On second order nonlinearities of cubic monomial Boolean functions

Ruchi Gode and Sugata Gangopadhyay
Department of Mathematics
Indian Institute of Technology
Roorkee - 247 667 Uttarakhand INDIA
E-mail: gsugata@gmail.com

November 26, 2009

Abstract

We study cubic monomial Boolean functions of the form $Tr_1^n(\mu x^{2^i+2^j+1})$ where $\mu \in \mathbb{F}_{2^n}$. We prove that the functions of this form do not have any affine derivative if $n \neq i+j$ or $n \neq 2i-j$. Lower bounds on the second order nonlinearities of these functions are derived.

Keywords: Boolean functions, monomial functions, cubic functions, derivatives, second order nonlinearity.

1 Introduction

Suppose $\mathbb{F}_{2^n}$ is the extension field of degree n over $\mathbb{F}_2$, the prime field of characteristic 2. Any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables. The set of all n-variable Boolean functions is denoted by $\mathcal{B}_n$. Suppose $B = \{b_1, \ldots, b_n\}$ is a basis of $\mathbb{F}_{2^n}$. Then any $x \in \mathbb{F}_{2^n}$ can be written as

$$x = x_1 b_1 + \ldots + x_n b_n \text{ where } x_i \in \mathbb{F}_2, \text{ for all } i = 1, \ldots, n.$$

The n-tuple $(x_1, \ldots, x_n)$ is said to be the coordinates of $x \in \mathbb{F}_{2^n}$ with respect to the basis B. Once a basis B of $\mathbb{F}_{2^n}$ is fixed, any function $f \in \mathcal{B}_n$ can be written as a polynomial in $x_1, \ldots, x_n$ over $\mathbb{F}_2$, said to be the algebraic normal form (ANF)

$$f(x_1, x_2, \ldots, x_n) = \sum_{a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_a (\prod_{i=1}^{n} x_i^{a_i}), \text{ where } \mu_a \in \mathbb{F}_2.$$

Given the ANF of $f \in \mathcal{B}_n$, the value of f at a point $x \in \mathbb{F}_{2^n}$ is obtained by substituting in the ANF of f the coordinates of x with respect to B and evaluating the resulting summation modulo 2. The Hamming weight, or weight, of an n-tuple $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, denoted by $wt(x)$, is defined as $wt(x) = \sum_{i=1}^{n} x_i$, where the sum is over $\mathbb{Z}$, the ring of integers. Let m be a positive integer with binary representation $m = \sum_{i=0}^{l-1} m_i 2^i$ where $m_i \in \{0, 1\}$ for all $i = 0, \ldots, l-1$. The weight of m, $wt(m) := \sum_{i=0}^{l-1} m_i$, where the sum is taken over the ring of integers. The algebraic degree of f, $\deg(f) := \max\{wt(a) : \mu_a \neq 0, a \in \mathbb{F}_{2^n}\}$. For any two functions $f, g \in \mathcal{B}_n$, $d(f, g) = |\{x : f(x) \neq g(x), x \in \mathbb{F}_{2^n}\}|$ is said to be the Hamming distance between f and g. The trace function $Tr_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined by

$$Tr_1^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}, \text{ for all } x \in \mathbb{F}_{2^n}.$$

Given any $x, y \in \mathbb{F}_{2^n}$, $Tr_1^n(xy)$ is an inner product of x and y. For any $\lambda \in \mathbb{F}_{2^n}$, $\phi_\lambda \in \mathcal{B}_n$ denotes the linear function defined by $\phi_\lambda(x) = Tr_1^n(\lambda x)$ for all $x \in \mathbb{F}_{2^n}$. A Boolean function $f \in \mathcal{B}_n$ is said to be a monomial Boolean function if there exits $\lambda \in \mathbb{F}_{2^n}$ and a positive integer d such that $f(x) = Tr_1^n(\lambda x^d)$ for all $x \in \mathbb{F}_{2^n}$. The positive integer d is said to be the exponent defining the function f, whereas $\deg(f) = wt(d)$. The Walsh transform of $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_{2^n}$ is defined by

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + Tr_1^n(\lambda x)}.$$

The multiset $[W_f(\lambda) : \lambda \in \mathbb{F}_{2^n}]$ is said to be the Walsh spectrum of f. Two Boolean functions $f, g \in \mathcal{B}_n$ are said to be affine equivalent if there exists $A \in GL(n, \mathbb{F}_2)$, that is the group of invertible $n \times n$ matrices over $\mathbb{F}_2$, $b, \lambda \in \mathbb{F}_{2^n}$ and $\epsilon \in \mathbb{F}_2$ such that

$$g(x) = f(Ax + b) + \phi_\lambda(x) + \epsilon, \text{ for all } x \in \mathbb{F}_{2^n}.$$

The set of all Boolean functions of n variables of degree at most r is said to be the Reed-Muller code, $RM(r, n)$, of length 2^n and order r.

Definition 1 *Suppose $f \in \mathcal{B}_n$. For every integer r, $0 < r \leq n$, the minimum of the Hamming distances of f from all the functions belonging to $RM(r, n)$ is said to be the rth-order nonlinearity of the Boolean function f. 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 idea of first-order nonlinearity, usually referred to as nonlinearity, was introduced by Rothaus [33]. The relationship between nonlinearity and explicit attack on symmetric ciphers was discovered by Matsui [29]. For results on constructions of Boolean functions with high nonlinearity we refer to [6, 7, 1, 22, 23, 31, 32, 33, 34]. Following is the relationship between Nonlinearity and Walsh spectrum of $f \in \mathcal{B}_n$:

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_{2^n}} |W_f(\lambda)|.$$

By Parseval's identity

$$\sum_{\lambda \in \mathbb{F}_{2^n}} W_f(\lambda)^2 = 2^{2n}$$

it can be shown that $|W_f(\lambda)| \geq 2^{n/2}$ which implies that $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. Thus, the nonlinearity of $f \in \mathcal{B}_n$ is bounded above by $2^{n-1} - 2^{\frac{n}{2}-1}$.

