On lower bounds of second-order nonlinearities of cubic bent functions constructed by concatenating Gold functions

Ruchi Gode and Sugata Gangopadhyay
Department of Mathematics
Indian Institute of Technology
Roorkee - 247 667 Uttarakhand INDIA

May 5, 2010

Abstract

In this paper we consider cubic bent functions obtained by Leander and McGuire (J. Comb. Th. Series A, 116 (2009) 960-970) which are concatenations of quadratic Gold functions. A lower bound of second-order nonlinearities of these functions is obtained. This bound is compared with the lower bounds of second-order nonlinearities obtained for functions belonging to some other classes of functions which are recently studied.

Keywords: Boolean functions, cubic functions, derivatives, second-order nonlinearity, low order approximations.

1 Introduction

Cryptographic Boolean functions play a prominent role in design and security of stream ciphers and block ciphers. In general, resistance of Boolean function against various cryptanalytic attacks depends upon its various cryptographic properties. One of the most important requirement for the design of Boolean functions is their good nonlinearity. It measures the extent to which linear cryptanalytic attacks [24] and best affine approximation attacks [10] can be resisted. The advent of recent algebraic attacks [9] and low order approximation attacks [15, 16, 18, 25, 26, 27, 31] necessitate the construction of Boolean functions that cannot be approximated by low degree functions and thus lead to generalized notion of nonlinearity called rth-order ($r > 1$) nonlinearity. High first-order nonlinearity of a Boolean function does not ensure that its rth-order ($r > 1$) nonlinearity is also good. It is

to be noted that very little is known about $nl_r(f)$ for $r > 1$. The best known asymptotic upper bound on $nl_r(f)$ found in [8] which is as follows:

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

The first-order nonlinearity of a Boolean function on n variables can be computed by using fast Walsh transform in time $O(n2^n)$. For results on constructions of Boolean functions with high nonlinearity we refer to [1, 6, 7, 17, 19, 20, 28, 29, 30]. For $r > 2$ there is no efficient algorithm to compute rth-order nonlinearity of a Boolean function. An algorithm based on list decoding techniques of Reed-Muller codes, proposed by Dumer, Kabatiansky and Tavernier [11] and later improved by Fourquet and Tavernier [12], works well for $r = 2$ and $n \leq 11$ ($n \leq 13$ in some cases). However, it is inefficient for $r \geq 3$. Carlet [4] for the first time performed a systematic study on higher-order nonlinearities of Boolean functions. He developed a recursive approach to compute the lower bounds on rth-order nonlinearities of a function f by using the $(r-1)$th-order nonlinearities of the derivatives of the f. In the same paper Carlet obtained lower bounds of the second-order nonlinearities of several classes of functions, Welch function and the inverse function being among them. In another paper [5] Carlet efficiently lower bounded the nonlinearity profile of Dillon type bent functions. Using Carlet's approach Sun and Wu [32], Gangopadhyay, Sarkar and Telang [13], Gode and Gangopadhyay [14] obtained the lower bounds of the second-order nonlinearities of several classes of Boolean functions. Iwata-Kurosawa [16] provides Boolean functions with lower bounded rth-order nonlinearity, but the bound obtained is small. In this paper we consider cubic bent functions obtained by Leander and McGuire [21] which are concatenations of quadratic Gold functions. A lower bound of second-order nonlinearities of these functions is obtained. This bound is compared with the lower bounds of second-order nonlinearities obtained for functions belonging to some other classes of functions which are recently studied.

