1 Introduction

Boolean functions play an important role in the design of the symmetric cryptography and coding theory, see [1,2,5]. The r-th order nonlinearities of Boolean functions are of great interest, for being the most important cryptographic criteria for the symmetric cryptography. This cryptographic criterion, denoted by $nl_r(f)$, measures the minimum Hamming distance of the Boolean function f in n variables to the set of all functions in n variables of algebraic degree at most $r \leq n$, where r is a positive number. The Boolean functions used in symmetric cryptography must have high r-th order nonlinearities for being against attacks illustrated in several papers [6, 11, 12, 14]. In coding theory, $nl_r(f)$ equals the distance from f to the Reed-Muller code $\mathcal{RM}(r,n)$ of length 2^n and of order r. Thus, the maximum r-th order nonlinearity of all Boolean functions in n variables equals the covering radius of $\mathcal{RM}(r,n)$ [5]. This parameter is also related to the Gowers norm in theoretical computer science, since the correlation between a Boolean function f to the closest degree d polynomial is at most its $(d+1)$-th Gowers norm [1].

However, computing the r-th order nonlinearity of a given Boolean function with algebraic degree strictly greater than r is a hard task for $r > 1$, even the second-order nonlinearity is known only for a few peculiar functions and functions with small number of variables. Fortunately, in the case of $r = 1$ (we call the first order nonlinearity of f by the nonlinearity of f and denote it by $nl(f)$ instead of $nl_1(f)$), the nonlinearity is related with Walsh transform, which can be computed by the algorithm. For the second-order nonlinearity, Kabatiansky and Tavernier [13] proposed an algorithm using list decoding of second-order Reed-Muller codes. Soon, Fourquet and Tavernier improved and implemented this algorithm to quadratic Boolean functions up to $n = 11$ and some special quadratic functions up to $n = 13$ in [7].

It is also a difficult task that proving lower bounds on the r-th order nonlinearity of functions, even for $r = 2$. In [3], Carlet gives two lemmas about lower bounds on the nonlinearity profile of a Boolean function by a recursive approach. Meanwhile, he derives some lower bounds on the nonlinearity profiles of Maiorana-McFarland, Welch, Kasami and inverse functions. Thanks to Carlet's recursive approach, numerous authors have obtained lower bounds on r-th order nonlinearities of special functions, mostly for $r = 2, 3$ [8–10, 15–17, 19, 21–23, 25, 26].

In this article, we derive a lower bound on the third-order nonlinearity of the simplest $\mathcal{PS}$ bent functions $f(x,y)$. Using the Carlet's lemma twice, we only need to determine the nonlinearities of the second-order derivatives of $f(x,y)$ for all possible pairs (α,β). To obtain the nonlinearities of $D_\beta D_\alpha f(x,y)$, the Walsh transform makes it equivalent to determine the values of the special character sums with all cases of $(\alpha,\beta) \in \mathbb{F}_{2^k}^2$. By simple algebraic geometry lemmas and the calculation, an upper bound on the nonlinearities of $D_\beta D_\alpha f(x,y)$ for all trivial cases is derived. While for general cases, we obtain the nonlinearities of $D_\beta D_\alpha f(x,y)$ by determining the number of solutions of the system of trace functions. We derive then, explictly and straightforward, a lower bound on the third-order nonlinearity of the simplest $\mathcal{PS}$ bent functions $f(x,y)$.

In the present paper, we derive a lower bound on the third-order nonlinearity of the simplest $\mathcal{PS}$ bent functions $f(x,y) = \mathrm{Tr}_1^k\left(\frac{\lambda x}{y}\right)$. We improve the previous lower bounds in [4, 23], and the comparsion of those three lower bounds can be found in Table 1 for small concrete values. Specifically, our lower bound is asymptotically equivalent to $2^{n-1} - 2^{\frac{7n}{8}-\frac{1}{2}}$, whose improvement is approximate $(\sqrt{2}-1)2^{\frac{7n}{8}-\frac{1}{2}}$, compared with Carlet bound. Additionally, the lower bound we obtained is much more efficient than the previous lower bounds when n is small as we have showed.

The remainder of this paper is organized as follows. Section 2 introduces some basic notions which will be used in the manuscript. In Section 3, we present some lemmas, which are useful in Section 4. Based on known lemmas, Section 4 determines the lower bounds on the third-order nonlinearities of the simplest $\mathcal{PS}$ bent functions. Finally, Section 5 is a conclusion. Throughout this work, for any integer $n > 0$, let $\mathbb{F}_{2^n}$ denote the finite field with 2^n elements. For any integers $m \mid n$, denote Tr_m^n the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. For any set S, $\#S$ denotes the cardinality of S. And for the integer n, denote $|n|$ the absolute value

of n.

2 Preliminaries

Let $\mathbb{F}_2$ be the field with two elements $\{0,1\}$ and $\mathbb{F}_2^n$ be the vector space of n-tuples over $\mathbb{F}_2$. Let $\mathbb{F}_{2^n}$ be the finite field of order 2^n, which can be viewed as an n-dimensional vector space over $\mathbb{F}_2$. The Hamming weight of the vector $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$ is $\mathrm{wt}(\boldsymbol{a}) = \#\{1 \le i \le n \mid a_i \neq 0\}$. Meanwhile, the Hamming weight of an integer a is the Hamming weight of the binary expansion of a, that is, $\mathrm{wt}(\bar{a})$, where $\bar{a} = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$ and $a = \sum_{i=0}^{n-1} a_i 2^i$. The Hamming distance between two vectors $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$ is defined as $d_H(\boldsymbol{a}, \boldsymbol{b}) = \mathrm{wt}(\boldsymbol{a} \oplus \boldsymbol{b})$, where $\oplus$ is the addition in $\mathbb{F}_2^n$. We call n-variable Boolean functions the functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The set of all n-variables Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ will be denoted by $\mathcal{B}_n$.

Any $f \in \mathcal{B}_n$ with variables $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ can be represented by its algebraic normal form (ANF)

$$f(x_1, \ldots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} a_u \boldsymbol{x}^u,$$

where $a_u \in \mathbb{F}_2$ and the term $\boldsymbol{x}^u = \prod_{i=1}^n x_j^{u_j}$ is called a monomial. The algebraic degree of the Boolean function f is denoted by $\deg(f) = \max\{W_H(u) \mid a_u \neq 0\}$. Note that a Boolean function is affine if and only if it has algebraic degree at most 1.

Due to the isomorphism between the finite field $\mathbb{F}_{2^n}$ and the vector space $\mathbb{F}_2^n$, any n-variable Boolean function can also be defined over $\mathbb{F}_{2^n}$ and represented uniquely as a univariate polynomial over $\mathbb{F}_{2^n}$, that is with variable $x \in \mathbb{F}_{2^n}$,

$$f(x) = \sum_{i=0}^{2^n-1} \delta_i x^i,$$

where $\delta_0, \delta_{2^n-1} \in \mathbb{F}_2$ and for every $i = 1, 2, \ldots, 2^n - 2$, $\delta_{2i \pmod{2^n-1}} = \delta_i^2$. In this case, the algebraic degree of f is $\max\{\mathrm{wt}(\bar{i}) \mid \delta_i \neq 0, 1 \le i \le n\}$.

