Cryptography and Communications (2023) 15:821–830
https://doi.org/10.1007/s12095-023-00643-5

RESEARCH

On higher order nonlinearities of Boolean functions

Sampada Tiwari[1] · **Deepmala Sharma**[1]

Received: 28 November 2022 / Accepted: 30 March 2023 / Published online: 30 May 2023

Abstract
When analyzing the security of block ciphers and stream ciphers, the $r-th$ order nonlinearity of a Boolean function is crucial. They also have a prominent place in coding theory because the $r-th$ order nonlinearity of Boolean functions is connected to the covering radius of $\mathcal{RM}(r,m)$, i.e., Reed-Muller code. In this study, we determine the lower bound for the higher-order nonlinearity of the two classes of Boolean functions listed below.

1. $f_\alpha(u) = tr_1^m(\alpha u^d)$, where d is the Niho exponent constructed by Dobbertin et al. (J. Comb. Theory Ser. A 113:779–798, 2006).
2. $g_\alpha(u) = tr_1^m(\alpha u^d)$, where $d = 2^p - 2$. For all $u \in \mathbb{F}_{2^m}$, $\alpha \in \mathbb{F}_{2^m}^*$ and $m = 2p$.

Keywords Nonlinearity · Walsh Hadamard transform · Boolean functions · Niho power functions

Mathematics Subject Classification (2010) 94A60 · 94C10 · 06E30

1 Introduction

In cryptography, Boolean functions are used extensively (block ciphers and stream ciphers). They are also elementary units of error-correcting codes. Let $h : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function in m-variable. An essential cryptographic technique that significantly contributes to the security of symmetric cryptosystems is the nonlinearity of Boolean functions [2, 5, 7]. They are also crucial in preventing Best Affine Approximation Attacks as well as Fast Correlation Attacks. In coding theory, nonlinearity and its property are vital as the covering radius of Reed-Muller code having length 2^m and order r is equal to the maximum value of the $r-th$ order nonlinearity of Boolean functions in m-variable [8]. Recently Wang et al. [25] showed that the covering radius of $RM(2,7)$ is at most 42. Also, $RM(3,7)$, i.e., the covering radius of third order Reed-Muller has been discussed by Gao et al. [13]. They

✉ Deepmala Sharma
deepsha.maths@nitrr.ac.in

Sampada Tiwari
sampadatiwari15@gmail.com

[1] Department of Mathematics, National Institute of Technology Raipur, G E Road, Raipur 492010, Chhattisgarh, India

corroborate that for a function $f \in \mathcal{B}_{7,2}$, the third order nonlinearity $nl_3(f) > 20$ does not hold.

In 1976, Rothaus [23] was the first to established the concept of nonlinearity. A few known results exist about $r-th$ order nonlinearity of a Boolean function h, i.e., $nl_r(h)$, for $r > 1$. In 2006, Carlet et al. [6] provided the best asymptotic upper bound, which is given as:

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

Boolean functions with algebraic degrees strictly greater than r exhibit $r-th$ order nonlinearity, which is difficult to compute. A lot of research has been done so far to compute the $nl_r(h)$ for $r > 1$, as there is a relation between the nonlinearity and the Walsh Hadamard transform (WHT) of Boolean functions and the Walsh-Hadamard transform is easily computed by FFT (fast Fourier transform). In [10, 21] Kabatiansky and Tavernier proposed an algorithm later enhanced and resolved by Fourquet et al. [11] for $r = 2$ and $m \leq 11$. It is also applicable for $m \leq 13$ (in some cases). A special algorithm is still missing in the literature for the computation of $nl_r(h)$ when $r \geq 3$. Iwata et al. [20] proposed a bent function with nonlinearity of $r-th$ order having lower bound $2^{m-r-3}(r+4)$, for $r \leq m-3$. In this area of research, Carlet had a great contribution. He developed the recursive approach to get a lower bound on the nonlinearity of the $r-th$ order of a Boolean function [3]. To analyze the lower bounds of second as well as third order nonlinearity many authors contributed their work to distinct classes of Boolean functions [12, 14, 15, 18, 19, 24]. In this article, for $m = 2p$, we analyze the lower bounds on higher order nonlinearity of a Boolean function $f_\alpha(u) = tr_1^m(\alpha u^{(2^p-1)3+1})$, for all $u \in \mathbb{F}_{2^m}$, $\alpha \in \mathbb{F}_{2^m}^*$ and a Boolean function $g_\alpha(u) = tr_1^m(\alpha u^{2^p-2})$, for all $u \in \mathbb{F}_{2^m}$, $\alpha \in \mathbb{F}_{2^m}^*$.

