Hindawi Publishing Corporation
International Journal of Engineering Mathematics
Volume 2014, Article ID 937386, 7 pages
http://dx.doi.org/10.1155/2014/937386

Research Article

On Third-Order Nonlinearity of Biquadratic Monomial Boolean Functions

Brajesh Kumar Singh

Department of Mathematics, School of Allied Sciences, Graphic Era Hill University, Dehradun, Uttarakhand 248002, India

Correspondence should be addressed to Brajesh Kumar Singh; bksingh0584@gmail.com

Received 30 January 2014; Accepted 28 February 2014; Published 1 April 2014

Academic Editor: J. A. Tenreiro Machado

The rth-order nonlinearity of Boolean function plays a central role against several known attacks on stream and block ciphers. Because of the fact that its maximum equals the covering radius of the rth-order Reed-Muller code, it also plays an important role in coding theory. The computation of exact value or high lower bound on the rth-order nonlinearity of a Boolean function is very complicated problem, especially when $r > 1$. This paper is concerned with the computation of the lower bounds for third-order nonlinearities of two classes of Boolean functions of the form $\mathrm{Tr}_1^n(\lambda x^d)$ for all $x \in \mathbb{F}_{2^n}$, $\lambda \in \mathbb{F}_{2^n}^*$, where (a) $d = 2^i + 2^j + 2^k + 1$, where i, j, and k are integers such that $i > j > k \geq 1$ and $n > 2i$, and (b) $d = 2^{3\ell} + 2^{2\ell} + 2^{\ell} + 1$, where ℓ is a positive integer such that $\gcd(\ell, n) = 1$ and $n > 6$.

1. Introduction

Boolean functions are the building blocks for the design and the security of symmetric cryptographic systems and for the definition of some kinds of error correcting codes, sequences, and designs. The rth-order nonlinearity, $\mathrm{nl}_r(f)$, of a Boolean function $f \in \mathscr{B}_n$ is defined by the minimum Hamming distance of f to $\mathrm{RM}(r,n)$-*Reed-Muller code* of length 2^n and order r ($\mathrm{RM}(r,n) := \{f \in \mathscr{B}_n : \deg(f) \leq r\}$). The nonlinearity of f is given by $\mathrm{nl}(f) = \mathrm{nl}_1(f)$ and is related to the immunity of f against *best affine approximation attacks* [1] and *fast correlation attacks* [2], when f is used as a combiner function or a filter function in a stream cipher. The rth-order nonlinearity is an important parameter, which measures the resistance of the function against various *low-order approximation attacks* [1, 3, 4]. In cryptographic framework, within a tradeoff with the other important criteria, the rth-order nonlinearity must be as large as possible; see [5–9]. Since, the maximal rth-order nonlinearity of all Boolean functions equals the *covering radius* of $\mathrm{RM}(r,n)$, it also has an application in coding theory. Besides these applications, an interesting connection between the rth-order nonlinearity and the *fast algebraic attacks* has been introduced, recently in [9], which claims that a cryptographic Boolean function should have high rth-order nonlinearity to resist the *fast algebraic attack*.

Unlike nonlinearity there is no efficient algorithm to compute second-order nonlinearities for $n > 11$. The most efficient algorithm is introduced by Fourquet and Tavernier [10] which works for $n \leq 11$ and up to $n = 13$ for some special functions. Thus, to identify a class of Boolean function with high rth-order nonlinearity, even for $r = 2$, is a very relevant area of research. In 2008, Carlet has devolved a technique to compute rth-order nonlinearity recursively in [11], and using this technique he has obtained the lower bounds of nonlinearity profiles for functions belonging to several classes of functions: Kasami functions, Welch functions, inverse functions, and so forth. Based on this technique, the lower bound for rth-order nonlinearity, for $r \geq 2$, is obtained for some specific classes of Boolean functions, in many articles; see, for example, [11–14] and the references therein. The best known asymptotic upper bound for $\mathrm{nl}_3(f)$ given by Carlet and Mesnager [15] is as follows:

$$\mathrm{nl}_3(f) \leq 2^{n-1} - \sqrt{15} \cdot \left(1 + \sqrt{2}\right) \cdot 2^{n/2-1} + O(n). \qquad (1)$$

The classes of Boolean functions for which the lower bound of third nonlinearity is known are inverse functions [11], Dillon functions [16], and Kasami functions, $f(x) = \mathrm{Tr}_1^n(\lambda x^{57})$ [12]. In this paper, we deduce the theoretical lower bounds on third-order nonlinearities of two classes of biquadratic

monomial Boolean functions $\mathrm{Tr}_1^n(\lambda x^d)$ for all $x \in \mathbb{F}_{2^n}$, where $\lambda \in \mathbb{F}_{2^n}^*$ and (a) $d = 2^i+2^j+2^k+1$, where i, j, and k are integers such that $i > j > k \geq 1$ and $n > 2i$, and (b) $d = 2^{3\ell}+2^{2\ell}+2^{\ell}+1$, where ℓ is a positive integer such that $\gcd(\ell, n) = 1$ and $n > 6$.

