Cryptography and Communications (2021) 13:695–725
https://doi.org/10.1007/s12095-021-00496-w

A class of linear codes with their complete weight enumerators over finite fields

Pavan Kumar[1] · **Noor Mohammad Khan**[1]

Received: 2 August 2020 / Accepted: 16 May 2021 / Published online: 10 June 2021

Abstract

For any positive integer $m > 2$ and an odd prime p, let $\mathbb{F}_{p^m}$ be the finite field with p^m elements and let Tr_e^m be the trace function from $\mathbb{F}_{p^m}$ onto $\mathbb{F}_{p^e}$ for a divisor e of m. In this paper, for the defining set $D = \{x \in \mathbb{F}_{p^m} : \mathrm{Tr}_e^m(x) = 1 \text{ and } \mathrm{Tr}_e^m(x^2) = 0\} = \{d_1, d_2, \ldots, d_n\}$(say), we define a p^e-ary linear code $\mathcal{C}_D$ by

$$\mathcal{C}_D = \{\mathbf{c}_a = \left(\mathrm{Tr}_e^m(ad_1), \mathrm{Tr}_e^m(ad_2), \ldots, \mathrm{Tr}_e^m(ad_n)\right) : a \in \mathbb{F}_{p^m}\}.$$

Then we determine the complete weight enumerator and weight distribution of the linear code $\mathcal{C}_D$. The presented code is optimal with respect to the Griesmer bound provided that $\frac{m}{e} = 3$. In fact, it is MDS when $\frac{m}{e} = 3$. This paper gives the results of S. Yang, X. Kong and C. Tang (Finite Fields Appl. 48 (2017)) if we take $e = 1$. In addition to the generalization of the results of Yang et al., we study the dual code $\mathcal{C}_D^{\perp}$ of the code $\mathcal{C}_D$ as well as find some optimal constant composition codes.

Keywords Linear code · Complete weight enumerator · Gauss sum · Cyclotomic number · Constant composition code

Mathematics Subject Classification 2010 94B05 · 11T71

1 Introduction

Throughout this paper, let p be an odd prime, and let $m = es$, where m, e and s (> 2) are positive integers. $\mathbb{F}_{p^m}$ denotes a finite field with p^m elements. The trace function from $\mathbb{F}_{p^m}$ onto $\mathbb{F}_{p^e}$ is denoted by Tr_e^m. Moreover, the absolute trace functions of $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^e}$ are denoted by Tr_1^m and Tr_1^e respectively. An (n, M) code over $\mathbb{F}_{p^e}$ is a subset of $\mathbb{F}_{p^e}^n$ of size M. A linear code $\mathcal{C}$ of length n over $\mathbb{F}_{p^e}$ is a subspace of $\mathbb{F}_{p^e}^n$. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_{p^e}$ is a k-dimensional subspace of $\mathbb{F}_{p^e}^n$ with minimum distance d. The members of

✉ Pavan Kumar
pavan4957@gmail.com

Noor Mohammad Khan
nm_khan123@yahoo.co.in

1 Department of Mathematics, Aligarh Muslim University, Aligarh 202002, India

the code $\mathcal{C}$ are known as *codewords*. The number of nonzero coordinates in $\mathbf{c} \in \mathcal{C}$ is called the Hamming-weight wt($\mathbf{c}$) of the codeword $\mathbf{c}$. Let A_i denote the number of codewords with Hamming weight i in a linear code $\mathcal{C}$ of length n. The weight enumerator of the code $\mathcal{C}$ is a polynomial defined by

$$1 + A_1x + A_2x^2 + \cdots + A_nx^n,$$

where $(1, A_1, \ldots, A_n)$ is called the *weight distribution* of the code $\mathcal{C}$. There is much literature on the weight distribution of some special linear codes [2, 5, 6, 11, 13]. The complete weight enumerator of a linear code $\mathcal{C}$ gives the frequency of each symbol contained in each codeword (see [18]). Assume $\mathbb{F}_{p^e} = \{w_0, w_1, \ldots, w_{p^e-1}\}$, where $w_0 = 0$. Composition of a vector $\mathbf{v}$=$(v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_{p^e}^n$, denoted by comp($\mathbf{v}$), is defined as

$$\text{comp}(\mathbf{v}) = (k_0, k_1, \ldots, k_{p^e-1}),$$

where k_j is the number of components $v_i (0 \le i \le n-1)$ of $\mathbf{v}$ that equal w_j. It is obvious that $\sum_{j=0}^{p^e-1} k_j = n$. Let $A(k_0, k_1, \ldots, k_{p^e-1})$ be the number of codewords $\mathbf{c} \in \mathcal{C}$ with comp($\mathbf{c}$)=$(k_0, k_1, \ldots, k_{p^e-1})$. Then the complete weight enumerator of the code $\mathcal{C}$ is the polynomial

$$\begin{aligned} \text{CWE}(\mathcal{C}) &= \sum_{\mathbf{c}\in\mathcal{C}} w_0^{k_0} w_1^{k_1} \cdots w_{p^e-1}^{k_{p^e-1}} \\ &= \sum_{(k_0,k_1,\ldots,k_{p^e-1})\in\mathbb{B}_n} A(k_0, k_1, \ldots, k_{p^e-1}) w_0^{k_0} w_1^{k_1} \cdots w_{p^e-1}^{k_{p^e-1}}, \end{aligned}$$

where $\mathbb{B}_n = \{(k_0, k_1, \ldots, k_{p^e-1}) : 0 \le k_j \le n, \sum_{j=0}^{p^e-1} k_j = n\}$. The complete weight enumerators of linear codes not only give the weight enumerators but also demonstrate the frequency of each symbol appearing in each codeword. Consequently, the complete weight enumerators of linear codes have been of fundamental importance to theories and practices. Recently, linear codes with their complete weight enumerators have been studied extensively. Ding et al. in [7, 8] showed that complete weight enumerators can be applied to the calculation of the deception probabilities of certain authentication codes. Constructions of some families of optimal constant composition codes and the complete weight enumerators of some constant composition codes were given in [3, 4, 9].

In [1, 12, 16, 21–24], authors constructed linear codes with their complete weight enumerators over $\mathbb{F}_p$ by employing absolute trace function. Construction of linear codes over $\mathbb{F}_{p^e}$ by considering Tr_e^m in place of Tr_1^m result in improved relative minimum distance of the codes compared with [13, 22] (see Remarks 3.13 and 3.21, Tables 9 and 10).

In the present work, we find linear codes over $\mathbb{F}_{p^e}$ by considering new defining set obtained by replacing Tr by Tr_e^m in the defining set D given in [22]. Now, we define the trace function from $\mathbb{F}_{p^m}$ onto $\mathbb{F}_{p^e}$ as follows:

$$\text{Tr}_e^m(x) = \sum_{k=0}^{s-1} x^{p^{ke}}.$$

Set $D = \{x \in \mathbb{F}_{p^m} : \text{Tr}_e^m(x) = 1 \text{ and } \text{Tr}_e^m(x^2) = 0\} = \{d_1, d_2, \ldots, d_n\}$. We define a linear code $\mathcal{C}_D$ associated with D by

$$\mathcal{C}_D = \left\{\mathbf{c}_a = \left(\text{Tr}_e^m(ad_1), \text{Tr}_e^m(ad_2), \ldots, \text{Tr}_e^m(ad_n)\right) : a \in \mathbb{F}_{p^m}\right\}. \tag{1}$$

We determine the complete weight enumerator and weight distribution of the linear code $\mathcal{C}_D$ of (1). We show that the several constructed linear codes are optimal with respect to the Griesmer bound. In fact, the constructed optimal codes are MDS. In [22], it is shown that there exists a unique MDS code when $m = 3$ while we have shown that there are infinitely many MDS codes when $s = 3$. Moreover, we have constructed some optimal dual codes of the codes defined by (1), and finally we have shown an application to constant composition codes.

Rest of the paper is organized as follows. In Section 2, we give some definitions and results on cyclotomic numbers and Gauss sums over finite fields. In Section 3.1, we present the complete weight enumerator and weight distribution of the proposed linear code $\mathcal{C}_D$. Some examples to illustrate our main results also discussed in Section 3.1. In Section 3.2, we give some optimal dual codes. In Section 4, we have shown an application of complete weight enumerator to constant composition codes. Section 5 concludes the paper with some concluding remarks.

