The Lower Bounds on the Second Order Nonlinearity of Cubic Boolean Functions

Xuelian Li[1,2] Yupu Hu[2] Juntao Gao[2]

1.Department of Applied Mathematics of Xidian University, Xi'an 710071, China. E-mail: xuelian202@163.com.
2. Key Laboratory of Computer Networks and Information Security of Xidian University, Ministry of Education, Xi'an 710071, China.

Abstract. It is a difficult task to compute the r-th order nonlinearity of a given function with algebraic degree strictly greater than $r > 1$. Even the lower bounds on the second order nonlinearity is known only for a few particular functions. We investigate the lower bounds on the second order nonlinearity of cubic Boolean functions $F_u(x) = Tr(\sum_{l=1}^{m} \mu_l x^{d_l})$, where $u_l \in F_{2^n}^*$, $d_l = 2^{i_l} + 2^{j_l} + 1$, i_l and j_l are positive integers, $n > i_l > j_l$. Especially, for a class of Boolean functions $G_u(x) = Tr(\sum_{l=1}^{m} \mu_l x^{d_l})$, we deduce a tighter lower bound on the second order nonlinearity of the functions, where $u_l \in F_{2^n}^*$, $d_l = 2^{i_l\gamma} + 2^{j_l\gamma} + 1$, $i_l > j_l$ and $\gamma \neq 1$ is a positive integer such that $gcd(n, \gamma) = 1$.
The lower bounds on the second order nonlinearity of cubic monomial Boolean functions, represented by $f_\mu(x) = Tr(\mu x^{2^i+2^j+1})$, $\mu \in F_{2^n}^*$, i and j are positive integers such that $i > j$, have recently (2009) been obtained by Gode and Gangopadhvay. Our results have the advantages over those of Gode and Gangopadhvay as follows. We first extend the results from monomial Boolean functions to Boolean functions with more trace terms. We further generalize and improve the results to a wider range of n. Also, our bounds are better than those of Gode and Gangopadhvay for monomial functions $f_\mu(x)$.
Key Words: cryptography, derivative, the second nonlinearity, trace function, quadratic form

1 Introduction

Boolean functions are important components in the design of stream ciphers as well as block ciphers. Nonlinearity profile of a Boolean function is a cryptographic criterion which plays an important role with respect to the security of the cryptosystems in which the functions are involved. It is also important in coding theory as it is related to the covering radii of Reed-Muller code [1]. Let f be an n-variable Boolean function. The r-th order nonlinearity of f, denoted by $nl_r(f)$, is the minimum Hamming distance between f and all n-variable Boolean functions of degree at most r, a nonnegative integer less than or equal to n. The sequence of values $nl_r(f)$ for r ranging from 1 to $n-1$ is said to be the nonlinearity profile of f. The first order nonlinearity of f is referred to as the nonlinearity of f and denoted by $nl(f)$.

Computation of the r-th order nonlinearity (even the second-order nonlinearity) of a given function with algebraic degree strictly greater than r is itself a difficult problem for $r > 1$. Instead of computing the r-th order nonlinearity, one hopes to obtain a tight lower bound of r-th order nonlinearity which can be useful to estimate the security of Boolean functions. However, it is also a quite difficult task to find a good lower bound, even for the second order nonlinearity. Efforts are made to compute the second order nonlinearity by using decoding techniques of the second order Reed-Muller codes. As far as we known, there are only the algorithms developed in [2] [3] [4] which compute the second order nonlinearity for $n \leq 11$ and for $n \leq 13$ for some special cases. In 2008, Carlet [5] introduced a method to determine the lower bound of the r-th order nonlinearity of a function from the maximum value or the lower bounds of the $(r-1)$-th order nonlinearity of its first derivatives, and obtained the lower bounds on the second order nonlinearities of some functions including Welch function and multiplicative inverse function and so on. Sun and Wu [6], Gangopadhvay, Sarkar and Telang [7] gained the lower bounds on the second nonlinearity of some particular cubic monomial Boolean functions with high nonlinearities. Gode and Gangopadhvay [8] recently have obtained the lower bounds on the second order nonlinearity of cubic monomial Boolean functions of the form $f_\mu(x) = Tr(\mu x^{2^i+2^j+1})$ for $n > 2i$ where $\mu \in F^*_{2^n}$, $i > j$ are positive integers, and the ones of a class of functions $g_\mu(x) = Tr(\mu x^{2^{2\gamma}+2^\gamma+1})$ for $n \geq 4$, where $\mu \in F^*_{2^n}$ and γ is a positive integer such that $gcd(n, \gamma) = 1$. However, both of the two bounds are valid only if $n \neq i + j$ and $n \neq 2i - j$.

In this paper we study the lower bounds on the second order nonlinearity of cubic functions on F_{2^n}. The cubic function can be represented by a polynomial form of

$$F_u(x) = Tr(\sum_{l=1}^{m} \mu_l x^{d_l}),$$

where $u_l \in F^*_{2^n}$, $d_l = 2^{i_l} + 2^{j_l} + 1$ and $n > i_l > j_l$. For a class of Boolean functions, represented by $G_u(x) = Tr(\sum_{l=1}^{m} \mu_l x^{d_l})$ which are different from the functions in [6] and [7], we deduce a tighter lower bound of the second order nonlinearity, where $u_l \in F^*_{2^n}$, $d_l = 2^{i_l\gamma} + 2^{j_l\gamma} + 1$, $i_l > j_l$, $\gamma \neq 1$ is a positive integer such that $gcd(n, \gamma) = 1$. Most interesting, we improve and generalize the results of [8]. More specifically,

1. we extend the results from monomial Boolean functions to Boolean functions with more trace terms. Our functions include the monomial Boolean functions $f_\mu(x)$ and $g_\mu(x)$ in [8] as proper subsets;
2. we give better lower bounds than those of [8] for functions $f_\mu(x)$;
3. Our lower bounds are valid for a wider range of n. For example, Gode and Gangopadhvay [8] deduced the lower bounds on the second order nonlinearity of $f_\mu(x)$ for $n > 2i$. However, for $f_\mu(x)$, our lower bounds not only hold for $n > 2i$, but also hold for $n \leq 2i$. Moreover, we deduce the lower bounds on the second order nonlinearity of some $f_\mu(x)$ for $n = i + j$ and $n = 2i - j$.

This paper is organized as follows. In Section 2, we introduce some concepts and definitions which will be used throughout this paper. In Section 3, we first deduce the general lower bounds on the second order nonlinearity of a class of functions $F_u(x)$. We further give the improvement of the bounds for the functions satisfying the conditions of Theorem 1 (2) and (3). The tighter lower bounds on a class of functions $G_u(x)$ are also given in Section 3. Concluding remarks and discussions will be given in Section 4.

2 Preliminaries

A Boolean function on F_{2^n} is a function of the form $Tr(R(x))$, where $R(x)$ is any polynomial in $F_{2^n}[x]$ and Tr is the trace function from F_{2^n} to F_2.

For any t dividing n and $n = mt$, we denote the trace function from F_{2^n} onto F_{2^t} as follows:

$$T^n_t(x) = x + x^{2^t} + \cdots + x^{2^{t(m-1)}}, \quad x \in F_{2^n}.$$

The notation Tr is used for $t = 1$.

Let d be a positive integer whose binary representation is $(d_1, d_2, \ldots, d_n)$. If the Hamming weight of d is w, then $Tr(x^d)$ is called a Boolean function with degree w.