Remainder of the paper is organized as follows. In Section 2 some basic definitions and notations required for the subsequent sections are reviewed. 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.

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 $\mathbb{F}_{2^n}^*$. A function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables; the set of such functions is denoted by $\mathscr{B}_n$. 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

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

where n_s is the smallest positive integer such that $s \equiv s2^{n_s} \pmod{2^n - 1}$ [17, page 104]. 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 $\mathrm{Tr}_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined by $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ for all $x \in \mathbb{F}_{2^n}$. The trace representation [18] of a function $f \in \mathscr{B}_n$ is

$$f(x) = \sum_{k\in\Gamma(n)} \mathrm{Tr}_1^{n_k}\left(A_k x^k\right) + A_{2^n-1}x^{2^n-1}, \quad \forall x \in \mathbb{F}_{2^n}, \tag{3}$$

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* if its trace representation consists of single trace term. The *binary representation* of an integer $d \in \mathbb{Z}$ is

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

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 $\mathrm{supp}(f) = \{x \in \mathbb{F}_{2^n} : f(x) \neq 0\}$. 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 $d_H(f, g) = |\{x \in \mathbb{F}_{2^n} : f(x) \neq g(x)\}|$.

The *Walsh-Hadamard transform* (WHT) of a Boolean function $f \in \mathscr{B}_n$ at $\lambda \in \mathbb{F}_{2^n}$ is defined by $W_f(\lambda) := \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(\lambda x)}$. The nonlinearity of $f \in \mathscr{B}_n$ in terms of its *Walsh-Hadamard spectrum* (WHS) is given by

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2}\max_{\lambda\in\mathbb{F}_{2^n}} \left|W_f(\lambda)\right|. \tag{5}$$

The set $\{W_f(\lambda) : \lambda \in \mathbb{F}_{2^n}\}$ is referred to as the WHS of $f \in B_n$ which satisfies the Parseval's identity: $\sum_{\lambda\in\mathbb{F}_2^n} W_f(\lambda)^2 = 2^{2n}$ which implies that $\max\{|W_f(\lambda)| : \lambda \in \mathbb{F}_{2^n}\} \geq 2^{n/2}$, and so $\mathrm{nl}(f) \leq 2^{n-1} - 2^{(n/2)-1}$. The function $f \in \mathscr{B}_n$ achieving maximum possible nonlinearity $2^{n-1} - 2^{n/2-1}$ are said to be bent functions (exists only for even n), were introduced by Rothaus [19].

The derivative of $f \in \mathscr{B}_n$ with respect to $a \in \mathbb{F}_{2^n}$ is defined by $D_a f(x) = f(x) + f(x + a)$ for all $x \in \mathbb{F}_{2^n}$. The second-order derivatives of $f \in \mathscr{B}_n$ with respect to $V = \langle a, b\rangle$ is the Boolean function $D_V f \in \mathscr{B}_n$ which is defined by $D_V f(x) = D_b D_a f(x) = f(x) + f(x + a) + f(x + b) + f(x + a + b)$, where V is two-dimensional subspace of $\mathbb{F}_{2^n}$ generated by a and b; for details on higher derivatives, see [5, 11]. The rth-order nonlinearity of $f \in \mathscr{B}_n$ is defined as

$$\begin{aligned}\mathrm{nl}_r(f) &= \min_{h\in\mathrm{RM}(r,n)} d_H(f, h)\\ &= 2^{n-1} - \frac{1}{2}\max_{h\in\mathrm{RM}(r,n)}\left|\sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+h(x)}\right|.\end{aligned} \tag{6}$$

The sequence $\{\mathrm{nl}_r(f)\}_{r=1}^{n-1}$ is called the nonlinearity profile of f. Also, $\mathrm{nl}_r(f) \leq \mathrm{nl}_{r-1}(f)$ because $\mathrm{RM}(r-1, n) \subset \mathrm{RM}(r, n)$. The notion of rth-order bent functions was introduced by Iwata and Kurosawa [4]. A function $f \in \mathscr{B}_n$ is said to be rth-order bent (for $r \leq n-3$) if and only if $\mathrm{nl}_r(f) \geq 2^{n-r-3}(r+4)$, for even r, and $\mathrm{nl}_r(f) \geq 2^{n-r-3}(r+5)$, for odd r.

Carlet's [11] recursive lower bounds for third-order nonlinearities which we use to compute our bounds, are given below in Propositions 1 and 2.