Definition 2 *Suppose n is an even integer. A function $f \in \mathcal{B}_n$ is said to be a bent function if and only if $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ (i.e., $W_f(\lambda) \in \{2^{\frac{n}{2}}, -2^{\frac{n}{2}}\}$ for all $\lambda \in \mathbb{F}_{2^n}$).*

For odd $n \geq 9$, the tight upper bound of nonlinearities of Boolean functions in $\mathcal{B}_n$ is not known.

The idea of higher order nonlinearity has been used in cryptanalysis by Courtois, Golic, Iwata-Kurosawa, Knudsen-Robshaw, Maurer, and Millan [11, 18, 19, 24, 28, 30]. Thus there is a need to construct Boolean functions with controlled nonlinearity profile. Algorithms to compute higher order nonlinearities of Boolean functions are found in [15, 16, 20]. However these algorithms can compute second order nonlinearities for $n \leq 11$ and for $n \leq 13$ for some special cases. Thus there is a need to find out lower bounds of the second order nonlinearity of Boolean functions and in general lower bounds for r-th order nonlinearity of Boolean functions (for $r \geq 1$) which is satisfied for all values of n. A systematic study of higher order nonlinearity and nonlinearity profile of a Boolean functions along with development of techniques to obtain bounds of these characteristics for several classes of Boolean functions is initiated by Carlet [5, 9]. We also refer to results due to Carlet-Mesnager [8], and Sun-Wu [35]. The best known asymptotic upper bound on $nl_r(f)$ is obtained by Carlet and Mesnager [8], which is

$$nl_r(f) = 2^{n-1} - \frac{\sqrt{15}}{2} \cdot (1+\sqrt{2})^{r-2} \cdot 2^{\frac{n}{2}} + O(n^{r-2}).$$

In [9], Carlet deduced the lower bounds of the second order nonlinearity of several classes of monomial Boolean functions, such as the Welch function $f(x) = Tr_1^n(x^{2^t+3})$, when $t = n-1$ and n odd, or when $t = n+1$ and n odd, and the inverse function $f(x) = Tr_1^n(x^{2^n-2})$. Sun and Wu [35] and Gangopadhyay, Sarkar and Telang [17] recently have obtained the lower bounds of the second order nonlinearity of several classes of cubic monomial Boolean functions. In this paper we study cubic monomial Boolean functions of the form $Tr_1^n(\mu x^{2^i+2^j+1})$ where $\mu \in \mathbb{F}_{2^n}$. We prove that the functions of this form do not have any affine derivative if $n \neq i+j$ or $n \neq 2i-j$. Lower bounds on the second order nonlinearities of these functions are derived.

2 Preliminary results

2.1 Recursive lower bounds of higher-order nonlinearities

Following are some of the results proved by Carlet [9].

Definition 3 *The derivative of $f \in \mathcal{B}_n$ with respect to $a \in \mathbb{F}_{2^n}$, denoted by $D_a f$, is defined as $D_a f(x) = f(x) + f(x+a)$ for all $x \in \mathbb{F}_{2^n}$.*

The higher-order derivatives are defined as follows.

Definition 4 *Let V be an m-dimensional subspace of $\mathbb{F}_{2^n}$ generated by $a_1, \ldots, a_m$, i.e., $V = \langle a_1, \ldots, a_m \rangle$. The mth-order derivative of $f \in \mathcal{B}_n$ with respect to V, denoted by $D_V f$ or $D_{a_1} \ldots D_{a_m} f$, is defined by*

$$D_V f(x) = D_{a_1} \ldots D_{a_m} f(x) \text{ for all } x \in \mathbb{F}_{2^n}.$$

It is to be noted that the mth-order derivative of f depends only on the choice of the m-dimensional subspace V and independent of the choice of the basis of V.

Proposition 1 ([9], Proposition 2) *Let $f(x)$ be any n-variable Boolean function and r a positive integer smaller than n, i a non-negative integer smaller than r. Then*

$$nl_r(f) \geq \frac{1}{2^i} \max_{a_1, a_2, \ldots a_i \in \mathbb{F}_{2^n}} nl_{r-i}(D_{a_1} D_{a_2} \ldots D_{a_i} f).$$

In particular, for $r = 2$,

$$nl_2(f) \geq \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}} nl(D_a f).$$

If some lower bound on $nl(D_a f)$ is known for all a, then we have the following corollary.

Corollary 1 ([9], Corollary 2) *Let f be any n-variable function and r a positive integer smaller than n. Assume that, for some nonnegative integers M and m, we have $nl_{r-1}(D_a f) \geq 2^{n-1} - M2^m$ for every nonzero $a \in \mathbb{F}_{2^n}$. Then*

$$\begin{aligned} nl_r(f) &\geq 2^{n-1} - \tfrac{1}{2}\sqrt{(2^n - 1)M2^{m+1} + 2^n} \\ &\approx 2^{n-1} - \sqrt{M}2^{\frac{n+m-1}{2}}. \end{aligned}$$

The Propositions 1 and Corollary 1 are applicable for computation of the lower bounds of the second order nonlinearities of cubic Boolean functions. This is due to the fact that any first derivative of a cubic Boolean function has algebraic degree at most 2 and the Walsh spectrum of a quadratic Boolean function (degree 2 Boolean function) is completely characterized by the dimension of the kernel of the bilinear form associated with it.