Specifically, when n is even, the third representation of an n-variable Boolean function f is possible, which is a bivariate polynomial of the form $f(x,y) = \sum_{0 \le i,j \le 2^{n/2}-1} f_{i,j} x^i y^j$, where $f_{i,j}$'s are elements of the field $\mathbb{F}_{2^{n/2}}$ and $(x,y) \in \mathbb{F}_{2^{n/2}}^2$. The algebraic degree under bivariate polynomial representation is defined as $\max\{\mathrm{wt}(\bar{i}) + \mathrm{wt}(\bar{j}) \mid f_{i,j} \neq 0, 1 \le i,j \le n\}$. Note that all of three definition of the algebraic degree are the same. Besides, the r-th order Reed-Muller code of length 2^n is denoted by $\mathcal{RM}(r,n)$. It can be presented by the set of n-variable Boolean functions of algebraic degree not greater than r. With above knowledgment, we introduce the definition of r-th order nonlinearity.

Definition 1. *Let f be an n-variable Boolean function. Let r be a positive integer such that $r < n$. The r-th order nonlinearity of f is the minimum Hamming distance from f to all elements of $\mathcal{RM}(r,n)$. We denote the r-th order nonlinearity of f by $nl_r(f)$.*

To bound the third-order nonlinearity of a Boolean function, we must consider the nonlinearities of its second-order derivatives.

Definition 2. *The first-order derivative of a Boolean function f over $\mathbb{F}_{2^n}$ at the point of $\alpha \in \mathbb{F}_{2^n}$ is defined as $D_\alpha f(x) = f(x) + f(x+\alpha)$. And the second-order derivative of a Boolean function f in the pair of $(\alpha, \beta) \in \mathbb{F}_{2^n}^2$ is defined as $D_\beta D_\alpha f(x) = f(x) + f(x+a) + f(x+\beta) + f(x+\alpha+\beta)$.*

As mentioned in the introduction, one of the essential tools to determine $nl(f)$ for any Boolean function f is called Walsh transform.

Definition 3. *Let f be a Boolean function over $\mathbb{F}_2^n$. The Walsh transform of f at the point $\boldsymbol{a} \in \mathbb{F}_2^n$ is defined as*

$$W_f(\boldsymbol{a}) = \sum_{\boldsymbol{x} \in \mathbb{F}_2^n} (-1)^{f(\boldsymbol{x}) + \boldsymbol{a} \cdot \boldsymbol{x}},$$

where $\boldsymbol{a} \cdot \boldsymbol{x}$ is the usual inner product in $\mathbb{F}_2^n$.

If f is over $\mathbb{F}_{2^n}$, the Walsh transform of f at the point $\alpha \in \mathbb{F}_{2^n}$ is defined as

$$W_f(\alpha) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(\alpha x)}.$$

In addition, if $n = 2k$ is even and $f(x, y)$ is the bivariate polynomial form of f, the Walsh transform of f at $(\alpha, \beta) \in \mathbb{F}_{2^k}^2$ is defined as

$$W_f(\alpha, \beta) = \sum_{(\alpha,\beta) \in \mathbb{F}_{2^k}^2} (-1)^{f(x,y)+\mathrm{Tr}_1^k(\alpha x+\beta y)}.$$

Therefore, the nonlinearity of a Boolean function $f \in \mathcal{B}_n$ can be computed as

$$\begin{aligned} nl(f) &= 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_f(a)| \\ &= 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_{2^n}} |W_f(\alpha)| \\ &= 2^{n-1} - \frac{1}{2} \max_{(\alpha,\beta) \in \mathbb{F}_{2^k}^2} |W_f(\alpha, \beta)|, \text{ if } n = 2k \text{ is even.} \end{aligned}$$

The above equation points out the importance of Walsh transform for computing the nonlinearity of a Boolean function.

To achieve the goal of efficiently bounding the r-order nonlinearity of a given function, a lemma derived in [3] are introduced, when lower bounds exist for the $(r-1)$-th order nonlinearities of the derivatives of f:

Lemma 1. *Let f be an n-variable Boolean function, and let $0 < r < n$ be an integer. We have*

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

We ignore another lemma in [3], since the bound deduced from it, in general, is not tighter than the bound derived from Lemma 1.

There is a class of character sums with polynomial arguments needed to be treated in the proof of the main theorem. To solve this, we need the following lemma about algebraic geometry.

Lemma 2 ([20])**.** *Let $K = F(X, Y)$, where X, Y are transcendentals over F. Then the genus g of the function field K/F satisfies:*

$$g \leq ([K : F(X)] - 1)([K : F(Y)] - 1).$$

3 The multiplicative inverse function

In this section, we are going to provide a prelude about the multiplicative inverse function, which is useful for proving our main theorem.

For any finite field $\mathbb{F}_{2^n}$, the multiplicative inverse function of $\mathbb{F}_{2^n}$, denoted by I, is defined as $I(x) = x^{2^n-2}$. In the sequel, we will use x^{-1} or $\frac{1}{x}$ to denote x^{2^n-2} with the convention that $x^{-1} = \frac{1}{x} = 0$ when $x = 0$. We recall that, for any $v \neq 0$, $I_v(x) = \mathrm{Tr}_1^n(vx^{-1})$ is a component function of I. The Walsh transform of I_1 at any point α is commonly known as Kloosterman sum over $\mathbb{F}_{2^n}$ at α, which is usually denoted by $\mathcal{K}(\alpha)$, *i.e.*, $\mathcal{K}(\alpha) = \widehat{I_1}(\alpha) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x^{-1}+\alpha x)}$. The original Kloosterman sums are generally defined on the multiplicative group $\mathbb{F}_{2^n}^*$. We extend them to 0 by assuming $(0)^{-1} = 1$. Regarding the Kloosterman sums, the following results are well known and we will use them in the sequel.

Lemma 3 ([24]). *Let $n \geq 3$ be an arbitrary integer. We define*

$$L = \# \left\{ c \in \mathbb{F}_{2^n} : \mathrm{Tr}_1^n \left(\frac{1}{c^2+c+1} \right) = \mathrm{Tr}_1^n \left(\frac{c^2}{c^2+c+1} \right) = 0 \right\}.$$

Then we have $L = 2^{n-2} + \frac{3}{4}(-1)^n \widehat{I_1}(1) + \frac{1}{2}(1-(-1)^n)$, where $\widehat{I_1}(1) = 1 - \sum_{t=0}^{\lfloor n/2 \rfloor} (-1)^{n-t} \frac{n}{n-t} \binom{n-t}{t} 2^t$.

Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. For any $\gamma, \eta \in \mathbb{F}_{2^n}$ and $\omega \in \mathbb{F}_{2^m}$, let us define

$$\mathcal{S}_f(\gamma, \eta, \omega) = \{ x \in \mathbb{F}_{2^n} : f(x) + f(x+\gamma) + f(x+\eta) + f(x+\eta+\gamma) = \omega \},$$

associated with $\mathcal{N}_f(\gamma, \eta, \omega) = \#\mathcal{S}_f(\gamma, \eta, \omega)$.

