

1 Introduction

2 Preliminaries

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

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

3 The Walsh spectra of the derivatives of the inverse function

For any integer $n > 0$, let us define $I_\nu(x) = \text{Tr}_1^n(\nu x^{-1})$ over \mathcal{B}_n . The Kloosterman sums over \mathbb{F}_{2^n} are defined as $\mathcal{K}(a) = \widehat{I}_1(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}_1^n(x^{-1} + ax)}$, where $a \in \mathbb{F}_{2^n}$. In fact, the Kloosterman sums are generally defined on the multiplicative group $\mathbb{F}_{2^n}^*$. We extend them to 0 by assuming $(-1)^0 = 1$.

Proof For any $\mu, \nu, \tau \in \mathbb{F}_{2^n}^*$, we have (still using the convention $\frac{1}{0} = 0$)

$$\begin{aligned} & C_{\mu, \nu}(\tau) \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}_1^n(\frac{\mu}{x} + \frac{\nu}{x+\tau})} \\ &= \sum_{x \in \mathbb{F}_{2^n} \setminus \{0, \tau\}} (-1)^{\text{Tr}_1^n(\frac{\mu}{x} + \frac{\nu}{x+\tau})} + (-1)^{\text{Tr}_1^n(\frac{\mu}{\tau})} + (-1)^{\text{Tr}_1^n(\frac{\nu}{\tau})} \\ &= \sum_{x \in \mathbb{F}_{2^n} \setminus \{0, \tau^{-1}\}} (-1)^{\text{Tr}_1^n(\mu x + \frac{\nu x}{1+\tau x})} + (-1)^{\text{Tr}_1^n(\frac{\mu}{\tau})} + (-1)^{\text{Tr}_1^n(\frac{\nu}{\tau})} \\ &= \sum_{x \in \mathbb{F}_{2^n} \setminus \{0, \tau^{-1}\}} (-1)^{\text{Tr}_1^n(\mu x + \frac{1}{1+\tau x} \cdot \frac{\nu}{\tau} + \frac{\nu}{\tau})} + (-1)^{\text{Tr}_1^n(\frac{\mu}{\tau})} + (-1)^{\text{Tr}_1^n(\frac{\nu}{\tau})} \\ &= \sum_{x \in \mathbb{F}_{2^n} \setminus \{0, 1\}} (-1)^{\text{Tr}_1^n(\frac{\mu x}{\tau} + \frac{\nu}{\tau x} + \frac{\mu}{\tau} + \frac{\nu}{\tau})} + (-1)^{\text{Tr}_1^n(\frac{\mu}{\tau})} + (-1)^{\text{Tr}_1^n(\frac{\nu}{\tau})} \\ &= \sum_{x \in \mathbb{F}_{2^n} \setminus \{0, \frac{\tau}{\nu}\}} (-1)^{\text{Tr}_1^n(\frac{1}{x} + \frac{\mu \nu}{\tau^2} x) + \text{Tr}_1^n(\frac{\mu}{\tau} + \frac{\nu}{\tau})} + (-1)^{\text{Tr}_1^n(\frac{\mu}{\tau})} + (-1)^{\text{Tr}_1^n(\frac{\nu}{\tau})} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}_1^n(\frac{1}{x} + \frac{\mu \nu}{\tau^2} x) + \text{Tr}_1^n(\frac{\mu}{\tau} + \frac{\nu}{\tau})} - (-1)^{\text{Tr}_1^n(\frac{\mu}{\tau} + \frac{\nu}{\tau})} - (-1)^{\text{Tr}_1^n(0)} + (-1)^{\text{Tr}_1^n(\frac{\mu}{\tau})} + (-1)^{\text{Tr}_1^n(\frac{\nu}{\tau})} \end{aligned}$$

where the third, fifth, and sixth identities hold by changing x to $\frac{1}{x}$, $\frac{x+1}{\tau}$, and $\frac{\nu x}{\tau}$ respectively. Note that $-(-1)^{\text{Tr}_1^n(\frac{\mu}{\tau} + \frac{\nu}{\tau})} - (-1)^{\text{Tr}_1^n(0)} + (-1)^{\text{Tr}_1^n(\frac{\mu}{\tau})} + (-1)^{\text{Tr}_1^n(\frac{\nu}{\tau})}$ equals 0 or -4 . According to Lemma ??, we can see that $C_{\mu, \nu}(\tau)$ belongs to $[-2^{n/2+1} - 3, 2^{n/2+1} + 1]$ and is divisible by 4. This finishes the proof.