2.2 Quadratic Boolean functions

Suppose $f \in \mathcal{B}_n$ is a quadratic function. The bilinear form associated with f is defined by $B(x, y) = f(0) + f(x) + f(y) + f(x + y)$. The kernel [4, 27] of $B(x, y)$ is the subspace of $\mathbb{F}_{2^n}$ defined by

$$\mathcal{E}_f = \{x \in \mathbb{F}_{2^n} : B(x, y) = 0 \text{ for all } y \in \mathbb{F}_{2^n}\}.$$

Lemma 1 ([4], Proposition 1) *Let V be a vector space over a field $\mathbb{F}_q$ of characteristic 2 and $Q : V \longrightarrow \mathbb{F}_q$ be a quadratic form. Then the dimension of V and the dimension of the kernel of Q have the same parity.*

Lemma 2 ([4], Lemma 1) *Let f be any quadratic Boolean function. The kernel, $\mathcal{E}_f$, is the subspace of $\mathbb{F}_{2^n}$ consisting of those a such that the derivative $D_a f$ is constant. That is,*

$$\mathcal{E}_f = \{a \in \mathbb{F}_{2^n} : D_a f = \text{ constant } \}.$$

The Walsh spectrum of any quadratic function $f \in \mathcal{B}_n$ is given below.

Lemma 3 ([4, 27]) *If $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is a quadratic Boolean function and $B(x, y)$ is the quadratic form associated with it, then the Walsh Spectrum of f depends only on the dimension, k, of the kernel, $\mathcal{E}_f$, of $B(x, y)$. The weight distribution of the Walsh spectrum of f is:*

$W_f(\alpha)$	*number of* α
0	$2^n - 2^{n-k}$
$2^{(n+k)/2}$	$2^{n-k-1} + (-1)^{f(0)} 2^{(n-k-2)/2}$
$-2^{(n+k)/2}$	$2^{n-k-1} - (-1)^{f(0)} 2^{(n-k-2)/2}$

2.3 Linearized polynomials

Suppose q denotes a prime power.

Definition 5 ([26]) *A polynomial of the form*

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$$

with the coefficients in an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ is said to be a linearized polynomial (q-polynomial) over $\mathbb{F}_{q^m}$.

Below we list some properties of linearized polynomials and its zeroes [26].

1. The zeroes of $L(x)$ lie in some extension field $\mathbb{F}_{q^s}$ of $\mathbb{F}_{q^m}$ for some $s \geq m$. The zeroes form a $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^s}$.

2. Each zero of $L(x)$ has the same multicipility which is either 1 or a power of q.

3. Suppose $L(x)$ be a linearized polynomial over $\mathbb{F}_{q^m}$ and $F = \mathbb{F}_{q^s}$ is an extension field of $\mathbb{F}_{q^m}$. The map $L : \beta \in F \mapsto L(\beta) \in F$ is an $\mathbb{F}_q$-linear operator on F.

The following lemma is useful in our proofs.

Lemma 4 ([2]) *Let $g(x) = \sum_{i=0}^{v} r_i x^{2^{si}}$ be a linearized polynomial over $\mathbb{F}_{2^n}$, where $\gcd(n, s) = 1$. Then the equation $g(x) = 0$ has at most 2^v solutions in $\mathbb{F}_{2^n}$.*

3 Cubic monomial Boolean functions

The function $f_\mu \in \mathcal{B}_n$ given by

$$f_\mu(x) = Tr_1^n(\mu x^{2^i+2^j+1})$$

where $\mu \in \mathbb{F}_{2^n}$ and i, j are positive integers such that $i > j$, is a cubic monomial Boolean function.

Theorem 1 *Suppose $\phi_\mu \in \mathcal{B}_n$ defined as $\phi_\mu(x) = Tr_1^n(\mu x^{2^r+2^s+2^t})$, where r, s, t are integers such that $r > s > t \geq 0$ and $r - t = i, s - t = j$. Then ϕ_μ and f_μ are affinely equivalent Boolean functions.*

Proof : The functions $\phi_\mu(x) = Tr_1^n(\mu x^{2^r+2^s+2^t}) = Tr_1^n(\mu x^{2^t(2^{r-t}+2^{s-t}+1)})$. Since the mapping $T : x \to x^{2^{n-t}}$ is a linear transformation from $\mathbb{F}_{2^n}$ to itself. It follows that $\phi_\mu(x)$ and $\phi_\mu(T(x)) = \phi_\mu(x^{2^{n-t}})$ are affinely equivalent functions. Now,

$$\begin{aligned}
\phi_\mu(T(x)) &= \phi_\mu(x^{2^{n-t}}) \\
&= Tr_1^n(\mu(x^{2^{n-t}})^{2^t(2^{r-t}+2^{s-t}+1)}) = Tr_1^n(\mu x^{2^{n-t+t}(2^{r-t}+2^{s-t}+1)}) \\
&= Tr_1^n(\mu x^{2^{r-t}+2^{s-t}+1}) \\
&= f_\mu(x).
\end{aligned}$$

Therefore, f_μ and ϕ_μ are affinely equivalent Boolean functions. ■

Theorem 2 *The function f_μ posses no affine derivative if $n \neq i + j$ or $n \neq 2i - j$, where $i > j$.*