Lemma 4. *Let $n \geq 3$ be an integer. For $\alpha, \beta, \mu \in \mathbb{F}_{2^n}$ with $\lambda \in \mathbb{F}_{2^n}^*$, define $f(x) = \lambda x^{2^n-2}$, then*

$$S_f(\alpha, \beta, \mu) = \left\{ x \in \mathbb{F}_{2^n} : \frac{\lambda}{x} + \frac{\lambda}{x+\alpha} + \frac{\lambda}{x+\beta} + \frac{\lambda}{x+\alpha+\beta} = \mu \right\},$$

$\mathcal{N}_f(\alpha, \beta, \mu)$ can be determined:

(1) If $\alpha = \beta \in \mathbb{F}_{2^n}^*$ or $\alpha = 0$ or $\beta = 0$, then $\mathcal{N}_f(\alpha, \beta, \mu) = 2^n$ when $\mu = 0$ and $\mathcal{N}_f(\alpha, \beta, \mu) = 0$ when $\mu \in \mathbb{F}_{2^n}^*$.

(2) If $\alpha, \beta \in \mathbb{F}_{2^n}^*$ such that $\alpha \neq \beta$, we have:

(a) If $\lambda(\alpha^2 + \beta^2 + \alpha\beta) + \mu(\alpha^2\beta + \alpha\beta^2) = 0$, we have $\{0, \alpha, \beta, \alpha+\beta\} \subseteq \mathcal{S}_f(\alpha, \beta, \mu)$.

(b) If $\mu \neq 0$, $\mathrm{Tr}_1^n \left(\frac{\lambda\alpha}{\mu\beta(\alpha+\beta)} \right) = 0$ and $\mathrm{Tr}_1^n \left(\frac{\lambda\beta}{\mu\alpha(\alpha+\beta)} \right) = 0$, we have $\{y_0, y_0+\alpha, y_0+\beta, y_0+\alpha+\beta\} \subseteq \mathcal{S}_f(\alpha, \beta, \mu)$, where $y_0 \notin \{0, \alpha, \beta, \alpha+\beta\}$.

(c) If both conditions (a) and (b) cannot hold, $\mathcal{S}_f(\alpha, \beta, \mu) = \emptyset$ and then $\mathcal{N}_f(\alpha, \beta, \mu) = 0$.

Proof. The proof is analogue to the proof of Lemma 13 in [24] and we omit it. □

Remark 1. *For any $\alpha \in \mathbb{F}_{2^n}^*$, there exist L different β such that $\mathcal{N}_f(\alpha, \beta, \mu) = 8$ for some $\lambda \in \mathbb{F}_{2^n}^*$ and $\mu \in \mathbb{F}_{2^n}$. Indeed, the conditions $\alpha, \beta \in \mathbb{F}_{2^n}^*$, $\alpha \neq \beta$ and $\mu \neq 0$ can tell us $\mu(\alpha^2\beta + \alpha\beta^2) \neq 0$, resulting in $\lambda(\alpha^2 + \beta^2 + \alpha\beta) \neq 0$, which implies $\frac{\beta}{\alpha} \notin \mathbb{F}_4$. So take $\mu = \frac{\lambda(\alpha^2+\beta^2+\alpha\beta)}{\alpha^2\beta+\alpha\beta^2}$ into $\mathrm{Tr}_1^n \left(\frac{\lambda\alpha}{\mu\beta(\alpha+\beta)} \right) = 0$ and $\mathrm{Tr}_1^n \left(\frac{\lambda\beta}{\mu\alpha(\alpha+\beta)} \right) = 0$ respectively, we have $\mathrm{Tr}_1^n \left(\frac{1}{\gamma^2+\gamma+1} \right) = 0$ and $\mathrm{Tr}_1^n \left(\frac{\gamma^2}{\gamma^2+\gamma+1} \right) = 0$, where $\gamma = \frac{\beta}{\alpha} \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$. Therefore, according to Lemma 3, the number of $\gamma = \frac{\beta}{\alpha} \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ satisfying $\mathrm{Tr}_1^n \left(\frac{1}{\gamma^2+\gamma+1} \right) = 0$ and $\mathrm{Tr}_1^n \left(\frac{\gamma^2}{\gamma^2+\gamma+1} \right) = 0$ is L.*

4 The third-order nonlinearity of the simplest $\mathcal{PS}$ bent function

First, we begin with the definition of Dillon $\mathcal{PS}$ bent fucntions in this section. Then, the estimation for a class of character sums is given with the use of algebraic geometry. The lemmas, about the number of solutions for systems of trace functions, will be proved in the sequel. Therefore, we can determine the nonlinearities of the second-order derivatives of the given function. As a result, the lower bound on the third-order nonlinearity of the simplest $\mathcal{PS}$ bent function can be derived, which is tigher than the known lower bounds as illustrated in the table.

4.1 Dillon $\mathcal{PS}$ bent functions

Dillon presented a $\mathcal{PS}$ bent function class $f(x,y)$ from $\mathbb{F}_{2^n}=\mathbb{F}_{2^k}^2$ to $\mathbb{F}_2$ as

$$\mathcal{D}(x,y)=g\left(\frac{x}{y}\right),$$

where g is a balanced Boolean function on $\mathbb{F}_{2^k}$ with $g(0)=0$, and $\frac{x}{y}$ is defined to be 0 if $y=0$ (we shall always assume this kind of convention in the sequel).

In this paper, our goal is to give a lower bound on the third-order nonlinearity of the simplest $\mathcal{PS}$ bent function, *i.e.*

$$f(x,y)=\mathrm{Tr}_1^k\left(\frac{\lambda x}{y}\right),$$

where $(x,y)\in\mathbb{F}_{2^k}^2$, $\lambda\in\mathbb{F}_{2^k}^*$ and $\mathrm{Tr}_1^k(x)=\sum_{i=0}^{n-1}x^{2^i}$ is the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$.

4.2 The nonlinearities of the second-order derivatives of the simplest $\mathcal{PS}$ bent function

Before dealing with the nonlinearities of the second-order derivatives of the simplest $\mathcal{PS}$ bent function, We first introduce some useful lemmas about a class of character sums and the number of solutions for systems of trace functions that are needed in the sequel.

Lemma 5. *Let $k\geq 3$ be a positive integer and assume*

$$S(\alpha,\beta,v)=\sum_{x\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k\left(\frac{\alpha}{x+\beta}+\frac{\alpha}{x}+vx\right)},$$

where $\alpha,\beta,v\in\mathbb{F}_{2^k}^*$. We have

$$|S(\alpha,\beta,v)|\leq 2\left\lfloor 2^{\frac{k}{2}+1}\right\rfloor+4.$$

Proof. Note that $S(1,\beta/\alpha,v\alpha)=S(\alpha,\beta,v)$. Determine the value of $S(\alpha,\beta,v)$ is equivalent to determining the number of $x\in\mathbb{F}_{2^k}$ for which $\mathrm{Tr}_1^k\left(\frac{1}{x+\beta}+\frac{1}{x}+vx\right)=0$. By Hilbert's Theorem 90, this is equivalent to determining the number of solutions (x,y) in $\mathbb{F}_{2^k}$ of $y^2+y=\frac{1}{x+\beta}+\frac{1}{x}+vx$.