2 Preliminaries

We begin with some preliminaries by introducing the concept of cyclotomic numbers. Let a be a primitive element of $\mathbb{F}_{p^m}$, and let $p^m = Nh + 1$ for two positive integers $N > 1$ and $h > 1$. The *cyclotomic classes* of order N in $\mathbb{F}_{p^m}$ are the cosets $\mathcal{C}_i^{(N,p^m)} = a^i \langle a^N \rangle$ for $i = 0, 1, \ldots, N-1$, where $\langle a^N \rangle$ denotes the subgroup of $\mathbb{F}_{p^m}^*$ generated by a^N. It is obvious that $\#\mathcal{C}_i^{(N,p^m)} = h$, where $\#X$, for any set X, denotes the cardinality of the set X. For fixed i and j, we define the *cyclotomic number* $(i, j)^{(N,p^m)}$ to be the number of solutions of the equation

$$x_i + 1 = x_j \qquad \left(x_i \in \mathcal{C}_i^{(N,p^m)}, x_j \in \mathcal{C}_j^{(N,p^m)}\right),$$

where $1 = a^0$ is the multiplicative identity of $\mathbb{F}_{p^m}$. That is, $(i, j)^{(N,p^m)}$ is the number of ordered pairs (s, t) such that

$$a^{Ns+i} + 1 = a^{Nt+j} \qquad (0 \leq s, t \leq h - 1).$$

Now, we present, from [14], some notions and results about group characters and Gauss sums for later use. An additive character χ of $\mathbb{F}_{p^m}$ is a mapping from $\mathbb{F}_{p^m}$ into the multiplicative group of complex numbers of absolute value 1 with $\chi(g_1 + g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in \mathbb{F}_{p^m}$. By ([14], Theorem 5.7), for any $b \in \mathbb{F}_{p^m}$,

$$\chi_b(x) = \zeta_p^{\mathrm{Tr}_1^m(bx)} \quad (\forall\, x \in \mathbb{F}_{p^m}) \tag{2}$$

defines an additive character of $\mathbb{F}_{p^m}$, where $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$, and every additive character can be obtained in this way. An additive character defined by $\chi_0(x) = 1$ for all $x \in \mathbb{F}_{p^m}$ is called the trivial character while all other characters are called nontrivial characters. The character χ_1 in (2) is called the canonical additive character of $\mathbb{F}_{p^m}$. The orthogonal property of additive character χ of $\mathbb{F}_{p^m}$ can be found in ([14], Theorem 5.4) and is given as

$$\sum_{x \in \mathbb{F}_{p^m}} \chi(x) = \begin{cases} p^m, & \text{if } \chi \text{ trivial}, \\ 0, & \text{if } \chi \text{ non-trivial}. \end{cases} \tag{3}$$

Characters of the multiplicative group $\mathbb{F}_{p^m}^*$ of $\mathbb{F}_{p^m}$ are called multiplicative characters of $\mathbb{F}_{p^m}$. By ([14], Theorem 5.8), for each $j = 0, 1, \ldots, p^m - 2$, the function ψ_j with

$$\psi_j(g^k) = e^{\frac{2\pi\sqrt{-1}jk}{p^m-1}} \quad \text{for } k = 0, 1, \ldots, p^m - 2$$

defines a multiplicative character of $\mathbb{F}_{p^m}$, where g is a generator of $\mathbb{F}_{p^m}^*$. For $j=\frac{p^m-1}{2}$, we have the quadratic character $\eta=\psi_{\frac{p^m-1}{2}}$ defined by

$$\eta(g^k)=\begin{cases}-1, & \text{if } 2\nmid k,\\ 1, & \text{if } 2\mid k.\end{cases}$$

Moreover, we extend this quadratic character by letting $\eta(0)=0$. The quadratic Gauss sum $G=G(\eta,\chi_1)$ over $\mathbb{F}_{p^m}$ is defined by

$$G(\eta,\chi_1)=\sum_{x\in\mathbb{F}_{p^m}^*}\eta(x)\chi_1(x).$$

Now, let $\overline{\eta}$ and $\overline{\chi}_1$ denote the quadratic and canonical character of $\mathbb{F}_{p^e}$ respectively. Then we define quadratic Gauss sum $\overline{G}=G(\overline{\eta},\overline{\chi}_1)$ over $\mathbb{F}_{p^e}$ by

$$G(\overline{\eta},\overline{\chi}_1)=\sum_{x\in\mathbb{F}_{p^e}^*}\overline{\eta}(x)\overline{\chi}_1(x).$$

The explicit values of quadratic Gauss sums are given by the following lemma.

Lemma 2.1 [14, Theorem 5.15] *Let the symbols have the same meanings as before. Then*

$$G(\eta,\chi_1)=(-1)^{m-1}\sqrt{-1}^{\frac{(p-1)^2m}{4}}\sqrt{p^m},\quad G(\overline{\eta},\overline{\chi}_1)=(-1)^{e-1}\sqrt{-1}^{\frac{(p-1)^2e}{4}}\sqrt{p^e}.$$

Lemma 2.2 [20] *Let the notations have the same significations as before. Then, for $N=2$, the cyclotomic numbers are given by:*

1. *h even:* $(0,0)^{(2,p^m)}=\frac{h-2}{2}$, $(0,1)^{(2,p^m)}=(1,0)^{(2,p^m)}=(1,1)^{(2,p^m)}=\frac{h}{2}$;
2. *h odd:* $(0,0)^{(2,p^m)}=(1,0)^{(2,p^m)}=(1,1)^{(2,p^m)}=\frac{h-1}{2}$, $(0,1)^{(2,p^m)}=\frac{h+1}{2}$.

Lemma 2.3 [16, Lemma 2] *Let η and $\overline{\eta}$ be the quadratic characters of $\mathbb{F}_{p^m}^*$ and $\mathbb{F}_{p^e}^*$ respectively. Then the following assertions hold:*

1. *if $s\geq 2$ is even, then $\eta(y)=1$ for each $y\in\mathbb{F}_{p^e}^*$;*
2. *if s is odd, then $\eta(y)=\overline{\eta}(y)$ for each $y\in\mathbb{F}_{p^e}^*$.*

Lemma 2.4 [14, Theorem 5.33] *Let χ be a non-trivial additive character of $\mathbb{F}_{p^m}$ and let $f(x)=a_2x^2+a_1x+a_0\in\mathbb{F}_{p^m}[x]$ with $a_2\neq 0$. Then*

$$\sum_{x\in\mathbb{F}_{p^m}}\chi(f(x))=\chi(a_0-a_1^2(4a_2)^{-1})\eta(a_2)G(\eta,\chi).$$

Lemma 2.5 [14, Theorem 2.26] *Let Tr_1^m and Tr_1^e be the absolute trace functions of $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^e}$ respectively, and let Tr_e^m be the trace function from $\mathbb{F}_{p^m}$ onto $\mathbb{F}_{p^e}$. Then*

$$\mathrm{Tr}_1^m(x)=\mathrm{Tr}_1^e(\mathrm{Tr}_e^m(x))$$

for all $x\in\mathbb{F}_{p^m}$.

Lemma 2.6 [10, Griesmer bound] *Let $\mathcal{C}$ be an $[n,k,d]$ linear code over $\mathbb{F}_{p^e}$, where $k\geq 1$. Then*

$$n\geq\sum_{i=0}^{k-1}\left\lceil\frac{d}{p^{ei}}\right\rceil,$$

where the symbol $\lceil x \rceil$ *denotes the smallest integer not less than* x.

3 Main results

We divide this section into two subsections, namely 3.1 and 3.2.

3.1 Determination of the complete weight enumerator of $\mathcal{C}_D$

In this subsection, after proving some lemmas, we determine the complete weight enumerator and weight distribution of $\mathcal{C}_D$ defined by (1). It is clear that the length n of the linear code $\mathcal{C}_D$ is equal to $\# D$ which can be found in the following lemma.

