On second-order nonlinearities of some $\mathcal{D}_0$ type bent functions

Sugata Gangopadhyay, Brajesh Kumar Singh*

Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee 247667 INDIA
gsugata@gmail.com

Abstract. In this paper we study the lower bounds of second-order nonlinearities of bent functions constructed by modifying certain cubic Maiorana-McFarland type bent functions.

1 Introduction

The set of all Boolean functions of n variables of degree at most r is said to be the Reed-Muller code, $RM(r,n)$, of length 2^n and order r.

Definition 1. *Suppose $f \in \mathcal{B}_n$. For every integer r, $0 < r \leq n$, the minimum of the Hamming distances of f from all the functions belonging to $RM(r,n)$ is said to be the rth-order nonlinearity of the Boolean function f. The sequence of values $nl_r(f)$, for r ranging from 1 to $n-1$, is said to be the nonlinearity profile of f.*

The first-order nonlinearity (i.e., nonlinearity) of a Boolean function f, denoted $nl(f)$, is related to the immunity of f against "best affine approximation attacks" and "fast correlation attacks", 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 [6], Courtois [5]. For a complete literature survey we refer to Carlet [4]. Unlike first-order nonlinearity there is no efficient algorithm to compute second-order nonlinearities for $n > 11$. Most efficient algorithm due to Fourquet and Tavernier [7] works for $n \leq 11$ and, up to $n \leq 13$ for some special functions. Thus, identifying classes containing Boolean functions with "good" nonlinearity profile is an important problem. In this paper we use Proposition 2 to obtain second-order nonlinearities of bent functions in the class $\mathcal{D}_0$ derived from the cubic MMF type bent functions described in [8].

2 Preliminaries

2.1 Basic definitions

A function from $\mathbb{F}_2^n$, or $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a Boolean function on n-variables. Let $\mathcal{B}_n$ denote the set of all Boolean functions on n variables. The algebraic normal form (ANF) of $f \in \mathcal{B}_n$ is $f(x_1, x_2, \ldots, x_n) = \sum_{a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_a (\prod_{i=1}^n x_i^{a_i})$, where $\mu_a \in \mathbb{F}_2$. The algebraic degree of f, $\deg(f) := \max\{wt(a) : \mu_a \neq 0, a \in \mathbb{F}_{2^n}\}$. 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. The trace function $tr_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined by

$$tr_1^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}, \text{ for all } x \in \mathbb{F}_{2^n}.$$

* Research supported by CSIR, India

The inner product of $x, y \in \mathbb{F}_2^n$ is denoted by $x \cdot y$. If we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ then $x \cdot y = tr_1^n(xy)$. Let $\mathcal{A}_n$ be the set of all affine functions on n variables. Nonlinearity of $f \in \mathcal{B}_n$ is defined as $nl(f) = \min_{l \in \mathcal{A}_n}\{d(f, l)\}$. The Walsh Transform of $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_2^n$ is defined as

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + tr_1^n(\lambda x)}.$$

The multiset $[W_f(\lambda) : \ \lambda \in \mathbb{F}_2^n]$ is said to be the Walsh spectrum of f. Following is the relationship between nonlinearity and Walsh spectrum of $f \in \mathcal{B}_n$

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

By Parseval's identity

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

it can be shown that $|W_f(\lambda)| \geq 2^{n/2}$ which implies that $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.

Definition 2. *Suppose n is an even integer. A function $f \in \mathcal{B}_n$ is said to be a bent function if and only if $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ (i.e., $W_f(\lambda) \in \{2^{\frac{n}{2}}, -2^{\frac{n}{2}}\}$ for all $\lambda \in \mathbb{F}_2^n$).*

For odd $n \geq 9$, the tight upper bound of nonlinearities of Boolean functions in $\mathcal{B}_n$ is not known.

Definition 3. *The derivative of f, $f \in \mathcal{B}_n$, with respect to a, $a \in \mathbb{F}_2^n$, is the function $D_a f \in \mathcal{B}_n$ defined as $D_a f : x \to f(x) + f(x+a)$. The vector $a \in \mathbb{F}_2^n$ is called a linear structure of f if $D_a f$ is constant.*

The higher order derivatives are defined as follows.

Definition 4. *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 r-th order derivative of f, $f \in \mathcal{B}_n$ with respect to V, is the function $D_V f \in \mathcal{B}_n$, defined by*

$$D_V f : x \to D_{a_1} \ldots D_{a_r} f(x).$$

It is to be noted that the 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. Following result on Linearized polynomials is used in this paper.