Let us define

$$\mathcal{S}_{\beta,v}=\left\{(x,y)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}:y^2+y=\frac{1}{x+\beta}+\frac{1}{x}+vx\right\}.$$

Note that $y\mapsto y^2+y$ is 2-to-1, then we have

$$S(\alpha,\beta,v)=\frac{\#\mathcal{S}_{\beta,v}}{2}-\left(2^k-\frac{\#\mathcal{S}_{\beta,v}}{2}\right)=\#\mathcal{S}_{\beta,v}-2^k. \tag{1}$$

Note that $\#\mathcal{S}_{\beta,v}$ is even and then $S(\alpha,\beta,v)$ must be even, too. Consider the function field $K=\mathbb{F}_{2^k}(x,y)$ with defining equation

$$y^2+y=\frac{1}{x+\beta}+\frac{1}{x}+vx. \tag{2}$$

By Lemma 2, we can easily obtain that the genus of K is not greater than $2-\delta_v$, where $\delta_v=1$ if $v=0$ and $\delta_v=0$ otherwise. Denote by $\mathcal{N}$ the number of the places with degree one of $K/\mathbb{F}_{2^k}$. Then by Serre bound[18], we have

$$\left|\mathcal{N}-(2^k+1)\right|\leq g\left\lfloor 2^{\frac{k}{2}+1}\right\rfloor, \tag{3}$$

where g is the genus of the function field $K/\mathbb{F}_{2^k}$. And we also need to the equality

$$\mathcal{N} = \#\mathcal{S}_{\beta,v} - \mathcal{M}_{\beta,v}, \tag{4}$$

where $\mathcal{M}_{\beta,v}$ is the number of the points at infinity of equation (2). So we homogenize (2) to

$$\left(\frac{Y}{Z}\right)^2 + \frac{Y}{Z} = \frac{Z}{X+\beta Z} + \frac{Z}{X} + \frac{vX}{Z}. \tag{5}$$

Multiplying both sides of (5) by $Z^2X\left(X+\beta Z\right)$ and then let $Z=0$, we have

$$X^2Y^2 = 0,$$

hence the points at infinite are $(1:0:0)$ and $(0:1:0)$. We now consider the multiplicity of roots of $(0:1:0)$ and $(1:0:0)$, respectively. For the point $(0:1:0)$, *i.e.*, $Y=1$, we have

$$\left(\frac{1}{z}\right)^2 + \frac{1}{z} = \frac{z}{x+\beta z} + \frac{z}{x} + \frac{vx}{z}. \tag{6}$$

And multiplying (6) by $z^2x(x+\beta z)$ gives

$$x^2 + \beta xz + R_{\beta,v}(x,z) = 0,$$

where $R_{\beta,v}(x,z) = \beta xz^2 + x^2z + \beta z^4 + v\beta x^2z^2 + vx^3z$ is a polynomial such that its every monomial has algebraic degree at least 3. This gives $(0:1:0)$ is a root of multiplicity 2.

For the point $(1:0:0)$, *i.e.*, $X=1$, we have

$$\left(\frac{y}{z}\right)^2 + \frac{y}{z} = \frac{z}{1+\beta z} + z + \frac{v}{z}. \tag{7}$$

And multiplying (7) by $z^2(1+\beta z)$ gives

$$vz + v\beta z^2 + y^2 + zy + \beta y^2z + \beta yz^2 + \beta z^4 = 0.$$

Note that when $v=0$, we have

$$y^2 + zy + \beta y^2z + \beta yz^2 + \beta z^4 = 0,$$

which implies that $(1:0:0)$ is a root of multiplicity 2.

Therefore, equation (2) has at most 4 points at infinity, *i.e.* $\mathcal{M}_{\beta,v} \le 4$. So combining (1),(3),(4) and the fact that $S(\alpha,\beta,v)$ is even, we can get our assertion

$$|S(\alpha,\beta,v)| \le 2\left\lfloor 2^{\frac{k}{2}+1}\right\rfloor + 4.$$

□

Lemma 6. *Assume $k \ge 3$ be a positive integer, let*

$$N_{i,j} = \#\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k\left(\theta_1x+\gamma_1\right) = i, \mathrm{Tr}_1^k\left(\theta_2x+\gamma_2\right) = j\right\},$$

where $\gamma_1,\gamma_2 \in \mathbb{F}_{2^k}$ and $\theta_1,\theta_2 \in \mathbb{F}_{2^k}^*$ are distinct. Then $N_{0,0} = 2^{k-2}$.

Proof. We have

$$\begin{cases} N_{0,0} + N_{0,1} = \#\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k\left(\theta_1x+\gamma_1\right) = 0\right\} = 2^{k-1} \\ N_{1,1} + N_{0,1} = \#\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k\left(\theta_2x+\gamma_2\right) = 1\right\} = 2^{k-1}, \end{cases}$$

then we get $N_{0,0} = N_{1,1}$. Besides, $N_{0,0} + N_{1,1} = \#\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k\left((\theta_1+\theta_2)x + (\gamma_1+\gamma_2)\right) = 0\right\} = 2^{k-1}$ since the trace function is balanced if $\theta_1 \ne \theta_2$. Therefore $N_{0,0} = 2^{k-2}$. This completes the proof. □

Lemma 7. *Assume $k \geq 3$ be a positive integer, let*

$$N_{i_1,i_2,i_3} = \#\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k(\theta_1 x + \gamma_1) = i_1, \mathrm{Tr}_1^k(\theta_2 x + \gamma_2) = i_2, \mathrm{Tr}_1^k(\theta_3 x + \gamma_3) = i_3\right\},$$

where $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{F}_{2^k}$ and $\theta_1, \theta_2, \theta_3 \in \mathbb{F}_{2^k}^*$ are distinct and satisfy $\theta_3 \neq \theta_1 + \theta_2$. Then $N_{0,0,0} = 2^{k-3}$.

Proof. Using Lemma 6 we have

$$\begin{cases} N_{0,0,0} + N_{0,0,1} = \#\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k(\theta_1 x + \gamma_1) = 0, \mathrm{Tr}_1^k(\theta_2 x + \gamma_2) = 0\right\} = 2^{k-2} \\ N_{0,0,0} + N_{0,1,0} = \#\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k(\theta_1 x + \gamma_1) = 0, \mathrm{Tr}_1^k(\theta_3 x + \gamma_3) = 0\right\} = 2^{k-2} \\ N_{0,0,0} + N_{1,0,0} = \#\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k(\theta_2 x + \gamma_2) = 0, \mathrm{Tr}_1^k(\theta_3 x + \gamma_3) = 0\right\} = 2^{k-2}. \end{cases} \tag{8}$$

Thus, $N_{0,0,1} = N_{0,1,0} = N_{1,0,0}$. With the same reason we can also obtain $N_{0,1,1} = N_{1,0,1} = N_{1,1,0}$.