Lemma 3.1 *For* $\lambda, \mu \in \mathbb{F}_{p^e}$, *define*

$$N(\lambda, \mu) = \#\{x \in \mathbb{F}_{p^m} : \mathrm{Tr}_e^m(x^2) = \lambda \text{ and } \mathrm{Tr}_e^m(x) = \mu\}.$$

Then

1. *if* $2 \mid s$ *and* $p \mid s$, *we have*

$$N(\lambda, \mu) = \begin{cases} p^{m-2e} + p^{-e}(p^e - 1)G, & \text{if } \lambda = 0 \text{ and } \mu = 0, \\ p^{m-2e}, & \text{if } \lambda = 0 \text{ and } \mu \neq 0, \\ p^{m-2e} - p^{-e}G, & \text{if } \lambda \neq 0 \text{ and } \mu = 0, \\ p^{m-2e}, & \text{if } \lambda \neq 0 \text{ and } \mu \neq 0. \end{cases}$$

2. *if* $2 \mid s$ *and* $p \nmid s$, *we have*

$$N(\lambda, \mu) = \begin{cases} p^{m-2e}, & \text{if } \lambda = 0 \text{ and } \mu = 0, \\ p^{m-2e} + p^{-e}G, & \text{if } \lambda = 0 \text{ and } \mu \neq 0, \\ p^{m-2e}, & \text{if } \lambda \neq 0 \text{ and } \mu^2 - s\lambda = 0, \\ p^{m-2e} + \overline{\eta}(\mu^2 - s\lambda)p^{-e}G, & \text{if } \lambda \neq 0 \text{ and } \mu^2 - s\lambda \neq 0. \end{cases}$$

3. *if* $2 \nmid s$ *and* $p \mid s$, *we have*

$$N(\lambda, \mu) = \begin{cases} p^{m-2e}, & \text{if } \lambda = 0, \\ p^{m-2e} + \overline{\eta}(-\lambda)p^{-e}G\overline{G}, & \text{if } \lambda \neq 0 \text{ and } \mu = 0, \\ p^{m-2e}, & \text{if } \lambda \neq 0 \text{ and } \mu \neq 0. \end{cases}$$

4. *if* $2 \nmid s$ *and* $p \nmid s$, *we have*

$$N(\lambda, \mu) = \begin{cases} p^{m-2e} + \overline{\eta}(-s)p^{-2e}(p^e - 1)G\overline{G}, & \text{if } \mu^2 - s\lambda = 0, \\ p^{m-2e} - \overline{\eta}(-s)p^{-2e}G\overline{G}, & \text{if } \mu^2 - s\lambda \neq 0. \end{cases}$$

Proof By the properties of additive character and Lemma 2.5, we have

$$\begin{aligned} N(\lambda, \mu) &= p^{-2e} \sum_{x \in \mathbb{F}_{p^m}} \left(\sum_{y \in \mathbb{F}_{p^e}} \zeta_p^{\mathrm{Tr}_1^e\left(y(\mathrm{Tr}_e^m(x^2) - \lambda)\right)} \right) \left(\sum_{z \in \mathbb{F}_{p^e}} \zeta_p^{\mathrm{Tr}_1^e\left(z(\mathrm{Tr}_e^m(x) - \mu)\right)} \right) \\ &= p^{-2e} \sum_{x \in \mathbb{F}_{p^m}} \left(1 + \sum_{y \in \mathbb{F}_{p^e}^*} \zeta_p^{\mathrm{Tr}_1^e(y\mathrm{Tr}_e^m(x^2) - y\lambda)} \right) \left(1 + \sum_{z \in \mathbb{F}_{p^e}^*} \zeta_p^{\mathrm{Tr}_1^e(z\mathrm{Tr}_e^m(x) - z\mu)} \right) \\ &= p^{m-2e} + p^{-2e}(S_1 + S_2 + S_3), \end{aligned} \tag{4}$$

where

$$\begin{aligned}
S_1 &= \sum_{x\in\mathbb{F}_{p^m}}\sum_{z\in\mathbb{F}_{p^e}^*}\zeta_p^{\mathrm{Tr}_1^e(z\mathrm{Tr}_e^m(x)-z\mu)} = \sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-z\mu)\sum_{x\in\mathbb{F}_{p^m}}\chi_1(zx)=0,\\
S_2 &= \sum_{x\in\mathbb{F}_{p^m}}\sum_{y\in\mathbb{F}_{p^e}^*}\zeta_p^{\mathrm{Tr}_1^e(y\mathrm{Tr}_e^m(x^2)-y\lambda)} = \sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-y\lambda)\sum_{x\in\mathbb{F}_{p^m}}\chi_1(yx^2),\\
S_3 &= \sum_{x\in\mathbb{F}_{p^m}}\sum_{y\in\mathbb{F}_{p^e}^*}\zeta_p^{\mathrm{Tr}_1^e(y\mathrm{Tr}_e^m(x^2)-y\lambda)}\sum_{z\in\mathbb{F}_{p^e}^*}\zeta_p^{\mathrm{Tr}_1^e(z\mathrm{Tr}_e^m(x)-z\mu)}\\
&= \sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-y\lambda)\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-z\mu)\sum_{x\in\mathbb{F}_{p^m}}\chi_1(yx^2+zx).
\end{aligned}$$

By using Lemma 2.4, it is easy to prove that

$$S_2 = \begin{cases} G(p^e-1), & \text{if } \lambda=0 \text{ and } 2\mid s,\\ 0, & \text{if } \lambda=0 \text{ and } 2\nmid s,\\ -G, & \text{if } \lambda\neq 0 \text{ and } 2\mid s,\\ \overline{\eta}(-\lambda)G\overline{G}, & \text{if } \lambda\neq 0 \text{ and } 2\nmid s.\end{cases}$$

By Lemma 2.4, we have

$$\begin{aligned}
S_3 &= \sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-y\lambda)\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-z\mu)\sum_{x\in\mathbb{F}_{p^m}}\chi_1(yx^2+zx)\\
&= G\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-\lambda y)\eta(y)\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{sz^2}{4y}-\mu z\right),
\end{aligned}$$

and there are the following four cases to consider:
Case 1: Suppose $2\mid s$ and $p\mid s$. Then

$$\begin{aligned}
S_3 &= G\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-\lambda y)\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-\mu z)\\
&= \begin{cases} G(p^e-1)^2, & \text{if } \lambda=0 \text{ and } \mu=0,\\ -G(p^e-1), & \text{if } \lambda=0 \text{ and } \mu\neq 0,\\ -G(p^e-1), & \text{if } \lambda\neq 0 \text{ and } \mu=0,\\ G, & \text{if } \lambda\neq 0 \text{ and } \mu\neq 0.\end{cases}
\end{aligned}$$

Case 2: Suppose $2\mid s$ and $p\nmid s$. Then, by Lemma 2.4, we have

$$\begin{aligned}
S_3 &= G\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-\lambda y)\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{sz^2}{4y}-\mu z\right)\\
&= G\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{\mu^2-s\lambda}{s}y\right)\overline{\eta}\left(-\frac{s}{4y}\right)\overline{G} - G\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-\lambda y)\\
&= \begin{cases} -G(p^e-1), & \text{if } \lambda=0 \text{ and } \mu=0,\\ G, & \text{if } \lambda=0 \text{ and } \mu\neq 0,\\ G, & \text{if } \lambda\neq 0 \text{ and } \mu^2-s\lambda=0,\\ \left(\overline{\eta}(\mu^2-s\lambda)p^e+1\right)G, & \text{if } \lambda\neq 0 \text{ and } \mu^2-s\lambda\neq 0.\end{cases}
\end{aligned}$$

Case 3: Next, let $2 \nmid s$ and $p \mid s$. Then

$$\begin{aligned} S_3 &= G \sum_{y \in \mathbb{F}_{p^e}^*} \overline{\chi}_1(-\lambda y)\overline{\eta}(y) \sum_{z \in \mathbb{F}_{p^e}^*} \overline{\chi}_1(-\mu z) \\ &= \begin{cases} 0, & \text{if } \lambda = 0, \\ \overline{\eta}(-\lambda)(p^e-1)G\overline{G}, & \text{if } \lambda \neq 0 \text{ and } \mu = 0, \\ -\overline{\eta}(-\lambda)G\overline{G}, & \text{if } \lambda \neq 0 \text{ and } \mu \neq 0. \end{cases} \end{aligned}$$

Case 4: Finally, let $2 \nmid s$ and $p \nmid s$. Then, by Lemma 2.4, we have

$$\begin{aligned} S_3 &= G \sum_{y \in \mathbb{F}_{p^e}^*} \overline{\chi}_1(-\lambda y)\overline{\eta}(y) \sum_{z \in \mathbb{F}_{p^e}^*} \overline{\chi}_1\left(-\frac{sz^2}{4y} - \mu z\right) \\ &= G\overline{G} \sum_{y \in \mathbb{F}_{p^e}^*} \overline{\chi}_1(-\lambda y)\overline{\eta}(y)\overline{\chi}_1\left(\frac{\mu^2 y}{s}\right)\overline{\eta}\left(-\frac{s}{4y}\right) - G \sum_{y \in \mathbb{F}_{p^e}^*} \overline{\chi}_1(-\lambda y)\overline{\eta}(y) \\ &= \overline{\eta}(-s)G\overline{G} \sum_{y \in \mathbb{F}_{p^e}^*} \overline{\chi}_1\left(\frac{\mu^2 - s\lambda}{s} y\right) - G \sum_{y \in \mathbb{F}_{p^e}^*} \overline{\chi}_1(-\lambda y)\overline{\eta}(y) \\ &= \begin{cases} \overline{\eta}(-s)(p^e-1)G\overline{G}, & \text{if } \lambda = 0 \text{ and } \mu = 0, \\ -\overline{\eta}(-s)G\overline{G}, & \text{if } \lambda = 0 \text{ and } \mu \neq 0, \\ \left((p^e-1)\overline{\eta}(-s) - \overline{\eta}(-\lambda)\right)G\overline{G}, & \text{if } \lambda \neq 0 \text{ and } \mu^2 - s\lambda = 0, \\ -\left(\overline{\eta}(-s) + \overline{\eta}(-\lambda)\right)G\overline{G}, & \text{if } \lambda \neq 0 \text{ and } \mu^2 - s\lambda \neq 0. \end{cases} \end{aligned}$$