2 Preliminaries

Let $\mathbb{F}_2$ be the prime field of characteristic 2. The set of all n-tuples of elements of $\mathbb{F}_2$ is denoted by $\mathbb{F}_2^n$. Let $\mathbb{F}_{2^n}$ be the extension field of degree n over $\mathbb{F}_2$. The finite field $\mathbb{F}_{2^n}$ can be considered as an n dimensional vector space over $\mathbb{F}_2$. The set containing all invertible elements of $\mathbb{F}_{2^n}$ is denoted by $\mathbb{F}_{2^n}^*$. Any function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$ or equivalently from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ is called a Boolean function on n variables. The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$. For any set S, the cardinality of S is denoted by $|S|$. Support of $f \in \mathcal{B}_n$ denoted by $supp(f)$ is $|\{x \in \mathbb{F}_2^n : f(x) \neq 0\}|$. 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.
Consider $B = \{b_1, \ldots, b_n\}$ a basis of $\mathbb{F}_{2^n}$. 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 weight, $wt(x)$, of x is defined as $\sum_{i=1}^{n} x_i$, where the sum is over integers. Once a basis B of $\mathbb{F}_{2^n}$ is fixed, any function $f \in \mathcal{B}_n$ can be written as a function of $x_1, \ldots, x_n$ as follows

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

The algebraic degree, $\deg(f)$, of f is defined as $\max_{a\in\mathbb{F}_2^n}\{wt(a) : \mu_a \neq 0\}$.
The trace function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ is defined by

$$Tr_1^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}},$$

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. The set of affine functions $\mathcal{A}_n$ is defined as follows:

$$\mathcal{A}_n = \{f_\lambda + \epsilon : \lambda \in \mathbb{F}_{2^n}, \epsilon \in \mathbb{F}_2\}.$$

where $f_\lambda(x) = Tr_1^n(\lambda x)$, for all $x \in \mathbb{F}_{2^n}$.
The Walsh transform of $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_{2^n}$ is defined by

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

Nonlinearity of $f \in \mathcal{B}_n$ is defined as $nl(f) = \min_{l\in\mathcal{A}_n}\{d(f, l)\}$. The multiset $[\widehat{f}(\lambda) : \lambda \in \mathbb{F}_{2^n}]$ is said to be the Walsh spectrum of f. Nonlinearity and Walsh spectrum of $f \in \mathcal{B}_n$ is related as follows:

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

Using Parseval's identity

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

it can be shown that $\max\{|\widehat{f}(\lambda)| : \lambda \in \mathbb{F}_{2^n}\} \geq 2^{n/2}$, which implies $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.

Definition 1 *Suppose n is an even integer. A function $f \in \mathcal{B}_n$ is said to be a bent function if and only if it possesses maximum nonlinearity, i.e., $2^{n-1} - 2^{\frac{n}{2}-1}$.*

For a bent functions $f \in \mathcal{B}_n$, it is clear that $\widehat{f}(\lambda) \in \{2^{\frac{n}{2}}, -2^{\frac{n}{2}}\}$ for all $\lambda \in \mathbb{F}_{2^n}$. Since bent functions have the maximum nonlinearity, they are optimally resistant to best affine approximation attacks.

2.1 Higher-order nonlinearity of Boolean functions and recursive lower bounds

Definition 2 *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be an n-variable Boolean function. For every non-negative integer $r \leq n$ we denote by $nl_r(f)$ the minimum Hamming distance between f and all functions of algebraic degree at most r. For $r = 1$ we simply write $nl(f)$. The parameter $nl_r(f)$ is called the rth-order nonlinearity of f (simply the nonlinearity in the case $r = 1$).*

The $nl_r(f)$ is exactly the distance from f to the Reed-Muller code $\mathcal{R}(r,n)$ of order r and length 2^n. Therefore the maximum value of $nl_r(f)$, while f varies over the set of all n-variable Boolean functions is the covering radius of $\mathcal{R}(r,n)$. The nonlinearity profile of f is the sequence whose r-th term, for r varying in the range 1 to $n-1$, equals the rth-order nonlinearity of f.

Definition 3 ([16]) *$f \in \mathcal{B}_n$ is called rth-order bent if*

$$nl_r(f) \geq \begin{cases} 2^{n-r-3}(r+4), & \text{if } r \text{ is even,} \\ 2^{n-r-3}(r+5), & \text{if } r \text{ is odd.} \end{cases}$$

for $0 \leq r \leq n-3$.

The recursive lower bounds of higher-order nonlinearities of Boolean functions, obtained by Carlet [4], are dependent on the nonlinearities of their derivatives.

Definition 4 *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 5 *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. The following two propositions are due to Carlet [4].