Lemma 1 *[9] The trace function $T_t^n(x)$ from F_{2^n} onto F_{2^t} satisfies the following properties:*

1. *$T_t^n(\alpha+\beta) = T_t^n(\alpha) + T_t^n(\beta)$ for all $\alpha, \beta \in F_{2^n}$;*
2. *$T_t^n(\alpha^{2^t}) = T_t^n(\alpha)$ for all $\alpha \in F_{2^n}$;*
3. *$T_t^n(x)$ is a linear transformation from F_{2^n} onto F_{2^t}.*

Let f be any Boolean function on F_{2^n}. The Walsh transform of function f at $u \in F_{2^n}$ is defined by

$$W_f(u) = \sum_{x \in F_{2^n}} (-1)^{f(x)+Tr(ux)}, \ \ u \in F_{2^n}.$$

We define the Walsh spectrum of f as the set $\{W_f(u) : u \in F_{2^n}\}$. The relation between the nonlinearity and the Walsh transform of f is well known:

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{u \in F_{2^n}} |W_f(u)|.$$

The derivative of f with respect to $b \in F_{2^n}$, denoted by $D_b f$, is the Boolean function $D_b f : x \mapsto f(x) + f(x+b)$.

Definition 1 *[10] Let V be an n-dimensional vector space over F_{2^t}. A map $Q : V \mapsto F_{2^t}$ is called a quadratic form on V if*

1. *$Q(cx) = c^2 Q(x)$ for any $c \in F_{2^t}$ and $x \in V$;*
2. *$B(x,y) = Q(x+y) + Q(x) + Q(y)$ is bilinear on V.*

The kernel K of a quadratic form Q is the subspace of V defined by $K = \{x \in V : B(x,y) = 0$ for any $y \in V\}$.

Obviously, the vast majority of derivatives of the cubic Boolean functions are quadratic functions. The kernel K of quadratic Boolean functions have the following properties.

Lemma 2 *[10] Let f be any quadratic Boolean function. The kernel K of f is the subspace of those b such that the derivative $D_b f$ is constant.*

Lemma 3 *[10] Let V be a vector space over a field F_{2^t} and $Q : V \mapsto F_{2^t}$ be a quadratic form. Then the dimension of V and the dimension of the kernel of Q have the same parity.*

Table 1. The Walsh spectrum of f

$W_f(u)$	Number of u
0	$2^n - 2^{n-k}$
$2^{(n+k)/2}$	$2^{n-k-1} + (-1)^{f(0)} 2^{(n-k-2)/2}$
$-2^{(n+k)/2}$	$2^{n-k-1} - (-1)^{f(0)} 2^{(n-k-2)/2}$

It is easy to show that for any quadratic form $Q : F_{2^n} \mapsto F_2$ there is a unique $\delta_i \in F_{2^n}, 0 \leq i \leq \lfloor n/2 \rfloor$, such that

$$Q(x) = T_r(\sum_{i=0}^{\lfloor n/2 \rfloor} \delta_i x^{2^i+1}),$$

except when n is even, in which case $\lfloor n/2 \rfloor$ is only unique modulo $F_{2^{\lfloor n/2 \rfloor}}$ [11]. If $f : F_{2^n} \mapsto F_2$ is a Boolean quadratic form, then its Walsh spectrum only depends on the dimension k ($0 \leq k \leq n-2$) of the kernel of f. More precisely, the Walsh spectrum of f is given in Table 1.

Definition 2 *[12] A cyclotomic coset C_s modulo $p^n - 1$ (with respect to p) is defined to be*

$$C_s = \{s, sp, \dots, sp^{n_s - 1}\},$$

where n_s is the smallest positive integer such that $s \equiv sp^{n_s}(mod p^n - 1)$. The subscript s is chosen as the smallest integer in C_s, and s is called the coset leader of C_s.

3 The lower bounds on the second order nonlinearity of Boolean function $F_\mu(x)$

Before showing the main result, we firstly cite two useful propositions.

Proposition 1 *[5] Let f be any n-variable function and r a positive integer smaller than n. We have*

$$nl_r(f) \geq \frac{1}{2} \max_{a \in F_2^n} nl_{r-1}(D_a f).$$

Carlet [5] has also given a potentially stronger lower bound on the r-th order nonlinearity than that of Proposition 1, valid when a lower bound on the $(r-1)$-th order nonlinearity is known for all the derivatives (in nonzero directions) of the function.

Proposition 2 *[5] Let f be any n-variable function and r a positive integer smaller than n. We have*

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2 \sum_{a \in F_2^n} nl_{r-1}(D_a f)}.$$

Carlet has pointed out that both lower bounds are tight. Moreover, the bound of Proposition 2 will actually lead to an efficient bound.

Corollary 1 *Let f be any n-variable function and r a positive integer smaller than n. Assume that, for some nonnegative integers K and k, we have $nl_{r-1}(D_a f)$*
$\geq 2^{n-1} - K2^k$ for every nonzero $a \in F_2^n$, then

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)K2^{k+1} + 2^n}.$$

In [8], the authors give the lower bound on the second order nonlinearity of the Boolean function $f_\mu(x) = Tr(\mu x^{2^i + 2^j + 1})$ for $n > 2i$, where $\mu \in F_{2^n}^*$ and $i > j$ are positive integers.

Lemma 4 *[8] The function $f_\mu(x)$ possesses no affine derivative if $n \neq i + j$ or $n \neq 2i - j$, where $i > j$.*

Thus, $D_a f_\mu$ is always quadratic as $n \geq 2i$ (In this case, $n \neq i + j$ and $n \neq 2i - j$).

Lemma 5 *[8] The lower bound on the second order nonlinearity of $f_\mu(x) = Tr(\mu x^{2^i + 2^j + 1})$ for $n > 2i$ is given as*

If n is an even, then

$$nl_2(f_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{(n+2i)/2} + 2^n} \approx 2^{n-1} - 2^{(3n+2i-4)/4};$$

If n is an odd, then

$$nl_2(f_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{(n+2i-1)/2} + 2^n} \approx 2^{n-1} - 2^{(3n+2i-5)/4}.$$

We consider the following cubic Boolean function:

$$f_\mu(x) = Tr(\sum_{l=1}^{m} \mu_l x^{d_l}),$$

where $\mu_l \in F_{2^n}^*$, $d_l = 2^{i_l} + 2^{j_l} + 1$ and $n > i_l > j_l$. Let all of the power of 2 be positive integers in this paper.

We will deduce the lower bound on the second order nonlinearity of the Boolean function $F_\mu(x)$, and demonstrate that our results are the improvements and generalizations of those of [8].

By Proposition 2, if we can calculate the nonlinearity of $D_aF_\mu(x)$ for any $a \in F_{2^n}^*$ or their lower bounds on the nonlinearity, then it is possible to obtain a lower bound on the second order nonlinearity of $F_\mu(x)$.