Lemma 1. *[1] Let $p(x) = \sum_{i=0}^{v} c_i x^{2^{ik}}$ be a linearized polynomial over $\mathbb{F}_{2^n}$, where $\gcd(n, k) = 1$. Then the equation $p(x) = 0$ has at most 2^v solutions in $\mathbb{F}_{2^n}$.*

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, 9] of $B(x, y)$ is the subspace of $\mathbb{F}_2^n$ defined by

$$\mathcal{E}_f = \{x \in \mathbb{F}_2^n : B(x, y) = 0 \text{ for all } y \in \mathbb{F}_2^n\}.$$

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

Lemma 2 ([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 3 ([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 4 ([2, 9]). *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	$2^n - 2^{n-k}$
$2^{(n+k)/2}$	$2^{n-k-1} + (-1)^{f(0)} 2^{(n-k-2)/2}$
$-2^{(n+k)/2}$	$2^{n-k-1} - (-1)^{f(0)} 2^{(n-k-2)/2}$

Thus the Walsh spectrum of a quadratic Boolean function [2] is completely characterized by the dimension of the kernel of the bilinear form associated with it.

2.3 Recursive lower bounds of higher-order nonlinearities

Carlet [4] for the first time has put the computation of lower bounds on nonlinearity profiles of Boolean functions in a recursive framework. Following are some results proved by Carlet [4].

Proposition 1 ([4], Proposition 2). *Let $f \in \mathcal{B}_n$ and r be a positive integer ($r < n$), then we have*

$$nl_r(f) \geq \frac{1}{2} \max_{a \in \mathbb{F}_2^n} nl_{r-1}(D_a f)$$

in terms of higher order derivatives,

$$nl_r(f) \geq \frac{1}{2^i} \max_{a_1, a_2, \ldots, a_i \in \mathbb{F}_2^n} nl_{r-i}(D_{a_1} D_{a_2} \ldots D_{a_i} f)$$

for every non-negative integer $i < r$. In particular, for $r = 2$,

$$nl_2(f) \geq \frac{1}{2} \max_{a \in \mathbb{F}_2^n} nl(D_a f).$$

Proposition 2 ([4], Proposition 3). *Let $f \in \mathcal{B}_n$ and r be a positive integer ($r < n$), then we have*

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a \in \mathbb{F}_2^n} nl_{r-1}(D_a f)}.$$

Corollary 1 ([4], Corollary 2). *Let $f \in \mathcal{B}_n$ and r be a positive integer ($r < n$). Assume that, for some nonnegative integers M and m, we have $nl_{r-1}(D_a f) \geq 2^{n-1} - M2^m$ for every nonzero $a \in \mathbb{F}_2^n$. Then*

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

Carlet remarked that in general, the lower bound given by the Proposition 2 is potentially stronger than that given in Proposition 1 [4].

3 Second-order nonlinearity of $\mathcal{D}_0$ type functions

In this section $n = 2p$. A Boolean function on n variables $h : \mathbb{F}_{2^p} \times \mathbb{F}_{2^p} \longrightarrow \mathbb{F}_2$ is said to be a $\mathcal{D}_0$ type bent if $h(x, y) = x \cdot \pi(y) + \prod_{j=1}^{p}(x_j + 1)$ where π is a permutation on $\mathbb{F}_{2^p}$ and $x = (x_1, \ldots, x_n)$. This class is constructed by Carlet [3] and shown to be distinct from the complete class of MMF type bent functions.

3.1 Functions obtained by modifying $tr_1^p(xy^{2^i+1})$

Suppose $\pi(y) = y^{2^i+1}$, where i is an integer such that, $\gcd(2^i + 1, 2^p - 1) = 1$ and $\gcd(i, p) = e$. First we prove the following.

Lemma 5. *Let $h_\mu(x) = Tr_1^p(\mu x^{2^i+1})$, $\mu, x \in \mathbb{F}_{2^p}$, $\mu \neq 0$, i is integer such that $1 \leq i \leq p$, $\gcd(2^i + 1, 2^p - 1) = 1$, and $\gcd(i, p) = e$, then the dimension of the kernel associated with the bilinear form of h_μ is e.*

Proof. $h_\mu(x) = Tr_1^p(\mu x^{2^i+1})$. Let $a \in \mathbb{F}_{2^p}$, $a \neq 0$ be arbitrary.