4 Lemmas

Before giving the lower bound of third-order nonlinearity of the simplest \mathcal{PS} bent function, We first introduce some useful lemmas that are needed in the sequel.

4.1 The multiplicative inverse function

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 $v \neq 0$, $I_v(x) = \text{Tr}_1^n(vx^{-1})$ is a component function of I . The Walsh–Hadamard 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., $\mathcal{K}(\alpha) = \widehat{I}_1(\alpha) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}_1^n(x^{-1} + \alpha x)}$. The original Kloosterman sums are generally defined on the multiplicative group $\mathbb{F}_{2^n}^*$. We extend them to 0 by assuming $(-1)^0 = 1$. Regarding the Kloosterman sums, the following results are well known and we will use them in the sequel.

Lemma 1 *Let $n \geq 3$ be an arbitrary integer. We define*

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

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 an (n, m) -function. For any $\gamma, \eta \in \mathbb{F}_{2^n}$ and $\omega \in \mathbb{F}_{2^m}$, let us define

$$\mathcal{N}_F(\gamma, \eta, \omega) = \# \{ x \in \mathbb{F}_{2^n} : F(x) + F(x + \gamma) + F(x + \eta) + F(x + \eta + \gamma) = \omega \}. \quad (1)$$

It is clear that for $\gamma = 0$ or $\eta = 0$ or $\gamma = \eta$, we have $\mathcal{N}_F(\gamma, \eta, 0) = 2^n$, and when $\omega \neq 0$, $\mathcal{N}_F(\gamma, \eta, \omega) = 0$. If F is the multiplicative inverse function over \mathbb{F}_{2^n} , we denote $\mathcal{N}_I(\gamma, \eta, \omega)$ by $\mathcal{N}(\gamma, \eta, \omega)$.

Lemma 2 *Let $n \geq 3$ be a positive integer and $\mathcal{N}(\gamma, \eta, \omega)$ be defined as in (??). Let γ, η be two elements of $\mathbb{F}_{2^n}^*$ such that $\gamma \neq \eta$. Then for any $\omega \in \mathbb{F}_{2^n}$, we have $\mathcal{N}(\gamma, \eta, \omega) \in \{0, 4, 8\}$. Moreover, the number of $(\gamma, \eta, \omega) \in \mathbb{F}_{2^n}^3$ such that $\mathcal{N}(\gamma, \eta, \omega) = 8$ is*

$$\left(2^{n-2} + \frac{3}{4}(-1)^n \widehat{I}_1(1) - \frac{5}{2}(-1)^n - \frac{3}{2} \right) (2^n - 1).$$

4.2 The solutions of the system of trace functions

We explicitly give the number of solutions of systems of two or three trace functions since trace functions are balanced and \mathbb{F}_2 -linear in finite field \mathbb{F}_{2^n} .

Lemma 3 *Assume $k \geq 3$, let*

$$N_{i,j} = \left| \left\{ x \in \mathbb{F}_{2^k} \mid \text{Tr}_1^k(\theta_1 x + \gamma_1) = i, \text{Tr}_1^k(\theta_2 x + \gamma_2) = j \right\} \right|,$$

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*

$$\begin{cases} N_{0,0} + N_{0,1} = \left| \left\{ x \in \mathbb{F}_{2^k} \mid \text{Tr}_1^k(\theta_1 x + \gamma_1) = 0 \right\} \right| = 2^{k-1} \\ N_{1,1} + N_{0,1} = \left| \left\{ x \in \mathbb{F}_{2^k} \mid \text{Tr}_1^k(\theta_2 x + \gamma_2) = 1 \right\} \right| = 2^{k-1}, \end{cases}$$

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

Lemma 4 *Assume $k \geq 3$, let*

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

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 ?? we have

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

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

Because of $\theta_1 + \theta_2 + \theta_3 \neq 0$, we have

$$\begin{cases} N_{0,0,1} + N_{0,1,0} + N_{1,0,0} + N_{1,1,1} = \left| \left\{ x \in \mathbb{F}_{2^k} \mid \text{Tr}_1^k((\theta_1 + \theta_2 + \theta_3)x + (\gamma_1 + \gamma_2 + \gamma_3)) = 1 \right\} \right| = 2^{k-1} \\ N_{0,1,1} + N_{1,0,1} + N_{1,1,0} + N_{0,0,0} = \left| \left\{ x \in \mathbb{F}_{2^k} \mid \text{Tr}_1^k((\theta_1 + \theta_2 + \theta_3)x + (\gamma_1 + \gamma_2 + \gamma_3)) = 0 \right\} \right| = 2^{k-1}. \end{cases} \quad (3)$$