3.1 The derivative of $F_\mu(x)$

The derivative of $F_\mu(x)$ with respect to $a \in F_{2^n}^*$ is the function

$$\begin{aligned} D_aF_\mu(x) &= Tr(\sum_{l=1}^{m} \mu_l x^{d_l}) + Tr(\sum_{l=1}^{m} \mu_l (x+a)^{d_l}) \\ &= Tr(\sum_{l=1}^{m} \mu_l a^{d_l}(a^{-1}x)^{d_l}) + Tr(\sum_{l=1}^{m} \mu_l a^{d_l}(a^{-1}x+1)^{d_l}) \\ &= D_1F_{\mu_l a^{d_l}}(a^{-1}x). \end{aligned}$$

Let $\lambda_l = \mu_l a^{d_l}$ and $D_1F_{\mu_l a^{d_l}}(a^{-1}x) = g(x)$.

$$\begin{aligned} g(x) &= Tr(\sum_{l=1}^{m} \lambda_l x^{d_l}) + Tr(\sum_{l=1}^{m} \lambda_l (x+1)^{d_l}) \\ &= \sum_{l=1}^{m} Tr(\lambda_l(x^{2^{i_l}+2^{j_l}+1} + (x+1)^{2^{i_l}+2^{j_l}+1})) \\ &= \sum_{l=1}^{m} Tr(\lambda_l(x^{2^{i_l}+2^{j_l}} + x^{2^{i_l}+1} + x^{2^{j_l}+1} + x^{2^{i_l}} + x^{2^{j_l}} + x + 1)) \\ &= \sum_{l=1}^{m} Tr(\lambda_l^{2^{n-j_l}} x^{2^{i_l-j_l}+1} + \lambda_l x^{2^{i_l}+1} + \lambda_l x^{2^{j_l}+1} + \lambda_l x^{2^{i_l}} + \lambda_l x^{2^{j_l}} + \lambda_l x + \lambda_l)) \\ &= \sum_{l=1}^{m} Tr(\lambda_l^{2^{n-j_l}} x^{2^{i_l-j_l}+1} + \lambda_l x^{2^{i_l}+1} + \lambda_l x^{2^{j_l}+1} + (\lambda_l^{2^{n-i_l}} + \lambda_l^{2^{n-j_l}} + \lambda_l)x + \lambda_l)). \end{aligned}$$

To obtain the Walsh spectrum of the function $D_aF_\mu(x)$ for any $a \in F_{2^n}^*$ it is enough to consider the spectrum of the functions $g(x)$ because of $a \neq 0$. The Walsh spectrum of the function $g(x)$ coincides with that of the following function:

$$g_{\lambda_l}(x) = \sum_{l=1}^{m} Tr(\lambda_l^{2^{n-j_l}} x^{2^{i_l-j_l}+1} + \lambda_l x^{2^{i_l}+1} + \lambda_l x^{2^{j_l}+1}), \tag{1}$$

where $\lambda_l \neq 0$. Merging similar items, for your convenience, we can rewrite $g_{\lambda_l}(x)$ as

$$g_c(x) = \sum_i Tr(c_i x^{2^i+1}). \tag{2}$$

It is well known that 2^{i+1} and 2^{j+1} are in different cyclotomic cosets for $n \neq i+j$. Now, we improve the conclusions of Lemma 4 as follows.

Theorem 1 *If function $\sum_i Tr(c_i x^{2^i+1})$ satisfies one of the following conditions, then it is a quadratic Boolean function.*

1. *All of the power 2^{i+1} of x are in different cyclotomic cosets.*
2. *At least one power 2^{i+1} of x is in different cyclotomic coset from all the other power of x. Let all of the power 2^{i+1} of x are in different e cyclotomic cosets, $\sum_i Tr(c_i x^{2^i+1})$ can be rewritten as $\sum_{j=1}^{e} Tr(\sum_{j_l} c_{i_{j_l}} x^{2^{i_{j_l}}+1}) = \sum_{j=1}^{e} Tr(c_{i_j} x^{2^{i_j}+1})$, where $2^{i_j}+1$ $(1 \leq j \leq e)$ is the smallest positive integer of x's powers in the j-th cosets, and one of the following conditions is valid.*
   (a) *all $c_{i_j} \neq 0$;*
   (b) *some $c_{i_j} = 0$.*
3. *All of the power 2^{i+1} of x are in different e cyclotomic cosets, and every cyclotomic coset contains at least two powers of x. Then function $\sum_i Tr(c_i x^{2^i+1})$ can be rewritten as*

$$\sum_{j=1}^{e} Tr(\sum_{j_l} c_{i_{j_l}} x^{2^{i_{j_l}}+1}) = \sum_{j=1}^{e} Tr(c_{i_j} x^{2^{i_j}+1}),$$

   where $2^{i_j}+1$ $(1 \leq j \leq e)$ is the smallest positive integer of x's powers in the j-th cosets, and one of the following conditions is valid.
   (a) *All $c_{i_j} \neq 0$;*
   (b) *Some $c_{i_j} = 0$, and at least one c_{i_j} for all $a \in F_{2^n}^*$ is not equal to zero.*

If the quadratic terms of D_af satisfy the conditions of Theorem 1, we also call that $f(x)$ satisfies the conditions of Theorem 1.
Obviously $g_c(x)$ is belonging to the following class of functions:

$$h(x) = Tr(\sum_{i=1}^{n-1} c_i x^{2^i+1}), \tag{3}$$

where $c_i \in F_{2^n}$, and at least one c_i is not equal to zero. Let $s = \min\{i | c_i \neq 0, 1 \leq i \leq n-1\}$, $t = \max\{i | c_i \neq 0, 1 \leq i \leq n-1\}$ and $t_1 = max\{i | c_i \neq 0 \; and \; c_i \neq c_t\}$ if $s \neq t$ or $n \neq 2t$.

3.2 The Walsh spectrum of $h(x)$

In this section, we study the quadratic Boolean function $h(x)$ on F_{2^n}. Firstly, we determine the dimension k of the kernel of $h(x)$ by the properties of their derivatives. Then we evaluate the Walsh spectrum of $h(x)$.

Note that $h(x)$ is a quadratic form from F_{2^n} into F_2. Thus we can use the results of Section 2 to evaluate the Walsh spectrum of $h(x)$ as soon as the dimension of its kernel is known. Our next goal is to describe this kernel.

The following theorem implies that the kernel of $h(x)$ is determined by the roots of certain polynomial $P(x)$ or $L(x)$.

Theorem 2 *Let $K(h)$ be the kernel of the quadratic form $h(x)$. Then $K(h)$ is the subspace of the roots of $P(x)$ or $L(x)$ in $F_{2^n}[x]$ given by*

$$P(x) = \sum_{i=s}^{t}((c_i x)^{2^{n-i}} + c_i x^{2^i}), L(x) = \sum_{i=s}^{t}((c_i x)^{2^{t-i}} + c_i^{2^t} x^{2^{i+t}}).$$

where $s = \min\{i|c_i \neq 0, 1 \leq i \leq n-1\}$, $t = \max\{i|c_i \neq 0, 1 \leq i \leq n-1\}$.