2 Preliminaries

Assuming that $\mathbb{F}_2$ is the finite field and $\mathbb{F}_2^m$ is the vector space of all $m-$tuples over $\mathbb{F}_2$. $\mathcal{B}_{m,2}$ represents the set of all $m-$variable Boolean functions and is the function from $\mathbb{F}_2^m$ to $\mathbb{F}_2$. Since $\mathbb{F}_2^m$ is isomorphic to the finite field $\mathbb{F}_{2^m}$ therefore, a Boolean function can also be considered as a function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. The support of a Boolean function h is given by $S_h = \{u \in \mathbb{F}_2^m : h(u) \neq 0\}$, whose cardinality $\mid S_h \mid$ is known as the Hamming weight of h.

Boolean functions are represented by their truth table representation in which all the 2^m elements of $\mathbb{F}_2^m$ are in lexicographically increasing order that is

$$[h(0,0,...,0), h(0,0,...,1), ..., h(1,1,...,1)].$$

If the truth table of a Boolean function has the same number of $0's$ and $1's$, then the Boolean function is known as a balanced Boolean function. The balancedness of a Boolean function can also be defined with the help of its Hamming weight. That is, for a Boolean function $h \in \mathcal{B}_{m,2}$, if $wt(h) = 2^{m-1}$, then it is considered to be balanced . To study the cryptographic properties of Boolean functions it is not always favorable to represent Boolean functions by their truth table, so we study an another representation of Boolean functions which is known as Algebraic Normal Form (ANF).

The Algebraic Normal Form of a Boolean function h can be defined as

$$h(u_1, u_2, ..., u_m) = \sum_{a=(a_1,a_2,...,a_m)\in\mathbb{F}_2^m} \mu_a\Big(\prod_{i=1}^{m} u_i^{a_i}\Big),$$

where $\mu_a \in \mathbb{F}_2$. The number of variables in the highest order term of the Algebraic Normal Form of a Boolean function h for which $\mu_a \neq 0$ is known as the algebraic degree of h and is denoted by $deg(h)$.The trace function $tr_s^m : \mathbb{F}_{2^m} \to \mathbb{F}_{2^s}$, where $m = qs$ for some integer q can be defined as

$$tr_s^m(u) = u + u^{2^s} + u^{2^{2s}} + ... + u^{2^{m-s}},$$

for all $u \in \mathbb{F}_{2^m}$. When $s = 1$, the trace function $tr_1^m : \mathbb{F}_{2^m} \to \mathbb{F}_2$ is known as the absolute trace function. The absolute trace function $tr_1^m : \mathbb{F}_{2^m} \to \mathbb{F}_2$ has some properties which are as follows:

1. tr_1^m is a linear transformation from $\mathbb{F}_{2^m}$ into $\mathbb{F}_2$.
2. $tr_1^m(u^{2^i}) = tr_1^m(u)$, for all $u \in \mathbb{F}_{2^m}$ and i is any positive integer.

Suppose $u, v \in \mathbb{F}_2^m$. Let us define $\langle u, v\rangle = u_1v_1 + u_2v_2 + ... + u_mv_m$ which is known as the inner product of u and v. Also, $\langle u, v\rangle = tr_1^m(uv)$, for all $u, v \in \mathbb{F}_{2^m}$ is known as the trace of the product of u and v.

Let $h_1, h_2 \in \mathcal{B}_{m,2}$, then the Hamming distance $d(h_1, h_2)$ is defined by

$$d(h_1, h_2) = \mid \{u \in \mathbb{F}_{2^m} : h_1(u) \neq h_2(u)\} \mid .$$

The $r-th$ order nonlinearity of h_1 is the least hamming distance between h_1 and all the Boolean functions having algebraic degree at most r i.e.,

$$nl_r(h_1) = min_{h_2 \in \mathcal{B}_{m,2},\ deg(h_2) \leq r} d(h_1, h_2).$$

When $r = 1$, it is simply denoted by $nl(h_1)$.

