)$. If $x_1 + x_2 + \cdots + x_n = d$, then $G_n(x_1, x_2, \ldots, x_n)$ forms a partition of $\Theta(n, d, p)$. Let us consider the number of such partitions $g_{n,d}(p)$. From Remark 2, we get $g_{n,d}(p)$ is equal to the number of minimal functions with degree d. To compute it, we need to recall the well known inclusion–exclusion principle [15].

Lemma 2 (Inclusion–Exclusion Principle) *Let $A_1, \ldots, A_n$ be sets with finitely many elements. Then*

$$\begin{aligned} \left| \bigcup_{i=1}^{n} A_i \right| &= \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| \\ &\quad + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| \\ &\quad - \cdots + (-1)^{n-1} |A_1 \cap \ldots \cap A_n| \end{aligned} \tag{2}$$

In terms of Lemma 2, we enumerate these minimal functions having fixed degree.

Theorem 1 *We have*

$$g_{n,p}(d) = \sum_{r|gcd(n,d)} \left[\frac{1}{n/r} \sum_{s|gcd(n,d)/r} \mu(s)\theta(n/rs, d/rs, p) \right], \tag{3}$$

where $\mu(s)$ is Möbius function.

Proof. *For any $x \in \Theta(n,d,p)$, we have observed that $G_n(x) \subseteq \Theta(n,d,p)$ and there exists some integer $r|gcd(n,d)$ such that $\#G_n(x) = n/r$. Denote $N_{n/r}(d)$ by the number of such orbits which are of length n/r. Recall that $g_{n,p}(d)$ is the number of partitions of $\Theta(n,d,p)$, then we have*

$$g_{n,p}(d) = \sum_{r|gcd(n,d)} N_{n/r}(d).$$

In order to prove Theorem 1, it will suffice to calculate the value of $N_{n/r}(d)$.

Let $gcd(n,d)/r = p_1^{a_1} \dots p_l^{a_l}$ for distinct primes $p_1, \dots, p_l$ and $A_i = \{x \in \Theta(n/r, d/r, p) | \rho^{\frac{n}{rp_i}}(x) = x\}$ for $1 \le i \le l$. It follows that for any $x \in \Theta(n,d,p)$, $\#G_n(x) < n/r$ if and only if $x \in \bigcup_{i=1}^{l} A_i$. Note that the total number of elements belonging to $\Theta(n/r, d/r, p)$ is $\theta(n/r, d/r, p)$, and

$$\begin{aligned} |A_i| &= \theta(\frac{n}{rp_i}, \frac{d}{rp_i}, p), \\ |A_{j_1} \cap A_{j_2} \cap \dots \cap A_{j_t}| &= \theta(\frac{n}{rp_{j_1}p_{j_2}\dots p_{j_t}}, \frac{d}{rp_{j_1}p_{j_2}\dots p_{j_t}}, p), \\ &\quad \text{for } 1 \le j_1 < j_2 < \dots < j_t \le l. \end{aligned}$$

From Lemma 2, we have

$$\begin{aligned} N_{n/r}(d) &= \frac{1}{n/r} \left[\theta(\frac{n}{r}, \frac{d}{r}, p) - \left| \bigcup_{i=1}^{l} A_i \right| \right] \\ &= \frac{1}{n/r} \left[\theta(\frac{n}{r}, \frac{d}{r}, p) - \sum_{i=1}^{l} \theta(\frac{n}{rp_i}, \frac{d}{rp_i}, p) + \sum_{1 \le i < j \le l} \theta(\frac{n}{rp_ip_j}, \frac{d}{rp_ip_j}, p) \right. \\ &\quad \left. - \dots + (-1)^l \theta(\frac{n}{rp_1p_2\dots p_l}, \frac{d}{rp_1p_2\dots p_l}, p) \right] \\ &= \frac{1}{n/r} \sum_{s|gcd(n,d)/r} \mu(s)\theta(\frac{n}{rs}, \frac{d}{rs}, p), \end{aligned}$$

which leads to

$$g_{n,p}(d) = \sum_{r|gcd(n,d)} N_{n/r}(d)$$
$$= \sum_{r|gcd(n,d)} \left[\frac{1}{n/r} \sum_{s|gcd(n,d)/r} \mu(s)\theta(n/rs, d/rs, p) \right]. \quad (4)$$