Proposition 1 (see [11, Proposition 2]). *Let $f \in \mathscr{B}_n$; then $nl_3(f) \geq (1/4)\max\{nl(D_b D_a f) : a, b \in \mathbb{F}_{2^n}\}$.*

Proposition 2 (see [11, Equation (1)]). *Let $f \in \mathscr{B}_n$. Then*

$$nl_3(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{\sum_{a\in\mathbb{F}_{2^n}}\sqrt{2^{2n} - 2\sum_{b\in\mathbb{F}_{2^n}} nl(D_a D_b f)}}. \tag{7}$$

Proposition 3 (see [17, Chapter 15, Corollary 13] (*McEliece's theorem*)). *The rth-order nonlinearities of a Boolean function $f \in \mathscr{B}_n$ with algebraic degree d are divisible by $2^{\lceil n/d\rceil-1}$, where $\lceil u\rceil$ denotes the ceiling of u (the smallest integer greater than or equal to u).*

Proposition 4 (see [20, Corollary 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.*

The result in Proposition 4 above was introduced by Bracken et al. [20]. The bilinear form [17] associated with a quadratic Boolean function $f \in \mathscr{B}_n$ 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

$$\mathscr{E}_f = \left\{x \in \mathbb{F}_{2^n} : B(x, y) = 0 \ \forall y \in \mathbb{F}_{2^n}\right\}. \tag{8}$$

An element $c \in \mathscr{E}_f$ is called a linear structure of f. Next, if V is a vector space over a field $\mathbb{F}_q$ of characteristic 2 and $Q : V \to \mathbb{F}_q$ a quadratic form, then $\dim(V)$ and $\dim(\mathscr{E}_Q)$ have the same parity [21]. The distribution of the WHT values of a quadratic Boolean function $f \in \mathscr{B}_n$ is given in the following theorem which claims that the weight distribution of the values in the WHS of f depends only on the dimension k of $\mathscr{E}_f$.

Theorem 5 (see [17, 21]). *Let $f \in \mathscr{B}_n$ be a quadratic Boolean function and $k = \dim(\mathscr{E}_f)$, where $\mathscr{E}_f$ is defined in* (8)*; then the weight distribution of the WHT values of f is given by*

$$W_f(\lambda) = \begin{cases} 0, & 2^n - 2^{n-k} \text{ times}, \\ 2^{(n+k)/2}, & 2^{n-k-1} + (-1)^{f(0)} 2^{(n-k-2)/2} \text{ times}, \\ -2^{(n+k)/2}, & 2^{n-k-1} - (-1)^{f(0)} 2^{(n-k-2)/2} \text{ times}. \end{cases} \tag{9}$$

3. Main Results

In this section, using Carlet's recursive technique [11], the theoretical lower bounds for third-order nonlinearities of two general classes of monomial Boolean functions of degree 4 are obtained.

Theorem 6. *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 $\lambda \in \mathbb{F}_{2^n}^*$ and i, j, and k are integers such that $i > j > k \geq 1$ and $n > 2i$. Then*

$$nl_3(f_\lambda) \geq \begin{cases} 2^{n-3} - 2^{(n+2i-6)/2}, & \text{if } n = 0 \mod 2, \\ 2^{n-3} - 2^{(n+2i-7)/2}, & \text{if } n = 1 \mod 2. \end{cases} \tag{10}$$

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

$$nl_3(f_\lambda) \geq \begin{cases} 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{(3n+2i)/2} + 2^{n+1} - 2^{(n+2i+2)/2}}}, \\ \qquad \text{if } n = 0 \mod 2, \\ 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{(3n+2i-1)/2} + 2^{n+1} - 2^{(n+2i+1)/2}}}, \\ \qquad \text{if } n = 1 \mod 2. \end{cases} \tag{11}$$

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

$$\begin{aligned} D_a f_\lambda(x) &= f_\lambda(x+a) + f_\lambda(x) \\ &= \mathrm{Tr}_1^n\left(\lambda(x+a)^{2^i+2^j+2^k+1}\right) + \mathrm{Tr}_1^n\left(\lambda x^{2^i+2^j+2^k+1}\right) \\ &= \mathrm{Tr}_1^n\Big(\lambda\Big(a x^{2^i+2^j+2^k} + a^{2^i} x^{2^j+2^k+1} \\ &\qquad + a^{2^j} x^{2^i+2^k+1} + a^{2^k} x^{2^i+2^j+1}\Big)\Big) + q(x), \end{aligned} \tag{12}$$

