Some Results on the Inverse Function

1 Introduction

2 Preliminaries

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

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

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

$$\begin{aligned}
& C_{\mu,\nu}(\tau) \\
= & \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(\frac{\mu}{x}+\frac{\nu}{x+\tau})} \\
= & \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,\tau\}} (-1)^{tr_1^n(\frac{\mu}{x}+\frac{\nu}{x+\tau})} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})} \\
= & \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,\tau^{-1}\}} (-1)^{tr_1^n(\mu x+\frac{\nu x}{1+\tau x})} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})} \\
= & \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,\tau^{-1}\}} (-1)^{tr_1^n(\mu x+\frac{1}{1+\tau x}\cdot\frac{\nu}{\tau}+\frac{\nu}{\tau})} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})} \\
= & \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,1\}} (-1)^{tr_1^n(\frac{\mu x}{\tau}+\frac{\nu}{\tau x}+\frac{\mu}{\tau}+\frac{\nu}{\tau})} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})} \\
= & \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,\frac{\tau}{\nu}\}} (-1)^{tr_1^n(\frac{1}{x}+\frac{\mu\nu}{\tau^2}x)+tr_1^n(\frac{\mu}{\tau}+\frac{\nu}{\tau})} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})} \\
= & \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(\frac{1}{x}+\frac{\mu\nu}{\tau^2}x)+tr_1^n(\frac{\mu}{\tau}+\frac{\nu}{\tau})} - (-1)^{tr_1^n(\frac{\mu}{\tau}+\frac{\nu}{\tau})} - (-1)^{tr_1^n(0)} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})}
\end{aligned}$$

*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 $-(-1)^{tr_1^n(\frac{\mu}{\tau}+\frac{\nu}{\tau})} - (-1)^{tr_1^n(0)} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})}$ 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

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 $v \neq 0$, $I_v(x) = \mathrm{Tr}_1^n(vx^{-1})$ 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 *Let $n \geq 3$ be an arbitrary integer. We define*

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

Then we have $L = 2^{n-2} + \frac{3}{4}(-1)^n \widehat{I_1}(1) + \frac{1}{2}\left(1-(-1)^n\right)$, 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

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

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 *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*

$$\left(2^{n-2} + \frac{3}{4}(-1)^n \widehat{I_1}(1) - \frac{5}{2}(-1)^n - \frac{3}{2} \right) (2^n - 1).$$

Lemma 3 *Assume $k \geq 3$, let $N_{i,j} = |\{x \in \mathbb{F}_{2^k} | \operatorname{Tr}_1^n(\theta_1 x + \gamma_1) = i, \operatorname{Tr}_1^n(\theta_2 x + \gamma_2) = j\}|$ 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 2 *We have $N_{0,0} + N_{0,1} + N_{1,0} + N_{1,1} = 2^k$ and $N_{0,0} + N_{0,1} = 2^{k-1}$, $N_{1,1} + N_{0,1} = 2^{k-1}$, then we get $N_{0,0} = N_{1,1}$. Besides, $N_{0,0} + N_{1,1} = |\{x \in \mathbb{F}_{2^k} | \operatorname{Tr}_1^n((\theta_1+\theta_2)x + (\gamma_1+\gamma_2)) = 0\}| = 2^{k-1}$ since $\theta_1 \neq \theta_2$. Therefore $N_{0,0} = 2^{k-2}$.*

Lemma 4 *Assume $k \geq 3$, let $N_{i_1,i_2,i_3} = |\{x \in \mathbb{F}_{2^k} | \operatorname{Tr}_1^n(\theta_1 x + \gamma_1) = i_1, \operatorname{Tr}_1^n(\theta_2 x + \gamma_2) = i_2, \operatorname{Tr}_1^n(\theta_3 x + \gamma_3) = i_3\}|$, 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 3 *From equations*

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

we get $N_{0,0,1} = N_{0,1,0} = N_{1,0,0}$. With the same reason we can also obtain $N_{0,1,1} = N_{1,0,1} = N_{1,1,0}$. Because $\theta_1 + \theta_2 + \theta_3 \neq 0$, we can get equations:

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

Combine $N_{0,0,1} = N_{0,1,0} = N_{1,0,0}$, $N_{0,1,1} = N_{1,0,1} = N_{1,1,0}$, equations (3) with equations

$$\begin{cases} N_{0,0,0} + N_{0,0,1} + N_{0,1,0} + N_{0,1,1} = |\{x \in \mathbb{F}_{2^k} | \operatorname{Tr}_1^n(\theta_1 x + \gamma_1) = 0\}| = 2^{k-1} \\ N_{1,0,0} + N_{1,0,1} + N_{1,1,0} + N_{1,1,1} = |\{x \in \mathbb{F}_{2^k} | \operatorname{Tr}_1^n(\theta_1 x + \gamma_1) = 1\}| = 2^{k-1}. \end{cases} \tag{4}$$

we obtain the result $N_{0,0,1} = N_{0,1,1}$. Therefore from equations (2) and equations (4) we have

$$\begin{cases} N_{0,0,0} + N_{0,0,1} = 2^{k-2} \\ N_{0,0,0} + 3N_{0,0,1} = 2^{k-1}. \end{cases} \tag{5}$$

and the solution is $N_{0,0,0} = N_{0,0,1} = 2^{k-3}$.

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.*

$$f(x,y)=\mathrm{Tr}_1^k(\frac{\lambda x}{y}) \tag{6}$$

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 $\mathbb{F}_2$.

Let us consider the Walsh transform of the second-order derivative of f at points $\alpha=(\alpha_1,\alpha_2),\beta=(\beta_1,\beta_2)\in\mathbb{F}_{2^k}^2$. We have

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

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

Thus, we consider the solutions of the equation

$$\frac{\lambda}{y}+\frac{\lambda}{y+\alpha_2}+\frac{\lambda}{y+\beta_2}+\frac{\lambda}{y+\alpha_2+\beta_2}=\mu, \tag{8}$$

we have

(1) If $\alpha_2=\beta_2$ or $\alpha_2=0$ or $\beta_2=0$, then (8) has 0 solution when $\mu\neq 0$ and has 2^k solutions otherwise;

(2) If $\alpha_2\neq\beta_2$ and $\alpha_2,\beta_2\in\mathbb{F}_{2^k}^*$, then

   (a) when $\lambda(\alpha_2^2+\beta_2^2+\alpha_2\beta_2)+\mu(\alpha_2^2\beta_2+\alpha_2\beta_2^2)=0$, we confirm $\{0,\alpha_2,\beta_2,\alpha_2+\beta_2\}$ are 4 solutions of (8);

   (b) when $\mu=0$, we have (8) in the form

$$\frac{\lambda\alpha_2}{y(y+\alpha_2)}+\frac{\lambda\alpha_2}{y(y+\alpha_2)+\alpha_2\beta_2+\beta_2^2}=0.$$

   It has solutions only when $\alpha_2=0$ or $\beta_2=0$ or $\alpha_2=\beta_2$, contradiction, so it has 0 solution;

   (c) When $\mu\neq 0$, when $\mathrm{Tr}_1^n\left(\frac{\lambda\alpha_2}{\mu\beta_2(\alpha_2+\beta_2)}\right)=0$ and $\mathrm{Tr}_1^n\left(u\left(\left(\frac{\beta_2}{\alpha_2}\right)^2+\frac{\beta_2}{\alpha_2}\right)\right)=0\Leftrightarrow\mathrm{Tr}_1^n\left(\frac{\lambda\beta_2}{\mu\alpha_2(\alpha_2+\beta_2)}\right)=0$, we confirm $\{y_0,y_0+\alpha_2,y_0+\beta_2,y_0+\alpha_2+\beta_2\}$ are 4 solutions of (8), where y_0 is a solution of (8) and u is the solution of $t^2+t+\frac{\lambda\alpha_2}{\mu\beta_2(\alpha_2+\beta_2)}=0$ with $t=\frac{y(y+\alpha_2)}{\alpha_2\beta_2+\beta_2^2}$.

Thus, we conclude that (8) has 0 solution, 4 solutions (which are $\{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\}$ or $\{y_0, y_0 + \alpha_2, y_0 + \beta_2, y_0 + \alpha_2 + \beta_2\}$), 8 solutions (which are $\{0, \alpha_2, \beta_2, \alpha_2 + \beta_2, y_0, y_0 + \alpha_2, y_0 + \beta_2, y_0 + \alpha_2 + \beta_2\}$).