Proof : Derivative, $D_a f_\mu$, of f_μ with respect to $a \in \mathbb{F}_{2^n}^*$ is

$$\begin{aligned}
D_a f_\mu(x) &= f_\mu(x + a) + f_\mu(x) \\
&= Tr_1^n(\mu(x + a)^{2^i+2^j+1}) + Tr_1^n(\mu x^{2^i+2^j+1}) \\
&= Tr_1^n(\mu(x^{2^i+2^j} a + x^{2^i+1} a^{2^j} + x^{2^j+1} a^{2^i} + x^{2^i} a^{2^j+1} \\
&\quad + x^{2^j} a^{2^i+1} + x a^{2^i+2^j} + a^{2^i+2^j+1})).
\end{aligned}$$

The degree two part of the above equation is $Tr_1^n(\mu a x^{2^i+2^j}) + Tr_1^n(\mu a^{2^j} x^{1+2^i}) + Tr_1^n(\mu a^{2^i} x^{1+2^j})$. If $n \neq 2i - j$ then $2^i + 2^j$ and $2^i + 1$ are not in the same cyclotomic coset. If $n \neq i + j$ then $2^i + 1$ and $2^j + 1$ are not in the same cyclotomic coset. Therefore if either of the above two conditions are satisfied then the derivative $D_a f_\mu$ is not affine for any value of $a \neq 0$ and $\mu \neq 0$. ■

Theorem 3 *The lower bound of the second order nonlinearity of f_μ for $n > 2i$ is given as*

$$nl_2(f_\mu) \geq \begin{cases} 2^{n-1} - 2^{\frac{3n+2i-4}{4}}, & \text{if } n \equiv 0 \mod 2, \\ 2^{n-1} - 2^{\frac{3n+2i-5}{4}}, & \text{if } n \equiv 1 \mod 2. \end{cases}$$

Proof : Derivative, $D_a f_\mu$, of f_μ with respect to $a \in \mathbb{F}_{2^n}^*$ is

$$\begin{aligned} D_a f_\mu(x) &= f_\mu(x+a) + f_\mu(x) \\ &= Tr_1^n(\mu(x+a)^{2^i+2^j+1}) + Tr_1^n(\mu x^{2^i+2^j+1}) \\ &= Tr_1^n(\mu(x^{2^i+2^j}a + x^{2^i+1}a^{2^j} + x^{2^j+1}a^{2^i} + x^{2^i}a^{2^j+1} \\ &\quad + x^{2^j}a^{2^i+1} + xa^{2^i+2^j} + a^{2^i+2^j+1})). \end{aligned}$$

It is known from Theorem 2 that $D_a f_\mu$ is quadratic for all $a \in \mathbb{F}_{2^n}^*$ as $n > 2i$. Walsh spectrum of $D_a f_\mu$ is equivalent to the Walsh spectrum of following function

$$h_\mu(x) = Tr_1^n(\mu(x^{2^i+2^j}a + x^{2^i+1}a^{2^j} + x^{2^j+1}a^{2^i})).$$

Let $B(x,y)$ be the bilinear form associated with h_μ, $\mathcal{E}_f$ the kernel of $B(x,y)$, defined as

$$\mathcal{E}_f = \{x \in \mathbb{F}_{2^n} : B(x,y) = 0 \text{ for all } y \in \mathbb{F}_{2^n}\},$$

where

$$\begin{aligned} B(x,y) &= h_\mu(0) + h_\mu(x) + h_\mu(y) + h_\mu(x+y) \\ &= Tr_1^n(\mu(x^{2^i+2^j}a + x^{2^i+1}a^{2^j} + x^{2^j+1}a^{2^i})) \\ &\quad + Tr_1^n(\mu(y^{2^i+2^j}a + y^{2^i+1}a^{2^j} + y^{2^j+1}a^{2^i})) \\ &\quad + Tr_1^n(\mu((x+y)^{2^i+2^j}a + (x+y)^{2^i+1}a^{2^j} + (x+y)^{2^j+1}a^{2^i})) \\ &= Tr_1^n(\mu((xa^{2^j} + x^{2^j}a)y^{2^i} + (xa^{2^i} + x^{2^i}a)y^{2^j} + (x^{2^i}a^{2^j} + x^{2^j}a^{2^i})y)) \\ &= Tr_1^n(\mu(xa^{2^j} + x^{2^j}a)y^{2^i}) + Tr_1^n(\mu(xa^{2^i} + x^{2^i}a)y^{2^j}) \\ &\quad + Tr_1^n(\mu(x^{2^i}a^{2^j} + x^{2^j}a^{2^i})y) \\ &= Tr_1^n(\mu(xa^{2^j} + x^{2^j}a)y^{2^i})^{2^{n-i}} + Tr_1^n(\mu(xa^{2^i} + x^{2^i}a)y^{2^j})^{2^{n-j}} \\ &\quad + Tr_1^n(\mu(x^{2^i}a^{2^j} + x^{2^j}a^{2^i})y) \\ &= Tr_1^n(\mu^{2^{n-i}}(x^{2^{n-i}}a^{2^{n-i+j}} + x^{2^{n-i+j}}a^{2^{n-i}})y^{2^n}) \\ &\quad + Tr_1^n(\mu^{2^{n-j}}(x^{2^{n-j}}a^{2^{n+i-j}} + x^{2^{n+i-j}}a^{2^{n-j}})y^{2^n}) \\ &\quad + Tr_1^n(\mu(x^{2^i}a^{2^j} + x^{2^j}a^{2^i})y) \\ &= Tr_1^n(y(x^{2^i}a^{2^j}\mu + x^{2^j}a^{2^i}\mu + x^{2^{i-j}}a^{2^{-j}}\mu^{2^{-j}} + x^{2^{-j}}a^{2^{i-j}}\mu^{2^{-j}} \\ &\quad + x^{2^{-i}}a^{2^{j-i}}\mu^{2^{-i}} + x^{2^{j-i}}a^{2^{-i}}\mu^{2^{-i}})) \\ &= Tr_1^n(yP_{(\mu,a)}(x)). \end{aligned}$$