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

$$\begin{aligned} &D_b D_a f_\lambda(x) \\ &\quad = f_\lambda(x+a+b) + f_\lambda(x+a) + f_\lambda(x+b) + f_\lambda(x) \\ &\quad = \mathrm{Tr}_1^n\left(\lambda(x+a+b)^{2^i+2^j+2^k+1}\right) + \mathrm{Tr}_1^n\left(\lambda(x+b)^{2^i+2^j+2^k+1}\right) \\ &\qquad + \mathrm{Tr}_1^n\left(\lambda(x+a)^{2^i+2^j+2^k+1}\right) + \mathrm{Tr}_1^n\left(\lambda x^{2^i+2^j+2^k+1}\right) \\ &\quad = l(x) + \mathrm{Tr}_1^n\Big(\lambda\Big(\left(ab^{2^k} + a^{2^k}b\right)x^{2^i+2^j} \\ &\qquad + \left(ab^{2^j} + a^{2^j}b\right)x^{2^i+2^k} \\ &\qquad + \left(ab^{2^i} + a^{2^i}b\right)x^{2^j+2^k} \\ &\qquad + \left(a^{2^j}b^{2^k} + a^{2^k}b^{2^j}\right)x^{2^i+1} \\ &\qquad + \left(a^{2^i}b^{2^k} + a^{2^k}b^{2^i}\right)x^{2^j+1} \\ &\qquad + \left(a^{2^i}b^{2^j} + a^{2^j}b^{2^i}\right)x^{2^k+1}\Big)\Big), \end{aligned} \tag{13}$$

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

$$\begin{aligned} &h_\lambda(x) \\ &\quad = \mathrm{Tr}_1^n\Big(\lambda\Big(\left(ab^{2^k} + a^{2^k}b\right)x^{2^i+2^j} + \left(ab^{2^j} + a^{2^j}b\right)x^{2^i+2^k} \\ &\qquad + \left(a^{2^j}b^{2^k} + a^{2^k}b^{2^j}\right)x^{2^i+1} + \left(ab^{2^i} + a^{2^i}b\right)x^{2^j+2^k} \\ &\qquad + \left(a^{2^i}b^{2^k} + a^{2^k}b^{2^i}\right)x^{2^j+1} \\ &\qquad + \left(a^{2^i}b^{2^j} + a^{2^j}b^{2^i}\right)x^{2^k+1}\Big)\Big). \end{aligned} \tag{14}$$

Further, $\mathscr{E}_{h_\lambda} = \{x \in \mathbb{F}_{2^n} : B(x, y) = 0 \text{ for all } y \in \mathbb{F}_{2^n}\}$, where $B(x, y)$ is the bilinear form associated with h_λ. Now, using $x^{2^n} = x$, $y^{2^n} = y$, and $\mathrm{Tr}_1^n(x^{2^i}) = \mathrm{Tr}_1^n(x)$, for all $x, y \in \mathbb{F}_{2^n}$, we compute $B(x, y)$ as follows

$$\begin{aligned} B(x, y) &= h_\lambda(0) + h_\lambda(x) + h_\lambda(y) + h_\lambda(x+y) \\ &= \mathrm{Tr}_1^n\Big(\lambda\Big(y^{2^i}\Big(\left(ab^{2^k} + a^{2^k}b\right)x^{2^j} + \left(ab^{2^j} + a^{2^j}b\right)x^{2^k} \\ &\qquad + \left(a^{2^j}b^{2^k} + a^{2^k}b^{2^j}\right)x\Big) \\ &\qquad + y^{2^j}\Big(\left(ab^{2^k} + a^{2^k}b\right)x^{2^i} + \left(ab^{2^i} + a^{2^i}b\right)x^{2^k} \\ &\qquad + \left(a^{2^i}b^{2^k} + a^{2^k}b^{2^i}\right)x\Big) \end{aligned}$$

$$
\begin{aligned}
&+ y^{2^k}\Big(\Big(ab^{2^j} + a^{2^j}b\Big)x^{2^i} + \Big(ab^{2^i} + a^{2^i}b\Big)x^{2^j} \\
&\qquad + \Big(a^{2^i}b^{2^j} + a^{2^j}b^{2^i}\Big)x\Big) \\
&+ y\Big(\Big(a^{2^j}b^{2^k} + a^{2^k}b^{2^j}\Big)x^{2^i} \\
&\qquad + \Big(a^{2^i}b^{2^k} + a^{2^k}b^{2^i}\Big)x^{2^j} \\
&\qquad + \Big(a^{2^i}b^{2^j} + a^{2^j}b^{2^i}\Big)x^{2^k}\Big)\Big)\Big) \\
&= \mathrm{Tr}_1^n\left(yP(x)\right),
\end{aligned} \tag{15}
$$

