Noname manuscript No.
(will be inserted by the editor)

Third-order nonlinearities of some biquadratic monomial Boolean functions

Brajesh Kumar Singh

Received: April 2012 / Accepted: date

Abstract In this paper, we estimate the lower bounds on third-order nonlinearities of some biquadratic monomial Boolean functions of the form $Tr_1^n(\lambda x^d)$ for all $x \in \mathbb{F}_{2^n}$, where $\lambda \in \mathbb{F}_{2^n}^*$,

(1) $d = 2^i + 2^j + 2^k + 1$, i, j, k are integers such that $i > j > k \geq 1$ and $n > 2i$.
(2) $d = 2^{3\ell} + 2^{2\ell} + 2^{\ell} + 1$, ℓ is a positive integer such that $\gcd(i, n) = 1$ and $n > 6$.

Keywords Boolean functions · Walsh-Hadamard spectrum · Third-order nonlinearities · Linearized polynomial

1 Introduction

Let $\mathscr{B}_n$ be the set of all Boolean functions on n variables and let r be a positive integer smaller than n. Reed–Muller code, $RM(r,n)$, of order r and length 2^n is the set of all Boolean functions in $\mathscr{B}_n$ with algebraic degree less than or equal to r. The rth-order nonlinearity of any function $f \in \mathscr{B}_n$ is defined as $nl_r(f) = \min_{h \in RM(r,n)} d(f,h)$. The sequence of values, $nl_r(f)$, $1 \leq r \leq n-1$, is said to be the nonlinearity profile of f. Since $RM(r-1,n) \subset RM(r,n)$, therefore $nl_r(f) \leq nl_{r-1}(f)$.

The first order nonlinearity of f is $nl_1(f)$, is the nonlinearity of f which we denote by $nl(f)$. The nonlinearity of a Boolean function f is related to the immunity of f against "best affine approximation attacks" [9] and "fast correlation attacks" [14], when f is used as a combiner function or a filter function in a stream cipher. Attacks based on higher-order approximations of Boolean functions are found in Golić [9], Courtois [6]. Computing rth-order nonlinearity is not an easy task $(r \geq 2)$. Unlike the first-order nonlinearity there is no efficient algorithms to compute second-order nonlinearities for $n \geq 11$. Most efficient algorithm due to Fourquet and Tavernier [7] works for $n \leq 11$ and, up to $n = 13$ for some special functions. Thus, there is a need to construct Boolean functions with high rth-order nonlinearity. The following is the best known asymptotic upper bound on $nl_3(f)$ due to Carlet and Mesnager [5]

$$nl_3(f) \leq 2^{n-1} - \sqrt{15} \cdot (1+\sqrt{2}) \cdot 2^{\frac{n}{2}-1} + O(n).$$

Carlet [3] developed a technique for computing lower bounds of higher-order nonlinearities of Boolean functions recursively and using this approach he has obtained the lower bounds of nonlinearity profiles for functions belonging to several classes of functions such as Kasami functions, Welch functions, inverse functions etc.. The classes of Boolean functions for which the lower bound on third nonlinearity is known are inverse functions [3], Dillon functions [4] and Kasami functions, $f(x) = Tr_1^n(\lambda x^{57})$ [8]. In this paper, we deduce the lower bounds on third-order nonlinearities of some biquadratic monomial Boolean functions of the form $Tr_1^n(\lambda x^d)$ for all $x \in \mathbb{F}_{2^n}$, where $\lambda \in \mathbb{F}_{2^n}^*$,

(1) $d = 2^i + 2^j + 2^k + 1$, i, j, k are integers such that $i > j > k \geq 1$ and $n > 2i$.
(2) $d = 2^{3\ell} + 2^{2\ell} + 2^{\ell} + 1$, ℓ is a positive integer such that $\gcd(i, n) = 1$ and $n > 6$.

Remainder of the paper is organized as follows: The main results on lower bounds of third-order nonlinearities are presented in Section 3. The numerical compression of our bounds with the previous known results is provided in Section 4. Section 5 is conclusion.

Research supported by CSIR, INDIA.

