Enumeration of Homogeneous Rotation Symmetric Functions over GF(*p*)[1]

Shaojing Fu   Chao Li   Bing Sun

Department of Mathematatic and System Science, NUDT, Changsha, 410073

Abstract: We give a lower bound on the number of homogeneous rotation symmetric functions over finite field GF(*p*) by finding solutions of an equation system. Furthermore, we give a formula to count homogeneous rotation symmetric functions with prime degree more than 3, which partially solve the open problem in [7].

Key words: Rotation symmetry; Nonlinearity; Minimal function; Monic monomial

1. Introduction

In [1], Pieprzyk and Qu studied some functions, which they called *rotation symmetric* (*RotS*), as components in the rounds of a hashing algorithm. This class of functions is invariant under circular translation of indices, and it is clear that this class of functions is very rich in terms of many cryptographic properties such as nonlinearity and correlation immune. In[2-4], Stanica, Maitra and Clark gave out many counting results of *RotS* Boolean functions. They also investigated the correlation immune property of such functions. Dalai and Maitra studied *RotS* bent function in [5]. Maximov, Hell and Maitra got many interesting results on plateaued *RotS* functions in [6]. Yuan Li extended the concept of *RotS* from GF(2) to GF(*p*) , and got many results about their cryptographic properties and enumeration [7]. In this paper, by studying *RotS* functions over GF(*p*), we give a lower bound on the number of homogeneous *RotS* functions over GF(*p*), and one of the open problems in [7] is partially solved.

2. Preliminaries

In this paper, *p* is a prime number. Let GF(*p*) be the finite field of *p* elements, and GF(*p*)^n be the vector space of dimension *n* over GF(*p*). An *n*-variable function $f(x_1, x_2, \cdots, x_n)$ can be seen as a multivariate polynomial over GF(*p*), that is,

$$f(x_1, x_2, \cdots, x_n) = \sum_{y_1, y_2, \cdots, y_n = 0}^{p-1} a_{y_1, y_2, \cdots, y_n} x_1^{y_1} x_2^{y_2} \cdots x_n^{y_n}$$

where the coefficients $a_{y_1, y_2, \cdots, y_n}$ is a constant in GF(*p*). This representation of f is called the *algebraic normal form* (ANF) of f . The number $y_1 + y_2 + \cdots + y_n$ will be defined as the degree of term $a_{y_1, y_2, \cdots, y_n} x_1^{y_1} x_2^{y_2} \cdots x_n^{y_n}$ with nonzero coefficient $a_{y_1, y_2, \cdots, y_n}$. The greatest degree of all the terms of *f* is called the A*lgebraic degree,* denoted by deg(*f*). If the degrees of all the terms of *f* are equal, then we say *f* is homogeneous.

---

[1] Supported by the National Natural Science Foundation of China (60573028)
E-mail: shaojing1984@163.com

If $x_i \in \mathrm{GF}(p)$ for $1 \le i \le n$. and $0 \le k \le n-1$, we define

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

Let $x = (x_1, x_2, \cdots, x_n) \in \mathrm{GF}(p)^n$. Then we can extend the definition of ρ_n^k on tuples and monomials as follows:

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

and

$$\rho_n^k(x_1^{y_1} x_2^{y_2} \cdots x_n^{y_n}) = (\rho_n^k(x_1))^{y_1} (\rho_n^k(x_2))^{y_2} \cdots (\rho_n^k(x_n))^{y_n}$$

Definition 1 A function $f(x_1, x_2, \cdots, x_n)$ over $\mathrm{GF}(p)^n$ is *RotS* if for each input $(x_1, x_2, \cdots, x_n) \in \mathrm{GF}(p)^n$, $f(\rho_n^k(x_1, x_2, \cdots, x_n)) = f(x_1, x_2, \cdots, x_n)$ for any $0 \le k \le n-1$.

3. Enumeration of Homogeneous *RotS* Functions

In this section, we will do some enumeration on homogeneous *RotS* functions over GF(p). We start with the definition of the *minimal function*. A function $f(x_1, x_2, \cdots, x_n)$ is the *minimal function* of monic monomial $x_1^{y_1} x_2^{y_2} \cdots x_n^{y_n}$ if $f(x_1, x_2, \cdots, x_n)$ has the form

$$f(x_1, x_2, \cdots, x_n) = \sum_{k=0}^{N-1} \rho_n^k(x_1^{y_1} x_2^{y_2} \cdots x_n^{y_n})$$

where $N = \#\{\rho_n^k(x_1^{y_1} x_2^{y_2} \cdots x_n^{y_n}) \mid 0 \le k \le n-1\}$.