Therefore,

$$\mathcal{E}_f \quad = \quad \{x \in \mathbb{F}_{2^n} : P_{(\mu,a)}(x) = 0\}.$$

The number of elements in the kernel $\mathcal{E}_f$ is equal to the number of zeroes of $P_{(\mu,a)}(x)$, or equivalently to the number of zeroes of $(P_{(\mu,a)}(x))^{2^i}$. Let $(P_{(\mu,a)}(x))^{2^i} = L_{(\mu,a)}(x)$.

Thus,

$$\begin{aligned}
L_{(\mu,a)}(x) &= (x^{2^i}a^{2^j}\mu + x^{2^j}a^{2^i}\mu + x^{2^{i-j}}a^{2^{-j}}\mu^{2^{-j}} \\
&\quad x^{2^{-j}}a^{2^{i-j}}\mu^{2^{-j}} + x^{2^{j-i}}a^{2^{-i}}\mu^{2^{-i}} + x^{2^{-i}}a^{2^{j-i}}\mu^{2^{-i}})^{2^i} \\
&= x^{2^{2i}}a^{2^{i+j}}\mu^{2^i} + x^{2^{i+j}}a^{2^{2i}}\mu^{2^i} + x^{2^{2i-j}}a^{2^{i-j}}\mu^{2^{i-j}} \\
&\quad + x^{2^{i-j}}a^{2^{2i-j}}\mu^{2^{i-j}} + x^{2^j}a\mu + xa^{2^j}\mu.
\end{aligned}$$

$L_{(\mu,a)}(x)$ is a linearized polynomial in x and $\deg(L_{(\mu,a)}(x)) \leq 2^{2i}$.
Let k the dimension of $\mathcal{E}_g$. By Lemma 1, $k \leq 2i$ for n even and $k \leq 2i-1$ for n odd. These upper bounds of k are non-trivial as $n > 2i$. Thus, for all $\lambda \in \mathbb{F}_{2^n}$

$$W_{D_af_\mu}(\lambda) \leq \begin{cases} 2^{\frac{n+2i}{2}}, & \text{if } n \equiv 0 \mod 2, \\ 2^{\frac{n+2i-1}{2}}, & \text{if } n \equiv 1 \mod 2. \end{cases}$$

Since

$$nl(D_af_\mu) = 2^{n-1} - \frac{1}{2}\max_{\lambda \in \mathbb{F}_{2^n}} |W_{D_af_\mu}(\lambda)|,$$

We obtain

$$nl(D_af_\mu) \geq \begin{cases} 2^{n-1} - \frac{1}{2}2^{\frac{n+2i}{2}}, & \text{if } n \equiv 0 \mod 2, \\ 2^{n-1} - \frac{1}{2}2^{\frac{n+2i-1}{2}}, & \text{if } n \equiv 1 \mod 2 \end{cases} \tag{1}$$

for all $a \in \mathbb{F}_{2^n}^*$.
Comparing the inequality (1) and Corollary 1, we get

$$\begin{cases} M = 1 \text{ and } m = \frac{n+2i-2}{2}, & \text{if } n \equiv 0 \mod 2, \\ M = 1 \text{ and } m = \frac{n+2i-3}{2}, & \text{if } n \equiv 1 \mod 2. \end{cases}$$

So Corollary 1 gives,

- For even n

$$\begin{aligned} nl_2(f_\mu) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{\frac{n+2i}{2}} + 2^n} \\ &\approx 2^{n-1} - 2^{\frac{3n+2i-4}{4}}. \end{aligned} \tag{2}$$

- For odd n

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

■

Theorem 4 *Suppose g_μ be defined as*

$$g_\mu(x) = Tr_1^n(\mu x^{2^{2i}+2^i+1})$$

where $\mu \in \mathbb{F}_{2^n}$ and i a positive integer such that $gcd(n,i)=1$. Then for $n>4$

$$nl_2(g_\mu) \geq \begin{cases} 2^{n-1} - 2^{\frac{3n}{4}}, & \text{if } n \equiv 0 \mod 2, \\ 2^{n-1} - 2^{\frac{3n-1}{4}}, & \text{if } n \equiv 1 \mod 2. \end{cases}$$

Proof : Derivative, $D_a g_\mu$, of g_μ with respect to $a \in \mathbb{F}_{2^n}^*$ is

$$\begin{aligned} D_a g_\mu(x) &= g_\mu(x+a) + g_\mu(x) \\ &= Tr_1^n(\mu(x+a)^{2^{2i}+2^i+1}) + Tr_1^n(\mu x^{2^{2i}+2^i+1}) \\ &= Tr_1^n(\mu(x^{2^{2i}+2^i}a + x^{2^{2i}+1}a^{2^i} + x^{2^i+1}a^{2^{2i}} + x^{2^{2i}}a^{2^i+1} \\ &\quad + x^{2^i}a^{2^{2i}+1} + xa^{2^{2i}+2^i} + a^{2^{2i}+2^i+1})). \end{aligned}$$

