Journal of Mathematics Research; Vol. 7, No. 2; 2015
ISSN 1916-9795 E-ISSN 1916-9809
Published by Canadian Center of Science and Education

The Weight and Nonlinearity of 2-rotation Symmetric Cubic Boolean Function

Hongli Liu[1]

[1] Institute of Mathematics and Statistics, Zhejiang University of Finance and Economics, China

Correspondence: Hongli Liu, Institute of Mathematics and Statistics, Zhejiang University of Finance and Economics, 18 XueYuan Street, Xiasha Higher Education Zone, Hangzhou 310018, China. Tel: 86-137-5827-3108. E-mail: ooolhl@163.com

Received: March 25, 2015 Accepted: April 8, 2015 Online Published: May 23, 2015

doi:10.5539/jmr.v7n2p187 URL: http://dx.doi.org/10.5539/jmr.v7n2p187

The research is financed by the National Natural Science Foundation of China(Grant No:11302188), Zhejiang Provincial Natural Science Foundation of China (Grant No. LY14F010015).

Abstract

The conceptions of χ-value and K-rotation symmetric Boolean functions are introduced by Cusick. K-rotation symmetric Boolean functions are a special rotation symmetric functions, which are invariant under the $k-th$ power of ρ. In this paper, we discuss cubic 2-value 2-rotation symmetric Boolean function with $2n$ variables, which denoted by $F^{2n}(x^{2n})$. We give the recursive formula of weight of $F^{2n}(x^{2n})$, and prove that the weight of $F^{2n}(x^{2n})$ is the same as its nonlinearity.

Keywords: Rotation symmetric Boolean function, Nonlinearity, Weight, $\chi-$value

1. Introduction

Boolean functions have many applications in coding theory and cryptography. Rotation symmetric Boolean functions(RSBF) as invariant Boolean functions under rotation transform have been widely studied. Higher nonlinearity is a very important character of Boolean functions which are widely used in coding theory and S-box design. Rotation symmetric Boolean functions as a subclass of $K-rotation\ symmetric$ have not higher nonlinearity. So, $K-rotation\ symmetric$ Boolean functions which are the generalization of notion of rotation symmetric function were proposed by Selçk Kavut. The applications of the $k-rotation\ symmetric(k \geq 2)$ to coding theory and S-box design can be found in some papers. Cusick gave the definition of cubic $2-rotation\ symmetric$ Boolean functions and used the notation $\{2-(1,r,s)_{2n} : 2n \geq s\}$ as the cubic monomial 2-rotation symmetric functions (denoted by $2-functions$). Cusick also described the affine equivalence of cubic MRS 2-rotation symmetric, and proved that the sequence of Hamming weights of $\{2-(1,r,s)_{2n} : 2n \geq s\}$ satisfies a linear recursion with integer coefficients. In this paper, we will give the recursion formula of Hamming weight of $\{2-(1,2,3)_{2n}(2n \geq 10)\}$ and prove that the nonlinearity of $\{2-(1,2,3)_{2n}(2n \geq 10)\}$ is the same as its weight.

2. Preliminaries

Let $\mathbb{F}_2 = \{0,1\}$ be the binary field, $\mathbb{F}_2^n$ be the $n-$dimensional vector space of over $\mathbb{F}_2$. A Boolean function in n variables can be defined as a map from $\mathbb{F}_2^n$ into $\mathbb{F}_2$, denoted by $f^n(x^n)$, or f^n in brief, where $x^n = (x_1, x_2, \cdots, x_n)$. Every Boolean function f^n has a unique polynomial representation (usually called the algebraic normal form (ANF)), and the *degree* of f^n is the degree of this polynomial(deg(f^n) in brief). If every term in the algebraic normal form of f^n has the same degree, then the function is said to be *homogeneous*. A Boolean function f^n is called $affine$, if $def(f^n) = 1$. If f^n is affine and homogeneous(i.e.the constant term is 0), f^n is said to be *linear*. The *truth table* of f^n is defined to be the binary sequence $v_1, v_2, \cdots, v_{2^n}$, where the bits $v_1 = f((0,0,\cdots,0)), v_2 = f((0,0,\cdots,1)), \cdots, v_{2^n} = f((1,1,\cdots,1))$. The *Hamming weight* of a Boolean function f^n is defined as the number of nonzero coordinates in its truth table, denoted by $wt(f^n)$. The *Hamming distance* $d(f^n, g^n)$ between two Boolean functions f^n and g^n is defined as the number of their different coordinates, which equals the Hamming weight of their sum $f+g$, where $+$ denotes the addition on $\mathbb{F}_2$. Two Boolean functions f^n and g^n in n variables are said to be $affine\ equivalent$ if there exists an invertible matrix A with entries in $\mathbb{F}_2$ and $\mathbf{b} \in \mathbb{F}_2^n$ such that $f^n(\mathbf{x}) = g^n(A\mathbf{x}+\mathbf{b})$.