Definition 2 A monic monomial $x_1^{z_1} x_2^{z_2} \cdots x_n^{z_n}$ over $\mathrm{GF}(p)^n$ is *analogous* to $x_1^{y_1} x_2^{y_2} \cdots x_n^{y_n}$ if $\{y_1, y_2, \cdots, y_n\} = \{z_1, z_2, \cdots, z_n\}$

Considering the equation system Ω

$$\Omega: \begin{cases} y_1 + y_2 + \cdots + y_n = d \\ 0 \le y_n \le y_{n-1} \le \cdots \le y_2 \le y_1 \le p-1 \\ y_i \in Z \text{ for all } 1 \le i \le n \end{cases}$$

Let the number of solutions of the equation system Ω is N_Ω, and the solutions are

$$(y_1^{(1)}, y_2^{(1)}, \cdots, y_n^{(1)}), (y_1^{(2)}, y_2^{(2)}, \cdots, y_n^{(2)}), \cdots, (y_1^{(N_\Omega)}, y_2^{(N_\Omega)}, \cdots, y_n^{(N_\Omega)}) = (\underbrace{1, \cdots, 1}_{d}, 0, \cdots, 0)$$

Lemma 1 Let $m_i^{(j)} (0 \le i \le p-1)$ be the number of times that i appears in $\{y_1^{(j)}, y_2^{(j)}, \cdots, y_n^{(j)}\}$, then the number of monic monomials with degree d is $\sum_{j=1}^{N_\Omega} \frac{n!}{m_1^{(j)}! m_2^{(j)}! \cdots m_n^{(j)}!}$

Proof. For a fixed j and corresponding solution $(y_1^{(j)}, y_2^{(j)}, \cdots, y_n^{(j)})$, then the number of monic monomials *analogous* to $x_1^{y_1^{(j)}} x_2^{y_2^{(j)}} \cdots x_n^{y_n^{(j)}}$ is

$$\binom{n}{m_1^{(j)}}\binom{n-m_1^{(j)}}{m_2^{(j)}}\cdots\binom{n-\sum_{i=1}^{n-1}m_i^{(j)}}{m_n^{(j)}}=\frac{n!}{m_1^{(j)}!m_2^{(j)}!\cdots m_n^{(j)}!},$$

so the number of monic monomials with degree *d* is $\sum_{j=1}^{N_\Omega}\frac{n!}{m_1^{(j)}!m_2^{(j)}!\cdots m_n^{(j)}!}$. □

Theorem 1 Let NUM_d be the number of *n*-variable homogeneous *Rots* functions over GF(*p*) with degree *d* , then $NUM_d \ge p^{\sum_{j=1}^{N_\Omega}\frac{(n-1)!}{m_1^{(j)}!m_2^{(j)}!\cdots m_n^{(j)}!}}-1$

Proof. Let T_d be the number of minimal functions with degree *d*. Note that a homogeneous Rots function $f(x_1,x_2,\cdots,x_n)$ with degree *d* is a nonzero combination of degree *d* minimal function. That is

$$f(x_1,x_2,\cdots,x_n)=\sum_{m=1}^{T_d}a_{g_m}g_m(x_1,x_2,\cdots,x_n)$$

where $a_{g_m}\in$GF$(p)^n$, $g_m(x_1,x_2,\cdots,x_n)$ are minimal functions with degree *d*.

If a minimal function has the term $x_1^{y_1^{(j)}}x_2^{y_2^{(j)}}\cdots x_n^{y_n^{(j)}}$, then it has all the terms of the set $\{\rho_n^k(x_1^{y_1^{(j)}}x_2^{y_2^{(j)}}\cdots x_n^{y_n^{(j)}})\,|\,0\le k\le n-1\}$, It is easy to show that $\#\{\rho_n^k(x_1^{y_1^{(j)}}x_2^{y_2^{(j)}}\cdots x_n^{y_n^{(j)}})\,|\,0\le k\le n-1\}\le n$. From lemma 1 we know the number of monic monomials with degree *d* is $\sum_{j=1}^{N_\Omega}\frac{n!}{m_1^{(j)}!m_2^{(j)}!\cdots m_n^{(j)}!}$, so $T_d\le\sum_{j=1}^{N_\Omega}\frac{(n-1)!}{m_1^{(j)}!m_2^{(j)}!\cdots m_n^{(j)}!}$.