Let $h \in \mathcal{B}_{m,2}$ and $\alpha \in \mathbb{F}_2^m$ then the Walsh-Hadamard transform of h at α is defined as

$$W_h(\alpha) = \sum_{u \in \mathbb{F}_2^m} (-1)^{h(u)+\langle u,v\rangle}.$$

In terms of $tr_1^m(\alpha u)$, for all $\alpha, u \in \mathbb{F}_{2^m}$, the Walsh-Hadamard transform of a Boolean function $h \in \mathcal{B}_{m,2}$ can also be defined as

$$W_h(\alpha) = \sum_{u \in \mathbb{F}_{2^m}} (-1)^{h(u)+tr_1^m(\alpha u)}.$$

The multiset $[W_h(\alpha) : \alpha \in \mathbb{F}_2^m]$ is known as the Walsh spectrum of h. For a Boolean function $h \in \mathcal{B}_{m,2}$, the nonlinearity and the Walsh-Hadamard transform are correlated as follows:

$$nl(h) = 2^{m-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^m} \mid W_h(\alpha) \mid .$$

A Boolean function $h \in \mathcal{B}_{m,2}$ is known as bent function if h has maximum nonlinearity with $r = 1$ i.e., $nl(h) = 2^{m-1} - 2^{\frac{m}{2}-1}$.

The derivative of a Boolean function $h \in \mathcal{B}_{m,2}$ with respect to $x \in \mathbb{F}_2^m$ is defined as

$$D_x h(u) = h(u) + h(u + x),$$

for all $u \in \mathbb{F}_2^m$. The higher-order derivative can be obtained by extending the definition of the derivative of a Boolean function. Let W_j be a $j-$dimensional subspace of $\mathbb{F}_2^m$ having $x_1, x_2, ..., x_j$ as a basis. Then the $j-$th order derivative of h with respect to W_j is defined as

$$D_{W_j} h(u) = D_{x_1} D_{x_2} ... D_{x_j} h(u) = \sum_{w \in \mathbb{F}_2^j} h\left(u + \sum_{i=1}^{j} w_i x_i\right),$$

for all $u \in \mathbb{F}_2^m$.

Let the set of all invertible matrices of order $m \times m$ is denoted by $GL(m, \mathbb{F}_2)$. The entries of matrices of $GL(m, \mathbb{F}_2)$ are either 0 or 1. Let $g, h \in \mathcal{B}_{m,2}$ are two Boolean functions. For a matrix $M \in GL(m, \mathbb{F}_2)$, $y,\ \alpha \in \mathbb{F}_2^m$ and $\epsilon \in \mathbb{F}_2$ if

$$h(u) = g(Mu + y) + \langle \alpha, u \rangle + \epsilon,$$

for all $u \in \mathbb{F}_2^m$, then g and h are known as affine equivalent.

Let $d \in \{1, 2, ..., 2^m - 2\}$ be any integer. Then d is known as Niho exponent and if u^d is restricted to $\mathbb{F}_{2^p}$ linearly, it is known as Niho power function or we can say that if $d \equiv 2^i (mod\ 2^p - 1)$.

For any prime power k, a polynomial

$$P(u) = \sum_{i=0}^{m} \zeta_i u^{k^i},$$

where each $\zeta_i \in \mathbb{F}_{k^s}$ (an extension field of $\mathbb{F}_k$) is known as a linearized polynomial over $\mathbb{F}_{k^s}$.

Proposition 2.1 [3] Let $h \in \mathcal{B}_{m,2}$ and $r < m$ be any positive integer. Then for all $0 < j < r$,

$$nl_r(h) \geq \frac{1}{2^j} \max_{x_1, x_2, ..., x_j \in \mathbb{F}_{2^m}} nl_{r-j}(D_{x_1} D_{x_2} ... D_{x_j} h).$$

We shall use the notation $[l, x_1, x_2, ..., x_m]$ for any collection of integers with the aforementioned characteristics:

1. $\sum_{j=1}^{m} x_j = l$.
2. $x_j > 0$, for all $j = 1, 2, ..., m$.
3. $x_j \wedge x_k = 0$, for all $1 \leq j < k \leq m$, where $\wedge$ is the bitwise AND operation.