As a result of $\theta_1 + \theta_2 + \theta_3 \neq 0$, we arrive at

$$\begin{cases} N_{0,0,1} + N_{0,1,0} + N_{1,0,0} + N_{1,1,1} = \#\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k((\theta_1 + \theta_2 + \theta_3)x + (\gamma_1 + \gamma_2 + \gamma_3)) = 1\right\} = 2^{k-1} \\ N_{0,1,1} + N_{1,0,1} + N_{1,1,0} + N_{0,0,0} = \#\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k((\theta_1 + \theta_2 + \theta_3)x + (\gamma_1 + \gamma_2 + \gamma_3)) = 0\right\} = 2^{k-1}. \end{cases} \tag{9}$$

Combining equations (9) with equations

$$\begin{cases} N_{0,0,0} + N_{0,0,1} + N_{0,1,0} + N_{0,1,1} = \#\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k(\theta_1 x + \gamma_1) = 0\right\} = 2^{k-1} \\ N_{1,0,0} + N_{1,0,1} + N_{1,1,0} + N_{1,1,1} = \#\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k(\theta_1 x + \gamma_1) = 1\right\} = 2^{k-1}, \end{cases} \tag{10}$$

and by the facts $N_{0,0,1} = N_{0,1,0} = N_{1,0,0}$, $N_{0,1,1} = N_{1,0,1} = N_{1,1,0}$, we obtain $N_{0,0,1} = N_{0,1,1}$. Consequently, equations (8) and equations (10) become

$$\begin{cases} N_{0,0,0} + N_{0,0,1} = 2^{k-2} \\ N_{0,0,0} + 3N_{0,0,1} = 2^{k-1}. \end{cases}$$

Clearly, $N_{0,0,0} = N_{0,0,1} = 2^{k-3}$ is the solution. This completes the proof. □

With two lemmas proved above, we can give the nonlinearities of all the second-order derivatives of the simplest $\mathcal{PS}$ bent function.

Theorem 1. *Let $k \geq 3$ be an integer and $n = 2k$. For the nonlinearity of the second-order derivative of the simplest $\mathcal{PS}$ bent function $f(x, y) = \mathrm{Tr}_1^k(\frac{\lambda x}{y})$, we have three cases based on the value of the derivative $\alpha = (\alpha_1, \alpha_2)$ as follow:*

(1) For every $\alpha = (\alpha_1, \alpha_2) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ with $\alpha_2 \neq 0$, when β ranges over $\mathbb{F}_{2^n}$, we have

$$nl(D_\beta D_\alpha f) = \begin{cases} 2^{2k-1} - 2^{k+2}, & 2^k L \text{ times} \\ 2^{2k-1} - 2^{k+1}, & 2^k(2^k - 2 - L) \text{ times} \\ 0, & 1 \text{ time}, \end{cases} \tag{11}$$

with $nl(D_\beta D_\alpha f) \geq 2^{2k-1} - 2^k\left\lfloor 2^{\frac{k}{2}+1}\right\rfloor - 2^{k+1}$ occuring $2^{k+1} - 1$ times.

(2) For every $\alpha = (\alpha_1, 0) \in \mathbb{F}_{2^k}^* \times \{0\}$, when β ranges over $\mathbb{F}_{2^n}$, we have $nl(D_\beta D_\alpha f) = 0$ occuring 2^k times, otherwise, $nl(D_\beta D_\alpha f) \geq 2^{2k-1} - 2^k\left\lfloor 2^{\frac{k}{2}+1}\right\rfloor - 2^{k+1}$ occurs $2^{2k} - 2^k$ times.

(3) For $\alpha=(0,0)$, we have $nl(D_\beta D_\alpha f)=0$ occuring 2^n times.

Proof. Let us consider the Walsh transform of the second-order derivative of $f(x,y)=\mathrm{Tr}_1^k\left(\frac{\lambda x}{y}\right)$ at the points $\alpha=(\alpha_1,\alpha_2),\beta=(\beta_1,\beta_2)\in\mathbb{F}_{2^k}^2$ with $\lambda\in\mathbb{F}_{2^k}^*$. We have

$$\begin{aligned}
&W_{D_\beta D_\alpha f}(\mu,\nu)\\
&=\sum_{x\in\mathbb{F}_{2^k}}\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda x}{y}+\frac{\lambda(x+\alpha_1)}{y+\alpha_2}+\frac{\lambda(x+\beta_1)}{y+\beta_2}+\frac{\lambda(x+\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+\mu x+\nu y\right)}\\
&=\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+\nu y\right)}\\
&\quad\times\sum_{x\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k\left(\left(\frac{\lambda}{y}+\frac{\lambda}{y+\alpha_2}+\frac{\lambda}{y+\beta_2}+\frac{\lambda}{y+\alpha_2+\beta_2}+\mu\right)x\right)}\\
&=\begin{cases}2^k\sum_{y\in S}(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+\nu y\right)}, & \text{if } \frac{\lambda}{y}+\frac{\lambda}{y+\alpha_2}+\frac{\lambda}{y+\beta_2}+\frac{\lambda}{y+\alpha_2+\beta_2}=\mu \text{ has solutions}\\ 0, & \text{otherwise,}\end{cases}
\end{aligned}$$

where S is the set of solutions of equation

$$\frac{\lambda}{y}+\frac{\lambda}{y+\alpha_2}+\frac{\lambda}{y+\beta_2}+\frac{\lambda}{y+\alpha_2+\beta_2}=\mu. \tag{12}$$

Note that $nl(D_\beta D_\alpha f)=2^{2k-1}-\frac{1}{2}\max_{\mu,\nu}\left|W_{D_\beta D_\alpha f}(\mu,\nu)\right|$, we only need to consider $\max_{\mu,\nu}|W_{D_\beta D_\alpha f}(\mu,\nu)|$ for every points α,β. So we just consider the cases such that equation (12) has solutions, since we have $2^k\left|\sum_{y\in S}(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+\nu y\right)}\right|\geq 0$. Thanks to Lemma 4, it is enough to divide points α,β into three cases by the number of solutions of equation (12):

Case 1 If $\alpha_2=\beta_2\in\mathbb{F}_{2^k}^*$ or $\alpha_2=0$ or $\beta_2=0$ and $\mu=0$, equation (12) has 2^k solutions, which actually are all elements of $\mathbb{F}_{2^k}$, then we have

$$W_{D_\beta D_\alpha f}(0,\nu)=2^k\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+\nu y\right)}. \tag{13}$$

For the simple cases, if $\alpha=(\alpha_1,0),\beta=(\beta_1,0)\in\mathbb{F}_{2^k}^*\times\{0\}$ or $\alpha=(0,0)$ or $\beta=(0,0)$, equation (13) can be transformed into a simple form:

$$W_{D_\beta D_\alpha f}(0,\nu)=2^k\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k(\nu y)}.$$

And $\max_\nu|W_{D_\beta D_\alpha f}(0,\nu)|=|W_{D_\beta D_\alpha f}(0,0)|=2^{2k}$.