Definition 1 *The nonlinearity $NL(f^n)$ of a Boolean function $f^n(x^n)$ is defined as*

$$NL(f^n) = \text{Min}\{d(f^n(x^n), c^n \cdot x^n) | c^n \in \mathbb{F}_2^n\},$$

where $\cdot$ is the vector dot product.

It is easy to see that if f^n and g^n are affine equivalent, then $wt(f^n) = wt(g^n)$ and $NL(f^n) = NL(g^n)$. We say that the weight and nonlinearity are $affine\ invariants$.

Definition 2 *For a Boolean function $f^n(x^n)$. The Fourier transform of f^n at $c^n \in \mathbb{F}_2^n$ is defined as*

$$\widehat{f^n}(c^n) = \sum_{x^n \in F_2^n} (-1)^{f^n(x^n)+c^n \cdot x^n}.$$

Definition 3 *A Boolean function $f^n(x^n)$ is called rotation symmetric if*

$$f^n(x_1, x_2, \cdots, x_n) = f^n(\rho(x_1, x_2, \cdots, x_n)), for\ all\ (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n,$$

where $\rho(x_1, x_2, \cdots, x_{n-1}, x_n) = (x_n, x_1, x_2, \cdots, x_{n-1})$.

If a monomial $x_1x_2x_3$ appears in a rotation symmetric Boolean function as a term then all monomials in the orbit of $x_1x_2x_3$ should appear in the function as terms. A rotation symmetric function is said to be *monomial rotation symmetric*(MRS) if it is generated by applying powers of ρ to a single monomial. We use the notation $(1, r, s)_n$ for the cubic MRS function in n variables generated by the monomial $x_1x_rx_s$. A Boolean function is said to be $k-$ *rotation symmetric* if it is invariant under the $k - th$ power of ρ but not under any smaller power. A Boolean function is said to be *monomial* $k-$ *rotation symmetric* if it is generated by applying powers of ρ^k to a single monomial. For brevity, we refer to these functions as $k - functions$. In this paper, the cubic 2-functions shall be discussed. We use the notation $2 - (1, r, s)_{2n}$ for the cubic 2-function in 2n variables generated by the monomial $x_1x_rx_s$. If we assume $r < s \leq 2n$ then the formula

$$2 - (1, r, s)_{2n} = x_1x_rx_s + x_3x_{r+2}x_{s+2} + \cdots + x_{2n-1}x_{r-2}x_{s-2}.$$

is called a $standard\ form$ of the above 2-function.

A monomial $[a, b, c]$ in a cubic $2-$function is said to be $pure\ form$, if a, b, c are all even or odd. A monomial that is not pure form is said to be $mixed\ form$. It is obvious that every monomial of $2 - (1, r, s)_{2n}$ has the same form. A 2-function is said to be $mixed\ form\ 2 - function$ if it's terms are mixed form. Otherwise, it is said to be $pure\ form\ 2 - function$.

Definition 4 *($\chi - value$) Let $2 - (1, r, s)_{2n}$ be a mixed form 2-function with monomial $[a, b, c](a < b < c)$. Assume a is even(odd) and b, c are odd(even). Then the $\chi - value$ for $2 - (1, r, s)$ is defined as $\chi = c - b$.*

Theorem 1 *Two 2-functions $2 - (1, r, s)_{2n}$ and $2 - (1, p, q)_{2n}$ are affine equivalent by some permutation for all n if and only if their $\chi-$values are equal.*

Theorem 1 tells us that all 2-values functions with $2n$ variables have the same weights and nonlinearity. So, in the following section, we will discuss the weight and nonlinearity of 2-values function $2 - (1, 2, 3)_{2n}$.

3. The Weight of 2-values Function $F^{2n}(x^{2n})$

In this section, we shall study the recursive formula for weight of $2-(1, 2, 3)_{2n}$. Firstly, we give the standard form of 2-values function $2 - (1, 2, 3)_{2n}$, denoted by $F^{2n}(x^{2n})$or F^{2n}.

$$F^{2n}(x^{2n}) = x_1x_2x_3 + x_3x_4x_5 + \cdots + x_{2n-3}x_{2n-2}x_{2n-1} + x_{2n-1}x_{2n}x_1.$$

If T is a string , then $\bar{T}$ denotes the complemented string with 0 and 1 interchanged. If X is a $4-$bit block or a string of blocks, then $(X)_s$ or X_s is the string obtained by concatenation of s copies of X. The concatenation of two strings u, v will be denoted by uv or $u||v$. Now we define two sets of $4-$bit strings

$$T_1 = \{A = 0, 0, 1, 1; \bar{A} = 1, 1, 0, 0; B = 0, 1, 0, 1; \bar{B} = 1, 0, 1, 0; C = 0, 1, 1, 0; \bar{C} = 1, 0, 0, 1; D = 0, 0, 0, 0; \bar{D} = 1, 1, 1, 1\}$$

and

$$T_2 = \{U = 1, 0, 0, 0; \bar{U} = 0, 1, 1, 1; V = 0, 0, 0, 1; \bar{V} = 1, 1, 1, 0; X = 0, 1, 0, 0; \bar{X} = 1, 0, 1, 1; Y = 0, 0, 1, 0; \bar{Y} = 1, 1, 0, 1\}.$$

We give the following result about the truth tables of monomials for $F^{2n}(x^{2n})$.