It indicates that m non-empty disjoint groups are formed from one bit of the binary representation of l.

Lemma 2.2 [16] *Let $u, v \in \mathbb{F}_{2^m}$ and $l > 0$ then*

$$(u + v)^l = \sum_{[l,j,k]} u^j v^k + u^l + v^l.$$

Lemma 2.3 [16] *Let $t,\ l$ and $x_j > 0$ are positive integers then for all $j = 1, 2, ..., t$*

$$D_{x_1} D_{x_2} ... D_{x_t} u^l = \sum_{[l,\beta_0,\beta_1,...,\beta_t]} u^{\beta_0} x_1^{\beta_1} ... x_t^{\beta_t} + constant.$$

Let us assume a quadratic Boolean function $h \in \mathcal{B}_{m,2}$. It is said that the bilinear form $B(a, b)$ associated with h is $B(a, b) = h(0) + h(a) + h(b) + h(a + b)$. The kernel of $B(a, b)$ [1] is the subspace of $\mathbb{F}_{2^m}$ and is defined by

$$\varepsilon_h = \{a \in \mathbb{F}_{2^m} : B(a, b) = 0, \quad for\ all\ b \in \mathbb{F}_{2^m}\}.$$

Lemma 2.4 [1] *Let $\mathbb{F}_q$ be the field of characteristic 2 and W be the vector space of $\mathbb{F}_q$. If $Q : W \to \mathbb{F}_q$ is a quadratic form on W then the parity of the dimensions of W and the kernel of $B(u, v)$ is the same.*

Lemma 2.5 [1, 22] *Let $h : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be the Boolean quadratic form and the bilinear form associated with h is $B(u, v)$. Let b be the dimension of the kernel of $B(u, v)$. The Walsh spectrum of h depends only on the dimension b. Also the Walsh spectrum of h is given by:*

$W_h(\alpha)$	Number of α
0	$2^m - 2^{m-b}$
$2^{(m+b)/2}$	$2^{(m-b-1)/2} + (-1)^{h(0)}2^{(m-b-2)/2}$
$-2^{(m+b)/2}$	$2^{(m-b-1)/2} - (-1)^{h(0)}2^{(m-b-2)/2}$

3 Main result

In the below given results, we contributed our work to find the general lower bounds on the higher order nonlinearity of some classes of Boolean functions. In Theorem 3.1, we study the nonlinearity of Boolean function with higher order by using the Niho power function, which was given by Dobbertin et al. [9]. In Theorem 3.2, we compute the lower bound on higher order nonlinearity of the inverse Boolean function.

Theorem 3.1 Let $m = 2p$, where $p > 0$ and a Boolean function $f_\alpha \in \mathcal{B}_{m,2}$ of the form

$$f_\alpha(u) = tr_1^m(\alpha u^d),$$

where $d = (2^p - 1)3 + 1$, for all $u \in \mathbb{F}_{2^m}$, $\alpha \in \mathbb{F}_{2^m}^*$. Then

$$nl_{(r=p-1)} f_\alpha(u) \geq 2^{p+1} - 2^{\frac{p+1}{2}}.$$

Proof The Boolean function $f_\alpha(u)$ is of algebraic degree p [9]. By applying Proposition 2.1, we obtain

$$nl_{(r=p-1)} f_\alpha(u) \geq \frac{1}{2^{p-2}} \max_{x_1, x_2, \ldots, x_{p-2}} nl(D_{x_1} D_{x_2} \ldots D_{x_{p-2}}(f_\alpha(u))). \tag{3.1}$$

Let $x_1, x_2, \ldots, x_{p-2} \in \mathbb{F}_{2^m}$, then observe that

$$D_{x_1} D_{x_2} \ldots D_{x_{p-2}}(f_\alpha(u)) = D_{x_1} D_{x_2} \ldots D_{x_{p-2}}(tr_1^m(\alpha u^d)).$$

