On lower bounds on second–order nonliearities of bent functions obtained by using Niho power functions

Manish Garg and Sugata Gangopadhyay

Department of Mathematics
Indian Institute of Technology Roorkee
Roorkee–247667, INDIA
{manishiitr8, gsugata}@gmail.com

Abstract. In this paper we find a lower bound of the second-order nonlinearities of Boolean bent functions of the form $f(x) = Tr_1^n(\alpha_1 x^{d_1} + \alpha_2 x^{d_2})$, where d_1 and d_2 are Niho exponents. A lower bound of the second-order nonlinearities of these Boolean functions can also be obtained by using a result proved by Li, Hu and Gao (eprint.iacr.org/2010 /009.pdf). It is demonstrated that for large values of n the lower bound obtained in this paper are better than the lower bound obtained by Li, Hu and Gao.

Key words: Boolean function, derivative, Niho power function, Second-order nonlinearity, Walsh-spectrum.

1 Introduction

Let $\mathbb{F}_{2^n}$ be the extension field of degree n over $\mathbb{F}_2$, the prime field of characteristic 2, and let $\mathbb{F}_2^n$ be the n-dimensional vector space consisting of the n-tuples of elements of $\mathbb{F}_2$. The finite field $\mathbb{F}_{2^n}$ is also an n-dimensional vector space over $\mathbb{F}_2$. Let $\{b_1, \ldots, b_n\}$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Thus, for any $x \in \mathbb{F}_{2^n}$ there exists a vector $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$ such that $x = x_1 b_1 + \ldots + x_n b_n$. This establishes a natural $\mathbb{F}_2$-vector space isomorphism between $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$, both considered as vector spaces over the prime field $\mathbb{F}_2$. We shall frequently identify $x \in \mathbb{F}_{2^n}$ with the vector $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$ assuming a fixed basis $\{b_1, \ldots, b_n\}$. Any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ (equivalently from $\mathbb{F}_2^n$ to $\mathbb{F}_2$) is said to be a Boolean function on n variables. The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$. Let $\mathbb{Z}$ be the set of integers. The addition over $\mathbb{Z}$ and $\mathbb{F}_{2^n}$ is denoted by '+' and the addition over $\mathbb{F}_2^n$ is denoted by $\oplus$. The Hamming weight (or, weight) of x is defined as $wt(x) = \sum_{i=1}^{n} x_i$. The Hamming distance of $f, g \in \mathcal{B}_n$ is $d(f, g) = |\{x \in \mathbb{F}_{2^n} : f(x) \neq g(x)\}|$, where the cardinality of a set S is denoted by $|S|$. The algebraic normal form (ANF) of a Boolean function $f \in \mathcal{B}_n$ is

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

where $\mu_a \in \mathbb{F}_2$ for all $a \in \mathbb{F}_2^n$. The maximum value of $wt(a)$ such that $\mu_a \neq 0$ is said to be the algebraic degree of the Boolean function f and denoted by $\deg(f)$.

Boolean functions having algebraic degree at most 1 is said to be the affine functions. The set of affine functions in $\mathcal{B}_n$ is same as the first-order Reed–Muller code of length 2^n, denoted by $R(1, n)$. Similarly the set of all Boolean functions in $\mathcal{B}_n$ having algebraic degree at most r is same as the rth-order Reed–Muller code of length 2^n, denoted by $R(r, n)$.

Definition 1. *The rth-order nonlinearity ($r \geq 1$) of $f \in \mathcal{B}_n$, denoted $nl_r(f)$, is defined as*