Proof: We compute the derivatives of $h(x)$ with respect to any $b \in F_{2^n}^*$. From Lemma 1, we have

$$\begin{aligned} D_b h(x) &= Tr(\sum_{i=s}^{t} c_i x^{2^i+1}) + Tr(\sum_{i=s}^{t} c_i (x+b)^{2^i+1}) \\ &= Tr(\sum_{i=s}^{t} c_i (x^{2^i+1} + bx^{2^i} + b^{2^i}x + b^{2^i+1}) + c_i x^{2^i+1}) \\ &= Tr(\sum_{i=s}^{t} c_i b x^{2^i} + c_i b^{2^i} x) + h(b) \\ &= Tr(x\sum_{i=s}^{t}((c_i b)^{2^{n-i}} + c_i b^{2^i}) + h(b). \end{aligned}$$

Let

$$\begin{aligned} P(x) &= \sum_{i=s}^{t}((c_i x)^{2^{n-i}} + c_i x^{2^i}), \\ L(x) &= (\sum_{i=s}^{t}((c_i x)^{2^{n-i}} + c_i x^{2^i}))^{2^t} = \sum_{i=s}^{t}((c_i x)^{2^{t-i}} + c_i^{2^t} x^{2^{i+t}}). \end{aligned}$$

Obviously, $D_b h(x) = h(b)$ if $P(b) = 0$ or $L(b) = 0$. From Lemma 2, we have

$$K(h) = \{x \in F_{2^n} \mid P(x) = 0 \; or L(x) = 0\}.$$

□

Definition 3 *[9] A polynomial of the form $\sum_{i=0}^{n-1} a_i x^{q^i}$ with coefficients in an extension field F_{q^n} of F_q is called a q-polynomial (a linearized polynomial) over F_{q^n}.*

We known that the kernel and the image set of a q-polynomial are subspaces of F_{q^n} over F_q. In particular, these sets have cardinality q^k for some k. The polynomial $P(x)$ and $L(x)$ considered here is a 2-polynomial. If $n-s \geq t$, $P(x) = P'(x)^{2^s}$, then $n-t \geq s$(i.e., $n \geq s+t$), the degree of $P'(x)^{2^s}$ is 2^{n-2s}, and $K(h)$ has at most 2^{n-2s} elements; Otherwise, $n-s < t$ (i.e., $n < s+t$), then $n-t < s$, $P(x) = P''(x)^{2^{n-t}}$, the degree of $P''(x)^{2^{n-t}}$ is 2^{2t-n}, and $K(h)$ has at most 2^{2t-n} elements. On the other hand, let $n > 2t$, then the degree of $L(x)$ is 2^{2t}, and $K(h)$ has at most 2^{2t} elements; If $n = 2t$, then the degree of $L(x)$ is 2^{2t_1}, and $K(h)$ has at most 2^{2t_1} elements.

Theorem 3 *1. If $n < s+t$, then $W_h(u) \leq 2^t$;*

2. If $s+t \leq n < 2t$, then $W_h(u) \leq 2^{n-s}$;

3. If $n = 2t$, let $p = min\{n-2s, 2t_1\}$, then $W_h(u) \leq 2^{(n+p)/2}$;

4. If $n > 2t$ is an even, let $p = min\{n-2s, 2t\}$, then $W_h(u) \leq 2^{(n+p)/2}$; If $n > 2t$ is an odd, let $q = min\{n-2s, 2t-1\}$, then $W_h(u) \leq 2^{(n+q)/2}$.

Proof: Here, we only prove (1). From Lemma 3, when $n < s+t$ is an even (or odd), then $k \leq 2t-n$ must be even (or odd) too. By Table 1, we have $W_h(u) \leq 2^t$. In a similar way, one can obtain (2), (3) and (4). □

From section 3.1, we know the function $g_c(x)$ satisfying the conditions of Theorem 1 is the form of functions $h(x)$. So we can evaluate the Walsh spectrum of $g_c(x)$(i.e. the one of $D_aF_\mu(x)$) applying Theorem 3, and deduce its lower bound of nonlinearity.

Corollary 2 *1. If $n < s+t$, then $W_{D_aF_\mu}(u) \leq 2^t$, and $nl(D_aF_\mu) \geq 2^{n-1} - 2^{t-1}$;*

2. If $s+t \leq n < 2t$, then $W_{D_aF_\mu}(u) \leq 2^{n-s}$, and $nl(D_aF_\mu) \geq 2^{n-1} - 2^{n-s-1}$;

3. If $n = 2t$, let $p = min\{n-2s, 2t_1\}$, then $W_{D_aF_\mu}(u) \leq 2^{(n+p)/2}$, and $nl(D_aF_\mu) \geq 2^{n-1} - 2^{(n+p-2)/2}$;

4. If $n > 2t$ is an even, let $p = min\{n-2s, 2t\}$, then $W_{D_aF_\mu}(u) \leq 2^{(n+p)/2}$, and $nl(D_aF_u) \geq 2^{n-1} - 2^{(n+p-2)/2}$; If $n > 2t$ is an odd, let $q = min\{n-2s, 2t-1\}$, then $W_{D_aF_\mu}(u) \leq 2^{(n+q)/2}$, and $nl(D_aF_\mu) \geq 2^{n-1} - 2^{(n+q-2)/2}$.

3.3 The lower bound of $nl_2(F_\mu)$

Gode and Gangopadhvay [8] have derived the lower bounds on the second order nonlinearity of $f_\mu(x) = Tr(\mu x^{2^i+2^j+1})$ for $n > 2i$ (Therefore, $n \neq i+j$ and $n \neq 2i-j$). Now, we derive the lower bounds of $nl_2(F_\mu)$ for $n \geq 3$ in the following theorem, and demonstrate that our bounds are better than those of $f_\mu(x)$.

Theorem 4 *Let $F_\mu(x)$ satisfy the conditions of Theorem 1, then*

1. If $n < s+t$,

$$nl_2(F_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^t + 2^n} \approx 2^{n-1} - 2^{(n+t-2)/2};$$

2. If $s+t \leq n < 2t$,

$$nl_2(F_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{n-s} + 2^n} \approx 2^{n-1} - 2^{(2n-s-2)/2};$$

3. If $n = 2t$ and $s \neq t$, let $p = min\{n - 2s, 2t_1\}$,

$$nl_2(F_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{(n+p)/2} + 2^n} \approx 2^{n-1} - 2^{(3n+p-4)/4};$$

4. If $n > 2t$ is an even, let $p = min\{n - 2s, 2t\}$,

$$nl_2(F_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{(n+p)/2} + 2^n} \approx 2^{n-1} - 2^{(3n+p-4)/4};$$

If $n > 2t$ is an odd, let $q = min\{n - 2s, 2t - 1\}$,

$$nl_2(F_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{(n+q)/2} + 2^n} \approx 2^{n-1} - 2^{(3n+q-4)/4};$$

Proof: Case 1: $F_\mu(x)$ satisfies the conditions of Theorem 1 (1) or (2a) or (3a).
From Corollary 2, we have
(1). Corollary 1 with $K = 1$ and $k = t - 1$ implies that

$$nl_2(F_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^t + 2^n} \approx 2^{n-1} - 2^{(n+t-2)/2};$$

In a similar way, one can obtain (2), (3)and (4).
Case 2: $F_\mu(x)$ satisfies the conditions of Theorem 1 (2b) or (3b).
Let $s' = \min\{i|c_i \neq 0, 1 \leq i \leq n-1\}$, $t' = \max\{i|c_i \neq 0, 1 \leq i \leq n-1\}$ and $t_1' = max\{i|c_i \neq 0 \; and \; c_i \neq c_{t'}\}$. So $s' \geq s$, $t' \leq t$ and $t_1' \leq t_1$, where s, t and t_1 are the ones of Case 1. We only prove (1), let $n < s + t$.