$$\begin{aligned} D_a h_\mu(x) &= Tr_1^p(\mu(x+a)^{2^i+1}) + Tr_1^p(\mu x^{2^i+1}) \\ &= Tr_1^p(\mu(x^{2^i}a + xa^{2^i} + a^{2^i+1})) \\ &= Tr_1^p(a\mu x^{2^i} + \mu a^{2^i}x) + Tr_1^p(a^{2^i+1}) \\ &= Tr_1^p((a\mu)^{2^{t-i}} + \mu a^{2^i})x) + Tr_1^p(a^{2^i+1}) \end{aligned}$$

$D_a h_\mu$ is constant if and only if

$$(a\mu)^{2^{t-i}} + \mu a^{2^i} = 0.$$

$$i.e.,\ a\mu + (\mu a^{2^i})^{2^i} = 0.$$

$$i.e.,\ a\mu + \mu^{2^i}a^{2^{2i}} = 0.$$

Assuming $\mu \neq 0$

$$i.e.,\ \mu^{2^i-1}a^{2^{2i}-1} = 1.$$

$$i.e.,\ (\mu a^{2^i+1})^{2^i-1} = 1.$$

since $(\mu a^{2^i+1})^{2^i-1} = 1$ and $\gcd(i, p) = e$, therefore

$$\mu a^{2^i+1} \in \mathbb{F}_{2^e}^*$$

$$i.e.,\ a^{2^i+1} \in (\mu)^{-1}\mathbb{F}_{2^e}^*$$

Thus, the total number of ways in which a can be chosen so that $D_a h_\mu$ is constant is 2^e (including the case $\mu = 0$). Hence by Lemma 3 we have the dimension of the kernel associated with h_μ is e. $\square$

Remark 1. From Lemma 4 and Lemma 5 it is clear that the weight distribution of the Walsh spectrum of h_μ is:

$W_{h_\mu}(\alpha)$	number of α
0	$2^n - 2^{n-e}$
$2^{(n+e)/2}$	$2^{n-e-1} + 2^{(n-e-2)/2}$
$-2^{(n+e)/2}$	$2^{n-e-1} - 2^{(n-e-2)/2}$

Lemma 6. *Let $h(x,y) = f(x,y) + g(x)$, where $n = 2p$, $x, y \in \mathbb{F}_2^p$, $f(x,y) = x \cdot \pi(y)$, $g(x) = \prod_{i=1}^{p}(x_i + 1)$ and π is a permutation on $\mathbb{F}_2^p$ then*

- *The Walsh transform of $D_{(a,b)}h$ at $(\mu, \eta) \in \mathbb{F}_2^p \times \mathbb{F}_2^p$ is*

$$W_{D_{(a,b)}h}(\mu,\eta) = W_{D_{(a,b)}f}(\mu,\eta) - 2[(-1)^{\mu\cdot a} + (-1)^{\eta\cdot b}]W_{a\cdot\pi}(\eta), \quad \textit{and}$$

- $\mid W_{D_{(a,b)}h}(\mu,\eta) \mid \leq \mid W_{D_{(a,b)}f}(\mu,\eta) \mid +4 \mid W_{a\cdot\pi}(\eta) \mid$.

Proof. Let $h(x,y) = f(x,y) + g(x)$, $g(x) = \prod_{i=1}^{p}(x_i+1)$ and $(a,b) \in \mathbb{F}_2^p \times \mathbb{F}_2^p$ be arbitrary. Clearly

$$g(x) = \begin{cases} 1, & \text{if } (x,y) \in \{0\} \times \mathbb{F}_2^p, \\ 0, & \textit{otherwise.} \end{cases}$$

For $a \neq 0$ then

$$g(x+a) = \begin{cases} 1, & \text{if } (x,y) \in \{a\} \times \mathbb{F}_2^p, \\ 0, & \textit{otherwise.} \end{cases}$$

Thus

$$g(x) + g(x+a) = \begin{cases} 1, & \text{if } (x,y) \in \{0\} \times \mathbb{F}_2^p \bigcup \{a\} \times \mathbb{F}_2^p, \\ 0, & \textit{otherwise.} \end{cases}$$

The Walsh transform of $D_{(a,b)}h$ at $(\mu,\eta)\in\mathbb{F}_2^p\times\mathbb{F}_2^p$ is