Hence,

$$D_{x_1} D_{x_2} \ldots D_{x_{p-2}}(f_\alpha(u)) = tr_1^m\left(\alpha\left(D_{x_1} D_{x_2} \ldots D_{x_{p-2}}(u^d)\right)\right). \tag{3.2}$$

Now by applying Lemma 2.3, we get

$$D_{x_1} D_{x_2} \ldots D_{x_{p-2}}(u^d) = \sum_{[d, \gamma_0, \gamma_1, \ldots, \gamma_{p-2}]} u^{\gamma_0} x_1^{\gamma_1} \ldots x_{p-2}^{\gamma_{p-2}} + constant. \tag{3.3}$$

From Eqs. (3.2) and (3.3), we have

$$D_{x_1} D_{x_2} \ldots D_{x_{p-2}}(f_\alpha(u)) = tr_1^m(\alpha \sum_{[d, \gamma_0, \gamma_1, \ldots, \gamma_{p-2}]} u^{\gamma_0} x_1^{\gamma_1} \ldots x_{p-2}^{\gamma_{p-2}} + constant).$$

Also, it is very well known that in the binary form of $d = (2^p - 1)3 + 1$ there exist p ones and each $\gamma_i > 0$, for all i, must possess at least one of them. Again, in the binary form of

γ_0 there are $p-(p-2)=2$ ones. Therefore, the above Boolean function is a quadratic Boolean function. Let us assume that $g_\alpha(u)$ be an affine equivalent Boolean function to $D_{x_1}D_{x_2}...D_{x_{p-2}}(f_\alpha(u))$ which can be obtained from the above expression by eliminating all the terms with $wt(\gamma_0)=1$ and the constant terms in the sum. Since $D_{x_1}D_{x_2}...D_{x_{p-2}}(f_\alpha(u))$ and $g_\alpha(u)$ are affine equivalent, therefore they both have the same nonlinearity. The bilinear form $B(u,v)$ associated with $g_\alpha(u)$ is

$$B(u,v)=g_\alpha(0)+g_\alpha(u)+g_\alpha(v)+g_\alpha(u+v).$$

Then by applying Lemma 2.2, we have

$$B(u,v)=tr_1^m\left(\sum_{i=1}^{p}v^{\beta_i}\left(\sum_{[d,\lambda,\beta_i,\gamma_1,...,\gamma_{p-2}]}\alpha u^\lambda x_1^{\gamma_1}...x_{p-2}^{\gamma_{p-2}}\right)\right).$$

Then,

$$B(u,v)=tr_1^m(\sum_{i=1}^{p}v^{\beta_i}Q_i(u)),$$

where,

$$Q_i(u)=\sum_{[d,\lambda,\beta_i,\gamma_1,...,\gamma_{p-2}]}\alpha u^\lambda x_1^{\gamma_1}...x_{p-2}^{\gamma_{p-2}}.$$

Since in the binary form of d there are p ones and $\lambda,\beta_i,\gamma_i,...,\gamma_{p-2}$ are p in number for $i=1,2,...,p$. Consequently, they are all powers of 2. By applying the properties of linearity $v^{2^m}=v$ and the property of trace function, $tr_1^m(u^{2^i})=tr_1^m(u)$, for all $u\in\mathbb{F}_{2^m}$, $B(u,v)$ becomes to

$$B(u,v)=\sum_{i=1}^{p}tr_1^m(vQ_i(u)^{\frac{2^m}{\beta_i}}),$$

or

$$B(u,v)=tr_1^m(v\sum_{i=1}^{p}Q_i(u)^{\frac{2^m}{\beta_i}}).$$

Therefore,

$$B(u,v)=tr_1^m(vQ(u)),$$

where, $Q(u)=\sum_{i=1}^{p}Q_i(u)^{\frac{2^m}{\beta_i}}$.
By the definition, the kernel of $B(u,v)$ is $\varepsilon_f=\{u\in\mathbb{F}_{2^m}:B(u,v)=0,\ for\ all\ v\in\mathbb{F}_{2^m}\}$. So, ε_f has equal number of zeros of the polynomial $Q(u)$, where