Combining (4) and the values of S_1, S_2 and S_3, the proof of the lemma is completed. □

Lemma 3.2 *For $a \in \mathbb{F}_{p^m}^*$ and $c \in \mathbb{F}_{p^e}^*$, let*

$$\aleph_2 = \sum_{x \in \mathbb{F}_{p^m}} \sum_{y \in \mathbb{F}_{p^e}^*} \zeta_p^{\mathrm{Tr}_1^e\left(y(\mathrm{Tr}_e^m(x)-1)\right)} \sum_{w \in \mathbb{F}_{p^e}^*} \zeta_p^{\mathrm{Tr}_1^e\left(w(\mathrm{Tr}_e^m(ax)-c)\right)}.$$

Then

$$\aleph_2 = \begin{cases} (p^e-1)p^m, & \text{if } a \in \mathbb{F}_{p^e}^* \text{ and } c = a, \\ -p^m, & \text{if } a \in \mathbb{F}_{p^e}^* \text{ and } c \neq a, \\ 0, & \text{otherwise}. \end{cases}$$

Proof We have

$$\aleph_2 = \sum_{y \in \mathbb{F}_{p^e}^*} \sum_{w \in \mathbb{F}_{p^e}^*} \zeta_p^{\mathrm{Tr}_1^e(-y-cw)} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m((aw+y)x)}.$$

One may easily verify that the equation $aw + y = 0$ has solutions if and only if $a \in \mathbb{F}_{p^e}^*$ for $y, w \in \mathbb{F}_{p^e}^*$. Then $\aleph_2 = 0$ if $a \notin \mathbb{F}_{p^e}^*$. Hence, if $a \in \mathbb{F}_{p^e}^*$, we have

$$\aleph_2 = \sum_{w \in \mathbb{F}_{p^e}^*} \overline{\chi}_1\left((a-c)w\right) \sum_{x \in \mathbb{F}_{p^m}} \chi_1\left((aw+y)x\right) = p^m \sum_{w \in \mathbb{F}_{p^e}^*} \overline{\chi}_1\left((a-c)w\right).$$

By using orthogonal property of additive character, we get the lemma. □

Let $a \in \mathbb{F}_{p^m}^*$ and $c \in \mathbb{F}_{p^e}^*$, and let $s = \mathrm{Tr}_e^m(1)$. For the sake of simplicity, we denote $\nabla = (\mathrm{Tr}_e^m(a))^2 - s\mathrm{Tr}_e^m(a^2)$ and $\phi(c) = -sc^2 + 2c\mathrm{Tr}_e^m(a) - \mathrm{Tr}_e^m(a^2)$ in the rest of the paper.

Lemma 3.3 *For $a \in \mathbb{F}_{p^m}^*$ and $c \in \mathbb{F}_{p^e}^*$, let*

$$\aleph_3 = \sum_{x\in\mathbb{F}_{p^m}} \sum_{z\in\mathbb{F}_{p^e}^*} \zeta_p^{\mathrm{Tr}_1^e(z\mathrm{Tr}_e^m(x^2))} \sum_{w\in\mathbb{F}_{p^e}^*} \zeta_p^{\mathrm{Tr}_1^e\left(w(\mathrm{Tr}_e^m(ax)-c)\right)}.$$

Then

$$\aleph_3 = \begin{cases} -(p^e-1)G, & \text{if } 2 \mid s \text{ and } \mathrm{Tr}_e^m(a^2)=0, \\ G, & \text{if } 2 \mid s \text{ and } \mathrm{Tr}_e^m(a^2)\neq 0, \\ 0, & \text{if } 2 \nmid s \text{ and } \mathrm{Tr}_e^m(a^2)=0, \\ -\overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}, & \text{if } 2 \nmid s \text{ and } \mathrm{Tr}_e^m(a^2)\neq 0. \end{cases}$$

Proof By Lemmas 2.4 and 2.5, we have

$$\begin{aligned} \aleph_3 &= \sum_{w\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-cw) \sum_{z\in\mathbb{F}_{p^e}^*} \sum_{x\in\mathbb{F}_{p^m}} \chi_1(zx^2+awx) \\ &= \sum_{w\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-cw) \sum_{z\in\mathbb{F}_{p^e}^*} \overline{\chi}_1\left(-\frac{w^2\mathrm{Tr}_e^m(a^2)}{4z}\right)\eta(z)G \\ &= \begin{cases} G\sum_{w\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-cw) \sum_{z\in\mathbb{F}_{p^e}^*} \overline{\chi}_1\left(-\frac{w^2\mathrm{Tr}_e^m(a^2)}{4z}\right), & \text{if } 2 \mid s, \\ G\sum_{w\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-cw) \sum_{z\in\mathbb{F}_{p^e}^*} \overline{\chi}_1\left(-\frac{w^2\mathrm{Tr}_e^m(a^2)}{4z}\right)\overline{\eta}(z), & \text{if } 2 \nmid s, \end{cases} \end{aligned}$$

as required. □

Lemma 3.4 *For $a \in \mathbb{F}_{p^m}^*$ and $c \in \mathbb{F}_{p^e}^*$, let*

$$\aleph_4 = \sum_{x\in\mathbb{F}_{p^m}} \sum_{y\in\mathbb{F}_{p^e}^*} \zeta_p^{\mathrm{Tr}_1^e\left(y(\mathrm{Tr}_e^m(x)-1)\right)} \sum_{z\in\mathbb{F}_{p^e}^*} \zeta_p^{\mathrm{Tr}_1^e\left(z\mathrm{Tr}_e^m(x^2)\right)} \sum_{w\in\mathbb{F}_{p^e}^*} \zeta_p^{\mathrm{Tr}_1^e\left(w(\mathrm{Tr}_e^m(ax)-c)\right)}.$$

Then we have the following cases:

1. *If $2 \mid s$ and $p \mid s$, then*

$$\aleph_4 = \begin{cases} (p^e-1)G, & \text{if } \mathrm{Tr}_e^m(a^2)=0 \text{ and } \mathrm{Tr}_e^m(a)=0, \\ -G, & \text{if } \mathrm{Tr}_e^m(a^2)=0 \text{ and } \mathrm{Tr}_e^m(a)\neq 0, \\ -G, & \text{if } \mathrm{Tr}_e^m(a^2)\neq 0 \text{ and } \mathrm{Tr}_e^m(a)=0, \\ (p^{2e}-p^e-1)G, & \text{if } \mathrm{Tr}_e^m(a^2)\mathrm{Tr}_e^m(a)\neq 0 \text{ and } \mathrm{Tr}_e^m(a^2)=2c\mathrm{Tr}_e^m(a), \\ -(p^e+1)G, & \text{if } \mathrm{Tr}_e^m(a^2)\mathrm{Tr}_e^m(a)\neq 0 \text{ and } \mathrm{Tr}_e^m(a^2)\neq 2c\mathrm{Tr}_e^m(a). \end{cases}$$

2. *If $2 \mid s$ and $p \nmid s$, then*

$$\aleph_4 = \begin{cases} (p^{2e}-p^e-1)G, & \text{if } \mathrm{Tr}_e^m(a^2)\neq 0,\ \nabla=0 \text{ and } c\mathrm{Tr}_e^m(a)=\mathrm{Tr}_e^m(a^2), \\ (p^{2e}-p^e-1)G, & \text{if } \mathrm{Tr}_e^m(a^2)=0,\ \mathrm{Tr}_e^m(a)\neq 0 \text{ and } cs=2\mathrm{Tr}_e^m(a), \\ -(p^e+1)G, & \text{if } \mathrm{Tr}_e^m(a^2)\neq 0,\ \nabla=0 \text{ and } c\mathrm{Tr}_e^m(a)\neq \mathrm{Tr}_e^m(a^2), \\ -(p^e+1)G, & \text{if } \mathrm{Tr}_e^m(a^2)=0,\ \mathrm{Tr}_e^m(a)\neq 0 \text{ and } cs\neq 2\mathrm{Tr}_e^m(a), \\ (p^{2e}-2p^e-1)G, & \text{if } \mathrm{Tr}_e^m(a^2)\neq 0,\ \overline{\eta}(\nabla)=1 \text{ and } \phi(c)=0, \\ -(2p^e+1)G, & \text{if } \mathrm{Tr}_e^m(a^2)\neq 0,\ \overline{\eta}(\nabla)=1 \text{ and } \phi(c)\neq 0, \\ -G, & \text{if } \mathrm{Tr}_e^m(a^2)\neq 0 \text{ and } \overline{\eta}(\nabla)=-1 \text{ or } \mathrm{Tr}_e^m(a^2)=0 \text{ and } \mathrm{Tr}_e^m(a)=0. \end{cases}$$