Lemma 2 *The truth table of any monomial for $F^{2n}(x^{2n})$ is*

$x_i x_{i+1} x_{i+2} = (D_{2^{2n-i-2}}(D_{2^{2n-i-3}}(D_{2^{2n-i-4}}\bar{D}_{2^{n-i-4}})))_{2^{i-1}} \quad 1 \le i \le 2n-5$, and i is odd.

$x_{2n-3}x_{2n-2}x_{2n-1} = (DDDA)_{2^{2n-4}}$.

$x_{2n-1}x_{2n}x_1 = D_{2^{2n-3}}V_{2^{2n-3}}$.

From Lemma 2, we give the following algorithm as the output of truth table for $F^{2n}(x^{2n})$.

Algorithm 1

$Step\ 5: h_1^5 \leftarrow DDDADDDA, h_2^5 \leftarrow VVVYVVVY.$

$Step\ s: h_i^s \leftarrow (h_i^{s-2}\|\tilde{h}_i^{s-2})_2, i = 1, 2,$ for odd s.

$Output: H_1 \leftarrow h_1^{2n-1},\ H_2 \leftarrow \tilde{h}_2^{2n-1}$, where $\tilde{h}_i^s$ is the string obtained from h_i^s by complementing its last 2^{s-2} bits. Write $F^{2n} = H_1 \parallel H_2$.

From the above algorithm, we give the recursive relationship of weight for $F^{2n}(x^{2n})$.

Theorem 3 *The weight of Boolean function $F^{2n}(x^{2n})$ satisfy*

$$wt(F^{2n}) = 2wt(F^{2n-2}) + 4wt(F^{2n-4}) + 2^{2n-3}.$$

Proof. Using Algorithm 1, we have

$$wt(F^{2n}(x^{2n})) = wt(H_1) + wt(H_2) = wt(h_1^{2n-1}) + wt(\tilde{h}_2^{2n-1}) \tag{1}$$

and

$$h_1^{2n-1} = h_1^{2n-3}\tilde{h}_1^{2n-3}h_1^{2n-3}\tilde{h}_1^{2n-3} \qquad \tilde{h}_1^{2n-1} = h_1^{2n-3}\tilde{h}_1^{2n-3}h_1^{2n-3}\overline{\tilde{h}_1^{2n-3}}$$

$$h_1^{2n-3} = h_1^{2n-5}\tilde{h}_1^{2n-5}h_1^{2n-5}\tilde{h}_1^{2n-5} \qquad \tilde{h}_1^{2n-3} = h_1^{2n-5}\tilde{h}_1^{2n-5}h_1^{2n-5}\overline{\tilde{h}_1^{2n-5}}.$$

Therefore,

$$\begin{aligned} wt(h_1^{2n-1}) &= 2(wt(h_1^{2n-3}) + wt(\tilde{h}_1^{2n-3})) \\ &= 2(4wt(h_1^{2n-5}) + 2wt(\tilde{h}_1^{2n-5}) + 2^{2n-5}) \\ &= 2(2wt(h_1^{2n-5}) + 2(wt(h_1^{2n-5}) + wt(\tilde{h}_1^{2n-5})) + 2^{2n-5}) \\ &= 2(2wt(h_1^{2n-5}) + wt(h_1^{2n-3}) + 2^{2n-5}) \\ &= 4wt(h_1^{2n-5}) + 2wt(h_1^{2n-3}) + 2^{2n-4}. \end{aligned} \tag{2}$$

Similarly, we have

$$wt(\tilde{h}_1^{2n-1}) = 4wt(\tilde{h}_1^{2n-5}) + 2wt(\tilde{h}_1^{2n-3}) + 2^{2n-4}. \tag{3}$$

From (1), (2) and (3), we have

$$\begin{aligned} wt(F^{2n}(x^{2n})) &= wt(h_1^{2n-1}) + wt(\tilde{h}_2^{2n-1}) \\ &= 4wt(h_1^{2n-5}) + 2wt(h_1^{2n-3}) + 2^{2n-4} + 4wt(\tilde{h}_2^{2n-5}) + 2wt(\tilde{h}_2^{2n-3}) + 2^{2n-4} \\ &= 4wt(F^{2n-4}) + 2wt(F^{2n-2}) + 2^{2n-3}. \end{aligned}$$