- If $s' \geq s$, $t' = t$, then $n < s + t \leq s' + t$, from Corollary 2 $W_{D_aF_\mu}(u) \leq 2^{t'} = 2^t$, and $nl(D_aF_\mu) \geq 2^{n-1} - 2^{t-1}$;
- If $s' = s$, $t' \leq t$, then, (1). if $n < s + t' \leq s + t$, from Corollary 2 $W_{D_aF_\mu}(u) \leq 2^{t'}$. Therefore $W_{D_aF_\mu}(u) \leq 2^t$, and $nl(D_aF_\mu) \geq 2^{n-1} - 2^{t-1}$; (2). if $s + t' \leq n < s + t$, from Corollary 2 $W_{D_aF_\mu}(u) \leq 2^{n-s'} = 2^{n-s}$. Therefore $W_{D_aF_\mu}(u) < 2^t$, and $nl(D_aF_\mu) > 2^{n-1} - 2^{t-1}$;
- If $s' \geq s$, $t' \leq t$, one can also have $W_{D_aF_\mu}(u) \leq 2^t$, and $nl(D_aF_\mu) \geq 2^{n-1} - 2^{t-1}$.

Therefore, $W_{D_aF_\mu}(u) \leq 2^t$, and $nl(D_aF_\mu) \geq 2^{n-1} - 2^{t-1}$ for $n < s + t$. Applying Corollary 1 the proof can be completed for $n < s + t$. □

Example 1 *: Let $F_\mu(x) = f_u(x) = Tr(\mu x^{2^i+2^j+1})$ for $n > 2i$ and $0 < i-j < j$, then $F_\mu(x)$ satisfies the condition (1) of Theorem 1. And equation (1) is*

$$g_\lambda(x) = Tr(\lambda^{2^{n-j}} x^{2^{i-j}+1} + \lambda x^{2^i+1} + \lambda x^{2^j+1}).$$

Hence $s = i-j$ and $t = i$. Let $n = 20$, $i = 9$ and $j = 5$. By Theorem 4 we have $p = min\{n-2s, 2t\} = min\{12, 18\} = 12$, and

$$nl_2(F_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{(n+p)/2} + 2^n} = 2^{19} - \frac{1}{2}\sqrt{(2^{20} - 1)2^{16} + 2^{20}} \approx 2^{19} - 2^{17}.$$

While, by Lemma 5 one can obtain

$$nl_2(F_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{(n+2i)/2} + 2^n} = 2^{19} - \frac{1}{2}\sqrt{(2^{20} - 1)2^{19} + 2^{20}} \approx 2^{19} - 2^{18.5}.$$

Let $n = 19$, $i = 9$ and $j = 5$. By Theorem 4 we have $q = min\{n - 2s, 2t - 1\} = min\{11, 17\} = 11$, and

$$nl_2(F_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{(n+q)/2} + 2^n} = 2^{18} - \frac{1}{2}\sqrt{(2^{19} - 1)2^{15} + 2^{19}} \approx 2^{18} - 2^{16}.$$

While, by Lemma 5 one can obtain

$$nl_2(F_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{(n+2i-1)/2} + 2^n} = 2^{18} - \frac{1}{2}\sqrt{(2^{19} - 1)2^{18} + 2^{19}} \approx 2^{18} - 2^{17.5}.$$

Obviously, our lower bounds of $f_u(x)$ are tighter than those of [8] for $n > 2i$. And our results are valid for smaller n.
For $f_u(x)$, it is possible to deduce the lower bounds when $n \leq 2i$ from Theorem 4. This case has not been considered in [8]. For example, $n = i + j$ and $n = 2i - j$.

Corollary 3 *Let $n = i+j$ and $n = 2i-j$(i.e. $i = 2n/3$, $j = n/3$.). If $Tr^n_{n/3}(\mu) \neq 0$, then the lower bound of the second order nonlinearity of $f_\mu(x) = Tr(\mu x^{2^i+2^j+1})$ is given as follows,*

$$nl_2(f_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{2n/3} + 2^n} \approx 2^{n-1} - 2^{(5n-6)/6}.$$

Proof: The derivative of $f_\mu(x)$ with respect to $a \in F^*_{2^n}$ is the function

$$\begin{aligned} D_a f_\mu(x) &= Tr(\mu x^{2^i+2^j+1}) + Tr(\mu(x + a)^{2^i+2^j+1}) \\ &= Tr(\mu(ax^{2^i+2^j} + a^{2^j}x^{2^i+1} + a^{2^i}x^{2^j+1} + a^{2^j+1}x^{2^i} \\ &+ a^{2^i+1}x^{2^j} + a^{2^i+2^j}x + a^{2^i+2^j+1})). \end{aligned}$$

The Walsh spectrum of $D_a f_\mu(x)$ is equivalent to the Walsh spectrum of the following function,

$$g_\lambda(x) = Tr(\mu(ax^{2^i+2^j} + a^{2^j}x^{2^i+1} + a^{2^i}x^{2^j+1}).$$

If $n = i + j$, then $2^i + 1$ and $2^j + 1$ are in the same cyclotomic coset, $2^i + 1 = 2^{n-j} + 1 = 2^{-j}(2^n + 2^j)mod(2^n - 1) = 2^{n-j}(2^j + 1)mod(2^n - 1)$. If $n = 2i - j$, then $2^i + 2^j = 2^i + 2^{2i-n} = 2^{i-n}(2^n + 2^i)mod(2^n - 1) = 2^{i-n}(2^i + 1)mod(2^n - 1)$. If $n = i + j$ and $n = 2i - j$, then $2^i + 2^j = 2^{i-n}(2^i + 1)mod(2^n - 1) = 2^{i-j}(2^j + 1)mod(2^n - 1)$.

$$\begin{aligned} g_\lambda(x) &= Tr(\mu(ax^{2^i+2^j} + a^{2^j}x^{2^i+1} + a^{2^i}x^{2^j+1})) \\ &= Tr(\mu a x^{2^{i-j}(2^j+1)} + \mu a^{2^j}x^{2^{n-j}(2^j+1)} + \mu a^{2^i}x^{2^j+1}) \\ &= Tr((\mu a)^{2^{j-i}}x^{2^j+1} + (\mu a^{2^j})^{2^{j-n}}x^{(2^j+1)} + \mu a^{2^i}x^{2^j+1}) \\ &= Tr(((\mu a)^{2^{-n/3}} + (\mu a^{2^{n/3}})^{2^{n/3}} + \mu a^{2^{2n/3}})x^{2^j+1}) \\ &= Tr((\mu^{2^{2n/3}}a^{2^{2n/3}} + \mu^{2^{n/3}}a^{2^{2n/3}} + \mu a^{2^{2n/3}})x^{2^j+1}) \\ &= Tr((\mu^{2^{2n/3}} + \mu^{2^{n/3}} + \mu)a^{2^{2n/3}}x^{2^j+1}). \end{aligned}$$

It is known from Theorem 1(3a) that $g_\lambda(x)$ is quadratic for all $a \in F^*_{2^n}$ if $\mu^{2^{2n/3}} + \mu^{2^{n/3}} + \mu \neq 0$, equivalently, $Tr^n_{n/3}(\mu) \neq 0$. Applying Theorem 4(4), we obtain $s = t = j = n/3$, $n > 2t = 2n/3$, $p = min\{n - 2s, 2t\} = n/3$, $q = min\{n - 2s, 2t - 1\} = n/3$ and

$$nl_2(f_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{2n/3} + 2^n} \approx 2^{n-1} - 2^{(5n-6)/6}.$$

□

For the functions in case (2) or (3) of Theorem 1, we can improve the results of Theorem 4. For example, we obtain the following corollary when $f_\mu(x) = Tr(\mu x^{2^i+2^j+1})$ for $n = i+j$ and $n \neq 2i-j$.