$$
\begin{aligned}
W_{D_{(a,b)}h}(\mu,\eta) &= \sum_{(x,y)\in\mathbb{F}_2^p\times\mathbb{F}_2^p}(-1)^{f(x+a,y+b)+f(x,y)+g(x+a)+g(x)+\mu\cdot x+\eta\cdot y}\\
&= \sum_{(x,y)\in\mathbb{F}_2^p\times\mathbb{F}_2^p\setminus(\{0\}\times\mathbb{F}_2^p\bigcup\{a\}\times\mathbb{F}_2^p)}(-1)^{f(x+a,y+b)+f(x,y)+\mu\cdot x+\eta\cdot y}\\
&- \sum_{(x,y)\in\{0\}\times\mathbb{F}_2^p\bigcup\{a\}\times\mathbb{F}_2^p}(-1)^{f(x+a,y+b)+f(x,y)+\mu\cdot x+\eta\cdot y}\\
&= \sum_{(x,y)\in\mathbb{F}_2^p\times\mathbb{F}_2^p}(-1)^{f(x+a,y+b)+f(x,y)+\mu\cdot x+\eta\cdot y}\\
&-2\sum_{(x,y)\in\{0,a\}\times\mathbb{F}_2^p}(-1)^{f(x+a,y+b)+f(x,y)+\mu\cdot x+\eta\cdot y}\\
&= W_{D_{(a,b)}f}(\mu,\eta)-2\sum_{(x,y)\in\{0,a\}\times\mathbb{F}_2^p}(-1)^{f(x+a,y+b)+f(x,y)+\mu\cdot x+\eta\cdot y}\\
&= W_{D_{(a,b)}f}(\mu,\eta)-2[\sum_{y\in\mathbb{F}_2^p}(-1)^{f(0,y+b)+f(a,y)+\mu\cdot a+\eta\cdot y}\\
&+\sum_{y\in\mathbb{F}_2^p}(-1)^{f(a,y+b)+f(0,y)+\eta\cdot y}\,]\\
&= W_{D_{(a,b)}f}(\mu,\eta)-2[\,(-1)^{\mu\cdot a}\sum_{y\in\mathbb{F}_2^p}(-1)^{a\cdot\pi(y)+\eta\cdot y}+(-1)^{\eta\cdot b}\sum_{y\in\mathbb{F}_2^p}(-1)^{a\cdot\pi(y+b)+\eta\cdot(y+b)}\,]\\
&= W_{D_{(a,b)}f}(\mu,\eta)-2[\,(-1)^{\mu\cdot a}W_{a\cdot\pi}(\eta)+(-1)^{\eta\cdot b}W_{a\cdot\pi}(\eta)\,]\\
&= W_{D_{(a,b)}f}(\mu,\eta)-2[\,(-1)^{\mu\cdot a}+(-1)^{\eta\cdot b}\,]W_{a\cdot\pi}(\eta)
\end{aligned}
$$

Thus

$$\mid W_{D_{(a,b)}h}(\mu,\eta)\mid\leq\mid W_{D_{(a,b)}f}(\mu,\eta)\mid+4\mid W_{a\cdot\pi}(\eta)\mid.$$

□

Theorem 1. *Let $h(x,y)=Tr_1^p(xy^{2^i+1})+\prod_{i=1}^p(x_i+1)$, where $n=2p$, $x,y\in\mathbb{F}_2^p$, i is integer such that $1\leq i\leq p$, $\gcd(2^i+1,2^p-1)=1$, and $\gcd(i,p)=e$, then nonlinearity of $D_{(a,b)}h$ is*

$$nl(D_{(a,b)}h)\geq\begin{cases}2^{2p-1}-2^{p+e-1}, & \text{if } a=0 \text{ and } b\neq 0,\\ 2^{2p-1}-2^{p+e-1}-2^{\frac{p+e+2}{2}}, & \text{if } a\neq 0 \text{ and } b\neq 0,\\ 2^{2p-1}-2^{\frac{3p+e-2}{2}}-2^{\frac{p+e+2}{2}}, & \text{if } a\neq 0 \text{ and } b=0.\end{cases}$$

Proof. $h(x,y)=Tr_1^p(xy^{2^i+1})+\prod_{i=1}^p(x_i+1)$. Let $f(x,y)=Tr_1^p(xy^{2^i+1})$ and $g(x)=\prod_{i=1}^p(x_i+1)$, then by Lemma 6 the Walsh Hadamard transform of $D_{(a,b)}h$ at any point $(\mu,\eta)\in\mathbb{F}_2^p\times\mathbb{F}_2^p$ is

$$\mid W_{D_{(a,b)}h}(\mu,\eta)\mid\leq\mid W_{D_{(a,b)}f}(\mu,\eta)\mid+4\cdot\mid W_{a\cdot\pi}(\eta)\mid \tag{1}$$

It is given by Gangopadhyay, Sarkar and Telang [8] that the dimension of kernel $k(a,b)$ of bilinear form associated with $D_{(a,b)}f$ is

$$k(a,b) = \begin{cases} e+p, & \text{if } b = 0, \\ 2e, & \text{if } b \neq 0. \end{cases}$$