$D_a g_\mu$ is quadratic for all $a \in \mathbb{F}_{2^n}^*$ if $n \neq 3i$, from the conditions stated in this Theorem we observe that $D_a g_\mu$ is always quadratic.
Walsh spectrum of $D_a g_\mu$ is equivalent to the Walsh spectrum of following function

$$h_\mu(x) = Tr_1^n(\mu(x^{2^{2i}+2^i}a + x^{2^{2i}+1}a^{2^i} + x^{2^i+1}a^{2^{2i}})).$$

Let $B(x,y)$ be the bilinear form associated with h_μ, $\mathcal{E}_g$ the kernel of $B(x,y)$ and k the dimension of $\mathcal{E}_g$.

$$\mathcal{E}_g = \{x \in \mathbb{F}_{2^n} : B(x,y) = 0 \text{ for all } y \in \mathbb{F}_{2^n}\}.$$

$$\begin{aligned} B(x,y) &= h_\mu(0) + h_\mu(x) + h_\mu(y) + h_\mu(x+y) \\ &= Tr_1^n(\mu(x^{2^{2i}+2^i}a + x^{2^{2i}+1}a^{2^i} + x^{2^i+1}a^{2^{2i}})) \\ &\quad + Tr_1^n(\mu(y^{2^{2i}+2^i}a + y^{2^{2i}+1}a^{2^i} + y^{2^i+1}a^{2^{2i}})) \\ &\quad + Tr_1^n(\mu((x+y)^{2^{2i}+2^i}a + (x+y)^{2^{2i}+1}a^{2^i} + (x+y)^{2^i+1}a^{2^{2i}})) \\ &= Tr_1^n(\mu((xa^{2^i} + x^{2^i}a)y^{2^{2i}} + (xa^{2^{2i}} + x^{2^{2i}}a)y^{2^i} \\ &\quad + (x^{2^{2i}}a^{2^i} + x^{2^i}a^{2^{2i}})y)) \\ &= Tr_1^n(\mu(xa^{2^i} + x^{2^i}a)y^{2^{2i}})^{2^{n-2i}} + Tr_1^n(\mu(xa^{2^{2i}} + x^{2^{2i}}a)y^{2^i})^{2^{n-i}} \\ &\quad + Tr_1^n(\mu(x^{2^{2i}}a^{2^i} + x^{2^i}a^{2^{2i}})y) \\ &= Tr_1^n(\mu^{2^{n-2i}}(x^{2^{n-2i}}a^{2^{n-i}} + x^{2^{n-i}}a^{2^{n-2i}})y^{2^n}) \\ &\quad + Tr_1^n(\mu^{2^{n-i}}(x^{2^{n-i}}a^{2^{n+i}} + x^{2^{n+i}}a^{2^{n-i}})y^{2^n}) \\ &\quad + Tr_1^n(\mu(x^{2^{2i}}a^{2^i} + x^{2^i}a^{2^{2i}})y) \\ &= Tr_1^n(y(x^{2^{2i}}a^{2^i}\mu + x^{2^i}(a^{2^{2i}}\mu + a^{2^{-i}}\mu^{2^{-i}}) \\ &\quad + x^{2^{-i}}(a^{2^i}\mu^{2^{-i}} + a^{2^{-2i}}\mu^{2^{-2i}}) + x^{2^{-2i}}a^{2^{-i}}\mu^{2^{-2i}})). \end{aligned}$$

Therefore

$$\mathcal{E}_g = \{x \in \mathbb{F}_{2^n} : P_{(\mu,a)}(x) = 0\}.$$

The number of elements in the kernel $\mathcal{E}_g$ is equal to the number of zeroes of $(P_{(\mu,a)}(x))$ or we can say to the number of zeroes of $(P_{(\mu,a)}(x))^{2^{2i}}$. Let us denote $(P_{(\mu,a)}(x))^{2^{2i}}$ by $L_{(\mu,a)}(x)$. Thus,

$$\begin{aligned} L_{(\mu,a)}(x) &= (x^{2^{2i}} a^{2^i} \mu + x^{2^i} (a^{2^{2i}} \mu + a^{2^{-i}} \mu^{2^{-i}}) \\ &\quad + x^{2^{-i}} (a^{2^i} \mu^{2^{-i}} + a^{2^{-2i}} \mu^{2^{-2i}}) + x^{2^{-2i}} a^{2^{-i}} \mu^{2^{-2i}})^{2^{2i}} \\ &= x^{2^{4i}} a^{2^{3i}} \mu^{2^{2i}} + x^{2^{3i}} (a^{2^{4i}} \mu^{2^{2i}} + a^{2^i} \mu^{2^i}) \\ &\quad + x^{2^i} (a^{2^{3i}} \mu^{2^i} + a\mu) + x a^{2^i} \mu. \end{aligned}$$

Clearly the maximum degree of $L_{(\mu,a)}(x)$ considered as a linearized polynomial in x is 2^{4i}. By Lemma 4 we get that $L_{(\mu,a)}(x)$ can have at most 2^4 zeroes in $\mathbb{F}_{2^n}$. So $k \leq 4$ for even n and $k \leq 3$ for odd n . Thus, for all $\lambda \in \mathbb{F}_{2^n}$

$$W_{D_a g_\mu}(\lambda) \leq \begin{cases} 2^{\frac{n+4}{2}}, & \text{if } n \equiv 0 \mod 2, \\ 2^{\frac{n+3}{2}}, & \text{if } n \equiv 1 \mod 2. \end{cases}$$

So for all $a \in \mathbb{F}_{2^n}^*$

$$nl(D_a g_\mu) \geq \begin{cases} 2^{n-1} - \frac{1}{2} 2^{\frac{n+4}{2}}, & \text{if } n \equiv 0 \mod 2, \\ 2^{n-1} - \frac{1}{2} 2^{\frac{n+3}{2}}, & \text{if } n \equiv 1 \mod 2. \end{cases} \tag{4}$$