Combine equations (??) with $N_{0,0,1} = N_{0,1,0} = N_{1,0,0}$, $N_{0,1,1} = N_{1,0,1} = N_{1,1,0}$ and equations

$$\begin{cases} N_{0,0,0} + N_{0,0,1} + N_{0,1,0} + N_{0,1,1} = \left| \left\{ x \in \mathbb{F}_{2^k} \mid \text{Tr}_1^k(\theta_1 x + \gamma_1) = 0 \right\} \right| = 2^{k-1} \\ N_{1,0,0} + N_{1,0,1} + N_{1,1,0} + N_{1,1,1} = \left| \left\{ x \in \mathbb{F}_{2^k} \mid \text{Tr}_1^k(\theta_1 x + \gamma_1) = 1 \right\} \right| = 2^{k-1}, \end{cases} \quad (4)$$

we obtain $N_{0,0,1} = N_{0,1,1}$. Therefore from equations (??) and equations (??), the system

$$\begin{cases} N_{0,0,0} + N_{0,0,1} = 2^{k-2}, \\ N_{0,0,0} + 3N_{0,0,1} = 2^{k-1} \end{cases} \quad (5)$$

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

4.3 Higher-order nonlinearity

A theorem is introduced for efficiently bounding from below the nonlinearity profile of a given function when lower bounds exist for the $(r-1)$ -th order nonlinearities of the derivatives of f :

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

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

5 Profile of Dillon 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.*

$$f(x, y) = \text{Tr}_1^k\left(\frac{\lambda x}{y}\right) \quad (6)$$

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

Let $k \geq 3$ be an integer. Let us consider the Walsh transform of the second-order derivative of $f(x, y) = \text{Tr}_1^k\left(\frac{\lambda x}{y}\right)$ 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

$$\begin{aligned}
& W_{D_\beta D_\alpha f}(\mu, \nu) \\
&= \sum_{x \in \mathbb{F}_{2^k}} \sum_{y \in \mathbb{F}_{2^k}} (-1)^{\text{Tr}_1^k\left(\frac{\lambda x}{y} + \frac{\lambda(x+\alpha_1)}{y+\alpha_2} + \frac{\lambda(x+\beta_1)}{y+\beta_2} + \frac{\lambda(x+\alpha_1+\beta_1)}{y+\alpha_2+\beta_2} + \mu x + \nu y\right)} \\
&= \sum_{y \in \mathbb{F}_{2^k}} (-1)^{\text{Tr}_1^k\left(\frac{\lambda \alpha_1}{y+\alpha_2} + \frac{\lambda \beta_1}{y+\beta_2} + \frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2} + \nu y\right)} \\
&\quad \times \sum_{x \in \mathbb{F}_{2^k}} (-1)^{\text{Tr}_1^k\left(\left(\frac{\lambda}{y} + \frac{\lambda}{y+\alpha_2} + \frac{\lambda}{y+\beta_2} + \frac{\lambda}{y+\alpha_2+\beta_2} + \mu\right)x\right)} \\
&= \begin{cases} 2^k \sum_{y \in S} (-1)^{\text{Tr}_1^k\left(\frac{\lambda \alpha_1}{y+\alpha_2} + \frac{\lambda \beta_1}{y+\beta_2} + \frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2} + \nu y\right)}, & \text{if } \frac{\lambda}{y} + \frac{\lambda}{y+\alpha_2} + \frac{\lambda}{y+\beta_2} + \frac{\lambda}{y+\alpha_2+\beta_2} = \mu \text{ has solutions} \\ 0, & \text{otherwise,} \end{cases} \quad (7)
\end{aligned}$$

where S is the set of solutions of equation $\frac{\lambda}{y} + \frac{\lambda}{y+\alpha_2} + \frac{\lambda}{y+\beta_2} + \frac{\lambda}{y+\alpha_2+\beta_2} = \mu$.