The above equation can be written as

$$k(a,b) = \begin{cases} e+p, & \text{if } a \neq 0, b = 0, \\ 2e, & \text{if } a = 0, b \neq 0. \\ 2e, & \text{if } a \neq 0, b \neq 0. \end{cases} \tag{2}$$

Case 1. Consider the case $a = 0$. From (1) and (2) we have

$$\begin{aligned} W_{D_{(0,b)}h}(\mu,\eta) &= W_{D_{(0,b)}f}(\mu,\eta) \\ &= 2^{p+e} \end{aligned}$$

Therefore for $b \neq 0$ nonlinearity of $D_{(0,b)}h$ is

$$\begin{aligned} nl(D_{(0,b)}h) &= 2^{2p-1} - \frac{1}{2} max_{(\mu,\eta)\in\mathbb{F}_2^p\times\mathbb{F}_2^p} \mid W_{D_{(0,b)}f}(\mu,\eta) \mid \\ &= 2^{2p-1} - 2^{p+e-1} \end{aligned} \tag{3}$$

Case 2. Consider the case $a \neq 0$. Here $a \cdot \pi(y) = Tr_1^p(ay^{2^i+1})$, Using (1) & Remark 1 we have

$$\mid W_{D_{(a,b)}h}(\mu,\eta) \mid \leq \mid W_{D_{(a,b)}f}(\mu,\eta) \mid + 2^{\frac{p+e+4}{2}}.$$

From (2) we have

$$W_{D_{(a,b)}f}(\mu,\eta) = \begin{cases} 2^{p+e}, & \text{if } a \neq 0, b \neq 0, \\ 2^{\frac{3p+e}{2}}, & \text{if } a \neq 0, b = 0. \end{cases}$$

Therefore,

$$W_{D_{(a,b)}h}(\mu,\eta) \leq \begin{cases} 2^{p+e} + 2^{\frac{p+e+4}{2}}, & \text{if } a \neq 0, b \neq 0, \\ 2^{\frac{3p+e}{2}} + 2^{\frac{p+e+4}{2}}, & \text{if } a \neq 0, b = 0. \end{cases}$$

Therefore nonlinearity of $D_{(a,b)}h$ is

$$nl(D_{(a,b)}h) \geq \begin{cases} 2^{2p-1} - 2^{p+e-1} - 2^{\frac{p+e+2}{2}}, & \text{if } a \neq 0, b \neq 0, \\ 2^{2p-1} - 2^{\frac{3p+e-2}{2}} - 2^{\frac{p+e+2}{2}}, & \text{if } a \neq 0, b = 0. \end{cases} \tag{4}$$

Combining (3) and (4) we have

$$nl(D_{(a,b)}h) \geq \begin{cases} 2^{2p-1} - 2^{p+e-1}, & \text{if } a = 0 \text{ and } b \neq 0, \\ 2^{2p-1} - 2^{p+e-1} - 2^{\frac{p+e+2}{2}}, & \text{if } a \neq 0 \text{ and } b \neq 0, \\ 2^{2p-1} - 2^{\frac{3p+e-2}{2}} - 2^{\frac{p+e+2}{2}}, & \text{if } a \neq 0 \text{ and } b = 0. \end{cases} \tag{5}$$

□

Theorem 2. *Let $h(x,y)=Tr_1^p(xy^{2^i+1})+\prod_{i=1}^{p}(x_i+1)$, where $n=2p$, $x,y\in\mathbb{F}_2^p$, i is integer such that $1\le i\le p$, $\gcd(2^i+1,2^p-1)=1$, and $\gcd(i,p)=e$, then*

$$nl_2(h)\ge 2^{2p-1}-\frac{1}{2}\sqrt{2^{3p+e}+2^{2p}(1-2^e)+5(2^{\frac{5p+e}{2}}-2^{\frac{3p+e}{2}})}.$$

