Gen. Math. Notes, Vol. 16, No. 1, May, 2013, pp.12-19
ISSN 2219-7184;
www.i-csrs.org
Available free online at http://www.geman.in

On the Weight and Nonlinearity of Quadratic Rotation Symmetric Function with Two MRS Functions

Hongli-Liu

Institute of Mathematics and Statistics
Zhejiang University of Finance and Economics
Hangzhou, China
E-mail: ooolhl@163.com

(Received: 4-3-13 / Accepted: 7-4-13)

Abstract

The weight and nonlinearity of quadratic MRS function $f_{n,s}$ have been studied . This paper studies the weight and nonlinearity of odd variables quadratic rotation symmetric function which contains two MRS functions $f_{n,2}$ and $f_{n,3}$. First, we give the equivalent form of $f_{n,2} + f_{n,3}$ by using recursive formula and the equivalent form of $f_{n,2} + f_{n,3}$ which can be obtain by nonsingular affine transformation for $n = 3, 5, 7$. Furthermore, we characterize the weight and nonlinearity of $f_{n,2} + f_{n,3}$ from the existing research results.

Keywords: *Boolean function, Rotation symmetry, Weight, Nonlinearity, Affine equivalent.*

1 Introduction

Boolean functions have many applications in coding theory and cryptography. A detail account of the latter applications can be found in the book [1]. Rotation symmetric Boolean functions were first introduced at Eurocrypt 1998. Recently, rotation symmetric Boolean functions have attracted attention due to their simplicity-invariant under rotation transform - for efficient computation. In [2], rotation symmetric functions are used for fast hash function design.

It has been found that this class of functions is extremely rich in terms of cryptographically significant functions, and a lot of research about RotS functions in characteristic $GF(2)$ has been done in [3-9] where the authors studied some important cryptographic properties of these functions. Homogeneous rotation symmetric Boolean functions have been extensively studied because of their applications in cryptography. In [2], the weight and nonlinearity of quadratic rotation symmetric functions were estimated and exactly formulated for some specific functions. In [3], more formulations for the exact values were carried out. In [5], the weight and nonlinearity of quadratic MRS functions $f_{n,s}$ were characterized. By analyzing the naturally associated permutation of $f_{n,s}$, it showed that both values are directly connected to the cycle structure of the permutation. We will be interesting to examine the weight and nonlinearity of quadratic rotation symmetric functions which contain two MRS functions.

2 Notation and Preliminaries

We define V_n to be the vector space of dimensional n over the finite field $GF(2) = \{0, 1\}$. There are 2^n vectors in V_n. An n variable Boolean function $f(x_1, x_2, \cdots, x_n) = f(x)$ is a mapping from V_n to $GF(2)$. The set of all n variable Boolean functions is denoted by B_n. An n variable Boolean function can be seen as a multivariate polynomial over $GF(2)$. More precisely , $f(x_1, x_2, \cdots, x_n)$ can be written as $a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1 \le i < j \le n} a_{ij} x_i x_j + \cdots + a_{12\cdots n} x_1 x_2 \cdots x_n$, where the coefficients $a_0,\ a_i,\ a_{ij}, \cdots, a_{12\cdots n} \in \{0, 1\}$. This representation of f is called the*algebraic normal form* (ANF) of f. The number of variables in the highest order product term with nonzero coefficient is called the *algebraic degree* , or simply the degree of f. A Boolean function is said to be homogeneous if its ANF contains terms of the same degree only. Functions of degree at most 1 are called $affine$ functions. The set of all affine functions in B_n is denoted by A_n.We define the weight of a function by the number of $x \in V_n$ such that $f(x) = 1$, denoted by $wt(f)$. A function $f \in B_n$ is *balanced* if $wt(f) = 2^{n-1}$. The distance between two functions f and g,denoted by $d(f, g)$, is defined by $wt(f + g)$, where the addition $f + g$ is taking place in $GF(2)$. The set of all integers is denoted by Z.