$$nl_r(f) = \min\{d(f, g) : g \in R(r, n)\}. \tag{2}$$

The first-order nonlinearity is referred to as nonlinearity and usually denoted by $nl(f)$. When Boolean functions are used in stream or block ciphers their nonlinearities play an important role with respect to the security of the considered ciphers. A natural generalization of nonlinearity is the rth-order nonlinearity for $r > 1$. In fact for $f \in \mathcal{B}_n$ the sequence $\{nl_r(f)\}_{r=1}^{n-1}$, called the nonlinearity profile of f, provides the complete information on the approximations of f by using Boolean functions of lesser algebraic degrees. Unlike nonlinearity very little is known about higher-order nonlinearity. It is also extremely difficult to compute higher than the first-order nonlinearity of Boolean functions on large number of variables. Therefore finding out lower and upper bounds of higher-order nonlinearities of Boolean functions is an important problem. Carlet [2] provides a technique of computing lower bounds of higher-order nonlinearities recursively. In the same paper Carlet provides general lower bounds on the nonlinearity profiles of Boolean functions belonging to several important classes including Welch, Kasami and multiplicative inverse functions. In this paper we use the technique developed by Carlet to identify special classes of Boolean functions for which the lower bounds of second-order nonlinearities are significantly larger than the general bounds obtained in [2]. We believe that these investigations will be useful in identifying cryptographically significant Boolean functions with good nonlinearity profiles and also increase our understanding of the covering radius problem of Reed–Muller codes.

In 1976, Rothaus [17] introduced the idea of nonlinearity. For ($r \geq 1$) very little is known on $nl_r(f)$. The best known upper bound [4] on $nl_r(f)$ has the following asymptotic version

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

In [6, 7, 12] the list decoding algorithms for higher order Reed-Muller codes are used to compute second-order nonlinearities. These algorithms are efficient for $n \leq 11$ and for $n \leq 13$ for some particular functions. Thus there is a need to obtain bounds of rth-order nonlinearities of different classes of Boolean functions. Carlet [2] introduced a recursive technique to obtain a lower-bound rth-order nonlinearity of a given Boolean function f from the lower bounds on the $(r-1)$th-order nonlinearity of the derivatives of f. Since the results obtained by Carlet

are very general in nature, identifying special classes of Boolean functions which have high lower bounds of rth-order nonlinearities for some values of r remains an open problem. In this direction, Gode and Gangopadhyay [9] have obtained the lower bounds of the second order nonlinearities for the Boolean functions of the form $f_\mu(x) = Tr_1^n(\mu x^{2^i+2^j+1})$ for $n > 2i$. Li, Hu and Gao [14] have obtained the lower bounds of the second order nonlinearity for the Boolean functions of the form $F_\mu(x) = Tr_1^n(\sum_{l=1}^m \mu_l x^{d_l})$, where $\mu_l \in \mathbb{F}_{2^n}^*$, $d_l = 2^{i_l} + 2^{j_l} + 1$, i_l and j_l are positive integers with $n > i_l > j_l$. For more results in this direction we refer to [8, 10, 11, 18, 19]. In this paper, we find the lower bound of second-order nonlinearity of particular type of Boolean function $f(x) = Tr_1^n(\alpha_1 x^{d_1} + \alpha_2 x^{d_2})$. It is demonstrated that the lower bound of $f(x)$ obtained in this paper is better than the lower bound obtained by Li, Hu and Gao [14] for large values of n.

2 Preliminaries

Throughout this paper we take $n = 2e$. The derivative of Boolean function $f \in \mathcal{B}_n$ with respect to $a \in \mathbb{F}_{2^n}$ is defined as a function $D_a f(x) = f(x \bigoplus a) \bigoplus f(x)$ for all $x \in \mathbb{F}_2^n$. The trace function from $G = \mathbb{F}_{2^n}$ into $E = \mathbb{F}_{2^c}$ (where $c|n$) is defined as

$$Tr_c^n(x) = \sum_{i=0}^{\frac{n}{c}-1} x^{2^{ci}}, \text{for all } x \in \mathbb{F}_{2^n}.$$

Tr_1^n (or simply Tr) is said to be the absolute trace function. For any $x, y \in \mathbb{F}_{2^n}$, $Tr_1^n(xy)$ is an inner product of x and y . The Walsh transform of $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_2^n$ is defined as

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\lambda \cdot x}.$$

The multiset $[W_f(\lambda) : \lambda \in \mathbb{F}_2^n]$ is said to be the Walsh spectrum of the Boolean function f. The relation between nonlinearity and Walsh spectrum is given as follows:

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_2^n} |W_f(\lambda)|.$$

Using Parseval's equality it can be proved that for any positive integer n, their exists a $\lambda \in \mathbb{F}_2^n$, such that $|W_f(\lambda)| \geq 2^{\frac{n}{2}}$, which implies $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. For even integer n, a Boolean function which attains maximum nonlinearity i.e. $2^{n-1} - 2^{\frac{n}{2}-1}$, is said to be a bent function. Next we define the Niho power functions.