$$Q(u)=\sum_{i=1}^{p}\sum_{[d,\lambda,\beta_i,\gamma_1,...,\gamma_{p-2}]}\alpha^{\frac{2^m}{\beta_i}}u^{\frac{2^m\lambda}{\beta_i}}x_1^{\frac{2^m\gamma_1}{\beta_i}}...x_{p-2}^{\frac{2^m\gamma_{p-2}}{\beta_i}},$$

or

$$Q(u)=\sum_{i=1}^{p}\sum_{[d,\lambda,\beta_i,\gamma_1,...,\gamma_{p-2}]}\alpha^{\frac{1}{\beta_i}}u^{\frac{\lambda}{\beta_i}}x_1^{\frac{\gamma_1}{\beta_i}}...x_{p-2}^{\frac{\gamma_{p-2}}{\beta_i}}.$$

Since, there are same number of zeroes in $Q(u)$ and $Q(u)^{2^{p-1}}$. Therefore, the number of elements in ε_f and the number of zeroes of the polynomial $Q(u)^{2^{p-1}}$ are also same. Hence, we have,

$$Q(u)^{2^{p-1}} = \sum_{i=1}^{p} \sum_{[d,\lambda,\beta_i,\gamma_1,\ldots,\gamma_{p-2}]} \alpha^{\frac{2^{p-1}}{\beta_i}} u^{\frac{2^{p-1}\lambda}{\beta_i}} x_1^{\frac{2^{p-1}\gamma_1}{\beta_i}} \ldots x_{p-2}^{\frac{2^{p-1}\gamma_{p-2}}{\beta_i}},$$

a linearized polynomial in u whose degree is at most 2^{p-1}. Also, the kernel ε_f has at most 2^{p-1} number of elements. Let the kernel of $B(u, v)$ has dimension k, by applying Lemma 2.4, $k \leq p-1$, since m is even. Therefore, by using Lemma 2.5, for all $u \in \mathbb{F}_{2^m}$, we obtain,

$$W_{D_{x_1} D_{x_2} \ldots D_{x_{p-2}} f_\alpha}(u) \leq 2^{\frac{2^m+k}{2}} \leq 2^{\frac{3p-1}{2}}.$$

So,

$$nl_{D_{x_1} D_{x_2} \ldots D_{x_{p-2}} f_\alpha}(u) \geq 2^{2p-1} - 2^{\frac{3p-3}{2}}. \tag{3.4}$$

From Eqs. (3.1) and (3.4), we have,

$$nl_{(r=p-1) f_\alpha}(u) \geq 2^{p+1} - 2^{\frac{p+1}{2}}.$$

□

Theorem 3.2 Let $m = 2p$, where $p > 0$ and let g_α be a Boolean function of the form

$$g_\alpha(u) = tr_1^m(\alpha u^d),$$

where $d = (2^p - 2)$, for all $u \in \mathbb{F}_{2^m}$, $\alpha \in \mathbb{F}_{2^m}^*$. Then

$$nl_{(r=p-2) g_\alpha}(u) \geq 2^{p+2} - 2^{\frac{p+3}{2}}.$$

Table 1 Comparison of the lower bounds of the higher order nonlinearity

r,p,m	3,4,8	4,5,10	5,6,12	6,7,14	7,8,16	8,9,18	9,10,20	10,11,22
Lower bounds acquired in [4]	0	0	0	0	0	0	0	0
Lower bounds acquired in [17]	16	32	64	128	256	512	1024	2048
Lower bounds acquired in Theorem 3.1	26.343	56	116.686	240	489.373	992	2002.745	4032

Proof For any positive integer p, we know that $2^p - 2 = 2^{p-1} + 2^{p-2} + ... + 2^2 + 2$. Therefore, the binary expansion of $2^p - 2$ has $p - 1$ ones. Hence the algebraic degree of $g_\alpha(u)$ is $p - 1$. By Proposition 2.1, we obtain

$$nl_{(r=p-2)}g_\alpha(u) \geq \frac{1}{2^{p-3}} \max_{x_1,x_2,...,x_{p-3}} nl(D_{x_1}D_{x_2}...D_{x_{p-3}}(g_\alpha(u))). \tag{3.5}$$