Proof. $h(x,y)=Tr_1^p(xy^{2^i+1})+\prod_{i=1}^{p}(x_i+1)$ Let $f(x,y)=Tr_1^p(xy^{2^i+1})$ and $g(x)=\prod_{i=1}^{p}(x_i+1)$ Using (5) and Proposition 1 we have

$$nl_2(h)\ge 2^{2p-2}-2^{p+e-2}. \tag{6}$$

Using (5) we have

$$\begin{aligned}
&\sum_{(a,b)\in\mathbb{F}_{2^p}\times\mathbb{F}_{2^p}} nl(D_{(a,b)}h)\\
&=nl(D_{(0,0)}h)+\sum_{b\in\mathbb{F}_{2^p},b\neq0} nl(D_{(0,b)}h)+\sum_{a\in\mathbb{F}_{2^p},a\neq0} nl(D_{(a,0)}h)+\sum_{(a,b)\in\mathbb{F}_{2^p}\times\mathbb{F}_{2^p},a\neq0,b\neq0} nl(D_{(a,b)}h)\\
&\ge(2^p-1)(2^{2p-1}-2^{p+e-1})+(2^p-1)(2^{2p-1}-2^{\frac{3p+e-2}{2}}-2^{\frac{p+e+2}{2}})\\
&+(2^p-1)(2^p-1)(2^{2p-1}-2^{p+e-1}-2^{\frac{p+e+2}{2}})\\
&=(2^p-1)\{2^{2p}+2^{3p-1}-2^{2p+e-1}-2^{2p-1}-2^{\frac{3p+e+2}{2}}-2^{\frac{3p+e-2}{2}}\}\\
&=(2^p-1)\{2^{2p-1}+2^{3p-1}-2^{2p+e-1}-2^{\frac{3p+e+2}{2}}-2^{\frac{3p+e-2}{2}}\}\\
&=2^{4p-1}-2^{2p-1}-2^{3p+e-1}+2^{2p+e-1}+2^{\frac{3p+e+2}{2}}+2^{\frac{3p+e-2}{2}}-2^{\frac{5p+e+2}{2}}-2^{\frac{5p+e-2}{2}}\\
&=2^{4p-1}-2^{3p+e-1}-2^{2p-1}(1-2^e)-5(2^{\frac{5p+e-2}{2}}-2^{\frac{3p+e-2}{2}})
\end{aligned}$$

Using Proposition 2 we have

$$\begin{aligned}
nl_2(h)&\ge 2^{2p-1}-\frac{1}{2}\sqrt{2^{4p}-2\{2^{4p-1}-2^{3p+e-1}-2^{2p-1}(1-2^e)-5(2^{\frac{5p+e-2}{2}}-2^{\frac{3p+e-2}{2}})\}}\\
&=2^{2p-1}-\frac{1}{2}\sqrt{2^{3p+e}+2^{2p}(1-2^e)+5(2^{\frac{5p+e}{2}}-2^{\frac{3p+e}{2}})}
\end{aligned} \tag{7}$$

□

If $f(x,y)=tr_1^p(xy^{2^i+1})$, where i is an integer such that $1\le i\le p$, $\gcd(2^i+1,2^p-1)=1$, then from ([8], Theorem 2) we obtain

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

Thus, $nl_2(h)$ and $nl_2(f)$ are asymptotically equal. Below we provide comparisons among the lower bounds obtained from Theorem 2 and ([8], Theorem 2) and maximum known Hamming distances as computed in [7].

$n=2p$	6	10	12
i	$1,2$	$1,2,3,4$	$2,4$
$e=\gcd(i,p)$	1	1	2
Lower bounds in Theorem 2	10	351	1466
Lower bounds in [8]	15	378	1524
Hamming distances in [7]	18	400	1760

The inequality in Proposition 2 involves nonlinearities of $D_a f$, the first derivative of f, at each $a \in \mathbb{F}_2^n$. If f is a cubic function then $D_a f$ is at most quadric. The nonlinearities of quadratic and affine functions are well known ([9], Chap. 15). Therefore Proposition 2 is readily applicable to cubic Boolean functions. This is exploited in [4, 8, 11] to compute lower bounds of second-order nonlinearities for particular functions. In this paper we show that it is possible to use this knowledge in some cases to obtain information related to second-order nonlinearities of functions in the class $\mathcal{D}_0$, which are bent functions with maximum possible algebraic degree, p, for any given $n = 2p$.

3.2 Functions obtained by modifying $Tr_1^p(x(y^{2^{m+1}+1} + y^3 + y))$

Theorem 3. *Let $h(x, y) = Tr_1^p(x(y^{2^{m+1}+1} + y^3 + y)) + \prod_{i=1}^{p}(x_i + 1)$, where $n = 2p$, $x, y \in \mathbb{F}_2^p$, m is integer such that $p = 2m + 1$, then*

$$nl_2(h) \geq 2^{2p-1} - \frac{1}{2}\sqrt{2^{3p+2} - 3 \cdot 2^{2p} + 5 \cdot (2^{\frac{5p+3}{2}} - 2^{\frac{3p+3}{2}})}.$$