3. *If* $2 \nmid s$ *and* $p \mid s$*, then*

$$\aleph_4 = \begin{cases} 0, & \text{if } \mathrm{Tr}_e^m(a^2) = 0 \text{ and } \mathrm{Tr}_e^m(a) = 0, \\ \overline{\eta}(\frac{c\mathrm{Tr}_e^m(a)}{2}) p^e G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) = 0 \text{ and } \mathrm{Tr}_e^m(a) \neq 0, \\ \overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) \neq 0 \text{ and } \mathrm{Tr}_e^m(a) = 0, \\ \overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2)\mathrm{Tr}_e^m(a) \neq 0 \text{ and } \mathrm{Tr}_e^m(a^2) = 2c\mathrm{Tr}_e^m(a), \\ \overline{\eta}(2c\mathrm{Tr}_e^m(a) - \mathrm{Tr}_e^m(a^2)) p^e G\overline{G} & \\ \quad + \overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2)\mathrm{Tr}_e^m(a) \neq 0 \text{ and } \mathrm{Tr}_e^m(a^2) \neq 2c\mathrm{Tr}_e^m(a). \end{cases}$$

4. *If* $2 \nmid s$ *and* $p \nmid s$*, then*

$$\aleph_4 = \begin{cases} \overline{\eta}(-s)G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) = 0 \text{ and } \mathrm{Tr}_e^m(a) = 0, \\ \overline{\eta}(-s)G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) = 0,\ \mathrm{Tr}_e^m(a) \neq 0 \text{ and } cs = 2\mathrm{Tr}_e^m(a), \\ \left(\overline{\eta}(2c\mathrm{Tr}_e^m(a) - sc^2)p^e + \overline{\eta}(-s)\right) G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) = 0,\ \mathrm{Tr}_e^m(a) \neq 0 \text{ and } cs \neq 2\mathrm{Tr}_e^m(a), \\ -(p^e - 2)\overline{\eta}(-s)G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) \neq 0,\ \nabla = 0 \text{ and } c\mathrm{Tr}_e^m(a) = \mathrm{Tr}_e^m(a^2), \\ 2\overline{\eta}(-s)G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) \neq 0,\ \nabla = 0 \text{ and } c\mathrm{Tr}_e^m(a) \neq \mathrm{Tr}_e^m(a^2), \\ \left(\overline{\eta}(-\mathrm{Tr}_e^m(a^2)) + \overline{\eta}(-s)\right) G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) \neq 0,\ \nabla \neq 0 \text{ and } \phi(c) = 0, \\ \left(\overline{\eta}(\phi(c))p^e + \overline{\eta}(-\mathrm{Tr}_e^m(a^2)) + \overline{\eta}(-s)\right) G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) \neq 0,\ \nabla \neq 0 \text{ and } \phi(c) \neq 0. \end{cases}$$

Proof By Lemmas 2.4 and 2.5, we have

$$\begin{aligned} \aleph_4 &= \sum_{z\in\mathbb{F}_{p^e}^*} \sum_{y\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-y) \sum_{w\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-cw) \sum_{x\in\mathbb{F}_{p^m}} \chi_1\left(zx^2 + (aw+y)x\right) \\ &= \sum_{z\in\mathbb{F}_{p^e}^*} \sum_{y\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-y) \sum_{w\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-cw)\chi_1\left(-\frac{(aw+y)^2}{4z}\right)\eta(z)G \\ &= G\sum_{z\in\mathbb{F}_{p^e}^*} \eta(z) \sum_{y\in\mathbb{F}_{p^e}^*} \overline{\chi}_1\left(-\frac{s}{4z}y^2 - y\right) \sum_{w\in\mathbb{F}_{p^e}^*} \overline{\chi}_1\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}w^2 - \left(\frac{y\mathrm{Tr}_e^m(a)}{2z} + c\right)w\right). \end{aligned} \tag{5}$$

There are the following cases to consider:
Case 1: $s > 2$ is even and $p \mid s$;
Case 2: $s > 2$ is even and $p \nmid s$;
Case 3: $s \geq 3$ is odd and $p \mid s$;
Case 4: $s \geq 3$ is odd and $p \nmid s$.

Case 1: Suppose that $s > 2$ is even and $p \mid s$. Then, by (5), we obtain

$$\aleph_4 = G\sum_{z\in\mathbb{F}_{p^e}^*} \sum_{y\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-y) \sum_{w\in\mathbb{F}_{p^e}^*} \overline{\chi}_1\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}w^2 - \left(\frac{y\mathrm{Tr}_e^m(a)}{2z} + c\right)w\right).$$

If $\mathrm{Tr}_e^m(a^2) = 0$, then

$$\begin{aligned} \aleph_4 &= G\sum_{y\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-y) \sum_{w\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-cw) \sum_{z\in\mathbb{F}_{p^e}^*} \overline{\chi}_1\left(-\frac{yw\mathrm{Tr}_e^m(a)}{2z}\right) \\ &= \begin{cases} (p^e-1)G, & \text{if } \mathrm{Tr}_e^m(a) = 0, \\ -G, & \text{if } \mathrm{Tr}_e^m(a) \neq 0. \end{cases} \end{aligned}$$

If $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\mathrm{Tr}_e^m(a) = 0$, then, by Lemma 2.4, we have

$$\begin{aligned}
\aleph_4 &= G \sum_{z\in\mathbb{F}_{p^e}^*} \sum_{y\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-y) \sum_{w\in\mathbb{F}_{p^e}^*} \overline{\chi}_1\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z} w^2 - cw\right) \\
&= G \sum_{z\in\mathbb{F}_{p^e}^*} \sum_{y\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-y) \left(\overline{\chi}_1\left(\frac{c^2 z}{\mathrm{Tr}_e^m(a^2)}\right) \overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right)\overline{G} - 1\right) \\
&= G\overline{G} \sum_{z\in\mathbb{F}_{p^e}^*} \sum_{y\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-y)\overline{\chi}_1\left(\frac{c^2 z}{\mathrm{Tr}_e^m(a^2)}\right) \overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right) + (p^e-1)G \\
&= -\overline{\eta}(-1)G\overline{G}^2 + (p^e-1)G = -G.
\end{aligned}$$

If $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\mathrm{Tr}_e^m(a) \neq 0$, then, again from Lemma 2.4, we have

$$\begin{aligned}
\aleph_4 &= G \sum_{z\in\mathbb{F}_{p^e}^*} \sum_{y\in\mathbb{F}_{p^e}^*} \overline{\chi}(-y) \sum_{w\in\mathbb{F}_{p^e}^*} \overline{\chi}_1\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z} w^2 - \left(\frac{y\mathrm{Tr}_e^m(a)}{2z} + c\right) w\right) \\
&= G \sum_{z\in\mathbb{F}_{p^e}^*} \sum_{y\in\mathbb{F}_{p^e}^*} \overline{\chi}_1(-y) \left(\overline{\chi}_1\left(\frac{\left(\mathrm{Tr}_e^m(a)\right)^2}{4z\mathrm{Tr}_e^m(a^2)} y^2 + \frac{c\mathrm{Tr}_e^m(a)}{\mathrm{Tr}_e^m(a^2)} y + \frac{c^2}{\mathrm{Tr}_e^m(a^2)} z\right)\right. \\
&\quad \left.\times\, \overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right)\overline{G} - 1\right) \\
&= G\overline{G} \sum_{z\in\mathbb{F}_{p^e}^*} \overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right) \overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)} z\right) \sum_{y\in\mathbb{F}_{p^e}^*} \overline{\chi}_1\left(\frac{\left(\mathrm{Tr}_e^m(a)\right)^2}{4z\mathrm{Tr}_e^m(a^2)} y^2 + \left(\frac{c\mathrm{Tr}_e^m(a)}{\mathrm{Tr}_e^m(a^2)} - 1\right) y\right) \\
&\quad + (p^e-1)G \\
&= G\overline{G} \sum_{z\in\mathbb{F}_{p^e}^*} \overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right) \overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)} z\right) \overline{\chi}_1\left(-\frac{c^2}{\mathrm{Tr}_e^m(a^2)} z + \frac{2c\mathrm{Tr}_e^m(a) - \mathrm{Tr}_e^m(a^2)}{\left(\mathrm{Tr}_e^m(a)\right)^2} z\right) \\
&\quad \times \overline{\eta}\left(\frac{(\mathrm{Tr}_e^m(a))^2}{4z\mathrm{Tr}_e^m(a^2)}\right)\overline{G} - G\overline{G} \sum_{z\in\mathbb{F}_{p^e}^*} \overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right) \overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)} z\right) + (p^e-1)G \\
&= \overline{\eta}(-1)G\overline{G}^2 \sum_{z\in\mathbb{F}_{p^e}^*} \overline{\chi}_1\left(\frac{2c\mathrm{Tr}_e^m(a) - \mathrm{Tr}_e^m(a^2)}{(\mathrm{Tr}_e^m(a))^2} z\right) - \overline{\eta}(-1)G\overline{G}^2 + (p^e-1)G \\
&= \begin{cases} \overline{\eta}(-1)G\overline{G}^2(p^e-2) + (p^e-1)G, & \text{if } \mathrm{Tr}_e^m(a^2) = 2c\mathrm{Tr}_e^m(a) \\ -2\overline{\eta}(-1)G\overline{G}^2 + (p^e-1)G, & \text{if } \mathrm{Tr}_e^m(a^2) \neq 2c\mathrm{Tr}_e^m(a) \end{cases} \\
&= \begin{cases} (p^{2e} - p^e - 1)G, & \text{if } \mathrm{Tr}_e^m(a^2) = 2c\mathrm{Tr}_e^m(a), \\ -(p^e+1)G, & \text{if } \mathrm{Tr}_e^m(a^2) \neq 2c\mathrm{Tr}_e^m(a). \end{cases}
\end{aligned}$$