B. K. Singh
Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee 247667 INDIA
E-mail: bksingh0584@gmail.com

2 Preliminaries

Let $\mathbb{F}_{2^n}$ be the finite field consisting of 2^n elements. The group of units of $\mathbb{F}_{2^n}$, denoted by $\mathbb{F}_{2^n}^*$, is a cyclic group consisting of 2^n-1 elements. An element $\alpha \in \mathbb{F}_{2^n}$ is said to be a primitive element if it is a generator of the multiplicative group $\mathbb{F}_{2^n}^*$. Any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables. Let $\mathbb{Z}$ and $\mathbb{Z}_q$, where q is a positive integer, denote the ring of integers and integers modulo q, respectively. A cyclotomic coset modulo 2^n-1 of $s \in \mathbb{Z}$ is defined as [13, pp. 104]

$$C_s = \{s, s2, s2^2, \ldots, s2^{n_s-1}\}, \tag{1}$$

where n_s is the smallest positive integer such that $s \equiv s2^{n_s} \pmod{2^n-1}$. It is a convention to choose the subscript s to be the smallest integer in C_s and refer to it as the coset leader of C_s and n_s denotes the size of C_s. The trace function $Tr_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined as

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

The functions $(x,y) \mapsto Tr_1^n(xy)$ are inner products on $\mathbb{F}_{2^n}$. The trace representation [10] of a function $f \in \mathscr{B}_n$ is

$$f(x) = \sum_{k \in \Gamma(n)} Tr_1^{n_k}(A_k x^k) + A_{2^n-1} x^{2^n-1}, \text{ for all } x \in \mathbb{F}_{2^n}, \tag{3}$$

where $\Gamma(n)$ is the set of all coset leaders modulo 2^n-1 and $A_k \in \mathbb{F}_{2^{n_k}}$, $A_{2^n-1} \in \mathbb{F}_2$, for all $k \in \Gamma(n)$. A Boolean function is said to be a *monomial trace function* (sometimes *monomial Boolean function*) or said to "*have monomial trace representation*" if its trace representation consists of only one trace term. The *binary representation* of an integer $d \in \mathbb{Z}$ is

$$d = d_{m-1}2^{m-1} + d_{m-2}2^{m-2} + \ldots + d_1 2 + d_0, \tag{4}$$

where $d_0, d_1, \ldots, d_{m-1} \in \{0,1\}$. The Hamming weight of d is $w_H(d) = \sum_{i=0}^{m-1} d_i$, where the sum is over $\mathbb{Z}$. The algebraic degree, denoted by $\deg(f)$, of $f \in \mathscr{B}_n$, as represented in (3), is the largest positive integer w for which $w_H(k) = w$ and $A_k \neq 0$. The support of $f \in \mathscr{B}_n$ is $supp(f) = \{x \in \mathbb{F}_{2^n} : f(x) \neq 0\}$. The weight of f is $w_H(f) = |\{x \in \mathbb{F}_{2^n} : f(x) \neq 0\}|$, where $|S|$ is the cardinality of any set S. The Hamming distance between two functions $f, g \in \mathscr{B}_n$ is defined by $d(f,g) = |\{x \in \mathbb{F}_{2^n} : f(x) \neq g(x)\}|$.

The *Walsh–Hadamard transform* of $f \in \mathscr{B}_n$ at $\lambda \in \mathbb{F}_{2^n}$ is defined as

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

The multiset $\{W_f(\lambda) : \lambda \in \mathbb{F}_{2^n}\}$ is said to be the *Walsh-Hadamard spectrum* of f. The frequency distribution of the values in the Walsh-Hadamard spectrum of f is referred to as the *weight distribution* of the Walsh-Hadamard spectrum of f. The nonlinearity of a Boolean function $f \in \mathscr{B}_n$ in terms of its Walsh-Hadamard spectrum is given by

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

By Parseval's identity,

$$\sum_{\lambda \in \mathbb{F}_2^n} W_f(\lambda)^2 = 2^{2n},$$

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

Definition 1 [15] A function $f \in \mathscr{B}_n$ (for even n) is said to be a bent function if and only if $W_f(\lambda) \in \{2^{\frac{n}{2}}, -2^{\frac{n}{2}}\}$ for all $\lambda \in \mathbb{F}_{2^n}$ or equivalently f is bent if and only if $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$.

Definition 2 The derivative of $f \in \mathscr{B}_n$ with respect to $a \in \mathbb{F}_{2^n}$ is defined as

$$D_a f(x) = f(x) + f(x+a) \text{ for all } x \in \mathbb{F}_{2^n}.$$

The higher-order derivatives of a Boolean function are defined as follows.

Definition 3 Let V be an r-dimensional subspace of $\mathbb{F}_2^n$ generated by $a_1, \ldots, a_r$, i.e., $V = \langle a_1, \ldots, a_r \rangle$. The rth-order derivative of $f \in \mathscr{B}_n$ with respect to V, is the function $D_V f \in \mathscr{B}_n$, defined by $D_V f(x) = D_{a_1} \ldots D_{a_r} f(x)$.

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

The notion of rth-order bent functions have introduced by Iwata, Kurosawa [11] which is defined as follows.