Hence the proof is completed. □

Remark 3 *If $p = 2$, then $\theta(n/r, d/r, 2) = \binom{n/r}{d/r}$ with $r|gcd(n,d)$. From Theorem 1, we have*

$$g_{n,2}(d) = \sum_{r|gcd(n,d)} \left[\frac{1}{n/r} \sum_{s|gcd(n,d)/r} \mu(s) \binom{n/rs}{d/rs} \right]. \quad (5)$$

Thus the recurrence formula

$$g_{n,2}(d) = \frac{1}{n} \left[\binom{n}{d} - \sum_{k|'gcd(n,d)} \frac{n}{k} \cdot h_{n/k,d/k} \right] + \sum_{k|'gcd(n,d)} h(n/k, d/k)$$

in [8, Theorem 9] is simplified.

As an immediate corollary of Theorem 1, we obtain the number of homogeneous RotS functions over $GF(p)$.

Corollary 1 *The number of homogeneous RotS functions over $GF(p)$ with degree d is $p^{g_{n,p}(d)} - 1$.*

4 Conclusion

In this paper we focus on the open problem of the number of homogeneous RotS functions over $GF(p)$. We present complete enumeration results for these functions by using inclusion–exclusion principle. As a direct corollary, the known formula for counting homogeneous RotS Boolean functions in [8, Theorem 9] is simplified.

References

[1] J. Pieprzyk and C. X. Qu. Fast Hashing and Rotation-Symmetric Functions. Journal of Universal Computer Science, vol. 5, no. 1, pp. 20–31, 1999.

[2] 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, vol. 5, no. 5, pp. 1743-1751, 2007.

[3] S. Kavut, S. Maitra S. Sarkar and M. D. Yücel. Enumeration of 9-variable Rotation Symmetric Boolean Functions having Nonlinearity > 240. In INDOCRYPT 2006, LNCS 4329, Springer-Verlag, pp. 266–279, 2006.

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

[5] D. K. Dalai, K. C. Gupta and S. Maitra. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. In INDOCRYPT 2004, LNCS 3348, Springer-Verlag, pp. 92–106, 2004.

[6] Y. Li. Results on Rotation Symmetric Polynomials over F_p. Information Sciences Letters, vol. 178, pp. 280–286, 2008.

[7] S. J. Fu, C. Li and B. Sun. Enumeration of Homogeneous Rotation Symmetric Boolean function over $GF(p)$. In Proceeding of the 7th International Conference on Cryptology and Network Security, HongKong, China, LNCS 539, Springer-Verlag, pp. 278–284, 2008.

[8] P. Stănică and S. Maitra. Rotation Symmetric Boolean Functions–Count and Cryptographic Properties. Discrete Applied Mathematics, vol. 156, pp. 1567–1580, 2008.

[9] 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, pp. 161–177, 2004.

[10] A. Maximov. Classes of Plateaued Rotation Symmetric Boolean functions under Transformation of Walsh Spectra. In WCC 2005, pp. 325–334.

[11] M. Hell, A. Maximov and S. Maitra. On Efficient Implementation of Search Strategy for Rotation Symmetric Boolean Functions. In 9th International Workshop on Algebraic and Combinatoral Coding Theory, Black Sea Coast, Bulgaria, ACCT 2004, pp. 19–25, 2004.

[12] D. K. Dalai, S. Maitra, and S. Sarkar. Results on Rotaion Symmetric Bent Functions. Discrete Mathematics, vol. 309, no. 8, pp. 2398–2409, 2009.

[13] C. J. Mitchell. Enumerating Boolean Functions of Cryptographic Significance. Journal of Cryptology, vol. 2, no. 3, pp. 155–170, 1990.

[14] Y. X. Yang and B. Guo. Further Enumerating Boolean Functions of Cryptographic significance. Journal of Cryptology, vol. 8, no. 3, pp. 115–122, 1995.

[15] L. Comtet. Advanced Combinatorics. Amsterdam, The Netherlands: Reidel, 1974.