Definition 2.1 *The nonlinearity of a function $f \in B_n$ is the minimum distance between f and the set of all affine functions A_n, and denoted by $NL(f)$. That is, $NL(f) = min_{l \in A_n} d(f, l)$.*

Definition 2.2 *Two functions $f, g \in B_n$ are affinely equivalent if $g(x) = f(xA + b)$ for some nonsingular $n \times n$ matrix A over $GF(2)$ and $b \in V_n$. If f and g are affinely equivalent, we write them as $f \equiv g$.*

It can be easily checked that weight and nonlinearity are invariant under nonsingular affine transforms. That is, if $f \equiv g$ then $wt(f) = wt(g)$ and $NL(f) = NL(g)$. We say that the weight and nonlinearity are *affine invariants*. The following formula in Lemma 2.3 can be found in [10].

Lemma 2.3 *Let $h(x) = \sum_{i=1}^{k} x_{2i-1}x_{2i} + \sum_{i=2k+1}^{n} a_i x_i$ be an n variable function for $k \leq \frac{n}{2}$. Then the nonlinearity is given by $NL(h) = 2^{n-1} - 2^{n-k-1}$. If all the linear terms vanish then its weight is the same as the nonlinearity; otherwise it is balanced.*

Once a quadratic function is transformed to the equivalent function as in Lemma 2.3, its weight and nonlinearity can be found in Lemma 2.3.

Consider $\rho = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$, a permutation of rotation on $\{1, 2, \cdots, n\}$. The permutation ρ gives rise to an *action* on V_n such that, for $x = (x_1, x_2, \cdots, x_n) \in V_n$ and $k \in Z$, $\rho^k(x) = (x_{\rho^k(1)}, \cdots, x_{\rho^k(n)})$. The indices can be written explicitly as , for $i = 1, 2, \cdots, n$,

$$\rho^k(i) = \begin{cases} n & if\ (i+k) \equiv 0(mod n), \\ (i+k)(mod\ n) & otherwise. \end{cases}$$

The *orbit* of $x \in V_n$ under ρ is the set $\{\rho^k(x) | k \in Z\}$. Similarly, we can extend the action to a monomial $m(x) = x_{i_1} \cdots x_{i_d} \in B_n$ by defining $\rho^k(m(x)) = x_{\rho^k(i_1)} \cdots x_{\rho^k(i_d)}$. We define the orbit of $m(x)$ similarly by $\{\rho^k(m(x)) | k \in Z\}$.

Definition 2.4 *A function $f \in B_n$ is called rotation symmetric if and only if for any $(x_1, \cdots, x_n) \in V_n$, $f(x_1, \cdots, x_n) = f(\rho^k(x_1, \cdots, x_n))$ for any $1 \leq k \leq n$.*

If a monomial $m(x)$ appears in a rotation symmetric function as a term then all monomials in the orbit of $m(x)$ should also appear in the function as terms. An example of a quadratic rotation symmetric function in B_6 is $x_1x_3 + x_2x_4 + x_3x_5 + x_4x_6 + x_5x_1 + x_6x_2$. The simplest quadratic functions f generated by cyclic permutations of the variables in a single monomial. We call such functions *monomial rotation symmetric functions*, or MRS functions, for brevity. Thus any quadratic MRS function $f(x)$ in n variables can be written as

$$f_{n,j}(x) = x_1x_j + x_2x_{j+1} + \cdots + x_nx_{j-1} \tag{1}$$

for some j with $2 \leq j \leq [\frac{n+1}{2}]$, or, in the special case when n is even and $j = \frac{n}{2} + 1$, as

$$f_{n,\frac{n}{2}+1}(x) = x_1x_{\frac{n}{2}+1} + x_2x_{\frac{n}{2}+2} + \cdots + x_{\frac{n}{2}}x_n \tag{2}$$

The latter function (2) has only $\frac{n}{2}$ terms, whereas the functions in (1) have n terms. Because of this, we call the function $f_{n,\frac{n}{2}+1}(x)$ the *short quadratic function in n variables*. In [5], the weight and nonlinearity of MRS functions are characterized using the structure of the cycle decomposition of the associated permutation ρ_s, where

$$\rho_s = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ s & s+1 & \cdots & s-2 & s-1 \end{pmatrix}$$

for $2 \leq s \leq \left\lceil \frac{n}{2} \right\rceil$.