4. The Nonliearity of $F^{2n}(x^{2n})$

Cusick and Stănică conjectured that the nonlinearity of cubic 1-values function $F^n(x^n)$ is the same as the weight, and Zhang et al. proved the conjecture. In this section, we shall prove the same result for $F^{2n}(x^{2n})$, that is,

$$wt(F^{2n}) = NL(F^{2n}). \tag{4}$$

By the definitions of Fourier transform and Hamming weight, we can easily deduce that

$$wt(F^{2n}(x^{2n})) = \frac{1}{2}(2^{2n} - \widehat{F^{2n}(0)}).$$

Therefore, we can restate (4) as

$$\widehat{F^{2n}(0)} = \mathrm{Max}\{|\widehat{F^{2n}(c^{2n})}||c^{2n} \in \mathbb{F}^{2n}\}. \tag{5}$$

On the other hand, the recursion formula of $\widehat{F^{2n}(0)}$ can be obtained by applying the recursion formula of $wt(F^{2n}(x^{2n}))$.

$$\begin{array}{rcl} \widehat{F^{2n}(0)} & = & 2^{2n} - 2wt(F^{2n}) \\ & = & 2^{2n} - 2 \cdot [2wt(F^{2n-2}) + 4wt(F^{2n-4}) + 2^{2n-3}] \\ & = & 2[2^{2n-1} - 2wt(F^{2n-2}) - 4wt(F^{2n-4}) - 2^{2n-3}] \\ & = & 2[2^{2n-2} - 2wt(F^{2n-2}) + 2 \cdot 2^{2n-4} - 4wt(F^{2n-4})] \\ & = & 2[\widehat{F^{2n-2}(0)} + 2\widehat{F^{2n-4}(0)}]. \qquad (6) \end{array}$$

Before giving the proof of (5), we need some notation:

$t_{2n-1} = \sum_{1\leq i\leq 2n-3,\ i\ is\ odd} x_i x_{i+1} x_{i+2}$,

$f_1^{2n-1}(x_1, x_2, \cdots, x_{2n-1}) = t_{2n-1}$,

$f_2^{2n-1}(x_1, x_2, \cdots, x_{2n-1}) = t_{2n-1} + x_1$,

$f_3^{2n-1}(x_1, x_2, \cdots, x_{2n-1}) = t_{2n-1} + x_{2n-1}$,

$f_4^{2n-1}(x_1, x_2, \cdots, x_{2n-1}) = t_{2n-1} + x_{2n-1} + x_1$,

$f_5^{2n-1}(x_1, x_2, \cdots, x_{2n-1}) = t_{2n-1} + x_{2n-1}x_1$.

Firstly, we give the following recursive relations about $\widehat{f_i^{2n-1}}(c^{2n-1})$.

Lemma 4 *For every $c^{2n-1} = (c_1, c_2, \cdots, c_{2n-1}) \in \mathbb{F}^{2n-1}$, we have*

$$\widehat{f_i^{2n-1}}(c^{2n-1}) = (1 + (-1)^{c_{2n-1}} + (-1)^{c_{2n-2}})\widehat{f_i^{2n-3}}(c^{2n-3}) + (-1)^{c_{2n-2}+c_{2n-1}}\widehat{f_{i+2}^{2n-3}}(c^{2n-3}),\ i = 1, 2.$$

$$\widehat{f_i^{2n-1}}(c^{2n-1}) = (1 - (-1)^{c_{2n-1}} + (-1)^{c_{2n-2}})\widehat{f_i^{2n-3}}(c^{2n-3}) - (-1)^{c_{2n-2}+c_{2n-1}}\widehat{f_{i+2}^{2n-3}}(c^{2n-3}),\ i = 3, 4.$$

$$\widehat{f_5^{2n-1}}(c^{2n-1}) = (1 + (-1)^{c_{2n-2}})\widehat{f_1^{2n-3}}(c^{2n-3}) + (-1)^{c_{2n-1}}\widehat{f_2^{2n-3}}(c^{2n-3}) + (-1)^{c_{2n-2}+c_{2n-1}}\widehat{f_4^{2n-3}}(c^{2n-3}),$$

where c^{2n-2} and c^{2n-3} are the first $2n-2$ and $2n-3$ bits of c^{2n-1}.

proof We prove the relation for $i = 1$, since the proof of the others are similar.