where

$$
\begin{aligned}
P(x) = &\Big(\lambda\Big(ab^{2^k} + a^{2^k}b\Big)x^{2^j} + \lambda\Big(ab^{2^j} + a^{2^j}b\Big)x^{2^k} \\
&+\lambda\Big(a^{2^j}b^{2^k} + a^{2^k}b^{2^j}\Big)x\Big)^{2^{n-i}} \\
&+ \Big(\lambda\Big(ab^{2^j} + a^{2^j}b\Big)x^{2^i} \\
&\quad + \lambda\Big(ab^{2^i} + a^{2^i}b\Big)x^{2^j} + \lambda\Big(a^{2^i}b^{2^j} + a^{2^j}b^{2^i}\Big)x\Big)^{2^{n-j}} \\
&+ \Big(\lambda\Big(ab^{2^j} + a^{2^j}b\Big)x^{2^i} + \lambda\Big(ab^{2^i} + a^{2^i}b\Big)x^{2^j} \\
&\quad + \lambda\Big(a^{2^i}b^{2^j} + a^{2^j}b^{2^i}\Big)x\Big)^{2^{n-k}} \\
&+ \lambda\Big(a^{2^j}b^{2^k} + a^{2^k}b^{2^j}\Big)x^{2^i} \\
&+ \lambda\Big(a^{2^i}b^{2^k} + a^{2^k}b^{2^i}\Big)x^{2^j} + \lambda\Big(a^{2^i}b^{2^j} + a^{2^j}b^{2^i}\Big)x^{2^k}.
\end{aligned} \tag{16}
$$

Therefore,

$$
\mathscr{E}_{h_\lambda} = \left\{x \in \mathbb{F}_{2^n} : P(x) = 0 = P(x)^{2^i}\right\}. \tag{17}
$$

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

$$
\begin{aligned}
L_{(\lambda,a,b)}(x) &= (P(x))^{2^i} \\
&= \lambda\Big(\Big(ab^{2^j} + a^{2^j}b\Big)x^{2^k} \\
&\qquad + \Big(ab^{2^k} + a^{2^k}b\Big)x^{2^j} \\
&\qquad + \Big(a^{2^j}b^{2^k} + a^{2^k}b^{2^j}\Big)x\Big) \\
&\quad + \lambda^{2^i}\Big(\Big(a^{2^{i+j}}b^{2^{i+k}} + a^{2^{i+k}}b^{2^{i+j}}\Big)x^{2^{2i}} \\
&\qquad + \Big(a^{2^{i+k}}b^{2^{2i}} + a^{2^{2i}}b^{2^{i+k}}\Big)x^{2^{i+j}} \\
&\qquad + \Big(a^{2^{2i}}b^{2^{i+j}} + a^{2^{i+j}}b^{2^{2i}}\Big)x^{2^{i+k}}\Big) \\
&\quad + \lambda^{2^{i-j}}\Big(\Big(a^{2^{i-j}}b^{2^i} + a^{2^i}b^{2^{i-j}}\Big)x^{2^{2i-j}} \\
&\qquad + \Big(a^{2^{i-j}}b^{2^{2i-j}} + a^{2^{2i-j}}b^{2^{i-j}}\Big)x^{2^i} \\
&\qquad + \Big(a^{2^{2i-j}}b^{2^i} + a^{2^i}b^{2^{2i-j}}\Big)x^{2^{i-j}}\Big) \\
&\quad + \lambda^{2^{i-k}}\Big(\Big(a^{2^{i-k}}b^{2^{i+j-k}} + a^{2^{i+j-k}}b^{2^{i-k}}\Big)x^{2^{2i-k}} \\
&\qquad + \Big(a^{2^{i-k}}b^{2^{2i-k}} + a^{2^{2i-k}}b^{2^{i-k}}\Big)x^{2^{i+j-k}} \\
&\qquad + \Big(a^{2^{2i-k}}b^{2^{i+j-k}} + a^{2^{i+j-k}}b^{2^{2i-k}}\Big)x^{2^{i-k}}\Big).
\end{aligned} \tag{18}
$$

The coefficient of x in $L_{(\lambda,a,b)}(x)$ is zero if and only if $a^{2^j}b^{2^k} + a^{2^k}b^{2^j} = 0$; that is, $a^{2^{j-k}}b + ab^{2^{j-k}} = 0$ 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 the dimension of the kernel $\mathscr{E}_{D_bD_af_\lambda}$ associated with $D_bD_af_\lambda$ is $k(a,b) \leq 2i$ if n is even; otherwise $k(a,b) \leq 2i-1$. The WHT of $D_bD_af_\lambda$ at $\mu \in \mathbb{F}_{2^n}$ is

$$
W_{D_bD_af_\lambda}(\mu) \leq \begin{cases} 2^{(n+2i)/2}, & \text{if } n = 0 \mod 2, \\ 2^{(n+2i-1)/2}, & \text{if } n = 1 \mod 2. \end{cases} \tag{19}
$$

Therefore,

$$
\mathrm{nl}\left(D_bD_af_\lambda\right) = \begin{cases} 2^{n-1} - 2^{(n+2i-2)/2}, & \text{if } n = 0 \mod 2, \\ 2^{n-1} - 2^{(n+2i-3)/2}, & \text{if } n = 1 \mod 2. \end{cases} \tag{20}
$$

Using Proposition 1, we have

$$
\mathrm{nl}_3\left(f_\lambda\right) \geq \begin{cases} 2^{n-3} - 2^{(n+2i-6)/2}, & \text{if } n = 0 \mod 2, \\ 2^{n-3} - 2^{(n+2i-7)/2}, & \text{if } n = 1 \mod 2. \end{cases} \tag{21}
$$

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, (20) 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 the following.