Proposition 1 ([4], Proposition 2) *Let $f(x)$ be any n-variable Boolean function and r be a positive integer smaller than n, for every non-negative integer $i < r$, we have*

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

Proposition 2 ([4], Proposition 3) *Let f be any n-variable Boolean function and r be a positive integer smaller than n. We have*

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

Carlet remarked that in general, the lower bound given in Proposition 2 is potentially stronger than that given in Proposition 1. The Propositions 1 and 2 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 to it. For details refer to [2, 23] .

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 [2, 23] 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 ([2], 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 ([2], 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 ([2, 23]) *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 6 ([22]) *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 $\mathbb{F}_{q^m}$.

The polynomial

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

is called conventional q associate of $L(x)$.
Below we give some known results on the factorization of polynomials in finite field [22] which we use in the proof.

- It is well known that in any field $\mathbb{F}_{q^m}$ $x^s - 1 | x^r - 1$ if and only if $s|r$ and $\gcd(x^s - 1, x^r - 1) = x^d - 1$ where $d = \gcd(s, r)$.
- Conventional q associate of $x^{q^n} + x$ is $x^n + 1$, moreover if $\gcd(n, t) = 1$ then $\gcd(x^{q^n} + x, x^{q^t} + x) = x(x + 1)$ and $\gcd(x^n + 1, x^t + 1) = x + 1$.

3 Main Result

The following theorem is due to Leander and McGuire [21].

Theorem 1 ([21]) *Let $f(x)$ and $h(x)$ be two Boolean functions on $\mathbb{F}_{2^t}$ and let $\psi(x, y)$ on $\mathbb{F}_{2^t} \times \mathbb{F}_2$ defined by*

$$\psi(x, y) = yh(x) + (1 + y)f(x)$$

Then the following properties are equivalent

1. *ψ is bent.*
2. *f, h are near-bent and $supp(\widehat{f}) \cap supp(\widehat{h}) = \phi$.*

The function $Tr_1^n(x^d)$ is near bent if and only if x^d is almost bent(it has Walsh spectrum $[0, \pm 2^{\frac{n+1}{2}}]$) and $\gcd(d, 2^n - 1) = 1$. Gold functions $Tr_1^n(x^{2^k+1})$ where $\gcd(k, n) = 1$ and n is odd are near-bent functions. Leander and McGuire in Corollary 5 [21] constructed cubic bent functions by concatenating two quadratic Gold functions. We consider a special case of those functions. Let t be a odd prime, $n = t + 1$ and let j, k be two positive integers with $k < j \leq \frac{t-1}{2}$. Define $g : \mathbb{F}_{2^t} \times \mathbb{F}_2 \to \mathbb{F}_2$ as

$$g(x, y) = yTr_1^t(x^{2^j+1} + x) + (1 + y)Tr_1^t(x^{2^k+1}).$$

We analyze the second order nonlinearity of g.

Lemma 4

$$nl(D_{(a,b)}g) = \begin{cases} 0 & \text{if } a = 1, b = 0 \\ 2^{n-1} - 2^{\frac{n}{2}}, & \text{else .} \end{cases} .$$

Proof : $g(x,y) = yTr_1^t(x^{2^j+1}+x) + (1+y)Tr_1^t(x^{2^k+1})$
Derivative of $g(x,y)$ with respect to $(a,b) \in \mathbb{F}_{2^t} \times \mathbb{F}_2$ is

$$\begin{aligned} D_{(a,b)}g(x,y) &= (1+y+b)Tr_1^t((x+a)^{2^j+1}+x) + (1+y+b)Tr_1^t((x+a)^{2^k+1}) \\ &= yTr_1^t(ax^{2^j} + ax^{2^k} + x(a^{2^j}+a^{2^k}) + a^{2^j+1} + a^{2^k+1} + a) \\ &\quad +bTr_1^t(x^{2^j+1} + x^{2^k+1} + ax^{2^j} + ax^{2^k} + x(a^{2^j}+a^{2^k}+1) \\ &\quad +a^{2^j+1} + a^{2^k+1} + a) \\ &\quad +Tr_1^t(ax^{2^k} + xa^{2^k} + a^{2^k+1}). \end{aligned}$$