Since $nl(D_\beta D_\alpha f) = 2^{2k-1} - \frac{1}{2} \max_{\mu, \nu} |W_{D_\beta D_\alpha f}(\mu, \nu)|$, we only need to consider $\max_{\mu, \nu} |W_{D_\beta D_\alpha f}(\mu, \nu)|$ for every points α, β . According to the proof of Lemma ?? in , for $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$ such that $\alpha_2 \neq \beta_2$, we can always find some $\mu \in \mathbb{F}_{2^k}$ such that equaiton

$$\frac{\lambda}{y} + \frac{\lambda}{y+\alpha_2} + \frac{\lambda}{y+\beta_2} + \frac{\lambda}{y+\alpha_2+\beta_2} = \mu \quad (8)$$

has at least 4 solutions. When $\alpha_2 = \beta_2 \in \mathbb{F}_{2^k}^*$ or $\alpha_2 = 0$ or $\beta_2 = 0$, equation (??) has 2^k solutions for $\mu = 0$.

Thus we only consider $|W_{D_\beta D_\alpha f}(\mu, \nu)|$ for those μ since $\left| 2^k \sum_{y \in S} (-1)^{\text{Tr}_1^k\left(\frac{\lambda \alpha_1}{y+\alpha_2} + \frac{\lambda \beta_1}{y+\beta_2} + \frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2} + \nu y\right)} \right| \geq 0$. Therefore, two steps are needed for all points $\alpha = (\alpha_1, \alpha_2), \beta = (\beta_1, \beta_2) \in \mathbb{F}_{2^k}^2$ with $\lambda \in \mathbb{F}_{2^k}^*$:

- i) Find all $(\mu, \nu) \in \mathbb{F}_{2^k}^2$ such that equation (??) has solutions.
- ii) Determine the value of $\max_{\mu, \nu} |W_{D_\beta D_\alpha f}(\mu, \nu)|$ among those (μ, ν) .

Thus, we first consider when equation (??) has solutions:

- 1) If $\alpha_2 = \beta_2 \in \mathbb{F}_{2^k}^*$ or $\alpha_2 = 0$ or $\beta_2 = 0$, then (??) has 2^k solution when $\mu = 0$.
- 2) If $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$ such that $\alpha_2 \neq \beta_2$, then using Lemma 13 of [?], we have:

- (a) If $\lambda(\alpha_2^2 + \beta_2^2 + \alpha_2\beta_2) + \mu(\alpha_2^2\beta_2 + \alpha_2\beta_2^2) = 0$, $\{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\}$ are four solutions of (??);
- (b) If $\mu \neq 0$, $\text{Tr}_1^k\left(\frac{\lambda \alpha_2}{\mu \beta_2(\alpha_2 + \beta_2)}\right) = 0$ and $\text{Tr}_1^k\left(\frac{\lambda \beta_2}{\mu \alpha_2(\alpha_2 + \beta_2)}\right) = 0$, $\{y_0, y_0 + \alpha_2, y_0 + \beta_2, y_0 + \alpha_2 + \beta_2\}$ are four solutions of (??), where y_0 is a solution of (??) and $y_0 \notin \{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\}$.

Then the second step is to find all solutions of equation (??) and calculate maxmial absolute value of $2^k \sum_{y \in S} (-1)^{\text{Tr}_1^k\left(\frac{\lambda \alpha_1}{y+\alpha_2} + \frac{\lambda \beta_1}{y+\beta_2} + \frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2} + \nu y\right)}$.

5.1 A case where equation (??) has 2^k solutions

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

$$W_{D_\beta D_\alpha f}(0, \nu) = 2^k \sum_{y \in \mathbb{F}_{2^k}} (-1)^{\text{Tr}_1^k \left(\frac{\lambda \alpha_1}{y + \alpha_2} + \frac{\lambda \beta_1}{y + \beta_2} + \frac{\lambda(\alpha_1 + \beta_1)}{y + \alpha_2 + \beta_2} + \nu y \right)}. \quad (9)$$

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 (??) can be transformed into a simple form:

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

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

Therefore we need to give the upper bound of for other situations: W.L.O.G. we assume $\alpha_2 = \beta_2 \in \mathbb{F}_{2^k}^*$ and $\alpha_1 \neq \beta_1$, then we have