Corollary 4 *Let $n = i+j$, $n \neq 2i-j$ and $\beta = \sharp\{a|\mu^{2^j} a^{2^{2j}} + \mu a^{2^{n-j}} = 0\}$, then the lower bound on the second order nonlinearity of $f_\mu(x) = Tr(\mu x^{2^i+2^j+1})$ is given as*

1. *if $n < 3j$, for even n we have*

$$nl_2(f_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1 - \beta)2^{2j} + \beta 2^{(n+min\{4j-n,2n-4j\})/2} + 2^n};$$

for odd n we have

$$nl_2(f_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1 - \beta)2^{2j} + \beta 2^{(n+min\{4j-n,2n-4j-1\})/2}) + 2^n}.$$

2. *if $3j < n < 4j$, for even n we have*

$$nl_2(f_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1 - \beta)2^{n-j} + \beta 2^{(n+min\{4j-n,2n-4j\})/2} + 2^n};$$

for odd n we have

$$nl_2(f_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1 - \beta)2^{n-j} + \beta 2^{(n+min\{4j-n,2n-4j-1\})/2}) + 2^n}.$$

3. *if $n = 4j$,*

$$nl_2(f_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1 - \beta)2^{3j} + (\beta+1)2^n}.$$

4. *if $n > 4j$,*

$$nl_2(f_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1 - \beta)2^{n-j} + \beta 2^{n-2j} + 2^n}.$$

Proof: From the proof of Corollary 3, we can have the Walsh spectrum of $D_a f_\mu(x)$ is equivalent to the Walsh spectrum of the following function,

$$\begin{aligned}
g_\lambda(x) &= Tr(\mu(a x^{2^i+2^j} + a^{2^j} x^{2^i+1} + a^{2^i} x^{2^j+1})) \\
&= Tr((\mu a)^{2^{n-j}} x^{2^{i-j}+1} + \mu a^{2^j} x^{2^i+1} + \mu a^{2^i} x^{2^j+1}) \\
&= Tr((\mu a)^{2^{n-j}} x^{2^{i-j}+1} + (\mu a^{2^j})^{2^{j-n}} x^{2^j+1} + \mu a^{2^i} x^{2^j+1}) \\
&= Tr((\mu a)^{2^{n-j}} x^{2^{i-j}+1} + ((\mu a^{2^j})^{2^j} + \mu a^{2^i}) x^{2^j+1}) \\
&= Tr((\mu a)^{2^{n-j}} x^{2^{n-2j}+1} + (\mu^{2^j} a^{2^{2j}} + \mu a^{2^{n-j}}) x^{2^j+1}).
\end{aligned}$$

Clearly $n = i+j > 2j$ and $n \neq 3j$.

(1) If $\mu^{2^j} a^{2^{2j}} + \mu a^{2^{n-j}} \neq 0$, applying Theorem 3, we obtain,
if $n < 3j$, then $s = n-2j$, $t = j$ and $n > 2t$. $W_{g_\lambda}(u) \leq 2^{(n+p)/2}$, and $nl(g_\lambda) \geq 2^{n-1} - 2^{(n+p-2)/2}$ for even n; $W_{g_\lambda}(u) \leq 2^{(n+q)/2}$, and $nl(g_\lambda) \geq 2^{n-1} - 2^{(n+q-2)/2}$ for odd n, where $p = min\{n - 2s, 2t\} = min\{4j-n, 2j\} = 4j-n$, $q = min\{n-2s, 2t-1\} = min\{4j-n, 2j-1\} = 4j-n$.
if $3j < n < 4j$, then $s = j$, $t = n-2j$ and $n > 2t$. $W_{g_\lambda}(u) \leq 2^{(n+p)/2}$, and $nl(g_\lambda) \geq 2^{n-1} - 2^{(n+p-2)/2}$ for even n; $W_{g_\lambda}(u) \leq 2^{(n+q)/2}$, and $nl(g_\lambda) \geq 2^{n-1} - 2^{(n+q-2)/2}$ for odd n,

where $p = min\{n-2s, 2t\} = min\{n-2j, 2(n-2j)\} = n-2j$, $q = min\{n-2s, 2t-1\} = min\{n-2j, 2(n-2j)-1\} = n-2j$.
if $n = 4j$, then $s = t_1 = j$, $t = n-2j = 2j$, $n = 2t$ and $n-2s = 2t_1 = 2j$. $W_{g_\lambda}(u) \leq 2^{(n+2j)/2} = 2^{3j}$, and $nl(g_\lambda) \geq 2^{n-1} - 2^{3j-1}$.
if $n > 4j$, then $s = j$, $t = n-2j$ and $s+t < n < 2t$. $W_{g_\lambda}(u) \leq 2^{n-s} = 2^{n-j}$, and $nl(g_\lambda) \geq 2^{n-1} - 2^{n-j-1}$.

(2) If $\mu^{2^j} a^{2^{2j}} + \mu a^{2^{n-j}} = 0$, let $\beta = \sharp\{a | \mu^{2^j} a^{2^{2j}} + \mu a^{2^{n-j}} = 0\}$. Obviously $\beta < 2^n$.

$$g_\lambda(x) = Tr((\mu a)^{2^{n-j}} x^{2^{n-2j}+1}).$$

Clearly, $s = t = n-2j$. Applying Theorem 3, we have
if $n < 4j$, then $n > 2t$. $W_{g_\lambda}(u) \leq 2^{(n+p)/2}$, and $nl(g_\lambda) \geq 2^{n-1} - 2^{(n+p-2)/2}$ for even n; $W_{g_\lambda}(u) \leq 2^{(n+q)/2}$, and $nl(g_\lambda) \geq 2^{n-1} - 2^{(n+q-2)/2}$ for odd n, where $p = min\{n-2s, 2t\} = min\{4j-n, 2n-4j\}$, $q = min\{n-2s, 2t-1\} = min\{4j-n, 2n-4j-1\}$.
if $n = 4j$, then $n = 2t$ and $s = t$. Clearly $W_{g_\lambda}(u) \leq 2^{(n+n)/2} = 2^n$, and $nl(g_\lambda) \geq 2^{n-1} - 2^{n-1} = 0$.
if $n > 4j$, then $n < s+t$. So $W_{g_\lambda}(u) \leq 2^{n-2j}$, and $nl(g_\lambda) \geq 2^{n-1} - 2^{(n-2j-1)}$.