3 Main Results

In this paper, we will characterize the weight and nonlinearity of functions which contain two MRS function $f_{n,2}$ and $f_{n,3}$, where n is odd, and

$$f_{n,2} = x_1x_2 + x_2x_3 + \cdots + x_nx_1$$

$$f_{n,3} = x_1x_3 + x_2x_4 + \cdots + x_nx_2$$

In order to study the weight and nonlinearity of $f_{n,2} + f_{n,3}$, we need to find the recurrence relation of the function and affine equivalence function for $n = 3, 5, 7$.

Lemma 3.1 *For odd n, we have*

$$f_{n,2} + f_{n,3} \equiv y_1y_2 + y_3y_5 + y_4y_6 + f_{n-6,2} + f_{n-6,3} + y_8 + y_{n-1} + 1 \quad (3)$$

$$f_{n,2} + f_{n,3} + x_2 + x_{n-1} \equiv y_1y_2 + y_3y_5 + y_4y_6 + f_{n-6,2} + f_{n-6,3} \quad (4)$$

where $f_{n-6,2} = y_7y_8 + y_8y_9 + \cdots + y_ny_7$, $f_{n-6,3} = y_7y_9 + y_8y_{10} + \cdots + y_ny_8$.

Proof. We can obtain the affine equivalent functions of (3) and (4) by the different nonsingular affine transformation, respectively .
For (3), we define the affine transformation by

$y_1 = x_1 + x_3 + x_4 + x_n$ $\quad$ $y_2 = x_2 + x_3 + x_{n-1} + x_n$
$y_3 = x_3 + x_4 + x_6 + x_7$ $\quad$ $y_5 = x_5 + x_{n-1} + 1$
$y_4 = x_4 + x_5 + x_7 + x_8 + 1$ $\quad$ $y_6 = x_6 + x_n + 1$
$y_i = x_i, i > 6.$

For (4), we define the affine transformation by

$y_1 = x_1 + x_3 + x_4 + x_n + 1$ $\quad$ $y_2 = x_2 + x_3 + x_{n-1} + x_n$
$y_3 = x_3 + x_4 + x_6 + x_7$ $\quad$ $y_5 = x_5 + x_{n-1}$
$y_4 = x_4 + x_7 + x_8 + x_{n-1}$ $\quad$ $y_6 = x_6 + x_n$

$y_i = x_i, i > 6.$

Remark. From Lemma 3.1, we can obtain the equivalent form of $f_{n,2}+f_{n,3}$ if the equivalent forms of $f_{n,2} + f_{n,3}$ for smaller n are determined.
If $n = 3$, then $f_{3,2} + f_{3,3} = x_1x_2 + x_2x_3 + x_3x_1 + x_1x_3 + x_2x_1 + x_3x_2 = 0$.
If $n = 5$, then $f_{5,2} + f_{5,3} = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 + x_1x_3 + x_2x_4 +$
$x_3x_5 + x_4x_1 + x_5x_2 \equiv y_1y_2 + y_3y_4 + y_5$ (5)
$f_{5,2} + f_{5,3} + x_2 + x_4 \equiv y_1y_2 + y_3y_4 + y_5$ (6)
If $n = 7$, then $f_{7,2} + f_{7,3} = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_6 + x_6x_7 + x_7x_1 +$
$x_1x_3 + x_2x_4 + x_3x_5 + x_4x_6 + x_5x_7 + x_6x_1 + x_7x_2 \equiv y_1y_2 + y_3y_5 + y_4y_6$ (7)
$f_{7,2} + f_{7,3} + x_2 + x_6 \equiv y_1y_2 + y_3y_5 + y_4y_6$ (8)

We can get the results by the following nonsingular affine transformations,respectively.
For (5):

$y_1 = x_1 + x_3 + x_4 + x_5$ $\quad$ $y_2 = x_2 + x_3 + x_4 + x_5$
$y_3 = x_3 + x_5 + 1$ $\quad$ $y_4 = x_4 + x_5 + 1$
$y_5 = x_5$

For (6):