For other cases, we will give the upper bounds for $\max_v|W_{D_\beta D_\alpha f}(0,v)|$: w.l.o.g. assume $\alpha_2=\beta_2\in\mathbb{F}_{2^k}^*$ and $\alpha_1\neq\beta_1$, then we have

$$\left|W_{D_\beta D_\alpha f}(0,v)\right|=2^k\left|\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2}+\frac{\lambda(\alpha_1+\beta_1)}{y}+vy\right)}\right|\leq 2^{k+1}\left\lfloor 2^{\frac{k}{2}+1}\right\rfloor+2^{k+2}.$$

Therefore, in the cases of $\alpha_2=\beta_2\in\mathbb{F}_{2^k}^*$ or $\alpha_2=0$ or $\beta_2=0$, we have

$$\max_{\mu,\nu}|W_{D_\beta D_\alpha f}(\mu,\nu)|\leq 2^{k+1}\left\lfloor 2^{\frac{k}{2}+1}\right\rfloor+2^{k+2}.$$

Case 2 If $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$ such that $\alpha_2 \neq \beta_2$ and $\mu = \frac{\lambda(\alpha_2^2+\beta_2^2+\alpha_2\beta_2)}{\alpha_2^2\beta_2+\alpha_2\beta_2^2}$, we are sure that $\{0, \alpha_2, \beta_2, \alpha_2+\beta_2\}$ are solutions of equations (12), then we have two subcases based on the number of solutions is 8 or 4:

(1) If α_2, β_2 and μ satisfy the system

$$\begin{cases} \mu \neq 0 \\ \mathrm{Tr}_1^k\left(\dfrac{\lambda\alpha_2}{\mu\beta_2(\alpha_2+\beta_2)}\right) = 0 \\ \mathrm{Tr}_1^k\left(\dfrac{\lambda\beta_2}{\mu\alpha_2(\alpha_2+\beta_2)}\right) = 0, \end{cases} \tag{14}$$

then $\{y_0, y_0+\alpha_2, y_0+\beta_2, y_0+\alpha_2+\beta_2\}$ are also solutions of equation (12), where $y_0 \notin \{0, \alpha_2, \beta_2, \alpha_2+\beta_2\}$, therefore the number of solutions is 8.

(2) Otherwise, $\{0, \alpha_2, \beta_2, \alpha_2+\beta_2\}$ are the only 4 solutions.

So we calculate $W_{D_\beta D_\alpha f}(\mu, \nu)$ for some (μ, ν) in two cases.

Subcase A We first consider the case where equation (12) has 4 solutions $\{0, \alpha_2, \beta_2, \alpha_2+\beta_2\}$, then $S = \{0, \alpha_2, \beta_2, \alpha_2+\beta_2\}$. Assume $y \in S$, we have

$$\begin{aligned}
&W_{D_\beta D_\alpha f}(\mu, \nu) \\
=&2^k\left[1+(-1)^{\mathrm{Tr}_1^k((\alpha_1+\beta_1)\mu+(\alpha_2+\beta_2)\nu)}\right] \\
&\cdot\left[(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+y\nu\right)}+(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y}+\frac{\lambda\beta_1}{y+\alpha_2+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\beta_2}+(y+\alpha_2)\nu\right)}\right] \\
=&2^k\left[1+(-1)^{\mathrm{Tr}_1^k((\alpha_1+\beta_1)\mu+(\alpha_2+\beta_2)\nu)}\right] \\
&\cdot(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+y\nu\right)}\cdot\left[1+(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y}+\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\alpha_1}{y+\beta_2}+\frac{\lambda\alpha_1}{y+\alpha_2+\beta_2}+\nu\alpha_2\right)}\right] \\
=&2^k\left[1+(-1)^{\mathrm{Tr}_1^k((\alpha_1+\beta_1)\mu+(\alpha_2+\beta_2)\nu)}\right]\cdot\left[1+(-1)^{\mathrm{Tr}_1^k(\alpha_1\mu+\alpha_2\nu)}\right]\cdot(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+y\nu\right)} \\
=&\begin{cases} 2^{k+2}\cdot(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+y\nu\right)}, & \text{if } \mathrm{Tr}_1^k(\alpha_2\nu+\alpha_1\mu)=0 \text{ and } \mathrm{Tr}_1^k(\beta_2\nu+\beta_1\mu)=0 \\ 0, & \text{otherwise.} \end{cases}
\end{aligned} \tag{15}$$

Observing (15) we can find $|W_{D_\beta D_\alpha f}(\mu, \nu)|$ only has values $\{0, 2^{k+2}\}$. Furthermore, according to Lemma 6, for all $\alpha = (\alpha_1, \alpha_2), \beta = (\beta_1, \beta_2) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}^*$ such that $\alpha_2 \neq \beta_2$ and $\mu = \frac{\lambda(\alpha_2^2+\beta_2^2+\alpha_2\beta_2)}{\alpha_2^2\beta_2+\alpha_2\beta_2^2}$, the number of $\nu \in \mathbb{F}_{2^k}$ satisfying the system

$$\begin{cases} \mathrm{Tr}_1^k(\alpha_2\nu+\alpha_1\mu) = 0 \\ \mathrm{Tr}_1^k(\beta_2\nu+\beta_1\mu) = 0 \end{cases} \tag{16}$$

is 2^{k-2} greater than 0. Thus, for all points $\alpha, \beta \in \mathbb{F}_{2^k}^2$ with $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$, $\alpha_2 \neq \beta_2$ and $\mu = \frac{\lambda(\alpha_2^2+\beta_2^2+\alpha_2\beta_2)}{\alpha_2^2\beta_2+\alpha_2\beta_2^2}$ such that don't satisfy equations (14), we have

$$\max_{\mu,\nu}|W_{D_\beta D_\alpha f}(\mu, \nu)| = 2^{k+2}.$$

Subcase B The other is that if equation (12) has 8 solutions, that is, α_2, β_2 and μ satisfy system (14).

Then we have

$$\begin{aligned}
&W_{D_\beta D_\alpha f}(\mu,\nu)\\
=&2^k\left[1+(-1)^{\mathrm{Tr}_1^k((\alpha_1+\beta_1)\mu+(\alpha_2+\beta_2)\nu)}\right]\cdot\left[1+(-1)^{\mathrm{Tr}_1^k(\alpha_1\mu+\alpha_2\nu)}\right]\\
&\cdot\left[(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{\alpha_2}+\frac{\lambda\beta_1}{\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{\alpha_2+\beta_2}\right)}+(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y_0+\alpha_2}+\frac{\lambda\beta_1}{y_0+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y_0+\alpha_2+\beta_2}+y_0\nu\right)}\right]\\
=&(-1)^{c_0}2^k\cdot\left[1+(-1)^{\mathrm{Tr}_1^k((\alpha_1+\beta_1)\mu+(\alpha_2+\beta_2)\nu)}\right]\cdot\left[1+(-1)^{\mathrm{Tr}_1^k(\alpha_1\mu+\alpha_2\nu)}\right]\cdot\left[1+(-1)^{c_0+c_1}\right]\\
=&\begin{cases}2^{k+3}\cdot(-1)^{c_0}, & \text{if } \mathrm{Tr}_1^k(\alpha_1\mu+\alpha_2\nu)=0,\mathrm{Tr}_1^k(\beta_1\mu+\beta_2\nu)=0 \text{ and } c_0+c_1=0\\ 0, & \text{otherwise,}\end{cases}
\end{aligned}$$

where $y_0\notin\{0,\alpha_2,\beta_2,\alpha_2+\beta_2\}$ and

$$\begin{cases}c_0=\mathrm{Tr}_1^k\left(\dfrac{\lambda\alpha_1}{\alpha_2}+\dfrac{\lambda\beta_1}{\beta_2}+\dfrac{\lambda(\alpha_1+\beta_1)}{\alpha_2+\beta_2}\right)\\ c_1=\mathrm{Tr}_1^k\left(\dfrac{\lambda\alpha_1}{y_0+\alpha_2}+\dfrac{\lambda\beta_1}{y_0+\beta_2}+\dfrac{\lambda(\alpha_1+\beta_1)}{y_0+\alpha_2+\beta_2}+\nu y_0\right).\end{cases}$$