If $D_{(a,b)}g$ is quadratic then by Lemma 2 the kernel of the bilinear form associated to $D_{(a,b)}g$ is

$$\mathcal{E}_{D_{(a,b)}g} = \{(c,d) \in \mathbb{F}_{2^t} \times \mathbb{F}_2 | D_{(c,d)}D_{(a,b)}g = \text{ constant}\}.$$

Let $K(a,b)$ denotes the dimension of the kernel $\mathcal{E}_{D_{(a,b)}g}$.
Consider a 2-dimensional subspace V generated by two vectors (a,b) and (c,d). The second derivative of f at V is as follows:

$$\begin{aligned} D_V g(x,y) &= D_{(c,d)}D_{(a,b)}g(x,y) \\ &= yTr_1^t(a(c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}})) \\ &\quad +dTr_1^t((a^{2^j} + a^{2^{t-j}} + a^{2^k} + a^{2^{t-k}})x) + bTr_1^t((c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}})x) \\ &\quad +dTr_1^t(ca^{2^j} + ca^{2^k} + a^{2^j+1} + a^{2^k+1} + a) \\ &\quad +bTr_1^t(c^{2^j+1} + c^{2^k+1} + ac^{2^j} + ac^{2^k} + c(a^{2^j} + a^{2^k} + 1)) \\ &\quad +Tr_1^t(ac^{2^j} + ca^{2^j}). \end{aligned}$$

Consider the following cases:
Case 1: $a = 1, b = 0$

$$D_{(c,d)}D_{(1,0)}g(x,y) = yTr_1^t(c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}}) + constant.$$

$D_{(c,d)}D_{(1,0)}g(x,y)$ is constant if and only if
$Tr_1^t(c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}}) = 0$
Above equation holds for all $c \in \mathbb{F}_{2^t}$. So c can be chosen in 2^t ways and for each choice of c, d can take 2 values such that $D_{(c,d)}D_{(1,0)}g$ is constant. Therefore, $\mathcal{E}_{D_{(1,0)}g}$ contains exactly 2^{t+1} elements which implies that $K(1,0) = t+1 = n$.

Case 2: $a = 0, b = 1$

$$D_{(c,d)}D_{(0,1)}g(x,y) = Tr_1^t((c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}})x) + constant.$$

$D_{(c,d)}D_{(0,1)}g(x,y)$ is constant if and only if

$$c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}} = 0 \quad (1)$$

Applying Frobenius map j times to Equation (1), we obtain

$$c^{2^{2j}} + c^{2^{j+k}} + c^{2^{j-k}} + c \;=\; 0$$

Let $L(c) = c^{2^{2j}} + c^{2^{j+k}} + c^{2^{j-k}} + c$. The conventional associate of the linearized polynomial $L(c)$ is $l(c) = c^{2j} + c^{j+k} + c^{j-k} + 1$. By theory of associates $\gcd(L(c), c^{2^t} + c)$ is the linearized associate of $\gcd(l(c), c^t + 1)$, factorization of $l(c)$ is

$$l(c) = (c^{j+k} + 1)(c^{j-k} + 1)$$

Since t is odd prime and $j, k \leq \frac{t-1}{2}$, we observe that $\gcd(t, j+k) = \gcd(t, j-k) = 1$, this implies that $\gcd(l(c), c^t + 1) = c + 1$. Thus $L(c) = 0$ has only two solutions $c = 0, 1$ in $\mathbb{F}_{2^t}$. So c can be chosen in 2 ways and for each choice of c, d in 2 ways, therefore the total number of ways in which (c, d) can be chosen so that $D_{(c,d)}D_{(0,1)}g$ is constant is $2 \cdot 2 = 2^2$ ways. $\mathcal{E}_{D_{(0,1)}g}$ contains exactly 2^2 elements which implies that $K(0, 1) = 2$.