(i) When $n = 0 \mod 2$,

$$
\begin{aligned}
\mathrm{nl}_3\left(f_\lambda\right) &\geq 2^{n-1} \\
&\quad - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{2n} - 2(2^n-2)\left(2^{n-1} - 2^{(n+2i-2)/2}\right)}} \\
&= 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{(3n+2i)/2} + 2^{n+1} - 2^{(n+2i+2)/2}}}.
\end{aligned} \tag{22}
$$

(ii) When $n = 1 \bmod 2$,

$$\begin{aligned}\mathrm{nl}_3(f_\lambda) &\geq 2^{n-1} \\ &\quad - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{2n} - 2(2^n-2)\left(2^{n-1} - 2^{(n+2i-3)/2}\right)}} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{(3n+2i-1)/2} + 2^{n+1} - 2^{(n+2i+1)/2}}}.\end{aligned} \tag{23}$$

□

Theorem 7. *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*

$$nl_3(g_\lambda) \geq \begin{cases} 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{(3n+6)/2}+2^{n+1}-2^{(n+8)/2}}}, \\ \qquad\qquad \text{if } n = 0 \mod 2, \\ 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{(3n+5)/2}+2^{n+1}-2^{(n+7)/2}}}, \\ \qquad\qquad \text{if } n = 1 \mod 2. \end{cases} \tag{24}$$

Proof. The proof is similar to that of Theorem 6 up to (18). 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 (18) by 3ℓ, 2ℓ, and ℓ, respectively:

$$\begin{aligned} L_{(\lambda,a,b)}(x) &= P(x)^{2^{3\ell}} \\ &= \lambda^{2^{3\ell}}\left(\left(a^{2^{5\ell}}b^{2^{4\ell}} + a^{2^{4\ell}}b^{2^{5\ell}}\right)x^{2^{6\ell}} \right. \\ &\qquad + \left(a^{2^{4\ell}}b^{2^{6\ell}} + a^{2^{6\ell}}b^{2^{4\ell}}\right)x^{2^{5\ell}} \\ &\qquad \left. + \left(a^{2^{6\ell}}b^{2^{5\ell}} + a^{2^{5\ell}}b^{2^{6\ell}}\right)x^{2^{4\ell}}\right) \\ &\quad + \lambda^{2^\ell}\left(\left(a^{2^\ell}b^{2^{3\ell}} + a^{2^{3\ell}}b^{2^\ell}\right)x^{2^{4\ell}} \right. \\ &\qquad + \left(a^{2^\ell}b^{2^{4\ell}} + a^{2^{4\ell}}b^{2^\ell}\right)x^{2^{3\ell}} \\ &\qquad \left. + \left(a^{2^{4\ell}}b^{2^{3\ell}} + a^{2^{3\ell}}b^{2^{4\ell}}\right)x^{2^\ell}\right) \\ &\quad + \lambda^{2^{2\ell}}\left(\left(a^{2^{2\ell}}b^{2^{4\ell}} + a^{2^{4\ell}}b^{2^{2\ell}}\right)x^{2^{5\ell}} \right. \\ &\qquad + \left(a^{2^{2\ell}}b^{2^{5\ell}} + a^{2^{5\ell}}b^{2^{2\ell}}\right)x^{2^{4\ell}} \\ &\qquad \left. + \left(a^{2^{5\ell}}b^{2^{4\ell}} + a^{2^{4\ell}}b^{2^{5\ell}}\right)x^{2^{2\ell}}\right) \\ &\quad + \lambda\left(ab^{2^{2\ell}} + a^{2^{2\ell}}b\right)x^{2^\ell} + \lambda\left(ab^{2^\ell} + a^{2^\ell}b\right)x^{2^{2\ell}} \\ &\quad + \lambda\left(a^{2^{2\ell}}b^{2^\ell} + a^{2^\ell}b^{2^{2\ell}}\right)x. \end{aligned} \tag{25}$$