Since the constant 0 function is not counted, we get $NUM_d \ge p^{\sum_{j=1}^{N_\Omega}\frac{(n-1)!}{m_1^{(j)}!m_2^{(j)}!\cdots m_n^{(j)}!}}-1$ □

Note that if *n* is a prime, then $\#\{\rho_n^k(x_1^{y_1^{(j)}}x_2^{y_2^{(j)}}\cdots x_n^{y_n^{(j)}})\,|\,0\le k\le n-1\}=n$ for any $1\le j\le N_\Omega$, so we have the following Corollary.

Corollary 1 The lower bound in Theorem 1 can be reached if *n* is a prime number.

Theorem 2 If *d* is a prime number. The number of *n*-variable homogeneous *Rots* functions over GF(*p*) with degree *d* is $p^{\sum_{j=1}^{N_\Omega-1}\frac{(n-1)!}{m_1^{(j)}!m_2^{(j)}!\cdots m_n^{(j)}!}+\left\lceil\frac{(n-1)!}{(n-d)!d!}\right\rceil}-1$

Proof . Let $m_i^{(j)}(0\le i\le p-1)$ be the number of times that *i* appears in $\{y_1^{(j)},y_2^{(j)},\cdots,y_n^{(j)}\}$.
We distinguish two case.
Case 1:
$1\le j\le N_\Omega-1$, then $\#\{\rho_n^k(x_1^{y_1^{(j)}}x_2^{y_2^{(j)}}\cdots x_n^{y_n^{(j)}})\,|\,0\le k\le n-1\}=n$
Otherwise, if $\#\{\rho_n^k(x_1^{y_1^{(j)}}x_2^{y_2^{(j)}}\cdots x_n^{y_n^{(j)}})\,|\,0\le k\le n-1\}=N<n$
Then $N\,|\,n$, and $\rho_n^N(x_1^{y_1^{(j)}}x_2^{y_2^{(j)}}\cdots x_n^{y_n^{(j)}})=x_1^{y_1^{(j)}}x_2^{y_2^{(j)}}\cdots x_n^{y_n^{(j)}}$

$$\Rightarrow x_{N+1}^{y_1^{(j)}} x_{N+2}^{y_2^{(j)}} \cdots x_n^{y_{n-N}^{(j)}} x_1^{y_{n-N+1}^{(j)}} x_2^{y_{n-N+2}^{(j)}} \cdots x_N^{y_n^{(j)}} = x_1^{y_1^{(j)}} x_2^{y_2^{(j)}} \cdots x_n^{y_n^{(j)}}$$

$$\Rightarrow \sum_{j=1}^{N} y_1^{(j)} = \sum_{j=N+1}^{2N} y_1^{(j)} = \cdots = \sum_{j=n-N}^{n} y_1^{(j)}$$

It is clear that $\sum_{j=1}^{N} y_1^{(j)} \neq 1$ and $\sum_{j=1}^{N} y_1^{(j)} \mid d$, This contradict the fact that *d* is a prime number.

There are $\sum_{j=1}^{N_\Omega} \frac{n!}{m_1^{(j)}!m_2^{(j)}!\cdots m_n^{(j)}!}$ monic monomials, so the number of minimal function is $\sum_{j=1}^{d-1} \frac{(n-1)!}{m_1^{(j)}!m_2^{(j)}!\cdots m_n^{(j)}!}$.