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

At last we give the upper bound of absolute values of equation (??),

$$\max_{\mu, \nu} |W_{D_\beta D_\alpha f}(\mu, \nu)| \leq ***$$

5.2 The case where there are at least four solutions

If $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$ such that $\alpha_2 \neq \beta_2$ and $\mu = \frac{\lambda(\alpha_2^2 + \beta_2^2 + \alpha_2 \beta_2)}{\alpha_2^2 \beta_2 + \alpha_2 \beta_2^2}$, so $\{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\}$ are solutions of equations (??), then we have to determine the number of solutions is 8 or 4 in the following:

1) If α_2, β_2 and μ satisfy the system

$$\begin{cases} \mu \neq 0 \\ \text{Tr}_1^k \left(\frac{\lambda \alpha_2}{\mu \beta_2 (\alpha_2 + \beta_2)} \right) = 0 \\ \text{Tr}_1^k \left(\frac{\lambda \beta_2}{\mu \alpha_2 (\alpha_2 + \beta_2)} \right) = 0, \end{cases} \quad (10)$$

then $\{y_0, y_0 + \alpha_2, y_0 + \beta_2, y_0 + \alpha_2 + \beta_2\}$ are also solutions of equation (??), 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.

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

We first consider the case equation (??) has 4 solutions $\{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\}$. Then $S = \{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\}$

and $y' \in S$, we have

$$\begin{aligned}
& W_{D_\beta D_\alpha f}(\mu, \nu) \\
&= 2^k \left[1 + (-1)^{\text{Tr}_1^k(\mu(\alpha_1 + \beta_1) + \nu(\alpha_2 + \beta_2))} \right] \\
&\quad \cdot \left[(-1)^{\text{Tr}_1^k\left(\frac{\lambda\alpha_1}{y' + \alpha_2} + \frac{\lambda\beta_1}{y' + \beta_2} + \frac{\lambda(\alpha_1 + \beta_1)}{y' + \alpha_2 + \beta_2} + \nu y'\right)} + (-1)^{\text{Tr}_1^k\left(\frac{\lambda\alpha_1}{y'} + \frac{\lambda\beta_1}{y' + \alpha_2 + \beta_2} + \frac{\lambda(\alpha_1 + \beta_1)}{y' + \beta_2} + \nu(y' + \alpha_2)\right)} \right] \\
&= 2^k \left[1 + (-1)^{\text{Tr}_1^k(\mu(\alpha_1 + \beta_1) + \nu(\alpha_2 + \beta_2))} \right] \\
&\quad \cdot (-1)^{\text{Tr}_1^k\left(\frac{\lambda\alpha_1}{y' + \alpha_2} + \frac{\lambda\beta_1}{y' + \beta_2} + \frac{\lambda(\alpha_1 + \beta_1)}{y' + \alpha_2 + \beta_2} + \nu y'\right)} \cdot \left[1 + (-1)^{\text{Tr}_1^k\left(\frac{\lambda\alpha_1}{y'} + \frac{\lambda\alpha_1}{y' + \alpha_2} + \frac{\lambda\alpha_1}{y' + \beta_2} + \frac{\lambda\alpha_1}{y' + \alpha_2 + \beta_2} + \nu\alpha_2\right)} \right] \\
&= 2^k \left[1 + (-1)^{\text{Tr}_1^k(\mu(\alpha_1 + \beta_1) + \nu(\alpha_2 + \beta_2))} \right] \cdot \left[1 + (-1)^{\text{Tr}_1^k(\mu\alpha_1 + \nu\alpha_2)} \right] \cdot (-1)^{\text{Tr}_1^k\left(\frac{\lambda\alpha_1}{y' + \alpha_2} + \frac{\lambda\beta_1}{y' + \beta_2} + \frac{\lambda(\alpha_1 + \beta_1)}{y' + \alpha_2 + \beta_2} + \nu y'\right)} \\
&= \begin{cases} 2^{k+2} \cdot (-1)^{\text{Tr}_1^k\left(\frac{\lambda\alpha_1}{y' + \alpha_2} + \frac{\lambda\beta_1}{y' + \beta_2} + \frac{\lambda(\alpha_1 + \beta_1)}{y' + \alpha_2 + \beta_2} + \nu y'\right)}, & \text{if } \text{Tr}_1^k(\mu\alpha_1 + \nu\alpha_2) = 0 \text{ and } \text{Tr}_1^k(\mu\beta_1 + \nu\beta_2) = 0 \\ 0, & \text{otherwise.} \end{cases} \quad (11)
\end{aligned}$$