The coefficient of x in $L_{(\lambda,a,b)}(x)$ is zero if and only if $a^{2^{2\ell}}b^{2^\ell} + a^{2^\ell}b^{2^{2\ell}} = 0$; that is, $a^{2^\ell}b + ab^{2^\ell} = 0$. Moreover, $\gcd(\ell, n) = 1$ and so, by Proposition 4, $b \in a\mathbb{F}_2$. The polynomial $L_{(\lambda,a,b)}(x)$ as represented in (25) is of the form $\sum_{i=0}^{6} c_i x^{2^{i\ell}}$ and so, again 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 WHT of $D_bD_ag_\lambda$ at $\mu \in \mathbb{F}_{2^n}$ is

$$W_{D_bD_ag_\lambda}(\mu) \leq \begin{cases} 2^{(n+6)/2}, & \text{if } n = 0 \mod 2, \\ 2^{(n+5)/2}, & \text{if } n = 1 \mod 2. \end{cases} \tag{26}$$

Therefore,

$$\mathrm{nl}(D_bD_ag_\lambda) \geq \begin{cases} 2^{n-1} - 2^{(n+4)/2}, & \text{if } n = 0 \mod 2, \\ 2^{n-1} - 2^{(n+3)/2}, & \text{if } n = 1 \mod 2. \end{cases} \tag{27}$$

Using Proposition 1, we have

$$\mathrm{nl}_3(g_\lambda) \geq \begin{cases} 2^{n-3} - 2^{n/2}, & \text{if } n = 0 \mod 2, \\ 2^{n-3} - 2^{(n-1)/2}, & \text{if } n = 1 \mod 2. \end{cases} \tag{28}$$

Using Proposition 2, we have the following.

(i) When $n = 0 \bmod 2$,

$$\begin{aligned}\mathrm{nl}_3(g_\lambda) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{2n} - 2(2^n-2)\left(2^{n-1} - 2^{(n+4)/2}\right)}} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{(3n+6)/2} + 2^{n+1} - 2^{(n+8)/2}}}.\end{aligned} \tag{29}$$

(ii) When $n = 1 \bmod 2$,

$$\begin{aligned}\mathrm{nl}_3(g_\lambda) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{2n} - 2(2^n-2)\left(2^{n-1} - 2^{(n+3)/2}\right)}} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{(3n+5)/2} + 2^{n+1} - 2^{(n+7)/2}}}.\end{aligned} \tag{30}$$

□

Remark 8. Let $f \in \mathscr{B}_n$ be 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 $\mathrm{nl}_3(f) \geq 2^{n-4}$. This result follows from Proposition 1 and the fact that the nonlinearity of any quadratic function in $\mathscr{B}_n$ is at least 2^{n-2} [11, 22].

4. Comparison

The theoretical lower bounds for third-order nonlinearities obtained by using Theorem 6 for $i = 3, 4, 5$ and j, k are taken in such a way that $\gcd(j - k, n) = 1$ and reported in Tables 1 and 2. The bounds are compared with the general bounds for third-order nonlinearity: $\mathrm{nl}_3(f) \geq 2^{n-4}$, for any biquadratic

Table 1: The lower bounds on the third-order nonlinearities obtained by Theorem 6 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 2: The lower bounds on the third-order nonlinearities obtained by Theorem 6 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

Table 3: Comparison of the value of lower bounds on third-order nonlinearities obtained by Theorem 6 with the bound obtained in [4, 11, 12] for odd n.

n	Theorem 6	[12]	[4]	[11]
7	12	8	16	6
9	76	—	64	60
11	416	240	256	360
13	2048	992	1024	1864
15	9496	—	4096	8872
17	42368	16256	16384	40272
19	184208	65280	65536	177168

Table 4: Comparison of the value of lower bounds on third-order nonlinearities obtained by Theorem 6 with the bound obtained in [4, 11, 12] for even n.

n	Theorem 6	[12]	[4]	[11]
8	22	28	32	20
10	152	120	128	152
12	832	—	512	828
14	4096	2016	2048	4096
16	18992	—	8192	18992
18	84736	—	32768	84736
20	368416	130816	131072	368416

Boolean function. It is evident that the bounds for $i = 3, 4$ are efficiently large and decrease with increasing the value of i. It is to be noted that Class (a) is the more general class of biquadratic monomial Boolean functions containing several classes of highly nonlinear Boolean functions. In particular, for $i = 5$, $j = 4$, and $k = 3$ Class (a) coincides with Kasami functions of algebraic degree 4.

The theoretical bounds for third-order nonlinearities obtained by using Theorem 7 and Proposition 3 are compared with known classes of functions [4, 11, 12] and reported in Tables 3 and 4. It is to be noted that the lower bounds for third-order nonlinearities of the inverse functions $(\mathrm{nl}_3(f_{\mathrm{inv}}) \geq 2^{n-1} - 2^{(7n-2)/8})$ are larger than that of the Dillon functions $(\mathrm{nl}_3(f_{\mathrm{dillon}}) \geq 2^{n-1} - 2^{7n/8})$ for all n. Thus, it is demonstrated that the lower bound obtained by Theorem 7 is better than the bounds obtained by Gode and Gangopadhyay [12] for Kasami functions: $\mathrm{Tr}(\lambda x^{57})$, Iwata and Kurosawa's general bound [4] for all $n > 8$. Also these bounds are improved upon Carlet's [11] bound for inverse function when n is odd, or $n = 8, 12$, and equal for the rest of values of even n.