Case 2: Now, assume that $s > 2$ is even and $p \nmid s$. By (5), we obtain

$$\aleph_4 = G \sum_{z\in\mathbb{F}_{p^e}^*} \sum_{y\in\mathbb{F}_{p^e}^*} \overline{\chi}_1\left(-\frac{s}{4z} y^2 - y\right) \sum_{w\in\mathbb{F}_{p^e}^*} \overline{\chi}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z} w^2 - \left(\frac{y\mathrm{Tr}_e^m(a)}{2z} + c\right) w\right).$$

If $\mathrm{Tr}_e^m(a^2)=0$ and $\mathrm{Tr}_e^m(a)=0$, then, by Lemma 2.4, we have

$$\begin{aligned}\aleph_4 &= G\sum_{z\in\mathbb{F}_{p^e}^*}\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{s}{4z}y^2-y\right)\sum_{w\in\mathbb{F}_{p^e}^*}\overline{\chi}(-cw)\\ &= -G\sum_{z\in\mathbb{F}_{p^e}^*}\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{s}{4z}y^2-y\right)\\ &= -G\sum_{z\in\mathbb{F}_{p^e}^*}\left(\overline{\chi}_1\left(\frac{z}{s}\right)\overline{\eta}\left(-\frac{s}{4z}\right)\overline{G}-1\right)=-\overline{\eta}(-1)G\overline{G}^2+(p^e-1)G=-G.\end{aligned}$$

If $\mathrm{Tr}_e^m(a^2)=0$ and $\mathrm{Tr}_e^m(a)\neq 0$, then, by Lemma 2.4, we have

$$\begin{aligned}\aleph_4 &= G\sum_{z\in\mathbb{F}_{p^e}^*}\sum_{w\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-cw)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{s}{4z}y^2-\left(\frac{w\mathrm{Tr}_e^m(a)}{2z}+1\right)y\right)\\ &= G\sum_{z\in\mathbb{F}_{p^e}^*}\sum_{w\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-cw)\left(\overline{\chi}_1\left(\frac{z}{s}\left(\frac{w\mathrm{Tr}_e^m(a)}{2z}+1\right)^2\right)\overline{\eta}\left(-\frac{s}{4z}\right)\overline{G}-1\right)\\ &= G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}\left(-\frac{s}{4z}\right)\overline{\chi}_1\left(\frac{z}{s}\right)\sum_{w\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{(\mathrm{Tr}_e^m(a))^2}{4zs}w^2+\left(\frac{\mathrm{Tr}_e^m(a)}{s}-c\right)w\right)+(p^e-1)G\\ &= G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}\left(-\frac{s}{4z}\right)\overline{\chi}_1\left(\frac{z}{s}\right)\left(\overline{\chi}_1\left(-\frac{zs}{(\mathrm{Tr}_e^m(a))^2}\left(\frac{\mathrm{Tr}_e^m(a)}{s}-c\right)^2\right)\overline{\eta}\left(\frac{(\mathrm{Tr}_e^m(a))^2}{4zs}\right)\overline{G}-1\right)\\ &\quad +(p^e-1)G\\ &= \overline{\eta}(-1)G\overline{G}^2\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{2\mathrm{Tr}_e^m(a)-cs}{(\mathrm{Tr}_e^m(a))^2}cz\right)-\overline{\eta}(-1)G\overline{G}^2+(p^e-1)G\\ &= \begin{cases}(p^e-2)\overline{\eta}(-1)G\overline{G}^2+(p^e-1)G, & \text{if } cs=2\mathrm{Tr}_e^m(a)\\ -2\overline{\eta}(-1)G\overline{G}^2+(p^e-1)G, & \text{if } cs\neq 2\mathrm{Tr}_e^m(a)\end{cases}\\ &= \begin{cases}(p^{2e}-p^e-1)G, & \text{if } cs=2\mathrm{Tr}_e^m(a),\\ -(p^e+1)G, & \text{if } cs\neq 2\mathrm{Tr}_e^m(a).\end{cases}\end{aligned}$$

Recall that $\nabla=(\mathrm{Tr}_e^m(a))^2-s\mathrm{Tr}_e^m(a^2)$. If $\mathrm{Tr}_e^m(a^2)\neq 0$, then, by Lemma 2.4, we have

$$\begin{aligned}\aleph_4 &= G\sum_{z\in\mathbb{F}_{p^e}^*}\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{s}{4z}y^2-y\right)\overline{\chi}_1\left(\frac{(\mathrm{Tr}_e^m(a))^2}{4z\mathrm{Tr}_e^m(a^2)}y^2+\frac{c\mathrm{Tr}_e^m(a)}{\mathrm{Tr}_e^m(a^2)}y+\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)\\ &\quad\times\overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right)\overline{G}-G\sum_{z\in\mathbb{F}_{p^e}^*}\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{s}{4z}y^2-y\right)\\ &= G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right)\overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{\nabla}{4z\mathrm{Tr}_e^m(a^2)}y^2+\left(\frac{c\mathrm{Tr}_e^m(a)}{\mathrm{Tr}_e^m(a^2)}-1\right)y\right)\\ &\qquad -G\sum_{z\in\mathbb{F}_{p^e}^*}\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{s}{4z}y^2-y\right).\end{aligned}$$

Suppose that $\mathrm{Tr}_e^m(a^2)\neq 0$ and $\nabla=0$. Then

$$\begin{aligned}\aleph_4 &= G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right)\overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\left(\frac{c\mathrm{Tr}_e^m(a)}{\mathrm{Tr}_e^m(a^2)}-1\right)y\right)-G\\ &= \begin{cases}(p^e-1)\overline{\eta}(-1)G\overline{G}^2-G, & \text{if } c\mathrm{Tr}_e^m(a)=\mathrm{Tr}_e^m(a^2)\\ -\overline{\eta}(-1)G\overline{G}^2-G, & \text{if } c\mathrm{Tr}_e^m(a)\neq\mathrm{Tr}_e^m(a^2)\end{cases}\\ &= \begin{cases}(p^{2e}-p^e-1)G, & \text{if } c\mathrm{Tr}_e^m(a)=\mathrm{Tr}_e^m(a^2),\\ -(p^e+1)G, & \text{if } c\mathrm{Tr}_e^m(a)\neq\mathrm{Tr}_e^m(a^2).\end{cases}\end{aligned}$$

