1 Introduction

2 Preliminaries

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

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

3 The Walsh spectra of the derivatives of the inverse function

For any integer $n > 0$, let us define $I_\nu(x) = \mathrm{Tr}_1^n(\nu x^{-1})$ over $\mathcal{B}_n$. The Kloosterman sums over $\mathbb{F}_{2^n}$ are defined as $\mathcal{K}(a) = \widehat{I_1}(\alpha) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x^{-1}+\alpha x)}$, where $\alpha \in \mathbb{F}_{2^n}$. 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 $\frac{1}{0} = 0$)

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

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 $-(-1)^{\mathrm{Tr}_1^n(\frac{\mu}{\tau}+\frac{\nu}{\tau})} - (-1)^{\mathrm{Tr}_1^n(0)} + (-1)^{\mathrm{Tr}_1^n(\frac{\mu}{\tau})} + (-1)^{\mathrm{Tr}_1^n(\frac{\nu}{\tau})}$ 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. □

3.1 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 $v \neq 0$, $I_v(x) = \mathrm{Tr}_1^n(vx^{-1})$ 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., $\mathcal{K}(\alpha) = \widehat{I_1}(\alpha) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x^{-1}+\alpha x)}$. The original Kloosterman sums are generally defined on the multiplicative group $\mathbb{F}_{2^n}^*$. We extend them to 0 by assuming $(-1)^0 = 1$. Regarding the Kloosterman sums, the following results are well known and we will use them in the sequel.

Lemma 1. *[1] 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 an (n, m)-function. For any $\gamma, \eta \in \mathbb{F}_{2^n}$ and $\omega \in \mathbb{F}_{2^m}$, let us define

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

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. *[1] Let $n \geq 3$ be a positive integer and $\mathcal{N}(\gamma, \eta, \omega)$ be defined as in (1). 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*

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

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*

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

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

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.*

$$f(x, y) = \mathrm{Tr}_1^k \left(\frac{\lambda x}{y} \right) \tag{2}$$

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 $\mathbb{F}_2$.

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

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

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

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

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

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

then we get $N_{0,0} = N_{1,1}$. Besides, $N_{0,0} + N_{1,1} = \left|\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k\left((\theta_1 + \theta_2)x + (\gamma_1 + \gamma_2)\right) = 0\right\}\right| = 2^{k-1}$ 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*

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

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 3 we have

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

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

$$\begin{cases} N_{0,0,1} + N_{0,1,0} + N_{1,0,0} + N_{1,1,1} = \left|\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k\left(\left(\theta_1 + \theta_2 + \theta_3\right)x + \left(\gamma_1 + \gamma_2 + \gamma_3\right)\right) = 1\right\}\right| = 2^{k-1} \\ N_{0,1,1} + N_{1,0,1} + N_{1,1,0} + N_{0,0,0} = \left|\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k\left(\left(\theta_1 + \theta_2 + \theta_3\right)x + \left(\gamma_1 + \gamma_2 + \gamma_3\right)\right) = 0\right\}\right| = 2^{k-1}. \end{cases} \tag{4}$$

Combine equations (4) 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

$$\begin{cases} N_{0,0,0} + N_{0,0,1} + N_{0,1,0} + N_{0,1,1} = \left|\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k\left(\theta_1 x + \gamma_1\right) = 0\right\}\right| = 2^{k-1} \\ N_{1,0,0} + N_{1,0,1} + N_{1,1,0} + N_{1,1,1} = \left|\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{Tr}_1^k\left(\theta_1 x + \gamma_1\right) = 1\right\}\right| = 2^{k-1}, \end{cases} \tag{5}$$

we obtain $N_{0,0,1} = N_{0,1,1}$. Therefore from equations (3) and equations (5), the system

$$\begin{cases} N_{0,0,0} + N_{0,0,1} = 2^{k-2} \\ N_{0,0,0} + 3N_{0,0,1} = 2^{k-1} \end{cases} \tag{6}$$