Definition 4 [11] For any positive integer $r \leq n-3$, a function $f \in \mathscr{B}_n$ is said to be rth-order bent if and only if

$$nl_r(f) \geq \begin{cases} 2^{n-r-3}(r+4), & \text{if } r = 0 \mod 2, \\ 2^{n-r-3}(r+5), & \text{if } r = 1 \mod 2. \end{cases}$$

Following are some results on recursive lower bounds on third-order nonlinearities due to Carlet [3] which we use to estimate our bounds.

Proposition 1 *[3, Proposition 2] Let $f \in \mathscr{B}_n$. Then*

$$nl_3(f) \geq \frac{1}{4} \max_{a_1,a_2 \in \mathbb{F}_2^n} nl(D_{a_2}D_{a_1}f).$$

Proposition 2 *[3, Eq. 1] Let $f \in \mathscr{B}_n$. Then*

$$nl_3(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{\sum_{a \in \mathbb{F}_2^n} \sqrt{2^{2n} - 2\sum_{b \in \mathbb{F}_2^n} nl(D_aD_bf)}}.$$

The following result known as McEliece's Theorem is useful for improving the bounds of the rth-order nonlinearities.

Proposition 3 *[13, Chap. 15, Cor. 13] The rth-order nonlinearities of a Boolean function $f \in \mathscr{B}_n$ with algebraic degree d, is divisible by $2^{\lceil \frac{n}{d} \rceil - 1}$.*

Following proposition is due to Bracken et al. [1] which provides an information on the zeroes of the linearized polynomials [12,13] of particular type.

Proposition 4 *[1, Cor. 1] Let $L(x) = \sum_{i=0}^{v} c_i x^{2^{ik}}$ be a linearized polynomial over $\mathbb{F}_{2^n}$, where v,k are positive integers such that $\gcd(n,k) = 1$. Then zeroes of the linearized polynomial $L(x)$ in $\mathbb{F}_{2^n}$ are at most 2^v.*

2.1 Quadratic Boolean Functions

Suppose $f \in \mathscr{B}_n$ be a quadratic Boolean function. The bilinear form [13] associated with f is defined by $B(x,y) = f(0) + f(x) + f(y) + f(x+y)$ and the kernel, $\mathscr{E}_f$, of $B(x,y)$ is the subspace of $\mathbb{F}_{2^n}$ defined by

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

Any element $c \in \mathscr{E}_f$ is said to be a linear structure of f.

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.*

If $f \in \mathscr{B}_n$ is a quadratic Boolean function then the weight distribution of the Walsh-Hadamard spectrum to f depends only on the dimension k of $\mathscr{E}_f$ which is given in Table 1 [2,13].

Table 1 Weight distribution of the Walsh-Hadamard spectrum of a quadratic Boolean function $f \in \mathscr{B}_n$

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

3 Main results

In this section, we deduce the lower bounds of third-order nonlinearities of monomial Boolean functions of degree 4.

Theorem 1 *Let $f_\lambda(x) = Tr_1^n(\lambda x^{2^i+2^j+2^k+1})$, for all $x \in \mathbb{F}_{2^n}$, where $\lambda \in \mathbb{F}_{2^n}^*$, i,j,k are integers such that $i > j > k \geq 1$ and $n > 2i$. Then*

$$nl_3(f_\lambda) \geq \begin{cases} 2^{n-3} - 2^{\frac{n+2i-6}{2}}, & \text{if } n = 0 \mod 2, \\ 2^{n-3} - 2^{\frac{n+2i-7}{2}}, & \text{if } n = 1 \mod 2. \end{cases} \tag{5}$$

In particular, if $\gcd(j-k,n) = 1$, *then*

$$nl_3(f_\lambda) \geq \begin{cases} 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{\frac{3n+2i}{2}} + 2^{n+1} - 2^{\frac{n+2i+2}{2}}}}, & \text{if } n = 0 \mod 2, \\ 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{\frac{3n+2i-1}{2}} + 2^{n+1} - 2^{\frac{n+2i+1}{2}}}}, & \text{if } n = 1 \mod 2. \end{cases} \tag{6}$$

Proof Derivative of f_λ with respect to $a \in \mathbb{F}_{2^n}^*$ is

$$\begin{aligned} D_a f_\lambda(x) &= f_\lambda(x+a) + f_\lambda(x) = Tr_1^n(\lambda(x+a)^{2^i+2^j+2^k+1}) + Tr_1^n(\lambda x^{2^i+2^j+2^k+1}) \\ &= Tr_1^n(\lambda(ax^{2^i+2^j+2^k} + a^{2^i}x^{2^j+2^k+1} + a^{2^j}x^{2^i+2^k+1} + a^{2^k}x^{2^i+2^j+1})) + q(x), \end{aligned}$$

where q is a quadratic Boolean function. The second derivative $D_b D_a f_\lambda$ with respect to $a,b \in \mathbb{F}_{2^n}^*$, where $a \neq b$ is