Definition 2. *An integer $d \in \{1, \ldots, 2^n - 2\}$ is said to be a Niho exponent and x^d is said to be a Niho power function if the restrictionv of x^d to $\mathbb{F}_{2^e}$ is linear. In other words*

$$d \equiv 2^i \pmod{2^e - 1}$$

for some $i < n$. If $i = 0$, then d is said to be in the normalized form and has the following unique representation

$$d = (2^e - 1)s + 1.$$

The bilinear form associated with a quadratic Boolean function $f \in \mathcal{B}_n$ is defined by $B(x, y) = f(0) + f(x) + f(y) + f(x + y)$. The kernel $[1, 16]$ of $B(x, y)$ is the subspace of $\mathbb{F}_{2^n}$ defined by

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

The Walsh spectrum of a quadratic Boolean function (algebraic degree at most 2) is completely characterized by the dimension of the kernel of the bilinear form associated to it. For more details we refer to [1, 16].

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

Lemma 2 ([1, 16]). *If $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is a quadratic Boolean function and $B(x, y)$ is the quadratic form associated to 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	$2^n - 2^{n-k}$
$2^{\frac{n+k}{2}}$	$2^{\frac{n-k-1}{2}} + (-1)^{f(0)}2^{\frac{n-k-2}{2}}$
$-2^{\frac{n+k}{2}}$	$2^{\frac{n-k-1}{2}} - (-1)^{f(0)}2^{\frac{n-k-2}{2}}$

Definition 3. *Let $\mathbb{F}_{q^n}$ be the finite extension of $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^n}$. Then the set of elements $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{n-1}}$ are called the conjugates of α with respect to $\mathbb{F}_q$.*

The conjugate of $x \in \mathbb{F}_{2^n}$ over $\mathbb{F}_{2^e}$ is denoted by $\overline{x}$ and defined as $\overline{x} = x^{2^e}$. $\|x\|$ is defined as $\|x\| = \sqrt{x\overline{x}}$, where $\sqrt{x}$ stands for the inverse of the Frobenius mapping $\varphi(x) = x^2$.

Definition 4. *The set of conjugates of α with respect to $\mathbb{F}_q$ is called the conjugacy class of α with respect to $\mathbb{F}_q$.*

Definition 5. *The cyclotomic coset of z mod $(2^n - 1)$ is denoted by $C(z)$ and defined as*

$$C(z) = \{z' : z' = [2^i z], 0 \leq i \leq n - 1\}.$$

where $[y]_M \in \{0, 1, 2, ...m - 1\}$ such as $[y]_M = x \bmod M$.

Definition 6 ([15], Page 99). *A polynomial of the form*

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

with the coefficients β_i in an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ is called a linearized polynomial over $\mathbb{F}_{q^m}$.

The following result is proved by Carlet [2].

Proposition 1 ([2], Corollary 2) *Let f be an n-variable Boolean function and r be a positive integer smaller then n. Assume that, for some non-negative integers M and m, we have*

$$nl_{r-1}(D_a f) \geq 2^{n-1} - M2^m \tag{3}$$

for every nonzero $a \in \mathbb{F}_{2^n}$. Then we have

$$\begin{aligned} nl_r(f) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)M2^{m+1} + 2^n} \\ &\approx 2^{n-1} - \sqrt{M}2^{\frac{n+m-1}{2}}. \end{aligned} \tag{4}$$

Gode and Gangopadhyay [9] proved the following result.

Proposition 2 *The lower bound of the second-order nonlinearity for the Boolean function $f_\mu(x) = Tr_1^n(\mu x^{2^i+2^j+1})$, $i > j$, for $n > 2i$ ($n \neq i + j$ and $n \neq 2i - j$) is given as*

If n is an odd, then

$$nl_2 f_\mu(x) \geq 2^{n-1} - 2^{\frac{3n+2i-5}{4}};$$

If n is an even, then

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

Li, Hu and Gao [14] proved the following result.