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

Theorem 2. *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 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

$$nl(D_\beta D_\alpha f) = \begin{cases} 2^{2k-1} - 2^{k+2}, & 2^k L \ \textit{times} \\ 2^{2k-1} - 2^{k+1}, & 2^k(2^k - 2 - L) \ \textit{times} \\ 0, & 1 \ \textit{time}, \end{cases} \tag{7}$$

with $nl(D_\beta D_\alpha f) \geq 2^{2k-1} - **$ 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 $nl(D_\beta D_\alpha f) = 0$ 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 $\beta \in \mathbb{F}_{2^n}$.

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

$$\begin{aligned}
& W_{D_\beta D_\alpha f}(\mu, \nu) \\
&= \sum_{x \in \mathbb{F}_{2^k}} \sum_{y \in \mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda x}{y} + \frac{\lambda(x+\alpha_1)}{y+\alpha_2} + \frac{\lambda(x+\beta_1)}{y+\beta_2} + \frac{\lambda(x+\alpha_1+\beta_1)}{y+\alpha_2+\beta_2} + \mu x + \nu y\right)} \\
&= \sum_{y \in \mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2} + \frac{\lambda\beta_1}{y+\beta_2} + \frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2} + \nu y\right)} \\
&\quad \times \sum_{x \in \mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k\left(\left(\frac{\lambda}{y} + \frac{\lambda}{y+\alpha_2} + \frac{\lambda}{y+\beta_2} + \frac{\lambda}{y+\alpha_2+\beta_2} + \mu\right)x\right)} \\
&= \begin{cases} 2^k \sum_{y \in S} (-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2} + \frac{\lambda\beta_1}{y+\beta_2} + \frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2} + \nu y\right)}, & \text{if } \frac{\lambda}{y} + \frac{\lambda}{y+\alpha_2} + \frac{\lambda}{y+\beta_2} + \frac{\lambda}{y+\alpha_2+\beta_2} = \mu \text{ has solutions} \\ 0, & \text{otherwise}, \end{cases}
\end{aligned} \tag{8}$$

where S is the set of solutions of equation

$$\frac{\lambda}{y} + \frac{\lambda}{y+\alpha_2} + \frac{\lambda}{y+\beta_2} + \frac{\lambda}{y+\alpha_2+\beta_2} = \mu. \tag{9}$$

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 only consider $\left|W_{D_\beta D_\alpha f}(\mu,\nu)\right|$ for some μ such that equation (9) has solutions, since we have $2^k \left|\sum_{y \in S}(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2} + \frac{\lambda\beta_1}{y+\beta_2} + \frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2} + \nu y\right)}\right| \geq 0$. 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 (9) has solutions.

ii) Calculate the value $\max_{\mu,\nu}|W_{D_\beta D_\alpha f}(\mu,\nu)|$ among those (μ, ν).

So we first give the conditions such that equation (9) has solutions, whose proof is analogue to the proof of Lemma 13 in [1] and we omit it:

1) If $\alpha_2 = \beta_2 \in \mathbb{F}_{2^k}^*$ or $\alpha_2 = 0$ or $\beta_2 = 0$, then (9) 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 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 (9).

   (b) If $\mu \neq 0$, $\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_2}{\mu\beta_2(\alpha_2+\beta_2)}\right) = 0$ and $\mathrm{Tr}_1^k\left(\frac{\lambda\beta_2}{\mu\alpha_2(\alpha_2+\beta_2)}\right) = 0$, $\{y_0, y_0 + \alpha_2, y_0 + \beta_2, y_0 + \alpha_2 + \beta_2\}$ are four solutions of (9), where y_0 is a solution of (9) and $y_0 \notin \{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\}$.