Case 2:

$j = N_\Omega$, then $(y_1^{(N_\Omega)}, y_2^{(N_\Omega)}, \cdots, y_n^{(N_\Omega)})=(\underbrace{1,\cdots,1}_{d},0,\cdots,0)$

We know there are $\frac{n!}{(n-d)!d!}$ degree *d* monic monomials,

If $d \mid n$, Then there is only one minimal function has the $\frac{n}{d}$ term monic monomials, the other minimal functions have the *n* term monic monomials, the number of minimal functions is

$$\frac{1}{n}\left(\frac{n!}{(n-d)!d!} - \frac{n}{d}\right) + 1 = \left\lceil \frac{(n-1)!}{(n-d)!d!} \right\rceil$$

If $d \nmid n$, then all minimal functions have the *n* term monic monomials, the number of minimal functions is $\frac{(n-1)!}{(n-d)!d!}$.

so the total number of minimal functions is $\sum_{j=1}^{d-1} \frac{(n-1)!}{m_1^{(j)}!m_2^{(j)}!\cdots m_n^{(j)}!} + \left\lceil \frac{(n-1)!}{(n-d)!d!} \right\rceil$, then we get the count. □

Example 1 we count the number of homogeneous *Rots* functions with degree 5 over GF(*p*) ($p > 6$) .

First, we solve the equation system

$$\Omega : \begin{cases} y_1 + y_2 + \cdots + y_n = 5 \\ 0 \le y_n \le y_{n-1} \le \cdots \le y_2 \le y_1 \le p-1 \\ y_i \in Z \text{ for all } 1 \le i \le n \end{cases}$$

There are seven solutions: $(5,0,\cdots,0)$, $(4,1,0,\cdots,0)$, $(3,2,0,\cdots,0)$, $(3,1,1,0,\cdots,0)$, $(2,2,1,0,\cdots,0)$, $(2,1,1,1,0,\cdots,0)$, $(1,1,1,1,1,0,\cdots,0)$

Then $\sum_{j=1}^{d-1} \frac{(n-1)!}{m_1^{(j)}!m_2^{(j)}!\cdots m_n^{(j)}!} + \left\lceil \frac{(n-1)!}{(n-d)!d!} \right\rceil$

$$= \frac{(n-1)!}{(n-1)!} + \frac{(n-1)!}{(n-2)!} + \frac{(n-1)!}{(n-2)!} + \frac{(n-1)!}{2!(n-3)!} + \frac{(n-1)!}{2!(n-3)!} +$$

$$\frac{(n-1)!}{3!(n-4)!}+\left\lceil\frac{(n-1)!}{5!(n-5)!}\right\rceil$$

$$=\left\lceil\frac{(n-1)(n-2)(n-3)(n-4)}{5!}\right\rceil+\frac{(n-1)(n-2)(n-3)}{3!}+(n^2-n+1)$$

So the number of homogeneous *Rots* functions with degree 5over GF(p) equals p^M-1, where

$$M=\left\lceil\frac{(n-1)(n-2)(n-3)(n-4)}{5!}\right\rceil+\frac{(n-1)(n-2)(n-3)}{3!}+(n^2-n+1)$$

4. Conclusion

In this paper, we obtain some counting results about homogeneous rotation symmetric functions over finite field GF(p). We get a lower bound by finding solutions of an equation system, we show that this bound is tight when n is prime. We also partially solve the open problem in [7]. Besides, for general d (not a prime number), it is still an open problem to count the homogeneous rotation symmetric polynomials with degree d more than 3.

References

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

[2] P. Stanica, S. Maitra, Rotation symmetric Boolean functions-count and cryptographic properties, in: R.C. Bose Centenary Symposium on Discrete Mathematics and Applications, Electronic Notes in Discrete Mathematics, Elsevier, vol. 15, December 2002, pp. 139–145.

[3] P. Stanica, S. Maitra, A constructive count of rotation symmetric functions, Information Processing Letters 88 (2003) 299–304.

[4] P. Stanica, S. Maitra, J. Clark, Results on rotation symmetric bent and correlation immune Boolean functions, in: Fast Software Encryption Workshop (FSE 2004), New Delhi, India, LNCS, vol. 3017, Springer Verlag, 2004, pp. 161–177.

[5] D.K. Dalai, S. Maitra, S. Sarkar, Results on rotation symmetric bent functions, in: Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA’06, March 2006, pp. 137–156.

[6] A. Maximov, M. Hell, S. Maitra, Plateaued Rotation Symmetric Boolean Functions on Odd Number of Variables, in: First Workshop on Boolean Functions: Cryptography and Applications, BFCA 05, LIFAR, University of Rouen, France, March 7–9, 2005, pp. 83–104.

[7] Yuan Li, Results on rotation symmetric polynomials over GF(p), Information Sciences 178 (2008) 280–286.