$y_1 = x_1 + x_3 + x_4 + x_5 + 1$ $\quad$ $y_2 = x_2 + x_3 + x_4 + x_5$
$y_3 = x_3 + x_5 + 1$ $\quad$ $y_4 = x_4 + x_5$
$y_5 = x_5$

For (7):

$y_1 = x_1 + x_3 + x_4 + x_7$ $\quad$ $y_2 = x_2 + x_3 + x_6 + x_7$
$y_3 = x_3 + x_4 + x_6 + x_7$ $\quad$ $y_5 = x_5 + x_6 + 1$
$y_4 = x_4 + x_7$ $\quad$ $y_6 = x_6 + x_7 + 1$

For (8):

$y_1 = x_1 + x_3 + x_4 + x_7 + 1$ $\quad$ $y_2 = x_2 + x_3 + x_6 + x_7$
$y_3 = x_3 + x_4 + x_6 + x_7$ $\quad$ $y_5 = x_5 + x_6 + 1$
$y_4 = x_4 + x_7$ $\quad$ $y_6 = x_6 + x_7 + 1$

From Lemma 3.1, the recurrence relation of $f_{n,2} + f_{n,3}$ shows that the equivalent form of $f_{n,2} + f_{n,3}$ depends on the equivalent form of $f_{n-6,2} + f_{n-6,3}$. Therefore, for odd n, we just need to discuss the three congruence classes of mod 6.

Lemma 3.2 (1) *If* $n = 6k + 1, k = 2, 3, 4, \cdots$, *then*
$f_{n,2} + f_{n,3} \equiv x_1x_2 + x_3x_5 + x_4x_6 + x_7x_8 + x_9x_{11} + x_{10}x_{12} + \cdots + x_{6k-8}x_{6k-6}$
$+f_{7,2} + f_{7,3} + ax_{6k-4} + bx_{n-1} + 1$
where $a = b = 0$, k *is odd;* $a = b = 1$, k *is even.*
(2) *If* $n = 6k + 3, k = 1, 2, 3, 4, \cdots$, *then*
$f_{n,2} + f_{n,3} \equiv x_1x_2 + x_3x_5 + x_4x_6 + x_7x_8 + x_9x_{11} + x_{10}x_{12} + \cdots + x_{6k-2}x_{6k} + 1$
(3) *If* $n = 6k + 5, k = 1, 2, 3, 4, \cdots$, *then*
$f_{n,2} + f_{n,3} \equiv x_1x_2 + x_3x_5 + x_4x_6 + x_7x_8 + x_9x_{11} + x_{10}x_{12} + \cdots + x_{6k-2}x_{6k}$

$$+f_{5,2}+f_{5,3}+ax_{6k+2}+bx_{n-1}+1$$

where $a=b=0$, k *is even;* $a=b=1$, k *is odd.*

Proof. We only prove (1) here, and the proofs of (2) and (3) are similar.
If $n=6k+1$, and k is even, then $6k+1-7=6k-6=6(k-1)$ is odd multiple of 6, by lemma 3.1, thus

$$\begin{aligned}f_{n,2}+f_{n,3}&\equiv y_1y_2+y_3y_5+y_4y_6+f_{n-6,2}+f_{n-6,3}+y_8+y_{n-1}+1.\\&\equiv z_1z_2+z_3z_5+z_4z_6+z_7z_8+z_9z_{11}+z_{10}z_{12}+f_{n-12,2}+f_{n-12,3}+1.\\&\equiv x_1x_2+x_3x_5+x_4x_6+\cdots+x_{10}x_{12}+\cdots+x_{6k-8}x_{6k-6}+f_{7,2}+f_{7,3}\\&\quad+x_{6k-4}+x_{n-1}+1.\end{aligned}$$

If k is odd, then $6k+1-7=6k-6=6(k-1)$ is even multiple of 6, we have

$$\begin{aligned}f_{n,2}+f_{n,3}&\equiv y_1y_2+y_3y_5+y_4y_6+f_{n-6,2}+f_{n-6,3}+y_8+y_{n-1}+1.\\&\equiv z_1z_2+z_3z_5+z_4z_6+z_7z_8+z_9z_{11}+z_{10}z_{12}+f_{n-12,2}+f_{n-12,3}+1.\\&\equiv x_1x_2+x_3x_5+x_4x_6+\cdots+x_{10}x_{12}+\cdots+x_{6k-8}x_{6k-6}+f_{7,2}+f_{7,3}+1.\end{aligned}$$

Based on the results of Remark and Lemma 3.2, we can obtain the equivalent form of $f_{n,2}+f_{n,3}$.