So we have the following cases:

CASE.1 (trivial) If $\alpha_2 = \beta_2$ or $\alpha_2 = 0$ or $\beta_2 = 0$ with $\mu \neq 0$, then equation (8) has 0 solution, then

$$W_{D_\beta D_\alpha f}(\mu, \nu) = 0.$$

CASE.2 ?(nontrivial) If $\alpha_2 = \beta_2$ or $\alpha_2 = 0$ or $\beta_2 = 0$ with $\mu = 0$, then equation (8) has 2^k solutions, we confirm that

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

Furthermore, if $\alpha_1 = \beta_1$ or $\alpha_1 = 0$ or $\beta_1 = 0$, equation (9) can be transformed into a simple? form:

(1) If $\alpha_1 = \beta_1$, then

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

(2) If $\alpha_1 = 0$, then

$$W_{D_\beta D_\alpha f}(\mu, \nu) = 2^k \sum_{y \in \mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^n\left(\frac{\lambda\beta_1}{y+\beta_2} + \frac{\lambda\beta_1}{y+\alpha_2+\beta_2} + \nu y\right)}. \tag{11}$$

(3) If $\beta_1 = 0$, then

$$W_{D_\beta D_\alpha f}(\mu, \nu) = 2^k \sum_{y \in \mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^n\left(\frac{\lambda\alpha_1}{y+\alpha_2} + \frac{\lambda\alpha_1}{y+\alpha_2+\beta_2} + \nu y\right)}. \tag{12}$$

CASE.3 (trivial) If $\alpha_2 \neq \beta_2$ and $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$, when $\mu = 0$, we confirm (8) has 0 solution, then

$$W_{D_\beta D_\alpha f}(\mu, \nu) = 0.$$

CASE.4 (trivial) If $\alpha_2 \neq \beta_2$ and $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$, when $\mu \neq 0$, $\lambda(\alpha_2^2 + \beta_2^2 + \alpha_2\beta_2) + \mu(\alpha_2^2\beta_2 + \alpha_2\beta_2^2) \neq 0$ with $\mathrm{Tr}_1^n\left(\frac{\lambda\alpha_2}{\mu\beta_2(\alpha_2+\beta_2)}\right) = 1$ or $\mathrm{Tr}_1^n\left(\frac{\lambda\beta_2}{\mu\alpha_2(\alpha_2+\beta_2)}\right) = 1$, then (8) has 0 solution, we get

$$W_{D_\beta D_\alpha f}(\mu, \nu) = 0.$$

CASE.5 (nontrivial) If $\alpha_2 \neq \beta_2$ and $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$, when $\mu \neq 0$ and only one of the below two conditions holds:

1) $\lambda(\alpha_2^2 + \beta_2^2 + \alpha_2\beta_2) + \mu(\alpha_2^2\beta_2 + \alpha_2\beta_2^2) = 0 \Leftrightarrow \{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\}$ are solutions;

2) $\mathrm{Tr}_1^n\left(\frac{\lambda\alpha_2}{\mu\beta_2(\alpha_2+\beta_2)}\right) = 0$ and $\mathrm{Tr}_1^n\left(\frac{\lambda\beta_2}{\mu\alpha_2(\alpha_2+\beta_2)}\right) = 0 \Leftrightarrow \{y_0, y_0 + \alpha_2, y_0 + \beta_2, y_0 + \alpha_2 + \beta_2\}$ are solutions.

we confirm that (8) has 4 solution, assume 4 solutions are $S_4 = \{y', y' + \alpha_2, y' + \beta_2, y' + \alpha_2 + \beta_2\}$ where $y' = 0$ or $y' = y_0$, then we have Then we have

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

Observing (13) we can easily find it only has values $\{0, \pm 2^{k+2}\}$. Besides, when it arrives at the values $\pm 2^{k+2}$, we conclude that $\mathrm{Tr}_1^n(\mu\alpha_1 + \nu\alpha_2) = 0$ and $\mathrm{Tr}_1^n(\mu\beta_1 + \nu\beta_2) = 0$.

CASE.6 (nontrivial) If $\alpha_2 \neq \beta_2$ and $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$, when $\mu \neq 0$ and both two conditions holds:

1) $\lambda(\alpha_2^2+\beta_2^2+\alpha_2\beta_2)+\mu(\alpha_2^2\beta_2+\alpha_2\beta_2^2)=0$,

2) $\mathrm{Tr}_1^n\left(\frac{\lambda\alpha_2}{\mu\beta_2(\alpha_2+\beta_2)}\right)=0$ and $\mathrm{Tr}_1^n\left(\frac{\lambda\beta_2}{\mu\alpha_2(\alpha_2+\beta_2)}\right)=0$.

then equation (8) has 8 distinct solutions $\{0,\alpha_2,\beta_2,\alpha_2+\beta_2,y_0,y_0+\alpha_2,y_0+\beta_2,y_0+\alpha_2+\beta_2\}$.