Observing (??) we can easily find $|W_{D_\beta D_\alpha f}(\mu, \nu)|$ only has values $\{0, 2^{k+2}\}$. Furthermore, by Lemma ??, 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 $\mu = \frac{\lambda(\alpha_2^2 + \beta_2^2 + \alpha_2\beta_2)}{\alpha_2^2\beta_2 + \alpha_2\beta_2^2}$, there always exists $2^{k-2} \nu \in \mathbb{F}_{2^k}$ satisfying the system

$$\begin{cases} \text{Tr}_1^k(\mu\alpha_1 + \nu\alpha_2) = 0 \\ \text{Tr}_1^k(\mu\beta_1 + \nu\beta_2) = 0. \end{cases} \quad (12)$$

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 (??), we have

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

Remark 1 For every $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$ such that $\alpha_2 \neq \beta_2$, there exist some μ satisfying that $\{y_0, y_0 + \alpha_2, y_0 + \beta_2, y_0 + \alpha_2 + \beta_2\}$ are the only 4 solutions of equation (??), where $y_0 \notin \{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\}$. Fortunately, we don't need to treat with those μ since the maximal possible value

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

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 satisfies system (??).

So if equation (??) has only 4 solutions, $\max_{\mu, \nu} |W_{D_\beta D_\alpha f}(\mu, \nu)| = 2^{k+2}$.

CASE.2.2 Next case is that if equation (??) has 8 solutions, that is, α_2, β_2 and μ satisfy equations (??). Then we have

$$\begin{aligned}
& W_{D_\beta D_\alpha f}(\mu, \nu) \\
&= 2^k \left[1 + (-1)^{\text{Tr}_1^k(\mu(\alpha_1 + \beta_1) + \nu(\alpha_2 + \beta_2))} \right] \cdot \left[1 + (-1)^{\text{Tr}_1^k(\mu\alpha_1 + \nu\alpha_2)} \right] \\
&\quad \cdot \left[(-1)^{\text{Tr}_1^k\left(\frac{\lambda\alpha_1}{\alpha_2} + \frac{\lambda\beta_1}{\beta_2} + \frac{\lambda(\alpha_1 + \beta_1)}{\alpha_2 + \beta_2}\right)} + (-1)^{\text{Tr}_1^k\left(\frac{\lambda\alpha_1}{y_0 + \alpha_2} + \frac{\lambda\beta_1}{y_0 + \beta_2} + \frac{\lambda(\alpha_1 + \beta_1)}{y_0 + \alpha_2 + \beta_2} + \nu y_0\right)} \right] \\
&= (-1)^{c_0} 2^k \cdot \left[1 + (-1)^{\text{Tr}_1^k(\mu(\alpha_1 + \beta_1) + \nu(\alpha_2 + \beta_2))} \right] \cdot \left[1 + (-1)^{\text{Tr}_1^k(\mu\alpha_1 + \nu\alpha_2)} \right] \cdot \left[1 + (-1)^{c_0 + c_1} \right] \\
&= \begin{cases} 2^{k+3} \cdot (-1)^{c_0}, & \text{if } \text{Tr}_1^k(\mu\alpha_1 + \nu\alpha_2) = 0, \text{Tr}_1^k(\mu\beta_1 + \nu\beta_2) = 0 \text{ and } c_0 + c_1 = 0 \\ 0, & \text{otherwise,} \end{cases} \quad (13)
\end{aligned}$$

where

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

By Lemma ??, 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 $2^{k-3} \nu \in \mathbb{F}_{2^k}$ satisfying below equations,