$$\begin{aligned} D_b D_a f_\lambda(x) &= f_\lambda(x+a+b) + f_\lambda(x+a) + f_\lambda(x+b) + f_\lambda(x) = Tr_1^n(\lambda(x+a+b)^{2^i+2^j+2^k+1}) \\ &+ Tr_1^n(\lambda(x+b)^{2^i+2^j+2^k+1}) + Tr_1^n(\lambda(x+a)^{2^i+2^j+2^k+1}) + Tr_1^n(\lambda x^{2^i+2^j+2^k+1}) \\ &= l(x) + Tr_1^n(\lambda((ab^{2^k} + a^{2^k}b)x^{2^i+2^j} + (ab^{2^j} + a^{2^j}b)x^{2^i+2^k} + (ab^{2^i} + a^{2^i}b)x^{2^j+2^k} \\ &+ (a^{2^j}b^{2^k} + a^{2^k}b^{2^j})x^{2^i+1} + (a^{2^i}b^{2^k} + a^{2^k}b^{2^i})x^{2^j+1} + (a^{2^i}b^{2^j} + a^{2^j}b^{2^i})x^{2^k+1})), \end{aligned}$$

where l is an affine function. If $D_b D_a f_\lambda$ is quadratic, then the Walsh-Hadamard spectrum of $D_b D_a f_\lambda$ is equivalent to the Walsh-Hadamard spectrum of the function h_λ obtained by removing l from $D_b D_a f_\lambda$.

$$\begin{aligned} h_\lambda(x) = Tr_1^n(\lambda((&ab^{2^k} + a^{2^k}b)x^{2^i+2^j} + (ab^{2^j} + a^{2^j}b)x^{2^i+2^k} + (a^{2^j}b^{2^k} + a^{2^k}b^{2^j})x^{2^i+1} \\ &+ (ab^{2^i} + a^{2^i}b)x^{2^j+2^k} + (a^{2^i}b^{2^k} + a^{2^k}b^{2^i})x^{2^j+1} + (a^{2^i}b^{2^j} + a^{2^j}b^{2^i})x^{2^k+1})). \end{aligned}$$

Since $\mathscr{E}_{h_\lambda} = \{x \in \mathbb{F}_{2^n} : B(x,y) = 0 \text{ for all } y \in \mathbb{F}_{2^n}\}$, where $B(x,y)$ is the bilinear form associated with h_λ. Using $y^n = y$ and $Tr_1^n(x)^{2^i} = Tr_1^n(x)$ for all $x,y \in \mathbb{F}_{2^n}$. We compute

$$\begin{aligned} B(x,y) &= h_\lambda(0) + h_\lambda(x) + h_\lambda(y) + h_\lambda(x+y) \\ &= Tr_1^n(\lambda(y^{2^i}((ab^{2^k} + a^{2^k}b)x^{2^j} + (ab^{2^j} + a^{2^j}b)x^{2^k} + (a^{2^j}b^{2^k} + a^{2^k}b^{2^j})x) \\ &\quad + y^{2^j}((ab^{2^k} + a^{2^k}b)x^{2^i} + (ab^{2^i} + a^{2^i}b)x^{2^k} + (a^{2^i}b^{2^k} + a^{2^k}b^{2^i})x) \\ &\quad + y^{2^k}((ab^{2^j} + a^{2^j}b)x^{2^i} + (ab^{2^i} + a^{2^i}b)x^{2^j} + (a^{2^i}b^{2^j} + a^{2^j}b^{2^i})x) \\ &\quad + y((a^{2^j}b^{2^k} + a^{2^k}b^{2^j})x^{2^i} + (a^{2^i}b^{2^k} + a^{2^k}b^{2^i})x^{2^j} + (a^{2^i}b^{2^j} + a^{2^j}b^{2^i})x^{2^k}))) \\ &= Tr_1^n(yP(x)), \text{ where} \end{aligned}$$

$$\begin{aligned} P(x) = &(\lambda(ab^{2^k} + a^{2^k}b)x^{2^j} + \lambda(ab^{2^j} + a^{2^j}b)x^{2^k} + \lambda(a^{2^j}b^{2^k} + a^{2^k}b^{2^j})x)^{2^{n-i}} \\ &+(\lambda(ab^{2^j} + a^{2^j}b)x^{2^i} + \lambda(ab^{2^i} + a^{2^i}b)x^{2^j} + \lambda(a^{2^i}b^{2^j} + a^{2^j}b^{2^i})x)^{2^{n-j}} \\ &+(\lambda(ab^{2^j} + a^{2^j}b)x^{2^i} + \lambda(ab^{2^i} + a^{2^i}b)x^{2^j} + \lambda(a^{2^i}b^{2^j} + a^{2^j}b^{2^i})x)^{2^{n-k}} \\ &+\lambda(a^{2^j}b^{2^k} + a^{2^k}b^{2^j})x^{2^i} + \lambda(a^{2^i}b^{2^k} + a^{2^k}b^{2^i})x^{2^j} + \lambda(a^{2^i}b^{2^j} + a^{2^j}b^{2^i})x^{2^k}. \end{aligned}$$