Proof. $h(x, y) = Tr_1^p(x(y^{2^{m+1}+1} + y^3 + y)) + \prod_{i=1}^{p}(x_i + 1)$. Let $\phi(x, y) = Tr_1^p(x(y^{2^{m+1}+1} + y^3 + y))$ and $\phi_\mu(y) = \mu \cdot \pi(y) = Tr_1^p(\mu(y^{2^{m+1}+1} + y^3 + y))$, $0 \neq \mu \in \mathbb{F}_2^p$. Then by Lemma 6 Walsh transform of $D_{(a,b)}h$ at $(\mu, \eta) \in \mathbb{F}_2^p \times \mathbb{F}_2^p$ is

$$| W_{D_{(a,b)}h}(\mu, \eta) | \leq | W_{D_{(a,b)}\phi}(\mu, \eta) | + 4 | W_{a \cdot \pi}(\eta) | . \tag{8}$$

The first order derivative of ϕ_μ w. r. t. a, $a \in \mathbb{F}_{2^p}$ is

$$\begin{aligned}
D_a \phi_\mu(x) &= Tr_1^p(\mu((x + a)^{2^{m+1}+1} + (x + a)^3 + (x + a))) + Tr_1^p(\mu(x^{2^{m+1}+1} + x^3 + x)) \\
&= Tr_1^p(\mu(x^{2^{m+1}} a + a^{2^{m+1}} x + ax^2 + a^2 x)) \\
&= Tr_1^p(x^{2^{m+1}} a\mu + a^{2^{m+1}} \mu x + a\mu x^2 + a^2 \mu x) \\
&= Tr_1^p(x^{2^{m+1}} a\mu) + Tr_1^p(a\mu x^2) + Tr_1^p((a^2 \mu + a^{2^{m+1}} \mu)x) \\
&= Tr_1^p((a^{2^m} \mu^{2^m} + a^{2^{2m}} \mu^{2^{2m}} + a^{2^{m+1}} \mu + a^2 \mu)x)
\end{aligned}$$

$D_a \phi_\mu$ is constant if and only if

$$\begin{aligned}
& a^{2^m} \mu^{2^m} + a^{2^{2m}} \mu^{2^{2m}} + a^{2^{m+1}} \mu + a^2 \mu = 0 \\
\textit{i.e.,} \quad & (a^{2^m} \mu^{2^m} + a^{2^{2m}} \mu^{2^{2m}} + a^{2^{m+1}} \mu + a^2 \mu)^{2^{2m}} = 0
\end{aligned}$$

$$\textit{i.e.,} \quad a^{2^{4m}} \mu^{2^{4m}} + a^{2^{3m}} \mu^{2^{3m}} + a^{2^m} \mu^{2^{2m}} + \mu^{2^{2m}} a = 0 \quad . \tag{9}$$

Thus, for any nonzero $a \in \mathbb{F}_{2^p}$, $a^{2^{4m}} \mu^{2^{4m}} + a^{2^{3m}} \mu^{2^{3m}} + a^{2^m} \mu^{2^{2m}} + \mu^{2^{2m}} a$ is a linearized polynomial, then by Lemma 1, (9) have at most 2^4 solutions in $\mathbb{F}_{2^p}$. Hence by Lemma 3 we have the dimension of the kernel k associated with ϕ_μ is at most 4 i.e., $k \leq 4$. Since p is odd integer so that $k \leq 3$. Thus the walsh transform of ϕ_μ at any point $\alpha \in \mathbb{F}_{2^p}$ is

$$W_{\phi_\mu}(\alpha) = W_{\mu \cdot \pi}(\alpha) \leq 2^{\frac{p+3}{2}}. \tag{10}$$

It is given by Sarkar and Gangopadhyay [10] that the dimension of kernel $k(a,b)$ of bilinear form associated with $D_{(a,b)}\phi$ is

$$k(a,b) = \begin{cases} i+p, 0 \leq i \leq 4, & \text{if } b = 0, \\ r+j, 0 \leq r \leq 20 \leq j \leq 2, & \text{if } b \neq 0. \end{cases}$$

Since the kernel of the bilinear form associated with $D_{(a,b)}\phi$ is the subspace of $\mathbb{F}_{2^{2p}}$. therefore the kernel is $k(a,b)$ even. Thus,

$$k(a,b) \leq \begin{cases} p+3, & \text{if } b = 0, \\ 4, & \text{if } b \neq 0. \end{cases}$$

The above equation can be written as

$$k(a,b) \leq \begin{cases} p+3, & \text{if } a \neq 0, b = 0, \\ 4, & \text{if } a = 0, b \neq 0. \\ 4, & \text{if } a \neq 0, b \neq 0. \end{cases}$$

