Available online at www.sciencedirect.com
ScienceDirect
Information Sciences 178 (2008) 280–286
INFORMATION SCIENCES
AN INTERNATIONAL JOURNAL
www.elsevier.com/locate/ins

Results on rotation symmetric polynomials over $GF(p)$

Yuan Li *

Department of Mathematics and Computer Science, Alcorn State University, Lorman, MS 39096, USA

Received 7 October 2006; received in revised form 27 March 2007; accepted 31 March 2007

Abstract

In this paper, we generalize the recent counting results about rotation symmetric Boolean functions to the rotation symmetric polynomials over finite fields $GF(p)$. By using Möbius function, we obtain some formulas for more general n, the number of variables. Some known formula in Boolean case are simplified.

Keywords: Cryptography; Boolean function; Rotation symmetry; Finite fields; Polynomials; Euler function; Möbius function; Principle of inclusion and exclusion

1. Introduction

Rotation symmetric Boolean functions have received a lot of attention. These functions are invariant under circular translation of indices. This is a highly desirable property when efficient evaluation of the function is important, for instance in the implementation of MD4, MD5 or HAVAL, since evaluations from previous iterations can be reused. Besides, recently, for odd n, Kavut and etc. proved that n variable Boolean functions with nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ exist if and only if n is greater than 7 in [3]. Thus, a long standing (almost three decades) open problem is solved. Actually, the author found some nine variable rotation symmetric Boolean functions with high nonlinearity by some efficient search. It is clear that this class of functions is very rich in terms of many cryptographic properties such as nonlinearity and correlation immune. In [6–8], Stănică, Maitra and Clark gave out many counting results of rotation symmetric Boolean functions. They also investigated the correlation immune property of such functions. Dalai and Maitra studied rotation symmetric bent function in [1]. Maximov, Hell and Maitra got many interesting results on plateaued rotation symmetric functions in [5]. On the other hand, it is natural to extend the various cryptographic conceptions from $GF(2)$ to $GF(p)$ or $GF(p^n)$. For example, in [2], Hu and Xiao studied the resilient functions on $GF(p)$. In [4], Kumar, Scholtz and Welch studied the bent function over any finite fields. In this paper, by studying rotation symmetric functions over $GF(p)$, we get many results about their cryptographic property and enumeration . We also simplify some known formula in Boolean case.

* Tel.: +1 601 6181501.
E-mail addresses: yuanli7983@alcorn.edu, yuanli7983@gmail.com

0020-0255/$ - see front matter
doi:10.1016/j.ins.2007.03.031

2. Preliminaries

In this paper, p is a prime number. If $f : GF(p)^n \to GF(p)$, then f can be uniquely expressed in the following form, called the *algebraic normal form* (ANF):

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

where each coefficient $a_{k_1,k_2,\ldots,k_n}$ is a constant in $GF(p)$. The number $k_1 + k_2 + \cdots + k_n$ will be defined as the degree of term $a_{k_1,k_2,\ldots,k_n} x_1^{k_1}, x_2^{k_2}, \ldots, x_n^{k_n}$ with nonzero coefficient $a_{k_1,k_2,\ldots,k_n}$. 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 $x_i \in GF(p) = \{0, 1, \ldots, p-1\}$ for $1 \leqslant i \leqslant n$. For $1 \leqslant k \leqslant n$, we define $\rho_n^k(x_i) = x_{i+k}$ if $i + k \leqslant n$, and $= x_{i+k-n}$ if $i + k > n$. Let $(x_1, x_2, \ldots, x_n) \in GF(p)^n$. Then we extend the definition $\rho_n^k(x_1, x_2, \ldots, x_n) = (\rho_n^k(x_1), \rho_n^k(x_2), \ldots, \rho_n^k(x_n))$. All the vectors in $GF(p)^n$ can be put into order lexicographically. In other words, for different vectors $X = (x_1, x_2, \ldots, x_n)$ and $Y = (y_1, y_2, \ldots, y_n)$, we define $(x_1, x_2, \ldots, x_n) \lhd (y_1, y_2, \ldots, y_n)$ if and only if $x_1 < y_1$ or $x_i = y_i$ for $i = 1, 2, \ldots, k$ and $x_{k+1} < y_{k+1}$ for some k, where $1 < k \leqslant n - 1$. For convenience, we will say X is smaller than Y if $X \lhd Y$, $(0, 0, \ldots, 0)$ is the smallest and $(p-1, p-1, \ldots, p-1)$ the biggest. With this order, we interpret a function $f(x_1, x_2, \ldots, x_n)$ from $GF(p)^n$ to $GF(p)$ as a p-ary string of length p^n, $f = [f(0, 0, \ldots, 0), f(0, 0, \ldots, 1), \ldots, f(p-1, p-1, \ldots, p-1)]$.

Definition 2.1. A function f over $GF(p)^n$ is rotation symmetric if and only if $f(\rho_n^k(x_1, x_2, \ldots, x_n)) = f(x_1, x_2, \ldots, x_n)$ for any $(x_1, x_2, \ldots, x_n) \in GF(p)^n$ and any $1 \leqslant k \leqslant n$.

Note that there are p^n different input values corresponding to a function. From the above definition, it is clear that for rotation symmetric function, the function f possesses the same value corresponding to each of the subsets generated from the rotation symmetry. As example, for $n = 4$ and $p = 3$, one gets the following partitions:

$\{(0, 0, 0, 0)\}$,
$\{(0, 0, 0, 1), (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0)\}$,
$\{(0, 0, 0, 2), (2, 0, 0, 0), (0, 2, 0, 0), (0, 0, 2, 0)\}$,
$\{(0, 0, 1, 1), (1, 0, 0, 1), (1, 1, 0, 0), (0, 1, 1, 0)\}$,
$\{(0, 0, 1, 2), (2, 0, 0, 1), (1, 2, 0, 0), (0, 1, 2, 0)\}$,
$\{(0, 0, 2, 1), (1, 0, 0, 2), (2, 1, 0, 0), (0, 2, 1, 0)\}$,
$\{(0, 0, 2, 2), (2, 0, 0, 2), (2, 2, 0, 0), (0, 2, 2, 0)\}$,
$\{(0, 1, 0, 1), (1, 0, 1, 0)\}$,
$\{(0, 1, 0, 2), (2, 0, 1, 0), (0, 2, 0, 1), (1, 0, 2, 0)\}$,
$\{(0, 1, 1, 1), (1, 0, 1, 1), (1, 1, 0, 1), (1, 1, 1, 0)\}$,
$\{(0, 1, 1, 2), (2, 0, 1, 1), (1, 2, 0, 1), (1, 1, 2, 0)\}$,
$\{(0, 1, 2, 1), (1, 0, 1, 2), (2, 1, 0, 1), (1, 2, 1, 0)\}$,
$\{(0, 1, 2, 2), (2, 0, 1, 2), (2, 2, 0, 1), (1, 2, 2, 0)\}$,
$\{(0, 2, 0, 2), (2, 0, 2, 0)\}$,
$\{(0, 2, 1, 1), (1, 0, 2, 1), (1, 1, 0, 2), (2, 1, 1, 0)\}$,
$\{(0, 2, 1, 2), (2, 0, 2, 1), (1, 2, 0, 2), (2, 1, 2, 0)\}$,
$\{(0, 2, 2, 1), (1, 0, 2, 2), (2, 1, 0, 2), (2, 2, 1, 0)\}$,
$\{(0, 2, 2, 2), (2, 0, 2, 2), (2, 2, 0, 2), (2, 2, 2, 0)\}$,
$\{(1, 1, 1, 1)\}$.