Therefore,

$$\mathscr{E}_{h_\lambda} = \{x \in \mathbb{F}_{2^n} : P(x) = 0 = P(x)^{2^i}\}. \tag{7}$$

Let $L_{(\lambda,a,b)}(x) = P(x)^{2^i}$. Using $x^n = x$, $y^n = y$, $a^n = a$, $b^n = b$ and $\lambda^n = \lambda$, for all $x,y,a,b,\lambda \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned}
L_{(\lambda,a,b)}(x) &= (P(x))^{2^i} = \lambda\left((ab^{2^j}+a^{2^j}b)x^{2^k}+(ab^{2^k}+a^{2^k}b)x^{2^j}+(a^{2^j}b^{2^k}+a^{2^k}b^{2^j})x\right)\\
&+ \lambda^{2^i}\left((a^{2^{i+j}}b^{2^{i+k}}+a^{2^{i+k}}b^{2^{i+j}})x^{2^{2i}}+(a^{2^{i+k}}b^{2^{2i}}+a^{2^{2i}}b^{2^{i+k}})x^{2^{i+j}}+(a^{2^{2i}}b^{2^{i+j}}+\right.\\
&\left. a^{2^{i+j}}b^{2^{2i}})x^{2^{i+k}}\right)+\lambda^{2^{i-j}}\left((a^{2^{i-j}}b^{2^i}+a^{2^i}b^{2^{i-j}})x^{2^{2i-j}}+(a^{2^{i-j}}b^{2^{2i-j}}+a^{2^{2i-j}}b^{2^{i-j}})x^{2^i}\right.\\
&+ \left.(a^{2^{2i-j}}b^{2^i}+a^{2^i}b^{2^{2i-j}})x^{2^{i-j}}\right)+\lambda^{2^{i-k}}\left((a^{2^{i-k}}b^{2^{i+j-k}}+a^{2^{i+j-k}}b^{2^{i-k}})x^{2^{2i-k}}\right.\\
&+ \left.(a^{2^{i-k}}b^{2^{2i-k}}+a^{2^{2i-k}}b^{2^{i-k}})x^{2^{i+j-k}}+(a^{2^{2i-k}}b^{2^{i+j-k}}+a^{2^{i+j-k}}b^{2^{2i-k}})x^{2^{i-k}}\right). \qquad (8)
\end{aligned}$$

The coefficient of x in $L_{(\lambda,a,b)}(x)$ is zero if and only if $a^{2^j}b^{2^k}+a^{2^k}b^{2^j}=0$, i.e., $a^{2^{j-k}}b+ab^{2^{j-k}}=0$ which implies that $b \in a\mathbb{F}_{2^{j-k}}$. Therefore, for every $0 \neq a,b \in \mathbb{F}_{2^n}$ such that $b \notin a\mathbb{F}_{2^{j-k}}$, the degree of linearized polynomial, $L_{(\lambda,a,b)}$ in x is at most 2^{2i}, this implies that $k(a,b) \leq 2i$ if n is even otherwise $k(a,b) \leq 2i-1$.
The Walsh-Hadamard transform of $D_bD_af_\lambda$ at $\mu \in \mathbb{F}_{2^n}$ is

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

Therefore,

$$nl(D_bD_af_\lambda) = \begin{cases} 2^{n-1}-2^{\frac{n+2i-2}{2}}, & \text{if } n=0 \mod 2,\\ 2^{n-1}-2^{\frac{n+2i-3}{2}}, & \text{if } n=1 \mod 2.\end{cases} \qquad (9)$$

Using Proposition 1, we have

$$nl_3(f_\lambda) \geq \begin{cases} 2^{n-3}-2^{\frac{n+2i-6}{2}}, & \text{if } n=0 \mod 2,\\ 2^{n-3}-2^{\frac{n+2i-7}{2}}, & \text{if } n=1 \mod 2.\end{cases}$$

In particular, if $\gcd(j-k,n)=1$, we have $k(a,b) \leq 2i$ if n is even otherwise $k(a,b) \leq 2i-1$ for all $a,b \in \mathbb{F}_{2^n}$ such that $a \neq 0$ and $b \notin a\mathbb{F}_2$. Therefore, Eq. (9) holds for all $a,b \in \mathbb{F}_{2^n}$ such that $a \neq 0$ and $b \notin a\mathbb{F}_2$.
Using Proposition 2, we have