So, if $n < 3j$, for even n we have

$$\begin{aligned} nl_2(f_\mu) &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a \in F_2^n} nl(D_a f_\mu)} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2((2^n - 1 - \beta)(2^{n-1} - 2^{(n+4j-n-2)/2}) + \beta(2^{n-1} - 2^{(n+min\{4j-n,2n-4j\}-2)/2}))} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1 - \beta)2^{2j} + \beta 2^{(n+min\{4j-n,2n-4j\})/2} + 2^n}; \end{aligned}$$

for odd n we have

$$\begin{aligned} nl_2(f_\mu) &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a \in F_2^n} nl(D_a f_\mu)} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2((2^n - 1 - \beta)(2^{n-1} - 2^{(n+4j-n-2)/2}) + \beta(2^{n-1} - 2^{(n+min\{4j-n,2n-4j-1\}-2)/2}))} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1 - \beta)2^{2j} + \beta 2^{(n+min\{4j-n,2n-4j-1\})/2} + 2^n}. \end{aligned}$$

If $3j < n < 4j$, for even n we have

$$\begin{aligned} nl_2(f_\mu) &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a \in F_2^n} nl(D_a f_\mu)} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2((2^n - 1 - \beta)(2^{n-1} - 2^{(n+n-2j-2)/2}) + \beta(2^{n-1} - 2^{(n+min\{4j-n,2n-4j\}-2)/2}))} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1 - \beta)2^{n-j} + \beta 2^{(n+min\{4j-n,2n-4j\})/2} + 2^n}; \end{aligned}$$

for odd n we have

$$\begin{aligned} nl_2(f_\mu) &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a\in F_2^n} nl(D_a f_\mu)} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2((2^n-1-\beta)(2^{n-1} - 2^{(n+n-2j-2)/2}) + \beta(2^{n-1} - 2^{(n+min\{4j-n,2n-4j-1\}-2)/2}))} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1-\beta)2^{n-j} + \beta 2^{(n+min\{4j-n,2n-4j-1\})/2} + 2^n}. \end{aligned}$$

If $n = 4j$,

$$\begin{aligned} nl_2(f_\mu) &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a\in F_2^n} nl(D_a f_\mu)} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2((2^n-1-\beta)(2^{n-1} - 2^{3j-1}) + \beta * 0)} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1-\beta)2^{3j} + (\beta+1)2^n}. \end{aligned}$$

If $n > 4j$,

$$\begin{aligned} nl_2(f_\mu) &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a\in F_2^n} nl(D_a f_\mu)} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2((2^n-1-\beta)(2^{n-1} - 2^{n-j-1}) + \beta(2^{n-1} - 2^{(n-2j-1)}))} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1-\beta)2^{n-j} + \beta 2^{n-2j} + 2^n}. \end{aligned}$$

□

Remark 1 *If $\mu^{2^j} a^{2^{2j}} + \mu a^{2^{n-j}} = 0$, equivalently $a^{2^{3j}-1} = (\frac{1}{\mu^{2^j-1}})^{2^j}$. This is possible only if μ is a $(2^{2j} + 2^j + 1)$th power in F_{2^n}. Let $\mu = \nu^{2^{2j}+2^j+1}$, then $a = \nu^{-2^j}$, where $\nu \in F_{2^n}$. It is well known that the monomial ν^d is a permutation polynomial of F_{2^n} if and only if $gcd(d, 2^n - 1) = 1$. Hence, if μ is a $(2^{2j} + 2^j + 1)$th power in F_{2^n}, then $\beta = 1$ when $gcd(-2^j, 2^n - 1) = 1$; otherwise, $\beta = 0$.*

3.4 The lower bound on the second order nonlinearity of Boolean function $G_\mu(x)$

Gode and Gangopadhyay [8] obtained the lower bound on the second order nonlinearity of $g_\mu(x) = Tr(\mu x^{2^{2\gamma}+2^\gamma+1})$, where $\mu \in F_{2^n}^*$ and γ is a positive integer such that $gcd(n, \gamma) = 1$.

Lemma 6 *[13] Let $g(x) = \sum_{i=0}^{\nu} c_i x^{2^{i\gamma}}$ be a linearized polynomial over F_{2^n}, where $gcd(n, \gamma) = 1$. Then the equation $g(x) = 0$ has at most 2^ν solutions in F_{2^n}.*

Lemma 7 *[8] Suppose $g_\mu(x)$ be defined as $g_\mu(x) = Tr(\mu x^{2^{2\gamma}+2^\gamma+1})$, where $\mu \in F_{2^n}^*$ and γ is a positive integer such that $gcd(n, \gamma) = 1$. Then for $n \geq 4$,*
if n is an even,

$$nl_2(g_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{(n+4)/2} + 2^n} \approx 2^{n-1} - 2^{(3n)/4};$$

if n is an odd,

$$nl_2(g_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{(n+3)/2} + 2^n} \approx 2^{n-1} - 2^{(3n-1)/4}.$$

Now, we study the lower bounds on the second order nonlinearity of a larger class of functions given by

$$G_\mu(x) = Tr(\sum_{l=1}^{m} \mu_l x^{d_l}),$$

where $\mu_l \in F_{2^n}^*$, $d_l = 2^{i_l\gamma} + 2^{j_l\gamma} + 1$, $i_l > j_l$, $\gamma \neq 1$ is a positive integer and $gcd(n,\gamma) = 1$.

Theorem 5 *Suppose $t = max\{i_l | 1 \leq l \leq m\}$. If the function $G_\mu(x)$ satisfies the conditions of Theorem 1, then for $n \geq 2t$,*
if n is an even,

$$nl_2(G_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{(n+2t)/2} + 2^n} \approx 2^{n-1} - 2^{(3n+2t-4)/4};$$

if n is an odd,

$$nl_2(G_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{(n+2t-1)/2} + 2^n} \approx 2^{n-1} - 2^{(3n+2t-5)/4}.$$

Proof: The first derivative D_aG_μ of $G_\mu(x)$ with respect to $a \in F_{2^n}^*$ is

$$D_aG_\mu(x) = Tr(\textstyle\sum_{l=1}^{m} \mu_l x^{2^{i_l\gamma}+2^{j_l\gamma}+1}) + Tr(\sum_{l=1}^{m} \mu_l (x+a)^{2^{i_l\gamma}+2^{j_l\gamma}+1}).$$

We get the Walsh spectrum of $D_aG_\mu(x)$ is equivalent to the Walsh spectrum of the following function,

$$g_{\lambda_l}(x) = \sum_{l=1}^{m} Tr(\lambda_l^{2^{n-j_l\gamma}} x^{2^{i_l\gamma - j_l\gamma}+1} + \lambda_l x^{2^{i_l\gamma}+1} + \lambda_l x^{2^{j_l\gamma}+1}),$$

where $\lambda_l = \mu_l a^{2^{i_l\gamma}+2^{j_l\gamma}+1}$. Clearly, $\lambda_l \neq 0$, and $g_{\lambda_l}(x)$ satisfies the conditions of Theorem 1 (1) or (2). $g_{\lambda_l}(x)$ can be rewritten as $\sum_i Tr(c_i x^{2^{i\gamma}+1})$ and $t = max\{i_l | 1 \leq l \leq m\} = max\{i\}$. By Theorem 2, we have

$$L(x) = \sum_i Tr((c_i x)^{2^{t\gamma - i\gamma}} + c_i^{2^{t\gamma}} x^{2^{i\gamma + t\gamma}}).$$

The degree of $L(x)$ is $2^{2t\gamma}$. From Lemma 6 $K(h)$ has at most 2^{2t} elements for $n \geq 2t$. So $k \leq 2t$ for even n and $k \leq 2t-1$ for odd n. For all $u \in F_{2^n}^*$, if n is an even, $W_{D_aG_\mu}(u) \leq 2^{(n+2t)/2}$, and $nl(D_aG_\mu) \geq 2^{n-1} - 2^{(n+2t-2)/2}$; if n is an odd, $W_{D_aG_\mu}(u) \leq 2^{(n+2t-1)/2}$, and $nl(D_aG_\mu) \geq 2^{n-1} - 2^{(n+2t-3)/2}$. Applying Corollary 1, we get,
if n is an even,

$$nl_2(G_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{(n+2t)/2} + 2^n} \approx 2^{n-1} - 2^{(3n+2t-4)/4};$$

if n is an odd,

$$nl_2(G_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{(n+2t-1)/2} + 2^n} \approx 2^{n-1} - 2^{(3n+2t-5)/4}.$$

□

If $m = 1$, $G_\mu(x)$ can be written as $Tr(\mu x^{2^{i\gamma}+2^{j\gamma}+1})$. By Theorem 5, $t = i$. Therefore, one can get the following corollary.