$$\begin{array}{rcl} \widehat{f_1^{2n-1}}(c^{2n-1}) & = & \sum\limits_{x^{2n-1}:x_{2n-2}=0,x_{2n-1}=0} (-1)^{f_1^{2n-1}(x^{2n-1})+c^{2n-1}\cdot x^{2n-1}} + \sum\limits_{x^{2n-1}:x_{2n-2}=0,x_{2n-1}=1} (-1)^{f_1^{2n-1}(x^{2n-1})+c^{2n-1}\cdot x^{2n-1}} \\ & + & \sum\limits_{x^{2n-1}:x_{2n-2}=1,x_{2n-1}=0} (-1)^{f_1^{2n-1}(x^{2n-1})+c^{2n-1}\cdot x^{2n-1}} + \sum\limits_{x^{2n-1}:x_{2n-2}=1,x_{2n-1}=1} (-1)^{f_1^{2n-1}(x^{2n-1})+c^{2n-1}\cdot x^{2n-1}} \\ & = & \sum\limits_{x^{2n-3}} (-1)^{f_1^{2n-3}(x^{2n-3})+c^{2n-3}\cdot x^{2n-3}} + \sum\limits_{x^{2n-3}} (-1)^{f_1^{2n-3}(x^{2n-3})+c^{2n-3}\cdot x^{2n-3}+c_{2n-1}} \\ & + & \sum\limits_{x^{2n-3}} (-1)^{f_1^{2n-3}(x^{2n-3})+c^{2n-3}\cdot x^{2n-3}+c_{2n-2}} + \sum\limits_{x^{2n-3}} (-1)^{f_3^{2n-3}(x^{2n-3})+c^{2n-3}\cdot x^{2n-3}+c_{2n-2}+c_{2n-1}} \\ & = & \widehat{f_1^{2n-3}}(c^{2n-3}) + (-1)^{c_{2n-1}}\widehat{f_1^{2n-3}}(c^{2n-3}) + (-1)^{c_{2n-2}}\widehat{f_1^{2n-3}}(c^{2n-3}) + (-1)^{c_{2n-1}+c_{2n-2}}\widehat{f_3^{2n-3}}(c^{2n-3}) \\ & = & (1 + (-1)^{c_{2n-1}} + (-1)^{c_{2n-2}})\widehat{f_1^{2n-3}}(c^{2n-3}) + (-1)^{c_{2n-1}+c_{2n-2}}\widehat{f_3^{2n-3}}(c^{2n-3}). \end{array}$$

From lemma 4, we can easily deduce the following corollary.

Corolary 5 *For every $c^{2n-1} = (c_1, c_2, \cdots, c_{2n-1}) \in \mathbb{F}_2^{2n-1}$, we have*

$$\left.\begin{array}{ll} \widehat{f_i^{2n-1}}(c^{2n-1}) = 3\widehat{f_i^{2n-3}}(c^{2n-3}) + \widehat{f_{i+2}^{2n-3}}(c^{2n-3}) & i = 1,2 \\ \widehat{f_i^{2n-1}}(c^{2n-1}) = \widehat{f_{i-2}^{2n-3}}(c^{2n-3}) - \widehat{f_i^{2n-3}}(c^{2n-3}) & i = 3,4 \end{array}\right\} if\ c_{2n-2} = 0, c_{2n-1} = 0;$$

$$\left.\begin{array}{ll} \widehat{f_i^{2n-1}}(c^{2n-1}) = \widehat{f_i^{2n-3}}(c^{2n-3}) - \widehat{f_{i+2}^{2n-3}}(c^{2n-3}) & i = 1,2 \\ \widehat{f_i^{2n-1}}(c^{2n-1}) = 3\widehat{f_{i-2}^{2n-3}}(c^{2n-3}) + \widehat{f_i^{2n-3}}(c^{2n-3}) & i = 3,4 \end{array}\right\} if\ c_{2n-2} = 0, c_{2n-1} = 1;$$

$$\left.\begin{array}{ll} \widehat{f_i^{2n-1}}(c^{2n-1}) = \widehat{f_i^{2n-3}}(c^{2n-3}) - \widehat{f_{i+2}^{2n-3}}(c^{2n-3}) & i = 1,2 \\ \widehat{f_i^{2n-1}}(c^{2n-1}) = -\widehat{f_{i-2}^{2n-3}}(c^{2n-3}) + \widehat{f_i^{2n-3}}(c^{2n-3}) & i = 3,4 \end{array}\right\} if\ c_{2n-2} = 1, c_{2n-1} = 0;$$

$$\left.\begin{array}{ll} \widehat{f_i^{2n-1}}(c^{2n-1}) = -\widehat{f_i^{2n-3}}(c^{2n-3}) + \widehat{f_{i+2}^{2n-3}}(c^{2n-3}) & i = 1,2 \\ \widehat{f_i^{2n-1}}(c^{2n-1}) = \widehat{f_{i-2}^{2n-3}}(c^{2n-3}) - \widehat{f_i^{2n-3}}(c^{2n-3}) & i = 3,4 \end{array}\right\} if\ c_{2n-2} = 1, c_{2n-1} = 1.$$