After finding all $(\mu,\nu)\in\mathbb{F}_{2^k}^2$ such that equation (9) has solutions for every points $\alpha=(\alpha_1,\alpha_2),\beta=(\beta_1,\beta_2)$, we need to calculate maxmial value $2^k\left|\sum_{y\in S}(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+\nu y\right)}\right|$ between those (μ,ν).

Case 1 If $\alpha_2=\beta_2\in\mathbb{F}_{2^k}^*$ or $\alpha_2=0$ or $\beta_2=0$ and $\mu=0$, equation (9) has 2^k solutions, which are all elements of $\mathbb{F}_{2^k}$, then we have

$$W_{D_\beta D_\alpha f}(0,\nu)=2^k\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+\nu y\right)}. \tag{10}$$

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 (10) 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 of $\max_\nu|W_{D_\beta D_\alpha f}(0,\nu)|$: assume $\alpha_2=\beta_2\in\mathbb{F}_{2^k}^*$ and $\alpha_1\neq\beta_1$, then we have

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

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

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

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 (9), then we have two subcases in the following, that is:

1) If α_2,β_2 and μ satisfy the system

$$\begin{cases}\mu\neq 0\\ \mathrm{Tr}_1^k\left(\dfrac{\lambda\alpha_2}{\mu\beta_2(\alpha_2+\beta_2)}\right)=0\\ \mathrm{Tr}_1^k\left(\dfrac{\lambda\beta_2}{\mu\alpha_2(\alpha_2+\beta_2)}\right)=0,\end{cases} \tag{11}$$

then $\{y_0,y_0+\alpha_2,y_0+\beta_2,y_0+\alpha_2+\beta_2\}$ are also solutions of equation (9), 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.

Case A We first consider the case equation (9) 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

$$
\begin{aligned}
&W_{D_\beta D_\alpha f}(\mu,\nu)\\
=&2^k\left[1+(-1)^{\mathrm{Tr}_1^k((\alpha_1+\beta_1)\mu+(\alpha_2+\beta_2)\nu)}\right]\\
&\cdot\left[(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+y\nu\right)}+(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y}+\frac{\lambda\beta_1}{y+\alpha_2+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\beta_2}+(y+\alpha_2)\nu\right)}\right]\\
=&2^k\left[1+(-1)^{\mathrm{Tr}_1^k((\alpha_1+\beta_1)\mu+(\alpha_2+\beta_2)\nu)}\right]\\
&\cdot(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+y\nu\right)}\cdot\left[1+(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y}+\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\alpha_1}{y+\beta_2}+\frac{\lambda\alpha_1}{y+\alpha_2+\beta_2}+\nu\alpha_2\right)}\right]\\
=&2^k\left[1+(-1)^{\mathrm{Tr}_1^k((\alpha_1+\beta_1)\mu+(\alpha_2+\beta_2)\nu)}\right]\cdot\left[1+(-1)^{\mathrm{Tr}_1^k(\alpha_1\mu+\alpha_2\nu)}\right]\cdot(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+y\nu\right)}\\
=&\begin{cases}2^{k+2}\cdot(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+y\nu\right)}, & \text{if } \mathrm{Tr}_1^k(\alpha_2\nu+\alpha_1\mu)=0 \text{ and } \mathrm{Tr}_1^k(\beta_2\nu+\beta_1\mu)=0\\ 0, & \text{otherwise.}\end{cases}
\end{aligned}
\tag{12}
$$

Observing (12) we can find $|W_{D_\beta D_\alpha f}(\mu,\nu)|$ only has values $\{0, 2^{k+2}\}$. Furthermore, by Lemma 3, 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

$$
\begin{cases}\mathrm{Tr}_1^k(\alpha_2\nu+\alpha_1\mu)=0\\ \mathrm{Tr}_1^k(\beta_2\nu+\beta_1\mu)=0.\end{cases}
\tag{13}
$$