Proposition 3 *The lower bound of the second-order nonlinearity for the Boolean function $F_\mu(x) = Tr_1^n(\sum_{l=1}^m \mu_l x^{d_l})$, where $\mu_l \in \mathbb{F}_{2^n}^*$, $d_l = 2^{i_l} + 2^{j_l} + 1$, i_l and j_l are positive integers with $n > i_l > j_l$, are given as*

1. *if $n < s + t$,*
$$nl_2(F_\mu(x)) \geq 2^{n-1} - 2^{\frac{n+t-2}{2}},$$
2. *if $s + t \leq n < 2t$,*
$$nl_2(F_\mu(x)) \geq 2^{n-1} - 2^{\frac{2n-s-2}{2}},$$
3. *if $n = 2t$ and $s \neq t$, let $p = \min\{n - 2s, 2t_1\}$,*
$$nl_2(F_\mu(x)) \geq 2^{n-1} - 2^{\frac{3n+p-4}{4}},$$
4. *if $n > 2t$, is an even, let $p = \min\{n - 2s, 2t\}$,*
$$nl_2(F_\mu(x)) \geq 2^{n-1} - 2^{\frac{3n+p-4}{4}},$$
5. *if $n > 2t$, is an odd, let $q = \min\{n - 2s, 2t - 1\}$,*
$$nl_2(F_\mu(x)) \geq 2^{n-1} - 2^{\frac{3n+q-4}{4}}.$$

For descriptions of s, t, t_1 we refer to [14].

For the case $n = 2t$, we find a Boolean function whose lower bound of second order nonlinearity is better than the lower bound obtained by Li, Hu and Gao [14]

3 Main Result

The following theorem is proved by Dobbertin et al.

Theorem 1 ([5], Theorem 2). *Consider the Boolean function*

$$f(x) = Tr_1^n(\alpha_1 x^{d_1} + \alpha_2 x^{d_2})$$

on $G = \mathbb{F}_{2^n}$, where $n = 2e$, $\alpha_1, \alpha_2 \in G$ and $d_i = (2^e - 1)s_i + 1, i = 1, 2$, are Niho exponents. If $d_1 = (2^e - 1)\frac{1}{2} + 1$, $d_2 = (2^e - 1)\frac{1}{4} + 1$, $\alpha_1 + \overline{\alpha_1} = \| \alpha_2 \|$, and e is odd then f is a bent function of degree 3.

We observe the following:

Theorem 2. *Let $f(x) = Tr_1^n(\alpha_1 x^{d_1} + \alpha_2 x^{d_2})$, and $g(x) = Tr_1^n(\alpha_1^2 x^{2^e+1} + \alpha_2^4 x^{2^e+2+1})$, where $\alpha_1, \alpha_2 \in \mathbb{F}_{2^n}$, $n = 2e$, and $d_1 = (2^e-1)\frac{1}{2}+1$, $d_2 = (2^e-1)\frac{1}{4}+1$ are Niho exponents. Then the second-order nonlinearities of Boolean functions $f(x)$ and $g(x)$ are the same.*

Proof. The function

$$\begin{aligned} f(x) &= Tr_1^n(\alpha_1 x^{d_1} + \alpha_2 x^{d_2}) \\ &= Tr_1^n(\alpha_1 x^{d_1}) + Tr_1^n(\alpha_2 x^{d_2}). \end{aligned}$$

We know that $Tr_1^n(x)^{2^i} = Tr_1^n(x)$. We have

$$\begin{aligned} f(x) &= Tr_1^n(\alpha_1 x^{d_1})^2 + Tr_1^n(\alpha_2 x^{d_2})^{2^2} \\ &= Tr_1^n(\alpha_1^2 x^{2d_1}) + Tr_1^n(\alpha_2^4 x^{4d_2}) \\ &= Tr_1^n(\alpha_1^2 x^{2^e+1}) + Tr_1^n(\alpha_2^4 x^{2^e+3}) \\ &= Tr_1^n(\alpha_1^2 x^{2^e+1} + \alpha_2^4 x^{2^e+2+1}) \\ &= g(x), \end{aligned}$$

since $2d_1 = (2^e + 1)$ and $4d_1 = (2^e + 3)$. Hence, the second-order nonlinearity of $f(x)$ and $g(x)$ are the same. □

Finally we prove the main result concerning the lower bound of second-order nonlinearities of the functions under consideration.