Theorem 3.3 *When* $n=6k+5, k=1,2,3,4,\cdots$, *we have*

$$\begin{aligned}f_{n,2}+f_{n,3}&\equiv y_1y_2+y_3y_5+y_4y_6+y_7y_8+y_9y_{11}+y_{10}y_{12}+\cdots+y_{6k-2}y_{6k}+y_{6k+1}y_{6k+2}\\&\quad+y_{6k+3}y_{6k+4}+y_{6k+5}+1.\end{aligned}$$

When $n=6k+3, k=1,2,3,4,\cdots$,

$$f_{n,2}+f_{n,3}\equiv y_1y_2+y_3y_5+y_4y_6+y_7y_8+y_9y_{11}+y_{10}y_{12}+\cdots+y_{6k-2}y_{6k}+1.$$

When $n=6k+1, k=2,3,4,\cdots$,

$$f_{n,2}+f_{n,3}\equiv y_1y_2+y_3y_5+y_4y_6+y_7y_8+y_9y_{11}+y_{10}y_{12}+\cdots+y_{6k-2}y_{6k}+1.$$

Proof. For $n=3,5,7$, the equivalent form can be find in Remark. From Remark, we can obtain the proof for other n.
When $n=6k+1$,

$$\begin{aligned}f_{n,2}+f_{n,3}&\equiv y_1y_2+y_3y_5+y_4y_6+f_{n-6,2}+f_{n-6,3}+y_8+y_{n-1}+1\\&\equiv z_1z_2+z_3z_5+z_4z_6+z_7z_8+z_9z_{11}+z_{10}z_{12}+f_{n-12,2}+f_{n-12,3}+1\\&\equiv x_1x_2+x_3x_5+x_4x_6+x_7x_8+x_9x_{11}+x_{10}x_{12}+x_{13}x_{14}+\cdots+x_{6k-2}x_{6k}+1.\end{aligned}$$

When $n=6k+3$,

$$\begin{aligned}f_{n,2}+f_{n,3}&\equiv y_1y_2+y_3y_5+y_4y_6+f_{n-6,2}+f_{n-6,3}+y_8+y_{n-1}+1\\&\equiv z_1z_2+z_3z_5+z_4z_6+z_7z_8+z_9z_{11}+z_{10}z_{12}+f_{n-12,2}+f_{n-12,3}+1\\&\equiv x_1x_2+x_3x_5+x_4x_6+x_7x_8+x_9x_{11}+x_{10}x_{12}+x_{13}x_{14}+\cdots+x_{6k-2}x_{6k}+1.\end{aligned}$$

When $n=6k+5$,

$$\begin{aligned}f_{n,2}+f_{n,3}&\equiv y_1y_2+y_3y_5+y_4y_6+f_{n-6,2}+f_{n-6,3}+y_8+y_{n-1}+1\\&\equiv z_1z_2+z_3z_5+z_4z_6+z_7z_8+z_9z_{11}+z_{10}z_{12}+f_{n-12,2}+f_{n-12,3}+1\\&\equiv x_1x_2+x_3x_5+x_4x_6+x_7x_8+x_9x_{11}+x_{10}x_{12}+x_{13}x_{14}+\cdots+x_{6k-2}x_{6k}+1.\end{aligned}$$

Theorem 3.3 gives the equivalent form of function which contains two MRS functions. It is easy to computer $wt(f_{n,2}+f_{n,3})$ and $NL(f_{n,2}+f_{n,3})$ by Lemma 2.3.