Next, we consider that $\mathrm{Tr}_e^m(a^2)\neq 0$ and $\nabla\neq 0$. Then, by Lemma 2.4, we have

$$\begin{aligned}\aleph_4 &= G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right)\overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)\overline{\chi}_1\left(-\frac{z\mathrm{Tr}_e^m(a^2)}{\nabla}\left(\frac{c\mathrm{Tr}_e^m(a)}{\mathrm{Tr}_e^m(a^2)}-1\right)^2\right)\\ &\quad\times\overline{\eta}\left(\frac{\nabla}{4z\mathrm{Tr}_e^m(a^2)}\right)\overline{G}-G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right)\overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)-G\\ &= G\overline{G}^2\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(-\nabla)\overline{\chi}_1\left(\frac{z}{\nabla}\phi(c)\right)-\overline{\eta}(-1)G\overline{G}^2-G\\ &= G\overline{G}^2\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(-\nabla)\overline{\chi}_1\left(\frac{z}{\nabla}\phi(c)\right)-(p^e+1)G,\end{aligned}$$

where $\phi(c)=-sc^2+2c\mathrm{Tr}_e^m(a)-\mathrm{Tr}_e^m(a^2)$. From [14, Exercise 5.24], the equation $\phi(c)=0$ over $\mathbb{F}_{p^e}$ has two distinct solutions if and only if $\overline{\eta}(\nabla)=1$. Thus, when $\overline{\eta}(\nabla)=1$, we have

$$\begin{aligned}\aleph_4 &= \begin{cases}(p^e-1)\overline{\eta}(-1)G\overline{G}^2-(p^e+1)G, & \text{if } \phi(c)=0\\ -\overline{\eta}(-1)G\overline{G}^2-(p^e+1)G, & \text{if } \phi(c)\neq 0\end{cases}\\ &= \begin{cases}(p^{2e}-2p^e-1)G, & \text{if } \phi(c)=0,\\ -(2p^e+1)G, & \text{if } \phi(c)\neq 0.\end{cases}\end{aligned}$$

Similarly, when $\overline{\eta}(\nabla)=-1$, we must have $\phi(c)\neq 0$ for all $c\in\mathbb{F}_{p^e}^*$ and so

$$\aleph_4=\overline{\eta}(-1)G\overline{G}^2-(p^e+1)G=-G.$$

Case 3: Suppose that $s\geq 3$ is odd and $p\mid s$. Now, by (5), we obtain

$$\aleph_4=G\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-y)\sum_{w\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}w^2-\left(\frac{y\mathrm{Tr}_e^m(a)}{2z}+c\right)w\right).$$

If $\mathrm{Tr}_e^m(a^2)=0$, then

$$\begin{aligned}\aleph_4 &= G\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-y)\sum_{w\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-cw)\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\overline{\chi}_1\left(-\frac{y\mathrm{Tr}_e^m(a)}{2z}w\right)\\ &= \begin{cases}0, & \text{if } \mathrm{Tr}_e^m(a)=0\\ \overline{\eta}\left(-\frac{c\mathrm{Tr}_e^m(a)}{2}\right)G\overline{G}^3, & \text{if } \mathrm{Tr}_e^m(a)\neq 0\end{cases}\\ &= \begin{cases}0, & \text{if } \mathrm{Tr}_e^m(a)=0,\\ \overline{\eta}\left(\frac{c\mathrm{Tr}_e^m(a)}{2}\right)p^eG\overline{G}, & \text{if } \mathrm{Tr}_e^m(a)\neq 0.\end{cases}\end{aligned}$$

If $\mathrm{Tr}_e^m(a^2)\neq 0$ and $\mathrm{Tr}_e^m(a)=0$, then, from Lemma 2.4, we have

$$\begin{aligned}\aleph_4 &= G\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-y)\sum_{w\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}w^2-cw\right)\\ &= G\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-y)\left(\overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)\overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right)\overline{G}-1\right)\\ &= \overline{\eta}\left(-\mathrm{Tr}_e^m(a^2)\right)G\overline{G}\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-y)\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)=\overline{\eta}\left(-\mathrm{Tr}_e^m(a^2)\right)G\overline{G}.\end{aligned}$$

If $\mathrm{Tr}_e^m(a^2)\neq 0$ and $\mathrm{Tr}_e^m(a)\neq 0$, then, again from Lemma 2.4, we have

$$\begin{aligned}\aleph_4 &= G\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}(-y)\overline{\chi}_1\left(\frac{(\mathrm{Tr}_e^m(a))^2}{4z\mathrm{Tr}_e^m(a^2)}y^2+\frac{c\mathrm{Tr}_e^m(a)}{\mathrm{Tr}_e^m(a^2)}y+\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)\overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right)\overline{G}\\ &= \overline{\eta}\left(-\mathrm{Tr}_e^m(a^2)\right)G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{(\mathrm{Tr}_e^m(a))^2}{4z\mathrm{Tr}_e^m(a^2)}y^2+\left(\frac{c\mathrm{Tr}_e^m(a)}{\mathrm{Tr}_e^m(a^2)}-1\right)y\right)\\ &= \overline{\eta}\left(-\mathrm{Tr}_e^m(a^2)\right)G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)\overline{\chi}_1\left(-\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z+\frac{2c\mathrm{Tr}_e^m(a)-\mathrm{Tr}_e^m(a^2)}{(\mathrm{Tr}_e^m(a))^2}z\right)\\ &\quad\times\overline{\eta}\left(\frac{(\mathrm{Tr}_e^m(a))^2}{4z\mathrm{Tr}_e^m(a^2)}\right)\overline{G}-\overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)\\ &= \overline{\eta}(-1)G\overline{G}^2\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\overline{\chi}_1\left(\frac{2c\mathrm{Tr}_e^m(a)-\mathrm{Tr}_e^m(a^2)}{(\mathrm{Tr}_e^m(a))^2}z\right)+\overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}\\ &= \begin{cases}\overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2)=2c\mathrm{Tr}_e^m(a)\\ \overline{\eta}(-1)\overline{\eta}(2c\mathrm{Tr}_e^m(a)-\mathrm{Tr}_e^m(a^2))G\overline{G}^3+\overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2)\neq 2c\mathrm{Tr}_e^m(a)\end{cases}\\ &= \begin{cases}\overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2)=2c\mathrm{Tr}_e^m(a),\\ \left(\overline{\eta}(2c\mathrm{Tr}_e^m(a)-\mathrm{Tr}_e^m(a^2))p^e+\overline{\eta}(-\mathrm{Tr}_e^m(a^2))\right)G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2)\neq 2c\mathrm{Tr}_e^m(a).\end{cases}\end{aligned}$$

Case 4: Suppose that $s\geq 3$ is odd and $p\nmid s$. Now, by (5), we obtain

$$\aleph_4=G\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{s}{4z}y^2-y\right)\sum_{w\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}w^2-\left(\frac{y\mathrm{Tr}_e^m(a)}{2z}+c\right)w\right).$$

If $\mathrm{Tr}_e^m(a^2)=0$ and $\mathrm{Tr}_e^m(a)=0$, then

$$\begin{aligned}\aleph_4 &= G\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{s}{4z}y^2-y\right)\sum_{w\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-cw)\\ &= -G\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{s}{4z}y^2-y\right)\\ &= -G\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\left(\overline{\chi}_1\left(\frac{z}{s}\right)\overline{\eta}\left(-\frac{s}{4z}\right)\overline{G}-1\right)=\overline{\eta}(-s)G\overline{G}.\end{aligned}$$

If $\mathrm{Tr}_e^m(a^2)=0$ and $\mathrm{Tr}_e^m(a)\neq 0$, then

$$\begin{aligned}\aleph_4 &= G\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\sum_{w\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-cw)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{s}{4z}y^2-\left(\frac{w\mathrm{Tr}_e^m(a)}{2z}+1\right)y\right)\\ &= G\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\sum_{w\in\mathbb{F}_{p^e}^*}\overline{\chi}_1(-cw)\left(\overline{\chi}_1\left(\frac{z}{s}\left(\frac{w\mathrm{Tr}_e^m(a)}{2z}+1\right)^2\right)\overline{\eta}\left(-\frac{s}{4z}\right)\overline{G}-1\right)\\ &= \overline{\eta}(-s)G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{z}{s}\right)\sum_{w\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{(\mathrm{Tr}_e^m(a))^2}{4zs}w^2+\left(\frac{\mathrm{Tr}_e^m(a)}{s}-c\right)w\right)\\ &= \overline{\eta}(-s)G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{z}{s}\right)\left(\overline{\chi}_1\left(-\frac{zs}{(\mathrm{Tr}_e^m(a))^2}\left(\frac{\mathrm{Tr}_e^m(a)}{s}-c\right)^2\right)\overline{\eta}\left(\frac{(\mathrm{Tr}_e^m(a))^2}{4zs}\right)\overline{G}-1\right)\\ &= G\overline{G}^2\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(-z)\overline{\chi}_1\left(\frac{2\mathrm{Tr}_e^m(a)-cs}{(\mathrm{Tr}_e^m(a))^2}cz\right)+\overline{\eta}(-s)G\overline{G}\\ &= \begin{cases}\overline{\eta}(-s)G\overline{G}, & \text{if } cs=2\mathrm{Tr}_e^m(a)\\ \overline{\eta}(-1)G\overline{G}^3\overline{\eta}(2c\mathrm{Tr}_e^m(a)-sc^2)+\overline{\eta}(-s)G\overline{G}, & \text{if } cs\neq 2\mathrm{Tr}_e^m(a)\end{cases}\\ &= \begin{cases}\overline{\eta}(-s)G\overline{G}, & \text{if } cs=2\mathrm{Tr}_e^m(a),\\ \left(\overline{\eta}(2c\mathrm{Tr}_e^m(a)-sc^2)p^e+\overline{\eta}(-s)\right)G\overline{G}, & \text{if } cs\neq 2\mathrm{Tr}_e^m(a).\end{cases}\end{aligned}$$