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 (11), we have

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

Case B Next case is that if equation (9) has 8 solutions, that is, α_2, β_2 and μ satisfy system (11). Then we have

$$
\begin{aligned}
&W_{D_\beta D_\alpha f}(\mu,\nu)\\
=&2^k\left[1+(-1)^{\mathrm{Tr}_1^k((\alpha_1+\beta_1)\mu+(\alpha_2+\beta_2)\nu)}\right]\cdot\left[1+(-1)^{\mathrm{Tr}_1^k(\alpha_1\mu+\alpha_2\nu)}\right]\\
&\cdot\left[(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{\alpha_2}+\frac{\lambda\beta_1}{\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{\alpha_2+\beta_2}\right)}+(-1)^{\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_1}{y_0+\alpha_2}+\frac{\lambda\beta_1}{y_0+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y_0+\alpha_2+\beta_2}+y_0\nu\right)}\right]\\
=&(-1)^{c_0}2^k\cdot\left[1+(-1)^{\mathrm{Tr}_1^k((\alpha_1+\beta_1)\mu+(\alpha_2+\beta_2)\nu)}\right]\cdot\left[1+(-1)^{\mathrm{Tr}_1^k(\alpha_1\mu+\alpha_2\nu)}\right]\cdot\left[1+(-1)^{c_0+c_1}\right]\\
=&\begin{cases}2^{k+3}\cdot(-1)^{c_0}, & \text{if } \mathrm{Tr}_1^k(\alpha_1\mu+\alpha_2\nu)=0, \mathrm{Tr}_1^k(\beta_1\mu+\beta_2\nu)=0 \text{ and } c_0+c_1=0\\ 0, & \text{otherwise,}\end{cases}
\end{aligned}
\tag{14}
$$

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 4, 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,

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

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 (11), we have

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

Remark 1. *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 $\mathrm{Tr}_1^k\left(\frac{\lambda\alpha_2}{\mu\beta_2(\alpha_2+\beta_2)}\right) = 0$ and $\mathrm{Tr}_1^k\left(\frac{\lambda\beta_2}{\mu\alpha_2(\alpha_2+\beta_2)}\right) = 0$ respectively, we can transform two equations into $\mathrm{Tr}_1^k\left(\frac{1}{\gamma^2+\gamma+1}\right) = 0$ and $\mathrm{Tr}_1^k\left(\frac{\gamma^2}{\gamma^2+\gamma+1}\right) = 0$, where $\gamma = \frac{\beta_2}{\alpha_2} \in \mathbb{F}_{2^k} \setminus \mathbb{F}_4$. Furthermore, according to Lemma 1, the number of $\gamma = \frac{\beta_2}{\alpha_2} \in \mathbb{F}_{2^k} \setminus \mathbb{F}_4$ satisfying $\mathrm{Tr}_1^k\left(\frac{1}{\gamma^2+\gamma+1}\right) = 0$ and $\mathrm{Tr}_1^k\left(\frac{\gamma^2}{\gamma^2+\gamma+1}\right) = 0$ 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 $\max_{\mu,\nu} |W_{D_\beta D_\alpha f}(\mu,\nu)| = 2^{k+3}$.*

Case 3 For every $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$ such that $\alpha_2 \neq \beta_2$, there exist some μ satifying 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 (9), where $y_0 \notin \{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\}$. Fortunately, we don't need to treat with those μ since in that case, the maximal possible value is not greater than the result of Case 1 where equation (9) 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 (13).

□

Applying two times Theorem 1, we obtain the relation between the third-order nonlinearity of f and the nonlinearity of the second-order derivative of f:

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

Therefore, we can give the lower bound of third-order nonlinearity of the simplest $\mathcal{PS}$ bent function:

Theorem 3. *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:*

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

where

$$A = 2^{2n} - .$$

Proof. We have

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

where the second sign of inequality comes from Theorem 2. □

4.2 Comparison with the known results

Carlet has deduced that the rth-order nonlinearity of an (n, n) Dillon function is bounded from below by.... Therefore, the lower bound on

References

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