Comparing the inequality (4) and Corollary 1, we obtain

$$\begin{cases} M = 1 \text{ and } m = \frac{n+2}{2}, & \text{if } n \equiv 0 \mod 2, \\ M = 1 \text{ and } m = \frac{n+1}{2}, & \text{if } n \equiv 1 \mod 2. \end{cases}$$

By Corollary 1,

- For even n

$$\begin{aligned} nl_2(g_\mu) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1) 2^{\frac{n+4}{2}} + 2^n} \\ &\approx 2^{n-1} - 2^{\frac{3n}{4}}. \end{aligned} \tag{5}$$

- For odd n

$$\begin{aligned} nl_2(g_\mu) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1) 2^{\frac{n+3}{2}} + 2^n} \\ &\approx 2^{n-1} - 2^{\frac{3n-1}{4}}. \end{aligned} \tag{6}$$

■

4 Comparisons

- It is proved in [9] that, in general, the second order nonlinearities of n-variable cubic Boolean functions which do not have any affine derivative is bounded below by $2^{n-1} - 2^{n-\frac{3}{2}}$. Substracting this bound from those deduced in inequalities (2) and (3) respectively, we obtain

$$\begin{cases} 2^{n-\frac{3}{2}}(1 - 2^{\frac{-n+2i+2}{4}}) > 0, & \text{if } n \text{ is even and } n > 2i+2, \\ 2^{n-\frac{3}{2}}(1 - 2^{\frac{-n+2i+1}{4}}) > 0, & \text{if } n \text{ is odd and } n > 2i+1. \end{cases}$$

- Again substracting the general lower bound $2^{n-1} - 2^{n-\frac{3}{2}}$ given in [9] from the lower bounds obtained in inequalities (5) and (6) respectively, we get

$$\begin{cases} 2^{\frac{3n}{4}}(2^{\frac{n-6}{4}} - 1) > 0, & \text{if } n \text{ is even and } n > 6, \\ 2^{\frac{3n}{4}}(2^{\frac{n-5}{4}} - 1) > 0, & \text{if } n \text{ is odd and } n > 5. \end{cases}$$

Therefore the bounds deduced in this paper are larger than those obtained in [9] when n is not too small.

In the following tables we indicate for $5 \le n \le 20$ the values of lower bounds given by Theorem 3 and Theorem 4, compared with the values of general bound obtained in [9] for cubic functions which have no affine derivative.

For n odd

The values of the lower bound by Theorem 3

	$n=5$	$n=7$	$n=9$	$n=11$	$n=13$	$n=15$	$n=17$	$n=19$
$i=2$	5	32	166	768	3372	14336	59744	245760
$i=3$	0	19	128	662	3072	13488	57344	238974
$i=4$	–	0	75	512	2648	12288	53951	229376
$i=5$	–	–	0	300	2048	10592	49152	215803
$i=6$	–	–	–	0	1200	8192	42366	196608
$i=7$	–	–	–	–	0	4799	32768	169462
$i=8$	–	–	–	–	–	0	19195	131072
$i=9$	–	–	–	–	–	–	0	76781

	$n=5$	$n=7$	$n=9$	$n=11$	$n=13$	$n=15$	$n=17$	$n=19$
Theorem 4	5	32	166	768	3372	14336	59744	245760
Carlet [9]	5	19	75	300	1200	4799	19195	76781

<u>For n even</u>
The values of the lower bound by Theorem 3

	$n=6$	$n=8$	$n=10$	$n=12$	$n=14$	$n=16$	$n=18$	$n=20$
$i=2$	10	64	331	1536	6744	28672	119487	491520
$i=3$	0	38	256	1324	6144	26976	114688	477947
$i=4$	−	0	150	1024	5296	24576	107902	458752
$i=5$	−	−	0	600	4096	21183	98304	431606
$i=6$	−	−	−	0	2400	16384	84731	393216
$i=7$	−	−	−	−	0	9598	65536	338925
$i=8$	−	−	−	−	−	0	38390	262144
$i=9$	−	−	−	−	−	−	0	153560

	$n=6$	$n=8$	$n=10$	$n=12$	$n=14$	$n=16$	$n=18$	$n=20$
Theorem 4	10	64	331	1536	6744	28672	119487	491520
Carlet [9]	10	38	150	600	2400	9598	38390	153560

It is to be noted that for values of n smaller than $2i$ the bound of Theorem 3 gives negative numbers.

5 Conclusion

In this paper we deduced lower bounds on the second order nonlinearity of a subclass of cubic monomial Boolean functions which have no affine derivative. Our bounds are better than previously known general bound when n is not too small. Our results give the information about the choice of i such that the functions of form $Tr_1^n(\mu x^{2^i+2^j+1})$ show good behaviour with respect to second order nonlinearity. We expect that these results will be useful in chosing cryptographically significant Boolean functions. It leaves an open problem to identify more classes of Boolean functions and investigate their second order nonlinearities.

References

[1] E. R. Berlekamp and L. R. Welch, Weight distributions of the cosets of the $(32, 6)$ Reed-Muller code, IEEE Trans. Inform. Theory 18 (1) (1972) 203-207.

[2] C. Bracken, E. Byrne, N. Markin and Gary McGuire, Determining the Nonlinearity of a New Family of APN Functions, Proc. AAECC, LNCS, vol. 4851, Springer, Bangalore, India, 2007, pp. 72-79.