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

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 (??), we have

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

Remark 2 There must exist some points α, β such that $\max_{\mu, \nu} |W_{D_\beta D_\alpha f}(\mu, \nu)| = 2^{k+3}$. Indeed, the conditions $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*, \alpha_2 \neq \beta_2$ and $\mu \neq 0$ can tell us $\mu(\alpha_2^2\beta_2 + \alpha_2\beta_2^2) \neq 0$, resulting in $\lambda(\alpha_2^2 + \beta_2^2 + \alpha_2\beta_2) \neq 0$, which implies $\frac{\beta_2}{\alpha_2} \notin \mathbb{F}_4$. So take $\mu = \lambda(\alpha_2^2 + \beta_2^2 + \alpha_2\beta_2)/(\alpha_2^2\beta_2 + \alpha_2\beta_2^2)$ into $\text{Tr}_1^k \left(\frac{\lambda\alpha_2}{\mu\beta_2(\alpha_2 + \beta_2)} \right) = 0$ and $\text{Tr}_1^k \left(\frac{\lambda\beta_2}{\mu\alpha_2(\alpha_2 + \beta_2)} \right) = 0$ respectively, we can transform two equations into $\text{Tr}_1^k \left(\frac{1}{\gamma^2 + \gamma + 1} \right) = 0$ and $\text{Tr}_1^k \left(\frac{\gamma^2}{\gamma^2 + \gamma + 1} \right) = 0$, where $\gamma = \frac{\beta_2}{\alpha_2} \in \mathbb{F}_{2^k} \setminus \mathbb{F}_4$. Furthermore, according to Lemma ??, the number of $\gamma = \frac{\beta_2}{\alpha_2} \in \mathbb{F}_{2^k} \setminus \mathbb{F}_4$ satisfying $\text{Tr}_1^k \left(\frac{1}{\gamma^2 + \gamma + 1} \right) = 0$ and $\text{Tr}_1^k \left(\frac{\gamma^2}{\gamma^2 + \gamma + 1} \right) = 0$ is L , which means that for points $\alpha = (\alpha_1, \alpha_2) \in \mathbb{F}_{2^k}^2$ with $\alpha_2 \neq 0$, there exist L β_2 such that $\max_{\mu, \nu} |W_{D_\beta D_\alpha f}(\mu, \nu)| = 2^{k+3}$.

Therefore, we conclude that

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

(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

$$nl(D_\beta D_\alpha f) = \begin{cases} 2^{2k-1} - 2^{k+2}, & 2^k L \text{ times} \\ 2^{2k-1} - 2^{k+1}, & 2^k(2^k - 2 - L) \text{ times} \\ 0, & 1 \text{ time}^1, \end{cases} \quad (14)$$

with $nl(D_\beta D_\alpha f) \geq 2^{2k-1} - **$ occurring $2^{k+1} - 1$ 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 $nl(D_\beta D_\alpha f) = 0$ for $\beta = (\beta_1, 0) \in \mathbb{F}_{2^k} \times \{0\}$, otherwise, $nl(D_\beta D_\alpha f) \geq ***$.

(3) For $\alpha = (0, 0)$, we have $nl(D_\beta D_\alpha f) = 0$ for all $\beta \in \mathbb{F}_{2^n}$.

Using Theorem ??, we deduce the relation between the third-order nonlinearity of f and the nonlinearity of the second-order derivative of f :

$$nl_3(f) \geq 2^{n-1} - \frac{1}{2} \sqrt{\sum_{\alpha \in \mathbb{F}_{2^n}} \sqrt{2^{2n} - 2 \sum_{\beta \in \mathbb{F}_{2^n}} nl(D_\beta D_\alpha f)}}. \quad (15)$$

Thus we should calculate $nl(D_\beta D_\alpha f)$ for every the points $\alpha, \beta \in \mathbb{F}_{2^n}$.

Therefore, we can give the lower bound of third-order nonlinearity of the simplest PS bent function:

Theorem 3 Let $k \geq 3$ be an integer and $n = 2k$. For the simplest \mathcal{PS} bent function $f(x, y) = \text{Tr}_1^k(\frac{\lambda x}{y})$, we have:

$$nl_3(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - **}.$$

Proof We have

$$\begin{aligned} nl_3(f) &\geq 2^{n-1} - \frac{1}{2}\sqrt{\sum_{\alpha \in \mathbb{F}_{2^n}} \sqrt{2^{2n} - 2 \sum_{\beta \in \mathbb{F}_{2^n}} nl(D_\beta D_\alpha f)}} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{\sum_{\alpha=(\alpha_1, 0) \in \mathbb{F}_{2k} \times \{0\}} \sqrt{2^{2n} - 2 \sum_{\beta \in \mathbb{F}_{2^n}} nl(D_\beta D_\alpha f)} + \sum_{\substack{\alpha=(\alpha_1, \alpha_2) \in \mathbb{F}_{2k}^2 \\ \alpha_2 \neq 0}} \sqrt{2^{2n} - 2 \sum_{\beta \in \mathbb{F}_{2^n}} nl(D_\beta D_\alpha f)}} \\ &\geq \end{aligned}$$

where the second sign of inequality comes from Theorem ??.

Remark 3 We give a lower bound