Thus we have

$$W_{D_{(a,b)}\phi}(\mu,\eta) \leq \begin{cases} 2^{p+2}, & \text{if } a \neq 0, b \neq 0, \\ 2^{p+2}, & \text{if } a = 0, b \neq 0, \\ 2^{\frac{3p+3}{2}}, & \text{if } a \neq 0, b = 0. \end{cases} \tag{11}$$

Using (8), (10) and (11) we have

$$W_{D_{(a,b)}h}(\mu,\eta) \leq \begin{cases} 2^{p+2} + 2^{\frac{p+7}{2}}, & \text{if } a \neq 0, b \neq 0, \\ 2^{p+2}, & \text{if } a = 0, b \neq 0, \\ 2^{\frac{3p+4}{2}} + 2^{\frac{p+7}{2}}, & \text{if } a \neq 0, b = 0. \end{cases}$$

Therefore nonlinearity of $D_{(a,b)}h$ is

$$nl(D_{(a,b)}h) \geq \begin{cases} 2^{2p-1} - 2^{p+1} - 2^{\frac{p+5}{2}}, & \text{if } a \neq 0, b \neq 0, \\ 2^{2p-1} - 2^{p+1}, & \text{if } a = 0, b \neq 0, \\ 2^{2p-1} - 2^{\frac{3p+1}{2}} - 2^{\frac{p+5}{2}}, & \text{if } a \neq 0, b = 0. \end{cases}$$

$$\begin{aligned}
&\sum_{(a,b)\in\mathbb{F}_{2^p}\times\mathbb{F}_{2^p}} nl(D_{(a,b)}h) \\
&= nl(D_{(0,0)}h) + \sum_{b\in\mathbb{F}_{2^p}, b\neq 0} nl(D_{(0,b)}h) + \sum_{a\in\mathbb{F}_{2^p}, a\neq 0} nl(D_{(a,0)}h) + \sum_{(a,b)\in\mathbb{F}_{2^p}\times\mathbb{F}_{2^p}, a\neq 0, b\neq 0} nl(D_{(a,b)}h) \\
&\geq (2^p-1)(2^{2p-1} - 2^{p+1}) + (2^p-1)(2^{2p-1} - 2^{\frac{3p+1}{2}} - 2^{\frac{p+5}{2}}) \\
&+(2^p-1)(2^p-1)(2^{2p-1} - 2^{p+1} - 2^{\frac{p+5}{2}}) \\
&= (2^p-1)\{2^{3p-1} + 2^{2p-1} - 5\cdot 2^{\frac{3p+1}{2}} - 2^{2p+1}\} \\
&= 2^{4p-1} - 2^{3p+1} - 5(2^{\frac{5p+1}{2}} - 2^{\frac{3p+1}{2}}) + 3\cdot 2^{2p-1}
\end{aligned}$$

Using Proposition 2 we have

$$\begin{aligned}
nl_2(h) &\geq 2^{2p-1} - \frac{1}{2}\sqrt{2^{4p} - 2\{2^{4p-1} - 2^{3p+1} - 5(2^{\frac{5p+1}{2}} - 2^{\frac{3p+1}{2}}) + 3\cdot 2^{2p-1}\}} \\
&= 2^{2p-1} - \frac{1}{2}\sqrt{2^{3p+2} - 3\cdot 2^{2p} + 5\cdot(2^{\frac{5p+3}{2}} - 2^{\frac{3p+3}{2}})}.
\end{aligned}$$

□

References

1. C. Bracken, E. Byrne, N. Markin and Gary MacGuire, Determining the Nonlinearity a New Family of APN Functions, AAECC, LNCS 4851, springer, 2007, pp. 72-79.
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, Two new classes of bent functions, in Proc. EUROCRYPT '93, LNCS vol. 765, Springer, 1994, pp. 77-101.
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. N. Courtois, Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt, in: Proceedings of the ICISC'02, LNCS, vol. 2587, Springer, 2002, pp. 182-199.
6. J. Golić, Fast low order approximation of cryptographic functions, in: Proceedings of the EUROCRYPT'96, LNCS, vol. 1996, Springer, 1996, pp. 268-282.
7. 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.
8. 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.
9. F. J. MacWilliams and N. J. A. Sloane, The theory of error correcting codes, North-Holland, Amsterdam, 1977.
10. S. Sarkar and S. Gangopadhyay, On the Second Order Nonlinearity of a Cubic Maiorana-McFarland Bent Function, Finite Fields and their Applications, Fq 9, Dublin, Ireland, July 13-17, 2009.
11. 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.