Theorem 3. *Let $f(x) = Tr_1^n(\alpha_1 x^{d_1} + \alpha_2 x^{d_2})$, where $\alpha_1, \alpha_2 \in \mathbb{F}_{2^n}$, $n = 2e$, $\alpha_1 + \overline{\alpha_1} = \| \alpha_2 \|$ and $d_1 = (2^e - 1)\frac{1}{2} + 1$, $d_2 = (2^e - 1)\frac{1}{4} + 1$ are Niho exponents. then*

$$nl_2(f(x)) \geq 2^{n-1} - 2^{\frac{3n+e-3}{4}}.$$

Proof. Consider the Boolean function

$$\begin{aligned} g(x) &= Tr_1^n(\alpha_1^2 x^{2^e+1} + \alpha_2^4 x^{2^e+2+1}) \\ &= Tr_1^n(\alpha_1^2 x^{2^e+1}) + Tr_1^n(\alpha_2^4 x^{2^e+2+1}). \end{aligned}$$

It is clear that the algebraic degree of Boolean function $g(x)$ is 3. We know that the rth-order nonlinearity of a Boolean function $f(x)$ dose not alter if we add a Boolean function of degree at most r to $f(x)$. Therefore, the second-order nonlinearity of $g(x)$ is equal to the second-order nonlinearity of $g_1(x) = Tr_1^n(\alpha_2^4 x^{2^e+2+1})$. The derivative $D_a(g_1(x))$ with respect to $a \in \mathbb{F}_{2^n}^*$ is

$$\begin{aligned} D_a(g_1(x)) &= g_1(x+a) + g_1(x) \\ &= Tr_1^n(\alpha_2^2(x+a)^{2^e+2+1}) + Tr_1^n(\alpha_2^4 x^{2^e+2+1}) \\ &= Tr_1^n(\alpha_2^4 a^2 x^{2^e+1} + \alpha_2^4 a^{2^e} x^3 + \alpha_2^4 a x^{2^e+2} + \alpha_2^4 a^{2^e+2} x + \alpha_2^4 a^3 x^{2^e} \\ &\quad + \alpha_2^4 a^{2^e+1} x^2 + \alpha_2^4 a^{2^e+3}), \end{aligned}$$

which is a quadratic Boolean function. Therefore, the Walsh spectrum of the Boolean function $D_a(g_1(x))$ is equal to the Walsh spectrum of the function $h_\lambda(x)$, where $h_\lambda(x)$ contains only quadratic terms of $D_a(g_1(x))$. We have

$$h_\lambda(x) = Tr_1^n(\alpha_2^4 a^2 x^{2^e+1} + \alpha_2^4 a^{2^e} x^3 + \alpha_2^4 a x^{2^e+2}).$$

Let $B(x, y)$ be the bilinear form associated with $h_\lambda(x)$ and let k be the dimension of $\mathcal{E}_f$. The kernel of $B(x, y)$ is given as

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

where

$$\begin{aligned} B(x, y) &= h_\lambda(0) + h_\lambda(x) + h_\lambda(y) + h_\lambda(x+y) \\ &= Tr_1^n(\alpha_2^4(a^2 y x^{2^e} + a^2 y^{2^e} x + a^{2^e} y x^2 + a^{2^e} y^2 x + a y^2 x^{2^e} + a y^{2^e} x^2)) \\ &= Tr_1^n(\alpha_2^4(a^2 x^{2^e} + a^{2^e} x^2) y) + Tr_1^n(\alpha_2^4(a x^{2^e} + a^{2^e} x) y^2) \\ &\quad + Tr_1^n(\alpha_2^4(a^2 x + a x^2) y^{2^e}). \end{aligned}$$

We know that, $Tr_1^n(x^{2^i}) = Tr_1^n(x)$. Thus,

$$\begin{aligned} B(x, y) = Tr_1^n(\alpha_2^4(a^2 x^{2^e} + a^{2^e} x^2) y) + Tr_1^n(\alpha_2^4(a x^{2^e} + a^{2^e} x) y^2)^{2^{n-1}} \\ + Tr_1^n(\alpha_2^4(a^2 x + a x^2) y^{2^e})^{2^e}. \end{aligned}$$