5. Conclusion

In this paper, using recursive approach introduced in [11], we have computed the lower bounds of third-order nonlinearities of two general classes of biquadratic monomial Boolean functions. It is demonstrated that in some cases our bounds are better than the bounds obtained previously.

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The author would like to thank the anonymous referees for their time, effort, and extensive comments on the revision of the paper which improve the quality of the presentation of the paper. The work is supported by Council of Scientific and Industrial Research, New Delhi, India.

References

[1] J. Golic, "Fast low order approximation of cryptographic functions," in *Advances in Cryptology—EUROCRYPT '96*, vol. 1070 of *Lecture Notes in Computer Science*, pp. 268–282, Springer, 1996.

[2] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Advanced in Cryptology—EUROCRYPT*

'89, vol. 434 of *Lecture Notes in Computer Science*, pp. 549–562, Springer, 1990.

[3] N. Courtois, "Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt," in *Information Security and Cryptology—ICISC, 2002*, vol. 2587 of *Lecture Notes in Computer Science*, pp. 182–199, Springer, 2002.

[4] T. Iwata and K. Kurosawa, "Probabilistic higher order differential attack and higher order bent functions," in *Advances in Cryptology—ASIACRYPT '99*, vol. 1716 of *Lecture Notes in Computer Science*, pp. 62–74, Springer, 1999.

[5] C. Carlet, "Boolean functions for cryptography and error correcting codes," in *Boolean Models and Methods in Mathematics, Computer Science and Engineering*, Y. Crama and P. Hammer, Eds., chapter of the monograph, pp. 257–397, Cambridge University Press, 2010.

[6] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers*, vol. 561 of *Lecture Notes in Computer Science*, Springer, 1991.

[7] L. Knudsen and M. Robshaw, "Non-linear approximations in linear cryptanalysis," in *Advances in Cryptology—EUROCRYPT '96*, vol. 1070 of *Lecture Notes in Computer Science*, pp. 224–236, Springer, 1996.

[8] T. Shimoyama and T. Kaneko, "Quadratic relation of S-box and its application to the linear attack of full round DES," in *Advanced in Cryptology—CRYPTO '98*, vol. 1462 of *Lecture Notes in Computer Science*, pp. 200–211, Springer, 1998.

[9] Q. Wang and T. Johansson, "A note on fast algebraic attacks and higher order nonlinearities," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6584, pp. 404–414, 2011.

[10] R. Fourquet and C. Tavernier, "An improved list decoding algorithm for the second order Reed-Muller codes and its applications," *Designs, Codes, and Cryptography*, vol. 49, no. 1–3, pp. 323–340, 2008.

[11] C. Carlet, "Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 1262–1272, 2008.

[12] R. Gode and S. Gangopadhyay, "Third-order nonlinearities of a subclass of Kasami functions," *Cryptography and Communications*, vol. 2, no. 1, pp. 69–83, 2010.

[13] S. Gangopadhyay and B. K. Singh, "On second-order nonlinearities of some $\mathscr{D}_0$ type bent functions," *Fundamenta Informaticae*, vol. 114, no. 3-4, pp. 271–285, 2012.

[14] B. K. Singh, "On second-order nonlinearity and maximum algebraic immunity of some bent functions in $\mathscr{PS}^+$," *Journal of Applied Mathematics and Computing*, 2014.

[15] C. Carlet and S. Mesnager, "Improving the upper bounds on the covering radii of binary Reed-Muller codes," *IEEE Transactions on Information Theory*, vol. 53, no. 1, pp. 162–173, 2007.

[16] C. Carlet, "More vectorial Boolean functions with unbounded nonlinearity profile," *International Journal of Foundations of Computer Science*, vol. 22, no. 6, pp. 1259–1269, 2011.

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, The Netherlands, 1977.

[18] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar*, Cambridge University Press, 2005.

[19] O. S. Rothaus, "On "bent" functions," *Journal of Combinatorial Theory A*, vol. 20, no. 3, pp. 300–305, 1976.

[20] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "Determining the nonlinearity of a new family of APN functions," *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, vol. 4851, pp. 72–79, 2007.

[21] A. Canteaut, P. Charpin, and G. M. Kyureghyan, "A new class of monomial bent functions," *Finite Fields and Their Applications*, vol. 14, no. 1, pp. 221–241, 2008.

[22] J. Seberry, X. M. Zhang, and Y. Zheng, "Relationships among nonlinearity criteria," in *Advanced in Cryptology—EUROCRYPT '94*, vol. 950 of *Lecture Notes in Computer Science*, pp. 376–388, Springer, 1995.