Let $x_1, x_2, ..., x_{p-3} \in \mathbb{F}_{2^m}$, then observe that

$$D_{x_1}D_{x_2}...D_{x_{p-3}}(g_\alpha(u)) = D_{x_1}D_{x_2}...D_{x_{p-3}}(tr_1^m(\alpha u^d)).$$

Hence,

$$D_{x_1}D_{x_2}...D_{x_{p-3}}(g_\alpha(u)) = tr_1^m\left(\alpha\left(D_{x_1}D_{x_2}...D_{x_{p-3}}(u^d)\right)\right). \tag{3.6}$$

Now by applying Lemma 2.3, we get

$$D_{x_1}D_{x_2}...D_{x_{p-3}}(u^d) = \sum_{[d,\gamma_0,\gamma_1,...,\gamma_{p-3}]} u^{\gamma_0}x_1^{\gamma_1}...x_{p-3}^{\gamma_{p-3}} + constant. \tag{3.7}$$

From Eqs. (3.6) and (3.7), we have

$$D_{x_1}D_{x_2}...D_{x_{p-3}}(g_\alpha(u)) = tr_1^m(\alpha \sum_{[d,\gamma_0,\gamma_1,...,\gamma_{p-3}]} u^{\gamma_0}x_1^{\gamma_1}...x_{p-3}^{\gamma_{p-3}} + constant).$$

Since in the binary form of $d = (2^p - 2)$ there exist $p - 1$ ones and each $\gamma_i > 0$, for all i, must have at least one of them. Also, in the binary form of γ_0 there are 2 ones. Therefore, the Boolean function $g_\alpha(u)$is quadratic. Let us assume that $h_\alpha(u)$ be an affine equivalent Boolean function to $D_{x_1}D_{x_2}...D_{x_{p-3}}(g_\alpha(u))$ which can be obtained from the above expression by eliminating all the terms with $wt(\gamma_0) = 1$ and the constant terms in the sum. Since $D_{x_1}D_{x_2}...D_{x_{p-3}}(g_\alpha(u))$ and $h_\alpha(u)$ are affine equivalent, therefore they both have the same nonlinearity. The bilinear form $B(u, v)$ associated with $h_\alpha(u)$ is

$$B(u, v) = h_\alpha(0) + h_\alpha(u) + h_\alpha(v) + h_\alpha(u + v).$$

Also, we have

$$B(u, v) = tr_1^m(vQ'(u)),$$

where, $Q'(u) = \sum_{i=1}^{p-1} Q_i'(u)^{\frac{2^m}{\beta_i}}$.

Now on proceeding as Theorem 3.1, we can get

$$nl_{(r=p-2)}g_\alpha(u) \geq 2^{p+2} - 2^{\frac{p+3}{2}}.$$

□

4 Comparison

Carlet [4] has given the lower bounds of the higher order nonlinearity of the Dillon bent function. Also Garg [17] has computed lower bounds of the higher order nonlinearity of the monomial partial spread Boolean function. In the below Table 1, a comparison of the lower bounds acquired in Theorem 3.1 with those gained by Carlet and Garg is given.

5 Conclusion

The lower bounds on the higher order nonlinearity of Boolean function with Niho exponent and inverse Boolean function have been discussed in the article. Also, after the comparison, it has been discovered that the lower bounds obtained in this paper are better than the lower bounds obtained by Carlet and Garg. Hence, after analyzing the other properties of cryptography of these Boolean functions, they can be used in ciphers (block cipher and stream cipher) as combiners or filters. The future aspect of this paper is to study and compute the lower bounds of higher order nonlinearity of some other classes of Boolean functions.

Author Contributions Both authors made substantial contributions to the conception. Sampada Tiwari prepared the original draft of the Manuscript. Both authors reviewed the manuscript.

Declarations

Competing interests The authors declare no competing interests.