$$\widehat{f_5^{2n-1}}(c^{2n-1}) = \begin{cases} 2\widehat{f_1^{2n-3}}(c^{2n-3}) + \widehat{f_2^{2n-3}}(c^{2n-3}) + \widehat{f_4^{2n-3}}(c^{2n-3}) & c_{2n-2} = 0, c_{2n-1} = 0 \\ 2\widehat{f_1^{2n-3}}(c^{2n-3}) - \widehat{f_2^{2n-3}}(c^{2n-3}) - \widehat{f_4^{2n-3}}(c^{2n-3}) & c_{2n-2} = 0, c_{2n-1} = 1 \\ \widehat{f_2^{2n-3}}(c^{2n-3}) - \widehat{f_4^{2n-3}}(c^{2n-3}) & c_{2n-2} = 1, c_{2n-1} = 0 \\ -\widehat{f_2^{2n-3}}(c^{2n-3}) + \widehat{f_4^{2n-3}}(c^{2n-3}) & c_{2n-2} = 1, c_{2n-1} = 1. \end{cases}$$

Table 1. The values of $NL(F^{2n})$.

$2n = 8$	$2n = 10$	$2n = 12$	$2n = 14$	$2n = 16$	$2n = 18$
72	336	1472	6336	26752	111616

Table 2. The values of $\widehat{F^{2n}(0)}$.

$2n = 8$	$2n = 10$	$2n = 12$	$2n = 14$	$2n = 16$	$2n = 18$
112	352	1152	3712	12032	38912

The following lemma give the properties of $\widehat{F^{2n}}(0)$.

Lemma 6 $\widehat{F^{2n}}(0)$ *satisfies the relationship:* $\widehat{F^{2n}}(0) > 0$ *and* $2\widehat{F^{2n}}(0) < \widehat{F^{2n+2}}(0)$.

proof We prove it by math induction. From Table 2, we can see the two results are true for $2n = 6, 8, 10, 12, 14, 16, 18$. Assume that, for an arbitrary $2n$, the result is also true. Let's derive the correctness of conclusion for $2n + 2$ from this assumption.

From (6) and the assumption of induction, we have

$2\widehat{F^{2n+2}}(0) = 2(2\widehat{F^{2n}}(0) + 4\widehat{F^{2n-2}}(0)) < 2\widehat{F^{2n+2}}(0) + 4\widehat{F^{2n}}(0) = \widehat{F^{2n+4}}(0)$
and
$\widehat{F^{2n+2}}(0) = 2\widehat{F^{2n}}(0) + 4\widehat{F^{2n-2}}(0) > 0.$
Which exactly means that the result holds for $2n + 2$.

Lemma 7 *Let* $c^{2n-1} = (c_1, c_2, \cdots, c_{2n-1}) \in \mathbb{F}_2^{2n-1}$. *If* $c_1 = 1$, *then*

$$|\widehat{f_i^{2n-1}}(c^{2n-1})| < \frac{1}{2}\widehat{F^{2n}}(0), (i = 1, 5),\ |\widehat{f_i^{2n-1}}(c^{2n-1})| < \frac{1}{4}\widehat{F^{2n+2}}(0), (i = 2, 3, 4).$$

$$|\widehat{f_1^{2n-1}}(c^{2n-1})| < \frac{1}{10}\widehat{F^{2n+2}}(0),\ |\widehat{f_2^{2n-1}}(c^{2n-1})| < \frac{3}{40}\widehat{F^{2n+4}}(0).$$

proof

When $c_{2n-2} = 0, c_{2n-1} = 0$, we have

$\widehat{f_1^{2n-1}}(c^{2n-1}) = 3\widehat{f_1^{2n-3}}(c^{2n-3}) + \widehat{f_3^{2n-3}}(c^{2n-3})$

$\widehat{f_2^{2n-1}}(c^{2n-1}) = 3\widehat{f_2^{2n-3}}(c^{2n-3}) + \widehat{f_4^{2n-3}}(c^{2n-3})$

$\widehat{f_3^{2n-1}}(c^{2n-1}) = \widehat{f_1^{2n-3}}(c^{2n-3}) - \widehat{f_3^{2n-3}}(c^{2n-3})$

$\widehat{f_4^{2n-1}}(c^{2n-1}) = \widehat{f_2^{2n-3}}(c^{2n-3}) + \widehat{f_4^{2n-3}}(c^{2n-3})$

$\widehat{f_5^{2n-1}}(c^{2n-1}) = 2\widehat{f_1^{2n-3}}(c^{2n-3}) + \widehat{f_2^{2n-3}}(c^{2n-3}) + \widehat{f_4^{2n-3}}(c^{2n-3})$.