Theorem 3.4 (1) *If* $n=6k+5, k=1,2,3,4,\cdots$, *then*
$f_{n,2}+f_{n,3} \equiv x_1x_2+x_3x_5+x_4x_6+x_7x_8+x_9x_{11}+x_{10}x_{12}+\cdots+x_{6k-2}x_{6k}$
$+x_{n-4}x_{n-3}+x_{n-2}x_{n-1}+x_n+1,$
the function is balanced and $NL(f_{n,2}+f_{n,3})=2^{n-1}-2^{\frac{n-1}{2}}$.
(2) *If* $n=6k+3, k=1,2,3,4,\cdots$, *then*
$f_{n,2}+f_{n,3} \equiv x_1x_2+x_3x_5+x_4x_6+x_7x_8+x_9x_{11}+x_{10}x_{12}+\cdots+x_{n-5}x_{n-3}+1$
and $wt(f_{n,2}+f_{n,3})=2^{n-1}+2^{\frac{n+1}{2}}, NL(f_{n,2}+f_{n,3})=2^{n-1}-2^{\frac{n+1}{2}}$
(3) *If* $n=6k+1, k=2,3,4,\cdots$, *then*
$f_{n,2}+f_{n,3} \equiv x_1x_2+x_3x_5+x_4x_6+x_7x_8+x_9x_{11}+x_{10}x_{12}+\cdots+x_{n-3}x_{n-1}+1$
and $wt(f_{n,2}+f_{n,3})=2^{n-1}+2^{\frac{n-1}{2}}, NL(f_{n,2}+f_{n,3})=2^{n-1}-2^{\frac{n-1}{2}}$.

Proof. (1) is a directly result of Lemma 2.3. The nonlinearity of (2) and (3) can be find from Lemma 2.3. Because of the difference of quadratic form between (2)(3)and Lemma 2.3, the weight of (2) and (3) have changed.

4 Conclusion

In this paper, we give the weight and nonlinearity of quadratic function which contains two MRS functions $f_{n,2}$ and $f_{n,3}$ for odd n . First, we obtain the recurrence relation of $f_{n,2}+f_{n,3}$, and the equivalent forms of $f_{n,2}+f_{n,3}$ are determined for $n=3,5,7$. Secondly, we give the equivalent form of $f_{n,2}+f_{n,3}$ by discussing the value of n. Last, we get the weight and nonlinearity of $f_{n,2}+f_{n,3}$.

However, it seems difficult for us to extend our method for functions which contain more MRS functions. So, it will be interesting for us to continue working on finding the equivalent form of function which contain more MRS functions and characterizing the weight and nonlinearity of the functions. On the other hand, the weight and nonlinearity of functions which contain two different MRS functions would be another interesting problem.

References

[1] T.W. Cusick and P. Stabuca, *Cryptographic Boolean Functions and Applications*, Academic Press, San Diego, (2009).

[2] J. Pieprayk and C.X. Qu, Fast hashing and rotation-symmetric funtions, *Journal of Universal Computer Science*, 5(1999), 20-31.

[3] T.W. Cusick and P. Stabuca, Fast evaluation, weights and nonlinearity of rotation-symmetric functions, *Discrete Mathematics*, 258(2002), 289-301.

[4] D.K. Dalai, S. Maitra and S. Sarkar, Results on rotation symmetric bent functions, *Discrete Applied Mathematics*, 309(2009), 2398-2409.

[5] H. Kim, S.M. Park and S.G. Hahna, On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2, *Discrete Applied Mathematics*, 157(2008), 428-432.

[6] A. Maximov, M. Hell and S. Maitra, Plateaued rotation symmetric boolean functions on odd number of variables, *First Workshop on Boolean Functions BFCA*, 05(2005), 83-104.

[7] S. Sarkar, S. Maitra and J. Clark, Results on rotation symmetric bent and correlation immune Boolean function, *Fast Software Encryption Workshop FSE*, Springer-Verlag, 3017(2004), 161-177.

[8] P. Stabuca and S. Maitra, Rotation symmetric boolean funtions-count and cryptographic properties, *Discrete Applied Mathematics*, 156(2008), 1567-1580.

[9] S. Sarkar and S. Maitra, Construction of rotation symmetric boolean funtions with optimal algebraic immunity, *Computation Systems*, 12(2009), 267-284.

[10] F.J. MacWilliams and N.J. Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, (1977).