By Lemma 7, for all $\alpha=(\alpha_1,\alpha_2),\beta=(\beta_1,\beta_2)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}^*$ such that $\alpha_2\neq\beta_2$ and $y_0\notin\{0,\alpha_2,\beta_2,\alpha_2+\beta_2\}$, there always exists $\nu\in\mathbb{F}_{2^k}$ satisfying below equations,

$$\begin{cases}\mathrm{Tr}_1^k(\alpha_2\nu+\alpha_1\mu)=0\\ \mathrm{Tr}_1^k(\beta_2\nu+\beta_1\mu)=0\\ \mathrm{Tr}_1^k\left(y_0\nu+\dfrac{\lambda\alpha_1}{\alpha_2}+\dfrac{\lambda\beta_1}{\beta_2}+\dfrac{\lambda(\alpha_1+\beta_1)}{\alpha_2+\beta_2}+\dfrac{\lambda\alpha_1}{y_0+\alpha_2}+\dfrac{\lambda\beta_1}{y_0+\beta_2}+\dfrac{\lambda(\alpha_1+\beta_1)}{y_0+\alpha_2+\beta_2}\right)=0\end{cases}$$

and the number of those ν is 2^{k-3}. So we conclude that for all points α,β with $\alpha_2,\beta_2\in\mathbb{F}_{2^k}^*$ such that $\alpha_2\neq\beta_2$ and $\mu=\frac{\lambda(\alpha_2^2+\beta_2^2+\alpha_2\beta_2)}{\alpha_2^2\beta_2+\alpha_2\beta_2^2}$ satisfying equations (14), we have

$$\max_{\mu,\nu}|W_{D_\beta D_\alpha f}(\mu,\nu)|=2^{k+3}.$$

Case 3 For every $\alpha_2,\beta_2\in\mathbb{F}_{2^k}^*$ such that $\alpha_2\neq\beta_2$, there exist some μ such that $S=\{y_0,y_0+\alpha_2,y_0+\beta_2,y_0+\alpha_2+\beta_2\}$ are the only 4 solutions of equation (12), where $y_0\notin\{0,\alpha_2,\beta_2,\alpha_2+\beta_2\}$. Fortunately, we don't need to treat with those μ. Indeed, in that case, the maximal possible value is not greater than the result 2^{k+2} of Case 2 where equation (12) has 4 solutions $\{0,\alpha_2,\beta_2,\alpha_2+\beta_2\}$, that is,

$$|W_{D_\beta D_\alpha f}(\mu,\nu)|=2^k\left|\sum_{y\in S}(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+y\nu\right)}\right|\leq 2^{k+2}=|W_{D_\beta D_\alpha f}(\mu_0,\nu_0)|,$$

where $\mu_0=\frac{\lambda(\alpha_2^2+\beta_2^2+\alpha_2\beta_2)}{\alpha_2^2\beta_2+\alpha_2\beta_2^2}$ and ν_0 satisfy the system (16).

□

4.3 A lower bound on the third-order nonlinearity of the simplest $\mathcal{PS}$ bent function

Applying two times Lemma 1, that is, taking

$$nl_{r-1}(D_af)\geq 2^{n-1}-\frac{1}{2}\sqrt{2^{2n}-2\sum_{b\in\mathbb{F}_2^n}nl_{r-2}D_b(D_af)},$$

into the summation of right-hand side,

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

we obtain the relation between the third-order nonlinearity of f and the nonlinearities of the second-order derivatives of f:

$$nl_3(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{\sum_{\alpha\in\mathbb{F}_{2^n}} \sqrt{2^{2n} - 2\sum_{\beta\in\mathbb{F}_{2^n}} nl(D_\beta D_\alpha f)}}. \tag{17}$$

Therefore, we can give a lower bound on the third-order nonlinearity of the simplest $\mathcal{PS}$ bent function, which can be directly deduced from inequality (17) with results of Lemma 1:

Theorem 2. *Let $k \geq 3$ be an integer and $n = 2k$. For the third-order nonlinearity of the simplest $\mathcal{PS}$ bent function $f(x, y) = \mathrm{Tr}_1^k(\frac{\lambda x}{y})$ with $x, y \in \mathbb{F}_{2^k}$ and $\lambda \in \mathbb{F}_{2^k}^*$, we have:*

$$nl_3(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{A} \approx 2^{n-1} - 2^{\frac{7n}{8}-\frac{1}{2}},$$

where

$$\begin{aligned} A = 2^n &+ (2^{\frac{n}{2}} - 1)\sqrt{(2^{\frac{3n}{2}+1} - 2^{n+1})\left\lfloor 2^{\frac{n}{4}+1}\right\rfloor + 5\cdot 2^{\frac{3n}{2}} - 2^{n+2}} \\ &+ (2^n - 2^{\frac{n}{2}})\sqrt{2^{\frac{3n}{2}+2} + 2^n - 2^{\frac{n}{2}+2} + (2^{n+2} - 2^{\frac{n}{2}+1})\left\lfloor 2^{\frac{n}{4}+1}\right\rfloor + 2^{n+2}L}, \end{aligned}$$

and L is defined in Lemma 3.

Proof. We have

$$\begin{aligned} nl_3(f) &\geq 2^{n-1} - \frac{1}{2}\sqrt{\sum_{\alpha\in\mathbb{F}_{2^n}} \sqrt{2^{2n} - 2\sum_{\beta\in\mathbb{F}_{2^n}} nl(D_\beta D_\alpha f)}} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{\left(\sum_{\alpha=(0,0)} + \sum_{\alpha=(\alpha_1,0)\in\mathbb{F}_{2^k}^*\times\{0\}} + \sum_{\substack{\alpha=(\alpha_1,\alpha_2)\in\mathbb{F}_{2^k}^2 \\ \alpha_2\neq 0}}\right)\sqrt{2^{2n} - 2\sum_{\beta\in\mathbb{F}_{2^n}} nl(D_\beta D_\alpha f)}} \\ &\geq 2^{n-1} - \frac{1}{2}\Bigg[2^n + (2^{\frac{n}{2}} - 1)\sqrt{2^{2n} - 2(2^n - 2^{\frac{n}{2}})(2^{n-1} - 2^{\frac{n}{2}}\left\lfloor 2^{\frac{n}{4}+1}\right\rfloor - 2^{\frac{n}{2}+1})} \\ &\qquad + (2^n - 2^{\frac{n}{2}})\sqrt{2^{2n} - 2\left((2^{n-1} - 2^{\frac{n}{2}+1})(2^n - 1) - (2^{n+1} - 2^{\frac{n}{2}})\left\lfloor 2^{\frac{n}{4}+1}\right\rfloor - 2^{n+1}L\right)}\Bigg]^{\frac{1}{2}}, \end{aligned}$$

where the second sign of inequality comes from Lemma 1. Then, we have

$$\begin{aligned} A = 2^n &+ (2^{\frac{n}{2}} - 1)\sqrt{(2^{\frac{3n}{2}+1} - 2^{n+1})\left\lfloor 2^{\frac{n}{4}+1}\right\rfloor + 5\cdot 2^{\frac{3n}{2}} - 2^{n+2}} \\ &+ (2^n - 2^{\frac{n}{2}})\sqrt{2^{\frac{3n}{2}+2} + 2^n - 2^{\frac{n}{2}+2} + (2^{n+2} - 2^{\frac{n}{2}+1})\left\lfloor 2^{\frac{n}{4}+1}\right\rfloor + 2^{n+2}L}. \end{aligned}$$