Note that conditions $\alpha_2,\beta_2\in\mathbb{F}_{2^k}^*$, $\alpha_2\neq\beta_2$ and $\mu\neq 0$ can tell us $\mu(\alpha_2^2\beta_2+\alpha_2\beta_2^2)\neq 0$, hence $\lambda(\alpha_2^2+\beta_2^2+\alpha_2\beta_2)\neq 0$, implies $\frac{\beta_2}{\alpha_2}\notin\mathbb{F}_8$.

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 $\mathrm{Tr}_1^n\left(\frac{\lambda\alpha_2}{\mu\beta_2(\alpha_2+\beta_2)}\right)=0$ and $\mathrm{Tr}_1^n\left(\frac{\lambda\beta_2}{\mu\alpha_2(\alpha_2+\beta_2)}\right)=0$ respectively, we can get $\mathrm{Tr}_1^n\left(\frac{c}{c^2+c+1}\right)=0$ and $\mathrm{Tr}_1^n\left(\frac{c^2}{c^2+c+1}\right)=0$ where $c=\frac{\beta_2}{\alpha_2}$.

And take the 8 solutions into equation (7), we get the summation

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

where $c_0=\mathrm{Tr}_1^n\left(\frac{\lambda\alpha_1}{\alpha_2}+\frac{\lambda\beta_1}{\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{\alpha_2+\beta_2}\right)$ and $c_1=\mathrm{Tr}_1^n\left(\frac{\lambda\alpha_1}{y_0+\alpha_2}+\frac{\lambda\beta_1}{y_0+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y_0+\alpha_2+\beta_2}+\nu y_0\right)$.

Note that $c_0+c_1=\mathrm{Tr}_1^n\left(\frac{\lambda\alpha_1}{\alpha_2}+\frac{\lambda\beta_1}{\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{\alpha_2+\beta_2}+\frac{\lambda\alpha_1}{y_0+\alpha_2}+\frac{\lambda\beta_1}{y_0+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y_0+\alpha_2+\beta_2}+\nu y_0\right)$.

Therefore we need to determine for every points $\alpha=(\alpha_1,\alpha_2)$ and $\beta=(\beta_1,\beta_2)$ with $\frac{\beta_2}{\alpha_2}\in\mathbb{F}_{2^k}\setminus\mathbb{F}_{2^2}$ and $y_0\notin\{0,\alpha_2,\beta_2,\alpha_2+\beta_2\}$, whether or not there always exists $\nu\in\mathbb{F}_{2^k}$ s.t.

$$\begin{cases}\mathrm{Tr}_1^n(\mu\alpha_1+\nu\alpha_2)=0\\ \mathrm{Tr}_1^n(\mu\beta_1+\nu\beta_2)=0\\ \mathrm{Tr}_1^n\left(\dfrac{\lambda\alpha_1}{\alpha_2}+\dfrac{\lambda\beta_1}{\beta_2}+\dfrac{\lambda(\alpha_1+\beta_1)}{\alpha_2+\beta_2}+\dfrac{\lambda\alpha_1}{y_0+\alpha_2}+\dfrac{\lambda\beta_1}{y_0+\beta_2}+\dfrac{\lambda(\alpha_1+\beta_1)}{y_0+\alpha_2+\beta_2}+\nu y_0\right)=0.\end{cases}\tag{15}$$

In fact all of three equations are linear functions since μ are fixed once α_2,β_2 are fixed, and y_0 is also fixed since it's one of eight solutions of equation (8) and equation (8) is determined by λ,α_2,β_2 and μ.

Thus, using Lemma 4, we confirm that equations (15) have solutions $\nu\in\mathbb{F}_{2^k}$ for every points $\alpha=(\alpha_1,\alpha_2)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}^*$ and $\beta=(\beta_1,\beta_2)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}^*$ with $\gamma=\frac{\beta_2}{\alpha_2}\in\mathbb{F}_{2^k}\setminus\mathbb{F}_{2^2}$ satisfying $\mathrm{Tr}_1^n\left(\frac{1}{\gamma^2+\gamma+1}\right)=\mathrm{Tr}_1^n\left(\frac{\gamma^2}{\gamma^2+\gamma+1}\right)=0$ 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 equation (14) will always have points (μ,ν) leading to values $\pm 2^{k+3}$ for every points $\alpha=(\alpha_1,\alpha_2)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}^*$ and $\beta=(\beta_1,\beta_2)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}^*$ with $\gamma=\frac{\beta_2}{\alpha_2}\in\mathbb{F}_{2^k}\setminus\mathbb{F}_{2^2}$ satisfying $\mathrm{Tr}_1^n\left(\frac{1}{\gamma^2+\gamma+1}\right)=\mathrm{Tr}_1^n\left(\frac{\gamma^2}{\gamma^2+\gamma+1}\right)=0$.