References

1. Canteaut, A., Charpin, P., Kyureghyan, G.M.: A new class of monomial bent functions. Finit. Fields Appl. **14**, 221–241 (2008)
2. Carlet, C.: Vectorial boolean functions for cryptography. In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering, vol. 134, pp. 398–469 (2010)
3. Carlet, C.: Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications. IEEE Trans. Inf. Theory **54**, 1262–1272 (2008)
4. Carlet, C.: On the nonlinearity profile of the Dillon function, p. 577. IACR Cryptology ePrint Archive (2009)
5. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering, vol. 2, pp. 257–397 (2010)
6. Carlet, C., Mesnager, S.: Improving the upper bounds on the covering radii of binary Reed-Muller codes. IEEE Trans. Inf. Theory **53**, 162–173 (2006)
7. Carlet, C.: Boolean functions for cryptography and coding theory, pp. 1–562. Monograph in Cambridge University Press (2021)
8. Cohen, G., Honkala, I., Litsyn, S., Lobstein, A.: Covering Codes, p. 541. Elsevier, North Holland (1997)
9. Dobbertin, H., Leander, G., Canteaut, A., Carlet, C., Felke, P., Gaborit, P.: Construction of bent functions via Niho power functions. J. Comb. Theory Ser. A **113**, 779–798 (2006)
10. Dumer, I., Kabatiansky, G., Tavernier, C.: List decoding of Reed-Muller codes up to the Johnson bound with almost linear complexity. IEEE International Symposium on Information Theory-Proceedings, pp. 138–142. (2006)
11. Fourquet, R., Tavernier, C.: An improved list decoding algorithm for the second order reed-muller codes and its applications. Des Codes Crypt. **49**, 323–340 (2008)
12. Gangopadhyay, S., Sarkar, S., Telang, R.: On the lower bounds of the second order nonlinearities of some Boolean functions. Inform. Sci. **180**, 266–273 (2010)
13. Gao, J., Kan, H., Li, Y. and Wang, Q.: The Covering Radius of the Third-Order Reed-Muller Code RM(3,7) is 20. IEEE Trans. Inf. Theory. https://doi.org/10.1109/TIT.2023.3242966
14. Gao, Q., Tang, D.: A lower bound on the second-order nonlinearity of the generalized maiorana-mcfarland boolean functions. IEICE Trans. Fundam. Electron. Commun. Comput Sci. **101**, 2397-2401 (2018)
15. Garg, M., Gangopadhyay, S.: A lower bound of the second-order nonlinearities of boolean bent functions. Fundam. Informaticae **111**, 413–422 (2011)
16. Garg, M., Khalyavin, A.: Higher-order nonlinearity of Kasami functions. Int. J. Comput. Math. **89**, 1311–1318 (2012)
17. Garg, M.: Higher order-nonlinearities of two classes of Boolean functions. Int. J. Comput. Sci. Inf. Technol. **6**(5), 4251–4256 (2015)

18. Gode, R., Gangopadhyay, S.: On higher-order nonlinearities of monomial partial spreads type boolean functions. J. Comb. Inf. Syst. Sci. **35**, 341–360 (2010)
19. Gode, R., Gangopadhyay, S.: Third-order nonlinearities of a subclass of Kasami functions. Cryptogr. Commun. **2**, 69–83 (2010)
20. Iwata, T., Kurosawa, K.: Probabilistic higher order differential attack and higher order bent functions. In: International Conference on the Theory and Application of Cryptology and Information Security, pp. 62–74. Springer (1999)
21. Kabatiansky, G., Tavernier, C.: List decoding of second order reed-muller codes. Proc. 8Th Intern. Simp. Comm. Theory and Applications, Ambleside, UK (2005)
22. MacWilliams, F.J., Sloane, N.J.A.: The theory of Error-Correcting codes, vol. 16. Elsevier (1977)
23. Rothaus, O.S.: On ben functions. J. Comb. Theory. Ser. A **20**, 300–305 (1976)
24. Singh, B.K.: On third-order nonlinearity of biquadratic monomial boolean functions. Int. J. Eng. Math. **2014**, 1–7 (2014)
25. Wang, Q., Stănică, P.: New bounds on the covering radius of the second order Reed-Muller code of length 128. Cryptogr. Commun. **11**, 269–277 (2019)