[3] A. Canteaut and P. Charpin, Decomposing bent functions, IEEE Trans. Inform. Theory 49 (8) (2003) 2004-2019.

[4] A. Canteaut, P. Charpin and G. M. Kyureghyan, A new class of monomial bent functions, Finite Fields and their Applications 14 (2008) 221-241.

[5] C. Carlet, The complexity of Boolean functions from cryptographic viewpoint, in: Dagstuhl Seminar Complexity of Boolean Functions, 2006, 15 pp.

[6] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, in Boolean Methods and Models, Y. Crama and P. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press [Online]. Available: http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html l, to be published.

[7] C. Carlet, Vectorial (Multi-Output) Boolean Functions for Cryptography, in Boolean Methods and Models, Y. Crama and P. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press [Online]. Available: http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.htm, to be published.

[8] C. Carlet and S. Mesnager, Improving the upper bounds on the covering radii of binary Reed-Muller codes, IEEE Trans. Inform. Theory 53 (1) (2007) 162-173.

[9] C. Carlet, Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications, IEEE Trans. Inform. Theory 54 (3) (2008) 1262-1272.

[10] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, Covering Codes, North-Holland, 1997.

[11] N. Courtois, Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt, in: Proceedings of the ICISC'02, LNCS, vol. 2587, Springer, 2002, pp. 182-199.

[12] J. F. Dillon, H. Dobbertin, New Cyclic Difference Sets with Singer Parameters, Finite Fields And Applications (2004) 342-389.

[13] H. Dobbertin, Another proof of Kasami's Theorem, Des. Codes Cryptography 17 (1999) 177-180.

[14] H. Dobbertin, Almost Perfect Nonlinear Power Functions on $GF(2)^n$: the Niho case, Inform. Comput. 151 (1999) 57-72.

[15] I. Dumer, G. Kabatiansky and C. Tavernier, List decoding of second order Reed-Muller codes up to the Johnson bound with almost linear complexity, in: Proceedings of the IEEE International Symposium on Information Theory, Seattle, WA, July 2006, pp. 138-142.

[16] R. Fourquet and C. Tavernier, An improved list decoding algorithm for the second order ReedMuller codes and its applications, Designs Codes and Cryptography 49 (2008) 323-340.

[17] S. Gangopadhyay, S. Sarkar and R. Telang, On the lower bounds of the second order nonlinearities of some Boolean functions, Information Sciences 180 (2010) 266273.

[18] J. Golic, Fast low order approximation of cryptographic functions, in: Proceedings of the EUROCRYPT'96, LNCS, vol. 1996, Springer, 1996, pp. 268-282.

[19] T. Iwata and K. Kurosawa, Probabilistic higher order differential attack and higher order bent functions, in: Proceedings of the ASIACRYPT'99, LNCS, vol. 1716, Springer, 1999, pp. 62-74.

[20] G. Kabatiansky and C. Tavernier, List decoding of second order Reed-Muller codes, in: Proceedings of the eighth International Symposium of Communication Theory and Applications, Ambleside, UK, July 2005.

[21] T. Kasami, The Weight Enumerators for Several Classes of subcodes of the second order Binary Reed Muller codes, Information and Control 18 (1971) 369-394.

[22] S. Kavut, S. Maitra, S. Sarkar and M. D. Yücel, Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity > 240, in: Proceedings of the INDOCRYPT'06, LNCS, vol. 4329, Springer, 2006, pp. 266-279.

[23] S. Kavut and M. D. Yücel, Generalized rotation symmetric and dihedral symmetric Boolean functions - 9 variable Boolean functions with nonlinearity 242, in: Proceedings of the AAECC'07, LNCS, vol. 4851, Springer, 2007, pp. 266-279.

[24] L. R. Knudsen and M. J. B. Robshaw, Non-linear approximations in linear cryptanalysis, in: Proceedings of the EUROCRYPT'96, LNCS, vol. 1070, Springer, 1996, pp. 224-236.

[25] N. Kolokotronis, K. Limniotis and N. Kalouptsidis, Efficient Computation Of the Best Quadratic Approximation of Cubic Boolean Functions, in: Cryptography and Coding 2007, LNCS 4887, pp. 73-91, 2007.

[26] R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 1983.

[27] F. J. MacWilliams and N. J. A. Sloane, The theory of error correcting codes, North-Holland, Amsterdam, 1977.

[28] U. M. Maurer, New approaches to the design of self-synchronizing stream ciphers, in: Proceedings of the EUROCRYPT'91, LNCS, vol. 547, 1991, pp. 458-471.

[29] M. Matsui, Linear cryptanalysis method for DES cipher, in: Proceedings of the EUROCRYPT93, LNCS, vol. 765, 1994, pp. 386-397.

[30] W. Millan, Low order approximation of cipher functions, in: Cryptographic policy and algorithms, LNCS, vol. 1029, 1996, pp. 144-155.

[31] J. J. Mykkeltveit, The covering radius of the $(128, 8)$ Reed-Muller code is 56, IEEE Trans. Inform. Theory 26 (3) (1980) 359-362.

[32] N. J. Patterson and D. H. Wiedemann, The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276, IEEE Trans. Inform. Theory 29 (3) (1983) 354-356.

[33] O. S. Rothaus, On bent functions, Journal of Combinatorial Theory Series A 20 (1976) 300-305.

[34] P. Sarkar and S. Maitra, Construction of nonlinear Boolean functions with important cyrptographic properties, in: Proceedings of the EUROCRYPT 2000, LNCS, vol. 1870, 2000, pp. 485-506.

[35] G. Sun and 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.