Since $x, y, a, \alpha_2 \in \mathbb{F}_{2^n}$ and $n = 2e$, we have $x^{2^n} = x$, $y^{2^n} = y$, $a^{2^n} = a$, $\alpha_2^{2^n} = \alpha_2$, and

$$B(x, y) = Tr_1^n(yP(x)),$$

where $P(x)$ is given as

$$\begin{aligned} P(x) = \alpha_2^{2^2} a^2 x^{2^e} + \alpha_2^{2^2} a^{2^e} x^2 + \alpha_2^2 a^{2^{-1}} x^{2^{e-1}} + \alpha_2^2 a^{2^{e-1}} x^{2^{-1}} \\ + \alpha_2^{2^{e+2}} a^{2^{e+1}} x^{2^e} + \alpha_2^{2^{e+2}} a^{2^e} x^{2^{e+1}}. \end{aligned}$$

It is to be noted that the number of elements in $\mathcal{E}_f$ is equal to the number of zeros of $P(x)$ or equivalently the number of zeros of $P(x)^2$. Let it be denoted by $L_{(\alpha_2, a)}(x)$.

$$\begin{aligned} L_{(\alpha_2,a)}(x) = \alpha_2^{2^{e+3}} a^{2^{e+1}} x^{2^{e+2}} + (\alpha_2^{2^3} a^{2^2} + \alpha_2^{2^{e+3}} a^{2^{e+2}}) x^{2^{e+1}} \\ + \alpha_2^{2^2} a x^{2^e} + \alpha_2^{2^3} a^{2^{e+1}} x^{2^2} + \alpha_2^{2^2} a^{2^e} x, \end{aligned}$$

which is a linearized polynomial in x. The degree of $L_{(\alpha_2,a)}(x)$ is at most 2^{e+2}. Therefore, by Lemma 1, $k \leq e+1$. From this we obtain

$$W_{D_a g_1}(x) = 2^{\frac{n+k}{2}} \leq 2^{\frac{n+e+1}{2}}.$$

Substituting the above value in

$$nl(D_a(g_1(x))) = 2^{n-1} - \frac{1}{2} \max_{x \in \mathbb{F}_2^n} |W_{D_a g_1}(x)|,$$

we have

$$nl(D_a(g_1(x))) \geq 2^{n-1} - 2^{\frac{n+e-1}{2}},$$

and finally

$$nl(D_a(g(x))) \geq 2^{n-1} - 2^{\frac{n+e-1}{2}}. \tag{5}$$

From equation (3) and (5), we get $M = 1$ and $m = \frac{n+e-1}{2}$. Substituting the values of M and m in equation (4)

$$nl_2(g(x)) \geq 2^{n-1} - 2^{\frac{3n+e-3}{4}}.$$

Using Theorem 2 we obtain

$$nl_2(f(x)) \geq 2^{n-1} - 2^{\frac{3n+e-3}{4}}.$$

□

4 Comparison

The lower bound of second-order nonlinearities of $f(x) = Tr_1^n(\alpha_1 x^{d_1} + \alpha_2 x^{d_2})$ was not obtained by Gode and Gangopadhyay [9] (since in this case $n = 2i$). The lower bound of second-order nonlinearities of a Boolean function $f(x)$ can be obtained from Li, Hu and Gao [14, Theorem 4, Case 3] (i.e., $n = 2t$ and $s \neq t$). Let $p = \min\{n - 2s, 2t_1\}$). Then

$$nl_2(f(x)) \geq 2^{n-1} - 2^{\frac{3n+p-4}{4}},$$

which implies

$$nl_2(f(x)) \geq \begin{cases} 2^{n-1} - 2^{\frac{2n-3}{2}}, & \text{for } e \geq 3 \\ 0, & \text{for e} = 1. \end{cases} \tag{6}$$