Case 3: $a = 1, b = 1$

$$\begin{aligned} D_V g(x,y) &= D_{(c,d)}D_{(1,1)}g(x,y) \\ &= yTr_1^t(c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}}) \\ &\quad + Tr_1^t((c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}})x) + constant. \end{aligned}$$

$D_{(c,d)}D_{(1,1)}g(x, y)$ is constant if and only if
$Tr_1^t(c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}}) = 0$
and
$c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}} = 0$
Condition 1 and 2 together implies that c can take only two values 0 and 1. For each choice of c, d can be chosen in 2 ways such that $D_{(c,d)}D_{(1,1)}g$ is constant. Therefore, $\mathcal{E}_{D_{(1,1)}g}$ contains exactly 2^2 elements which implies that $K(1, 1) = 2$.

Case 4: $a \in \mathbb{F}_{2^t}^* \setminus \{1\}$
Subcase 1: $a \in \mathbb{F}_{2^t}^* \setminus \{1\}, b = 0$. In this case

$$\begin{aligned} D_V g(x,y) &= D_{(c,d)}D_{(a,0)}g(x,y) \\ &= yTr_1^t(a(c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}})) \\ &\quad + dTr_1^t((a^{2^j} + a^{2^{t-j}} + a^{2^k} + a^{2^{t-k}})x) \end{aligned}$$

$D_{(c,d)}D_{(a,0)}g(x, y)$ is constant if and only if
$dTr_1^t(a^{2^j} + a^{2^{t-j}} + a^{2^k} + a^{2^{t-k}}) = 0$
and
$Tr_1^t(a(c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}})) = 0$
Condition 2 is equivalent to $Tr_1^t(c(a^{2^j} + a^{2^{t-j}} + a^{2^k} + a^{2^{t-k}})) = 0$

Since $a \neq 0, 1$, therefore
$Tr_1^t(a(c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}})) = 0 = Tr_1^t(c(a^{2^j} + a^{2^{t-j}} + a^{2^k} + a^{2^{t-k}}))$ implies that c can take only two values 0 and 1 and condition 1 gives $d = 0$.
Therefore, the total number of ways in which (c, d) can be chosen so that $D_{(c,d)}D_{(a,0)}g$ is constant in this case is $2 \cdot 1 = 2$ ways.
Subcase 2: $a \in \mathbb{F}_{2^t}^* \setminus \{1\}, b = 1$. In this case

$$\begin{aligned} D_V g(x,y) &= D_{(c,d)}D_{(a,1)}g(x,y) \\ &= yTr_1^t(a(c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}})) \\ &\quad +dTr_1^t((a^{2^j} + a^{2^{t-j}} + a^{2^k} + a^{2^{t-k}})x) \\ &\quad +bTr_1^t((c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}})x) + constant. \end{aligned}$$

$D_{(c,d)}D_{(a,b)}g(x,y)$ is constant if and only if
$Tr_1^t(a(c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}})) = 0$
and
$dTr_1^t(a^{2^j} + a^{2^{t-j}} + a^{2^k} + a^{2^{t-k}}) = 0$
and
$c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}} = 0$
Condition 1 and 3 implies that $c^{2^j} + c^{2^{t-j}} + c^{2^k} + c^{2^{t-k}} = 0$, so $c = 0, 1$. Condition 2 gives $d = 0$ as $a \in \mathbb{F}_{2^t}^* \setminus \{1\}$. So in this subcase $D_{(c,d)}D_{(a,1)}g$ is constant only when $(c, d) = (0, 0)$ or $(c, d) = (1, 0)$.
Combining the two subcases of case 4 we conclude that the number of ways in which (c, d) can be chosen so that $D_{(c,d)}D_{(a,b)}f$ is constant for $a \in \mathbb{F}_{2^t}^* \setminus \{1\}$ is $2 + 2 = 4 = 2^2$ and thus $K(a, b) = 2$ in this case.