– When $n = 0 \mod 2$

$$\begin{aligned}
nl_3(g_\lambda) &\geq 2^{n-1}-\frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{2n}-2(2^n-2)(2^{n-1}-2^{\frac{n+2i-2}{2}})}}\\
&= 2^{n-1}-\frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{\frac{3n+2i}{2}}+2^{n+1}-2^{\frac{n+2i+2}{2}}}}. \qquad (10)
\end{aligned}$$

– When $n = 1 \mod 2$

$$\begin{aligned}
nl_3(g_\lambda) &\geq 2^{n-1}-\frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{2n}-2(2^n-2)(2^{n-1}-2^{\frac{n+2i-3}{2}})}}\\
&= 2^{n-1}-\frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{\frac{3n+2i-1}{2}}+2^{n+1}-2^{\frac{n+2i+1}{2}}}}. \qquad (11)
\end{aligned}$$

□

Theorem 2 *Let $g_\lambda(x) = Tr_1^n(\lambda x^{2^{3\ell}+2^{2\ell}+2^\ell+1})$, for all $x \in \mathbb{F}_2^n$ and $\lambda \in \mathbb{F}_{2^n}^*$, where ℓ is a positive integer such that $\gcd(\ell,n)=1$ and $n>6$. Then*

$$nl_3(g_\lambda) \geq \begin{cases} 2^{n-1}-\frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{\frac{3n+6}{2}}+2^{n+1}-2^{\frac{n+8}{2}}}}, & \text{if } n=0 \mod 2,\\ 2^{n-1}-\frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{\frac{3n+5}{2}}+2^{n+1}-2^{\frac{n+7}{2}}}}, & \text{if } n=1 \mod 2.\end{cases}$$

Proof The proof is similar to that of Theorem 1 upto Eq. (8). Here the kernel of $B(x,y)$ associated with $D_bD_ag_\lambda$ is $\mathscr{E} = \{x \in \mathbb{F}_{2^n} : P(x) = 0 = L_{(\lambda,a,b)}(x)\}$, where $L_{(\lambda,a,b)}(x)$ is obtained by replacing i, j and k in (8) by $3\ell, 2\ell$ and ℓ respectively

$$\begin{aligned}
L_{(\lambda,a,b)}(x) = P(x)^{2^{3\ell}} &= \lambda^{2^{3\ell}}\Big((a^{2^{5\ell}}b^{2^{4\ell}} + a^{2^{4\ell}}b^{2^{5\ell}})x^{2^{6\ell}} + (a^{2^{4\ell}}b^{2^{6\ell}} + a^{2^{6\ell}}b^{2^{4\ell}})x^{2^{5\ell}} \\
&+ (a^{2^{6\ell}}b^{2^{5\ell}} + a^{2^{5\ell}}b^{2^{6\ell}})x^{2^{4\ell}}\Big) + \lambda^{2^{\ell}}\Big((a^{2^{\ell}}b^{2^{3\ell}} + a^{2^{3\ell}}b^{2^{\ell}})x^{2^{4\ell}} + (a^{2^{\ell}}b^{2^{4\ell}} + a^{2^{4\ell}}b^{2^{\ell}})x^{2^{3\ell}} \\
&+ (a^{2^{4\ell}}b^{2^{3\ell}} + a^{2^{3\ell}}b^{2^{4\ell}})x^{2^{\ell}}\Big) + \lambda^{2^{2\ell}}\Big((a^{2^{2\ell}}b^{2^{4\ell}} + a^{2^{4\ell}}b^{2^{2\ell}})x^{2^{5\ell}} \\
&\quad + (a^{2^{2\ell}}b^{2^{5\ell}} + a^{2^{5\ell}}b^{2^{2\ell}})x^{2^{4\ell}} + (a^{2^{5\ell}}b^{2^{4\ell}} + a^{2^{4\ell}}b^{2^{5\ell}})x^{2^{2\ell}}\Big) \\
&+ \lambda(ab^{2^{2\ell}} + a^{2^{2\ell}}b)x^{2^{\ell}} + \lambda(ab^{2^{\ell}} + a^{2^{\ell}}b)x^{2^{2\ell}} + \lambda(a^{2^{2\ell}}b^{2^{\ell}} + a^{2^{\ell}}b^{2^{2\ell}})x. \qquad (12)
\end{aligned}$$