We prove it by math induction. The maximum values of $|\widehat{f_i^{11}}(c^{11})|(i = 1, \cdots, 5)$ can be obtained with the help of Matlab soft, which are $352, 672, 672, 672, 352$. From Talbe 2, we can see $\widehat{f_i^{11}}(c^{11})(i = 1, 5) < \frac{1}{2}\widehat{F^{12}}(0)$, $\widehat{f_i^{11}}(c^{11})(i = 2, 3, 4) < \frac{1}{4}\widehat{F^{14}}(0)$, $\widehat{f_1^{11}}(c^{11}) < \frac{1}{10}\widehat{F^{14}}(0)$, and $\widehat{f_2^{11}}(c^{11}) < \frac{3}{40}\widehat{F^{16}}(0)$.

Suppose the results are true for $2n - 1 (n \geq 6)$, we prove that it is true for $2n + 1$.

$|\widehat{f_1^{2n+1}}(c^{2n+1})| = |3\widehat{f_1^{2n-1}}(c^{2n-1}) + \widehat{f_3^{2n-1}}(c^{2n-1})|$

$= |2\widehat{f_1^{2n-1}}(c^{2n-1}) + \widehat{f_1^{2n-1}}(c^{2n-1}) + \widehat{f_3^{2n-1}}(c^{2n-1})|$

$= |2\widehat{f_1^{2n-1}}(c^{2n-1}) + 4\widehat{f_1^{2n-3}}(c^{2n-3})|$

$\leq 2|\widehat{f_1^{2n-1}}(c^{2n-1})| + 4|\widehat{f_1^{2n-3}}(c^{2n-3})|$

$< \frac{1}{2}(2\widehat{F^{2n}}(0) + 4\widehat{F^{2n-2}}(0))(< \frac{1}{10}(2\widehat{F^{2n+2}}(0) + 4\widehat{F^{2n}}(0)))$

$= \frac{1}{2}\widehat{F^{2n+2}}(0)(= \frac{1}{10}\widehat{F^{2n+4}}(0))$.

$|\widehat{f_2^{2n+1}}(c^{2n+1})| = |3\widehat{f_2^{2n-1}}(c^{2n-1}) + \widehat{f_4^{2n-1}}(c^{2n-1})|$

$= |2\widehat{f_2^{2n-1}}(c^{2n-1}) + \widehat{f_2^{2n-1}}(c^{2n-1}) + \widehat{f_4^{2n-1}}(c^{2n-1})|$

$= |2\widehat{f_2^{2n-1}}(c^{2n-1}) + 4\widehat{f_2^{2n-3}}(c^{2n-3})|$

$\leq 2|\widehat{f_2^{2n-1}}(c^{2n-1})| + 4|\widehat{f_2^{2n-3}}(c^{2n-3})|$

$< \frac{1}{4}(2\widehat{F^{2n+2}}(0) + 4\widehat{F^{2n}}(0))(< \frac{3}{40}(2\widehat{F^{2n+4}}(0) + 4\widehat{F^{2n+2}}(0)))$

$= \frac{1}{4}\widehat{F^{2n+4}}(0)((= \frac{3}{40}\widehat{F^{2n+6}}(0))$.

$|\widehat{f_3^{2n+1}}(c^{2n+1})| = |\widehat{f_1^{2n-1}}(c^{2n-1}) - \widehat{f_3^{2n-1}}(c^{2n-1})|$

$= |2\widehat{f_1^{2n-1}}(c^{2n-1}) - (\widehat{f_1^{2n-1}}(c^{2n-1}) + \widehat{f_3^{2n-1}}(c^{2n-1}))|$

$= |2\widehat{f_1^{2n-1}}(c^{2n-1}) - 4\widehat{f_1^{2n-3}}(c^{2n-3})|$

$\leq 2|\widehat{f_1^{2n-1}}(c^{2n-1})| + 4|\widehat{f_1^{2n-3}}(c^{2n-3})|$

$< \frac{1}{2}(2\widehat{F^{2n}}(0) + 4\widehat{F^{2n-2}}(0))$

$= \frac{1}{2}\widehat{F^{2n+2}}(0) \leq \frac{1}{4}\widehat{F^{2n+4}}(0)$.

$|\widehat{f_4^{2n+1}}(c^{2n+1})| = |\widehat{f_2^{2n-1}}(c^{2n-1}) - \widehat{f_4^{2n-1}}(c^{2n-1})|$

$= |2\widehat{f_2^{2n-1}}(c^{2n-1}) - (\widehat{f_2^{2n-1}}(c^{2n-1}) + \widehat{f_4^{2n-1}}(c^{2n-1}))|$