Combining the four cases we infer that

$$K(a,b) = \begin{cases} n, & \text{if } a = 1, b = 0, \\ 2, & \text{if } a = 1, b = 1, \\ 2, & \text{if } a = 0, b = 1, \\ 2, & \text{if } a \in \mathbb{F}_{2^t}^* \setminus \{1\}. \end{cases}$$

The nonlinearity of $D_{(a,b)}f$ is

$$\begin{aligned} nl(D_{(a,b)}g) &= 2^{n-1} - \frac{1}{2} \max_{(\lambda,\mu) \in \mathbb{F}_2^t \times \mathbb{F}_2} |W_{D_{(a,b)}f}(\lambda, \mu)| \\ &= 2^{n-1} - \frac{1}{2} 2^{\frac{n+K(a,b)}{2}} \end{aligned}$$

that is

$$nl(D_{(a,b)}g) = \begin{cases} 0 & \text{if } a = 1, b = 0, \\ 2^{n-1} - 2^{\frac{n}{2}}, & \text{else .} \end{cases} .$$

■

Remark 1 *It is to be noted that the derivative of g with respect to $(1,0)$ is affine.*

Theorem 2

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

Proof :

$$\begin{aligned}
&\sum_{(a,b)\in\mathbb{F}_{2^t}\times\mathbb{F}_2} nl(D_{(a,b)}g) \\
&= nl(D_{(0,0)}g) + nl(D_{(1,0)}g) + \sum_{(a,b)\in\mathbb{F}_{2^t}\times\mathbb{F}_2,(a,b)\neq(0,0),(1,0)} nl(D_{(a,b)}g) \\
&= 0 + 0 + (2^n - 2)\cdot(2^{n-1} - 2^{\frac{n}{2}}) \\
&= 2^{2n-1} - 2^n - 2^{\frac{3n}{2}} + 2^{\frac{n}{2}+1}.
\end{aligned}$$

By using Proposition 2, we get

$$\begin{aligned}
nl_2(g) &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\cdot(2^{2n-1} - 2^n - 2^{\frac{3n}{2}} + 2^{\frac{n}{2}+1})} \\
&= 2^{n-1} - \frac{1}{2}\sqrt{2^{n+1} + 2^{\frac{3n+2}{2}} - 2^{\frac{n+4}{2}}}.
\end{aligned}$$

■

Corollary 1 *Let t be odd and $n = t+1$ and let $0 \leq k < j < \frac{t+1}{2}$ such that $\gcd(j+k,t) = \gcd(j-k,t) = 1$. Define $h : \mathbb{F}_{2^t} \times \mathbb{F}_2 \to \mathbb{F}_2$ as*

$$h(x,y) = yTr_1^t(x^{2^j+1} + x) + (1+y)Tr_1^t(x^{2^k+1}).$$

Then

$$nl_2(h) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{n+1} + 2^{\frac{3n+2}{2}} - 2^{\frac{n+4}{2}}}.$$

■

4 Comparisons

t	3	5	7	9	11	13	15	17	19
n	4	6	8	10	12	14	16	18	20
bounds of Theorem 2	N/A	16	82	N/A	1684	7165	N/A	122873	501107
bounds of Corollary 1	2	16	82	383	1684	7165	29867	122873	501107
Maximum known distances [12]	2	18	84	400	1760	–	–	–	–

Remark 2 *Let d be the algebraic degree of the function. According to McEliece's Theorem [3, 23], the r-th order nonlinearity of a Boolean function is divisible by $2^{\lceil \frac{n}{d} \rceil - 1}$.*

Below we present the computational results by applying McEliece's Theorem on the bounds of Theorem 2 and Corollary 1 respectively.

t	3	5	7	9	11	13	15	17	19
n	4	6	8	10	12	14	16	18	20
bounds of Theorem 2	N/A	16	84	N/A	1688	7168	N/A	122880	501120
bounds of Corollary 1	2	16	84	384	1688	7168	29888	122880	501120
Maximum known distances [12]	2	18	84	400	1760	–	–	–	–

5 Concluding remarks

Sun and Wu [32] have recently obtained lower bounds on the second-order nonlinearity of some classes of cubic monomial Boolean functions of form $f(x) = Tr_1^n(x^{2^{m+1}+3})$ and $f(x) = Tr_1^n(x^{2^m+2^{\frac{m+1}{2}}+3})$ respectively, where $n = 2m$, m odd which are known to have high first-order nonlinearity and deduced

$$nl_2(f) \geq 2^{2m-1} - \frac{1}{2}\sqrt{2^{5m/2+1} + 2^{3m+1} - 2^{2m} - 2^{3m/2+1}}.$$