Corollary 5 *Suppose $G_\mu(x)$ be defined as $G_\mu(x) = Tr(\mu x^{2^{i\gamma}+2^{j\gamma}+1})$, where $\mu \in F_{2^n}^*$, $i > j$, $\gamma \neq 1$ and $gcd(n, \gamma) = 1$. Then for $n \geq 2i$,*
if n is an even,

$$nl_2(G_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{(n+2i)/2} + 2^n} \approx 2^{n-1} - 2^{(3n+2i-4)/4};$$

if n is an odd,

$$nl_2(G_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{(n+2i-1)/2} + 2^n} \approx 2^{n-1} - 2^{(3n+2i-5)/4}.$$

Proof: The first derivative D_aG_μ of $G_\mu(x)$ with respect to $a \in F_{2^n}^*$ is

$$\begin{aligned} D_aG_\mu(x) = Tr((\mu a)^{2^{-j\gamma}} x^{2^{(i-j)\gamma}} + \mu a^{2^{j\gamma}} x^{2^{i\gamma}+1} + \mu a^{2^{i\gamma}} x^{2^{j\gamma}+1} \\ + a^{(2^{j\gamma}+1)2^{-i\gamma}} x + a^{(2^{i\gamma}+1)2^{-j\gamma}} x + ax + a^{2^{i\gamma}+2^{j\gamma}+1}). \end{aligned}$$

Clearly, $n \neq (i\gamma + j\gamma)$ and $n \neq (2i\gamma - j\gamma)$. $G_\mu(x)$ satisfies the conditions of Theorem 1 (1) or (2), and $t = i$. So we have the Walsh spectrum of $D_aG_\mu(x)$ is equivalent to the Walsh spectrum of the following function,

$$h(x) = Tr((\mu a)^{2^{-j\gamma}} x^{2^{(i-j)\gamma}+1} + \mu a^{2^{j\gamma}} x^{2^{i\gamma}+1} + \mu a^{2^{i\gamma}} x^{2^{j\gamma}+1}).$$

If $n \geq 2i$, in the same way as Theorem 5 one can obtain
if n is an even,

$$nl_2(G_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{(n+2i)/2} + 2^n} \approx 2^{n-1} - 2^{(3n+2i-4)/4};$$

if n is an odd,

$$nl_2(G_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{(n+2i-1)/2} + 2^n} \approx 2^{n-1} - 2^{(3n+2i-5)/4}.$$

□

If $\gamma \neq 1$, $i = 2$ and $j = 1$, the function $G_\mu(x)$ of Corollary 5 has the same conclusions as the function $g_\mu(x)$ of Lemma 7.

It is well known that $nl(f) \geq nl_2(f)$ for any Boolean function f. So one can evaluated the nonlinearity of $F_\mu(x)$ and $G_\mu(x)$ by the lower bounds of their second order nonlinearity.

4 Conclusion

We have given a lower bound on the second order nonlinearity of a class of Boolean functions $F_\mu(x)$. For $gcd(n, \gamma) = 1$, the tighter lower bounds on the second order nonlinearity of a class of functions $G_\mu(x)$ are also given where $\gamma \neq 1$ is a positive integer. Our results show that the Boolean functions investigated here have large Hamming distance to the affine functions and quadratic functions when n is not too small. Therefore, these functions can resist the affine and quadratic function approximation attack.

Carlet [14] [15] have presented a relationship between algebraic immunity and the r-th order nonlinearity. For a cubic Boolean function, the algebraic immunity is at most 3. The lower bound on the second order nonlinearity of our cubic Boolean functions can not be obtained by the relationship in [14] [15].

5 Acknowledgments

This work was supported in part by 973 Project of China (No. 2007CB311201), the Notional Natural Science Foundation(No. 60833008, 60803149), and the Foundation of Guangxi Key Laboratory of Information and Communication(No. 20902).

References

1. G. Cohen, I. Honkala, S. Litsyn, A. Lobstein. Covering Codes. North-Holland, Amsterdam, The Netherlands, 1977.
2. G. Kabatiansky, C. Tavernier. List decoding of second order Reed-Muller codes. In 8th International Symposium of Communication theory and Applications, Ambleside, U. K. Jul. 2005.
3. I. Dumer, G. Kabatiansky, C. Tavernier. List decoding of second order Reed- Muller codes up to the Johnson bound with almost linear complexity. In Proc. IEEE Int. Symp. Information Theory In ISIT 2006, Seattle, WA, Jul. 2006 pp. 38-142.
4. R. Fourquet, C. Tavernier. List decoding of second order Reed-Muller codes and its covering radius implications. In WCC 2007, pp. 147-156.
5. C. Carlet. Recursive Lower Bounds on the Nonlinearity Profile of Boolean Functions and Their Applications. IEEE Trans.Information Theory, 54(3)(2008)1262-1272.
6. G. Sun,C. Wu. The lower bounds on the second order nonlinearity of three classes of Boolean functions with high nonlinearity. Information Sciences, 179(3)(2009)267-278.
7. S. Gangopadhyay, S. Sarkar, R. Telang. On the Lower Bounds of the Second Order Nonlinearity of some Boolean Functions. Information Sciences, 180(2)(2010)266-273.
8. Ruchi Gode, Sugata Gangopadhyay. On second order nonlinearities of cubic monomial Boolean functions. http://eprint.iacr.org/2009/502.pdf.
9. R. Lidl, H. Niederreiter. Finite fields. Cambridge, U.K: Combridge Univ. Press, 1983: 54-57, 107.
10. A. Canteaut, P. Charpin, G. M. Kyureghyan. A new class of monomial bent functions. Finite Fields and Their Applications, 14(2008)221-241.
11. V. S. Pless, W. C. Huffman. Handbook of coding theory. Elsevier, Amsterdam, 1998.
12. W. G. Solomn, G. Guang. Signal Design for Good Correlation for Wireless Communication, Cryptography, and Radar. Cambridge, New York: Cambridge Univ. Press, 2005: 42-45.
13. C. Bracken, E. Byrne, N. Markin and Gary McGuire, Determining the Nonlinearity of a New Family of APN Functions, Proc. AAECC, Lecture Notes in Computer Science 4851, Springer, Bangalore, India, 2007, pp. 72-79.
14. Carlet C. On the higher order nonlinearities of algebraic immune functions, in: Advances in Cryptology C CRYPTO 2006, LNCS 4117, Springer- Verlag, 2006, pp. 584-601.
15. Carlet C, Dalai D, Gupta K, Maitra S. Algebraic immunity for cryptographically significant Boolean functions: analysis and construction, IEEE Trans. Information Theory, 52(7)(2006) 3105-3121.