This completes the proof. □

Corollary 1. *The third-order nonlinearity of the simplest $\mathcal{PS}$ bent functions is lower bounded by approximately $2^{n-1} - 2^{\frac{7n}{8}-\frac{1}{2}}$.*

Remark 2. *We only compare in Table 1 the lower bounds on our third-order nonlinearity of the simplest $\mathcal{PS}$ bent function with the previously known bounds for some small concrete values. It can be seen that our lower bound on the third-order nonlinearity is always tighter than the bounds in [23] and [4]. And when n is not too large, our lower bound is much more efficient than others.*

Table 1: Comparison of the lower bounds on the third-order nonlinearity of f

n	Tang-Carlet-Tang bound in [23]	Carlet bound in [4]	Our bound in Theorem 2	Difference[1]
8	-10	-7	22	29
10	55	63	178	115
12	533	552	919	367
14	3156	3204	4352	1148
16	15984	16103	19952	3849
18	75003	75291	88967	13676
20	336633	337330	384819	47489
22	1468218	1469893	1628591	158698
24	6278535	6282550	6807016	524466
26	26469867	26479472	28237579	1758107

[1] The values in the table are the difference of our bound's values with Carlet bound's values.

References

[1] Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman. Optimal testing of reed-muller codes. In *51th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2010, October 23-26, 2010, Las Vegas, Nevada, USA*, pages 488–497. IEEE Computer Society, 2010.

[2] Claude Carlet. Boolean functions for cryptography and error correcting codes. pages 257–397, 11 2007.

[3] Claude Carlet. Recursive lower bounds on the nonlinearity profile of boolean functions and their applications. *IEEE Transactions on Information Theory*, 54(3):1262–1272, 2008.

[4] Claude Carlet. More vectorial boolean functions with unbounded nonlinearity profile. *Int. J. Found. Comput. Sci.*, 22(6):1259–1269, 2011.

[5] Gérard Cohen, Iiro Honkala, Simon Litsyn, and Antoine Lobstein. *Covering Codes*, volume 54 of *North-Holland Mathematical Library*. Elsevier, 1997.

[6] Nicolas T. Courtois. Higher order correlation attacks, XL algorithm and cryptanalysis of toyocrypt. In Pil Joong Lee and Chae Hoon Lim, editors, *Information Security and Cryptology - ICISC 2002, 5th International Conference Seoul, Korea, November 28-29, 2002, Revised Papers*, volume 2587 of *Lecture Notes in Computer Science*, pages 182–199. Springer, 2002.

[7] Rafaël Fourquet and Cédric Tavernier. An improved list decoding algorithm for the second order reed-muller codes and its applications. *Des. Codes Cryptogr.*, 49(1-3):323–340, 2008.

[8] Sugata Gangopadhyay, Sumanta Sarkar, and Ruchi Telang. On the lower bounds of the second order nonlinearities of some boolean functions. *Information Sciences*, 180(2):266–273, 2010.

[9] Qi Gao and Deng Tang. A lower bound on the second-order nonlinearity of the class of Maiorana-McFarland bent functions. In *Eighth International Workshop on Signal Design and Its Applications in Communications, IWSDA 2017, Sapporo, Japan, September 24-28, 2017*, pages 191–195. IEEE, 2017.

[10] Ruchi Gode and Sugata Gangopadhyay. Third-order nonlinearities of a subclass of Kasami functions. *Cryptography and Communications*, 2(1):69–83, 2010.

[11] Jovan Dj. Golić. Fast low order approximation of cryptographic functions. In Ueli Maurer, editor, *Advances in Cryptology — EUROCRYPT '96*, pages 268–282, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

[12] Tetsu Iwata and Kaoru Kurosawa. Probabilistic higher order differential attack and higher order bent functions. In Kwok-Yan Lam, Eiji Okamoto, and Chaoping Xing, editors, *Advances in Cryptology - ASIACRYPT'99*, pages 62–74, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[13] Grigory Kabatiansky and Cédric Tavernier. List decoding of second order Reed-Muller codes. *Proc. 8th Intern. Simp. Comm. Theory and Applications, Ambleside, UK*, 2005.

[14] Lars R. Knudsen and Matthew J. B. Robshaw. Non-linear approximations in linear cryptanalysis. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, volume 1070 of *Lecture Notes in Computer Science*, pages 224–236. Springer, 1996.

[15] Qian Liu. The lower bounds on the second-order nonlinearity of three classes of boolean functions. *Advances in Mathematics of Communications*, 17(2):418–430, 2023.

[16] Sihem Mesnager, Kwang Ho Kim, and Myong Song Jo. On the number of the rational zeros of linearized polynomials and the second-order nonlinearity of cubic boolean functions. *Cryptography and Communications*, 12(4):659–674, 2020.

[17] Sumanta Sarkar and S Gangopadhyay. On the second order nonlinearity of a cubic Maiorana-Mcfarland bent function. *Finite Fields and Their Applications*, 2009, 2009.

[18] Jean-Pierre Serre. Nombres de points des courbes algÉbriques sur f q. *Séminaire de Théorie des Nombres de Bordeaux*, pages 1–8, 1982.

[19] Brajesh Kumar Singh. On third-order nonlinearity of biquadratic monomial boolean functions. *Int. J. Eng. Math.*, 2014:1–7, 2014.

[20] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Springer Publishing Company, Incorporated, 2nd edition, 2008.

[21] Guanghong Sun and Chuankun Wu. The lower bounds on the second order nonlinearity of three classes of boolean functions with high nonlinearity. *Information Sciences*, 179(3):267–278, 2009.

[22] Guanghong Sun and Chuankun Wu. The lower bound on the second-order nonlinearity of a class of boolean functions with high nonlinearity. *Appl. Algebra Eng. Commun. Comput.*, 22(1):37–45, 2011.

[23] Deng Tang, Claude Carlet, and Xiaohu Tang. On the second-order nonlinearities of some bent functions. *Information Sciences*, 223:322–330, 2013.

[24] Deng Tang, Bimal Mandal, and Subhamoy Maitra. Further cryptographic properties of the multiplicative inverse function. *Discrete Applied Mathematics*, 307:191–211, 2022.

[25] Deng Tang, Haode Yan, Zhengchun Zhou, and Xiaosong Zhang. A new lower bound on the second-order nonlinearity of a class of monomial bent functions. *Cryptography and Communications*, 12(1):77–83, 2020.

[26] Haode Yan and Deng Tang. Improving lower bounds on the second-order nonlinearity of three classes of boolean functions. *Discrete Mathematics*, 343(5):111698, 2020.