It can be checked that

$$(2^{n-1} - 2^{\frac{3n+e-3}{4}}) - (2^{n-1} - 2^{\frac{2n-3}{2}}) > 0, \text{ for all } n \geq 10,$$

which implies that the bound obtained by Theorem 3 is strictly greater than that obtained by Li, Hu and Gao whenever $n \geq 10$. We compare the values of lower bound obtained in Theorem 3 and the values of lower bound obtained by the Li, Hu and Gao [14, Theorem 4, Case 3] in Table 1. We demonstrate that the lower bound obtained in Theorem 3 is better than that obtained by Li, Hu and Gao. Thus we identify a subclass of Boolean functions considered by Li, Hu and Gao which has potential of having higher second-order nonlinearities than the functions belonging to the wider class.

n	10	14	18	22	26	30
Lower bound obtained in Theorem 3	256	5296	98304	1726425	29360128	489417780
Lower bound obtained in [14, Theorem 4]	150	2400	38390	614242	9827866	157245850

Table 1. Comparison of the lower bounds of the second-order nonlinearities.

Acknowledgment

Manish Garg would like to thank Ministry of Human and Research Development (MHRD) of India for financial support.

References

1. A. Canteaut, P. Charpin and G. M. Kyureghyan. A new class of monomial bent functions. Finite Fields and their Applications, Vol. 14, pp. 221-241, 2008.
2. C. Carlet. Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications. IEEE Trans. Inf. Theory, 54(3), pp. 1262-1272, 2008.
3. C. Carlet. On the nonlinearity profile of the Dillon function. http:// eprint.iacr.org/2009/577.pdf.
4. C. Carlet and S. Mesnager.Improving the upper bounds on the covering radii of binary ReedMuller codes. IEEE Trans. Inf. Theory, vol.53, no. 1, pp. 162-173, jan. 2007.
5. H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke and P. Gaborit. Construction of bent functions via Niho power functions. Journal of Combinatorial Theory. Series A 113, pp. 779-798, 2006.
6. 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, pp. 138-142, WA 2006.
7. R. Fourquet and C. Tavernier. An improved list decoding algorithm for the second order Reed-Muller codes and its applications. Designs Codes Cryptogr., Vol, 49, pp. 323-340, 2008.
8. S. Gangopadhyay, S. Sarkar and R. Telang. On the lower bounds of the second-order nonlinearity of some Boolean functions. Inf. Sci. 180(2), pp. 266-273, 2010.

9. R. Gode and S. Gangopadhyay. On second order nonlinearities of cubic monomial Boolean functions. http: // eprint.iacr.org/2009/502.pdf.
10. R. Gode and S. Gangopadhyay. Third-order nonlinearities of a subclass of kasami functions. Cryptography. Commun, Vol. 2, pp. 69-83, 2010.
11. R. Gode and S. Gangopadhyay. On lower bounds of second-order nonlinearities of cubic bent functions constructed by concatenating Gold functions. Accepted in International journal of Computer mathematics, 2011.
12. G. Kabatiansky and C. Tavernier. List decoding of second order Reed-Muller codes. In : Proceedings of the Eighteen International Symposium of Communication Theory and Applications, Ambleside, UK, 2005.
13. L. R. Knudsen and M. J. B. Robshaw. Non-linear approximations in linear cryptanalysis. in Proc. EUROCRYPT'96 (Lecture Notes in Computer Science), Berlin, Germany: Springer-Verlag, vol.1070, pp. 224-236, 1996.
14. X. Li, Y. Hu and J. Gao. The lower bounds on the second order nonlinearity of cubic Boolean functions. http: // eprint.iacr.org/2010/009.pdf.
15. R. Lidi and H. Niederreiter. Introduction to finite fields and their applications. North-Holland, Amsterdam, 1994.
16. F. J. Macwilliams and N. J. A. Solane. The theory of Error-correcting Codes. Amsterdam: North-holland publishing Company, 1978.
17. O. S. Rothaus. On bent functions. Journal of Combinatorial Theory, Series A, 20, pp.300-305, 1976.
18. 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) pp. 267-278, 2009.
19. G. Sun and C. Wu. The lower bound on the second-order nonlinearity of a class of Boolean function with high nonlinearity. Appl. Algebra Engrg. Comm. Comput. (AAECC), vol. 22, pp. 37-45, 2011.