The Walsh Spectrum of Boolean functions of above classes is three valued $[0, \pm 2^{m+1}]$. Below we give the comparison between the bounds of Theorem 2, Iwata-Kurosawa bounds [16], bounds of other classes which have high first-order nonlinearity and the Hamming distances of the furthest power functions from $\mathcal{R}(2, n)$ obtained by Fourquet and Tavernier [12].

n	4	6	8	10	12	14	16	18	20
Bounds of Theorem 2	N/A	16	84	N/A	1688	7168	N/A	122880	501120
Iwata-Kurosawa's bounds	N/A	14	56	224	896	3584	14336	57344	229376
Bounds of Theorems 1, 2 [32]	2	15	79	375	1666	7125	29786	122706	500765
Bounds of Theorem 3 [32]	0	N/A	62	N/A	1525	N/A	28615	N/A	491277
Bounds of Theorem 2 [13]	N/A	15	N/A	378	1524	7139	N/A	122758	491288
Bounds of Dillon bent [5]	0	10	64	331	1536	6744	28672	119487	491520
Hamming distances in [12]	2	18	84	400	1760	–	–	–	–

From the above table it is observed that lower bound obtained in Theorem 2 is greater than those obtained for several known classes of Boolean functions having high first-order nonlinearities. Thus we identify a class of bent functions with high second-order nonlinearity.

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

[3] C. Carlet, On the Higher Order Nonlinearities of Algebraic Immune Functions, in: Proceedings of the CRYPTO 2006, LNCS 4117, pp. 584-601.

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

[5] C. Carlet, On the nonlinearity profile of the Dillon function, http://eprint.iacr.org/2009/577.pdf.

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

[7] C. Carlet, Vectorial Boolean Functions for Cryptography, in: Boolean Methods and Models, Y. Crama and P. Hammer (Eds.) Cambridge Univ. Press. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html (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] N. Courtois, W. Meier, Algebraic attacks on stream ciphers with linear feedback, in: Proceedings of the EUROCRYPT 2003, LNCS, vol. 2656, pp. 345-359.

[10] C. Ding, G. Xiao, W. Shan, The Stability Theory of Stream Ciphers, LNCS, vol. 561. Springer, Heidelberg (1991).

[11] 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.

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

[13] S. Gangopadhyay, S. Sarkar and R. Telang, On the lower bounds of the second order nonlinearities of some Boolean functions, Information Sciences 180 (2010) 266-273.

[14] R. Gode and S. Gangopadhyay, On second order nonlinearities of cubic monomial Boolean functions, http://eprint.iacr.org/2009/502.pdf.

[15] J. Golić, Fast low order approximation of cryptographic functions, in: Proceedings of the EUROCRYPT 1996, LNCS, vol. 1996, pp. 268-282.

[16] T. Iwata and K. Kurosawa, Probabilistic higher order differential attack and higher order bent functions, in: Proceedings of the ASIACRYPT 1999, LNCS, vol. 1716, pp. 62-74.

[17] 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 2006, LNCS, vol. 4329, pp. 266-279.

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

[19] 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 2007, LNCS, vol. 4851, pp. 266-279.

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

[21] G. Leander, G. McGuire, Construction of bent functions from near-bent functions, Journal of Combinatorial Theory, Series A, 116 (2009) 960-970.

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

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

[24] M. Matsui, Linear cryptanalysis method for DES cipher, in: Proceedings of the EUROCRYPT 1993, LNCS, vol. 765, pp. 386-397.

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

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

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

[28] 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.

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

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

[31] T. Shimoyama and T. Kaneko, Quadratic Relation of S-box and Its Application to the Linear Attack of Full Round DES, in: Proceedings of CRYPTO 1998, LNCS, Vol. 1462, pp. 200-211.

[32] 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.