$= |2\widehat{f_2^{2n-1}}(c^{2n-1}) - 4\widehat{f_2^{2n-3}}(c^{2n-3})|$

$\leq 2|\widehat{f_2^{2n-1}}(c^{2n-1})| + 4|\widehat{f_2^{2n-3}}(c^{2n-3})|$

$< \frac{1}{4}(2\widehat{F^{2n+2}}(0) + 4\widehat{F^{2n}}(0))$

$= \frac{1}{4}\widehat{F^{2n+4}}(0).$

$|\widehat{f_5^{2n+1}}(c^{2n+1})| = |2\widehat{f_1^{2n-1}}(c^{2n-1}) + \widehat{f_2^{2n-1}}(c^{2n-1}) + \widehat{f_4^{2n-1}}(c^{2n-1})|$

$= |2\widehat{f_1^{2n-1}}(c^{2n-1}) + 4\widehat{f_2^{2n-3}}(c^{2n-3})|$

$\leq 2|\widehat{f_1^{2n-1}}(c^{2n-1})| + 4|\widehat{f_2^{2n-3}}(c^{2n-3})|$

$< \frac{1}{5}\widehat{F^{2n+2}}(0) + \frac{3}{10}\widehat{F^{2n+2}}(0)$

$= \frac{1}{2}\widehat{F^{2n+2}}(0).$

When $c_{2n-2} = 1, c_{2n-1} = 0$, we have

$|\widehat{f_5^{2n+1}}(c^{2n+1})| = |\widehat{f_2^{2n-1}}(c^{2n-1}) - \widehat{f_4^{2n-1}}(c^{2n-1})|$

$\leq |\widehat{f_2^{2n-1}}(c^{2n-1})| + |\widehat{f_4^{2n-1}}(c^{2n-1})|$

$< \frac{1}{4}\widehat{F^{2n+2}}(0) + \frac{1}{4}\widehat{F^{2n+2}}(0)$

$= \frac{1}{2}\widehat{F^{2n+2}}(0).$

The others cases are similar.

From definition 3, $\widehat{F^{2n}}(c_1, c_2, \cdots, c_{2n}) = \widehat{F^{2n}}(c_{2n}, c_1, \cdots, c_{2n-1})$, for any $c^{2n} = (c_1, c_2, \cdots, c_{2n}) \in \mathbb{F}_2^{2n}$. Without lost of generality, if $c^{2n} \neq 0$, we can assume that $c_1 \neq 0$. Using lemma 4, we have the following theorem.

Theorem 8 *For all* $c^{2n} = (c_1, c_2, \cdots, c_{2n}) \neq 0$ *and* $n \geq 6$*, we have*

$$|\widehat{F^{2n}}(c^{2n})| < \widehat{F^{2n}}(0).$$

proof We factor $\widehat{F^{2n}}(c^{2n})$ into two sub-functions.

$|\widehat{F^{2n}}(c^{2n})| = |\widehat{f_1^{2n-1}}(c^{2n-1}) + \widehat{f_5^{2n-1}}(c^{2n-1})| \leq |\widehat{f_1^{2n-1}}(c^{2n-1})| + |\widehat{f_5^{2n-1}}(c^{2n-1})| < \frac{1}{2}\widehat{F^{2n}}(0) + \frac{1}{2}\widehat{F^{2n}}(0) = \widehat{F^{2n}}(0).$

Theorem 8 tells us that the nonlinearity of $F^{2n}(x^{2n})$ is the same as its weight.

4. Conclusion

This paper gives the recursive formula of weight about 2-values cubic Boolean functions with $2n$ variables, and proves that the weight of F^{2n} is the same as its nonlinearity. The recursive formula of weight about 2t-values(t=2,4,$\cdots$) cubic Boolean functions can be discussed and the relationship of weight between 2-value and 2t-value functions can also be studied.

Acknowledgements

The work was supported by the National Natural Science Foundation of China(Grant No:11302188), Zhejiang Provincial Natural Science Foundation of China (Grant No. LY14F010015).

References

Cusick, T. W., & Johns, B. (2014). *Theory of 2-rotation symmetric cubic Boolean functions: Des. Codes Cryptogr.* http://dx.doi.org/10.1007/s10623-014-9964-2

Cusick, T. W., & Padgett, D. (2012). *A recursive formula for weights of Boolean rotation symmetric functions: Discrete Applied Mathematics 160*, 391-397. http://dx.doi.org/10.1016/j.dam.2011.11.006

Cusick, T. W., & Stanica, P. (2009). *Cryptographic Boolean functions:Academic Press*. San Didgo.

Kavut, S. (2012). Results on rotation-symmetric S-boxes. *Information Sciences, 201*, 93-113. http://dx.doi.org/10.1016/j.ins.2012.02.030

Kavut, S., & Ycel, M. D. (2010). 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class. *Information Sciences, 208*(4), 341-350. http://dx.doi.org/10.1016/j.ic.2009.12.002

Kim, H., Park, S. M., & Hahn, S. G. (2009). On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2. *Discrete Applied Mathematics, 157*, 428-432. http://dx.doi.org/10.1016 /j.dam.2008.06.022

Copyrights