The coefficient of x in $L_{(\lambda,a,b)}(x)$ is zero if and only if $a^{2^{2\ell}}b^{2^{\ell}} + a^{2^{\ell}}b^{2^{2\ell}} = 0$, i.e., $a^{2^{\ell}}b + ab^{2^{\ell}} = 0$. But $\gcd(\ell,n) = 1$, therefore, by Proposition 4, we have $b \in a\mathbb{F}_2$. Moreover, $L_{(\lambda,a,b)}(x)$ is of the form $\sum_{i=0}^{6} c_i x^{2^{i\ell}}$, therefore by Proposition 4, the equation $L_{(\lambda,a,b)}(x) = 0$ has at most 2^6 roots for all $a, b \in \mathbb{F}_{2^n}$ such that $a \neq 0$ and $b \notin a\mathbb{F}_2$, this implies that $k(a,b) \leq 6$ if n is even otherwise $k(a,b) \leq 5$. The Walsh-Hadamard transform of $D_bD_ag_\lambda$ at $\mu \in \mathbb{F}_{2^n}$ is

$$W_{D_bD_ag_\lambda}(\mu) \leq \begin{cases} 2^{\frac{n+6}{2}}, & \text{if } n = 0 \mod 2, \\ 2^{\frac{n+5}{2}}, & \text{if } n = 1 \mod 2. \end{cases}$$

Therefore,

$$nl(D_bD_ag_\lambda) \geq \begin{cases} 2^{n-1} - 2^{\frac{n+4}{2}}, & \text{if } n = 0 \mod 2, \\ 2^{n-1} - 2^{\frac{n+3}{2}}, & \text{if } n = 1 \mod 2. \end{cases}$$

Using Proposition 1, we have

$$nl_3(g_\lambda) \geq \begin{cases} 2^{n-3} - 2^{\frac{n}{2}}, & \text{if } n = 0 \mod 2, \\ 2^{n-3} - 2^{\frac{n-1}{2}}, & \text{if } n = 1 \mod 2. \end{cases}$$

Using Proposition 2, we have

– When $n = 0 \mod 2$

$$\begin{aligned}
nl_3(g_\lambda) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{2n} - 2(2^n-2)(2^{n-1} - 2^{\frac{n+4}{2}})}} \\
&= 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{\frac{3n+6}{2}} + 2^{n+1} - 2^{\frac{n+8}{2}}}}. \qquad (13)
\end{aligned}$$

– When $n = 1 \mod 2$

$$\begin{aligned}
nl_3(g_\lambda) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{2n} - 2(2^n-2)(2^{n-1} - 2^{\frac{n+3}{2}})}} \\
&= 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{\frac{3n+5}{2}} + 2^{n+1} - 2^{\frac{n+7}{2}}}}. \qquad (14)
\end{aligned}$$

□

Remark 1 Let $f \in \mathscr{B}_n$ a biquadratic Boolean function. If there exists at least elements $a, b \in \mathbb{F}_2^n$ such that D_bD_af is quadratic, then the lower bound of third-order nonlinearity of $f \in \mathscr{B}_n$ is at least 2^{n-4}. This result is follows from Proposition 1 and the fact that the nonlinearity of any quadratic function in $\mathscr{B}_n$ is at least 2^{n-2} [3,16].

4 Comparison

In Table 2 and Table 3, we present the computational results of lower bounds of third-order nonlinearities obtained by Theorem 1 for $i = 3,4,5$ and j,k are taken in such a way that $\gcd(j-k,n) = 1$. We compare these bounds with the general bounds on third-order nonlinearity for any biquadratic Boolean function, i.e., $nl_3(f) \geq 2^{n-4}$. It is observed that the bounds for $i = 3,4$ are efficiently large and decreases with increasing the value of i. It is claimed that class (1) is more general class of biquadratic monomial Boolean functions

Table 2 The lower bounds on the third-order nonlinearities obtained by Theorem 1 for odd n and $i = 3,4,5$

n	7	9	11	13	15	17	19
$i = 3$	11	75	415	2047	9493	42361	184199
$i = 4$	$--$	41	330	1660	8191	37979	169457
$i = 5$	$--$	$--$	163	1200	6642	32767	151923
general bounds	8	32	128	512	2048	8192	32768

Table 3 The lower bounds on the third-order nonlinearities obtained by Theorem 1 for for even n and $i = 3,4,5$

n	8	10	12	14	16	18	20
$i = 3$	21	150	830	4094	18988	84726	368407
$i = 4$	$--$	82	560	3321	16283	75960	338919
$i = 5$	$--$	$--$	326	2400	13284	65535	303849
general bounds	16	64	256	1024	4096	16384	65536

containing several classes of highly nonlinear Boolean functions. For example, Kasami functions of degree 4 coincide with class (1) when $i = 5, j = 4, k = 3$.

In Table 4 and Table 5, we present the computational results on lower bounds of third-order nonlinearities obtained by Theorem 2 on applying Proposition 3 and compare these values with known classes of functions [8,3,11]. It is observed from Table 4 and Table 5 that the bound obtained by Theorem 2 is better than the bounds obtained by Gode et al. [8] for Kasami functions: $Tr(\lambda x^{57})$, Iwata and Kurosawa's general bound [11] for all $n > 8$. These bounds are also improved upon Carlet's [3] bound for inverse function when n is odd (see Table 4) or $n = 8,12$, and equal for the rest values of even n (see Table 5).

Table 4 Comparison of the value of lower bounds on third-order nonlinearities obtained by Theorem 2 with the bound obtained in [8], [11] and [3] for odd n

n	7	9	11	13	15	17	19
Bounds in Theorem 2	12	76	416	2048	9496	42368	184208
Bounds in [8]	8	$--$	240	992	$--$	16256	65280
Bounds in [11]	16	64	256	1024	4096	16384	65536
Carlet's bound [3]	6	60	360	1864	8872	40272	177168

Table 5 Comparison of the value of lower bounds on third-order nonlinearities obtained by Theorem 2 with the bound obtained in [8], [11] and [3] for even n

n	8	10	12	14	16	18	20
Bounds in Theorem 2	22	152	832	4096	18992	84736	368416
Bounds in [8]	28	120	$--$	2016	$--$	$--$	130816
Bounds in [11]	32	128	512	2048	8192	32768	131072
Carlet's bound [3]	20	152	828	4096	18992	84736	368416

5 Conclusion

In this paper, we obtained the lower bounds of third-order nonlinearities of two more general classes of biquadratic monomial Boolean functions. It is demonstrated that in some cases our bounds are better than the bounds obtained previously.

6 Acknowledgement

The author would like to thanks the *Council of Scientific and Industrial Research India* for supporting his research.

References

1. Bracken, C., Byrne, E., Markin, N., MacGuire, G.: Determining the Nonlinearity a New Family of APN Functions. AAECC, LNCS, 4851, Springer Verlag, 72-79 (2007).

2. Canteaut, A., Charpin, P., Kyureghyan, G. M.: A New Class of Monomial Bent Functions. Finite Fields and Their Applications, 14, 221-241 (2008).
3. Carlet, C.: Recursive Lower Bounds on the Nonlinearity Profile of Boolean Functions and Their Applications. IEEE Trans. Inform. Theory, 54(3), 1262-1272 (2008).
4. Carlet, C.: More vectorial Boolean functions with unbounded nonlinearity profile, Int'l J. of Found. of Comp. Sci., 22(6), 1259-1269, 2011.
5. Carlet, C., Mesnager, S.: Improving the Upper Bounds on the Covering Radii of Binary Reed-Muller Codes. IEEE Trans. Inform. Theory, 53 (1), 162-173 (2007).
6. Courtois, N.: Higher Order Correlation Attacks, XL Algorithm and Cryptanalysis of Toyocrypt. In Proc. of the ICISC'02, LNCS, 2587, 182-199, Springer Verlag (2002).
7. Fourquet, R., Tavernier, C.: An Improved List Decoding Algorithm for the Second Order Reed-Muller Codes and its Applications. Designs, Codes and Cryptography, 49, 323-340 (2008).
8. Gode, R., Gangopadhyay, S.: Third-Order Nonlinearities of a Subclass of Kasami Functions. Crypt. Communi.-Discrete Structures, Boolean Functions and Sequences, 2, 69-83 (2010).
9. Golic, J.: Fast Low Order Approximation of Cryptographic Functions. In Proc. of the EUROCRYPT'96, LNCS, Springer Verlag, 1070, 268-282 (1996).
10. S. W. Golomb and G. Gong, *Signal design for good correlation: for wireless communication, cryptography and radar*, Cambridge University Press, ISBN 0521821045, 2005.
11. Iwata, T., Kurosawa, K.: Probabilistic Higher Order Differential Attack and Higher Order Bent Functions. In Proc. of the ASIACRYPT'99, LNCS, Springer Verlag, 1716, 62-74, (1999).
12. Lidl, R., H. Niederreiter, H.: Introduction to Finite Fields and Their Applications, Cambridge University Press (1983).
13. MacWilliams, F. J., Sloane, N. J. A.: The Theory of Error Correcting Codes. North-Holland, Amsterdam (1977).
14. Meier, W., Staffelbach O.: Nonlinearity criteria for cryptographic functions. Adv. in Crypto. EUROCRYPT'89, LNCS, Springer Verlag, 434, 549562 (1990).
15. Rothaus, O. S.: On bent functions. J. Combin. Theory (A), 20, 300-305 (1976).
16. Seberry, J., Zhang, X. M. and Zheng, Y.: Relationships among nonlinearity criteria. Advances in Crypto. EUROCRYPT'94, LNCS, Springer-Verlag, 950, 376–388, (1995).