If $\mathrm{Tr}_e^m(a^2)\neq 0$, then we deduce that

$$\begin{aligned}\aleph_4 &= G\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{s}{4z}y^2-y\right)\overline{\chi}_1\left(\frac{(\mathrm{Tr}_e^m(a))^2}{4z\mathrm{Tr}_e^m(a^2)}y^2+\frac{c\mathrm{Tr}_e^m(a)}{\mathrm{Tr}_e^m(a^2)}y+\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)\\ &\quad\times\overline{\eta}\left(-\frac{\mathrm{Tr}_e^m(a^2)}{4z}\right)\overline{G}-G\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{s}{4z}y^2-y\right)\\ &= \overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{\nabla}{4z\mathrm{Tr}_e^m(a^2)}y^2+\left(\frac{c\mathrm{Tr}_e^m(a)}{\mathrm{Tr}_e^m(a^2)}-1\right)y\right)\\ &\quad -G\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(z)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(-\frac{s}{4z}y^2-y\right).\end{aligned}$$

If $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\nabla = 0$, then $\overline{\eta}(-\mathrm{Tr}_e^m(a^2)) = \overline{\eta}(-s)$ and

$$\begin{aligned}
\aleph_4 &= \overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)\sum_{y\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left((\frac{c\mathrm{Tr}_e^m(a)}{\mathrm{Tr}_e^m(a^2)}-1)y\right)+\overline{\eta}(-s)G\overline{G}\\
&= \begin{cases} \big(-(p^e-1)\overline{\eta}(-\mathrm{Tr}_e^m(a^2))+\overline{\eta}(-s)\big)G\overline{G}, & \text{if } c\mathrm{Tr}_e^m(a)=\mathrm{Tr}_e^m(a^2)\\ \big(\overline{\eta}(-\mathrm{Tr}_e^m(a^2))+\overline{\eta}(-s)\big)G\overline{G}, & \text{if } c\mathrm{Tr}_e^m(a)\neq\mathrm{Tr}_e^m(a^2)\end{cases}\\
&= \begin{cases} -(p^e-2)\overline{\eta}(-s)G\overline{G}, & \text{if } c\mathrm{Tr}_e^m(a)=\mathrm{Tr}_e^m(a^2),\\ 2\overline{\eta}(-s)G\overline{G}, & \text{if } c\mathrm{Tr}_e^m(a)\neq\mathrm{Tr}_e^m(a^2).\end{cases}
\end{aligned}$$

Suppose that $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\nabla \neq 0$. Recall that $\phi(c) = -sc^2 + 2c\mathrm{Tr}_e^m(a) - \mathrm{Tr}_e^m(a^2)$. Then

$$\begin{aligned}
\aleph_4 &= \overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)\overline{\chi}_1\left(-\frac{z\mathrm{Tr}_e^m(a^2)}{\nabla}\left(\frac{c\mathrm{Tr}_e^m(a)}{\mathrm{Tr}_e^m(a^2)}-1\right)^2\right)\\
&\quad\times\overline{\eta}\left(\frac{\nabla}{4z\mathrm{Tr}_e^m(a^2)}\right)\overline{G}-\overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\chi}_1\left(\frac{c^2}{\mathrm{Tr}_e^m(a^2)}z\right)+\overline{\eta}(-s)G\overline{G}\\
&= G\overline{G}^2\sum_{z\in\mathbb{F}_{p^e}^*}\overline{\eta}(-z\nabla)\overline{\chi}_1\left(\frac{z}{\nabla}\phi(c)\right)+\left(\overline{\eta}(-\mathrm{Tr}_e^m(a^2))+\overline{\eta}(-s)\right)G\overline{G}\\
&= \begin{cases} \big(\overline{\eta}(-\mathrm{Tr}_e^m(a^2))+\overline{\eta}(-s)\big)G\overline{G}, & \text{if } \phi(c)=0,\\ \big(\overline{\eta}(\phi(c))p^e+\overline{\eta}(-\mathrm{Tr}_e^m(a^2))+\overline{\eta}(-s)\big)G\overline{G}, & \text{if } \phi(c)\neq 0.\end{cases}
\end{aligned}$$

This completes the proof of the lemma. □

Lemma 3.5 *Suppose that $\lambda \in \mathbb{F}_{p^e}^*$ and $\mu \in \mathbb{F}_{p^e}$. For $i \in \{1, -1\}$, let K_i denote the number of pairs (λ, μ) such that $\overline{\eta}(\mu^2 - s\lambda) = i$. Then*

$$K_i = \begin{cases} \frac{1}{2}(p^e-1)(p^e-2), & \textit{if } i=1,\\ \frac{1}{2}(p^e-1)p^e, & \textit{if } i=-1.\end{cases}$$

Proof First, we take $\mu = 0$. Then $\mu^2 - s\lambda = -s\lambda$, and the number of pairs $(\lambda, 0)$ satisfying $\overline{\eta}(\mu^2 - s\lambda) = i$ is $\frac{(p^e-1)}{2}$. Further, we consider that $\mu \neq 0$. Then, for each pair $(\lambda, \mu) \in \mathbb{F}_{p^e}^* \times \mathbb{F}_{p^e}^*$ and fixed $s \in \mathbb{F}_{p^e}^*$, we define a mapping $\mathcal{L}$ from $\mathbb{F}_{p^e}^* \times \mathbb{F}_{p^e}^*$ into $\mathbb{F}_{p^e}$ by $\mathcal{L}(\lambda, \mu) = \mu^2 - s\lambda$. For each $c_0 \in \mathbb{F}_{p^e}^*$, let

$$\mathcal{A}_{c_0} = \{(\lambda, \mu) \in \mathbb{F}_{p^e}^* \times \mathbb{F}_{p^e}^* : \mathcal{L}(\lambda, \mu) = c_0\}.$$

Set $p^e = 2h + 1$. Now, for a fixed c_0 such that $\overline{\eta}(c_0) = 1$, the number of pairs (λ, μ^2) satisfying $\mu^2 - s\lambda = c_0$ is equal to $(0, 0)^{(2,p^e)} + (1, 0)^{(2,p^e)} = h - 1$ (by Lemma 2.2). Similarly, for a fixed c_0 such that $\overline{\eta}(c_0) = -1$, the number of pairs (λ, μ^2) satisfying $\mu^2 - s\lambda = c_0$ is equal to $(0, 1)^{(2,p^e)} + (1, 1)^{(2,p^e)} = h$ (from Lemma 2.2). Consequently, we have

$$\#\mathcal{A}_{c_0} = \begin{cases} 2(h-1), & \text{if } \overline{\eta}(c_0)=1,\\ 2h, & \text{if } \overline{\eta}(c_0)=-1.\end{cases}$$

We conclude that $K_1 = \frac{(p^e-1)}{2} + (p^e - 1)(h - 1)$ and $K_{-1} = \frac{(p^e-1)}{2} + (p^e - 1)h$. Thus, the result is established. □

Lemma 3.6 *Suppose that $\lambda \in \mathbb{F}_{p^e}^*$, $\mu \in \mathbb{F}_{p^e}$ and $\mu^2 - s\lambda \neq 0$. For $i \in \{1, -1\}$, let ψ_i denote the number of the pairs (λ, μ) such that $\overline{\eta}(\lambda) = i$. Then*

$$\psi_1 = \begin{cases} \frac{1}{2}(p^e-1)(p^e-2), & \text{if } \overline{\eta}(s) = 1, \\ \frac{1}{2}(p^e-1)p^e, & \text{if } \overline{\eta}(s) = -1, \end{cases}$$

and

$$\psi_{-1} = \begin{cases} \frac{1}{2}(p^e-1)p^e, & \text{if } \overline{\eta}(s) = 1, \\ \frac{1}{2}(p^e-1)(p^e-2), & \text{if } \overline{\eta}(s) = -1. \end{cases}$$

Proof Following the arguments similar to the arguments used in the proof of Lemma 3.5, one may easily get the proof of the lemma. So, the proof of the lemma is omitted. □

Let $c \in \mathbb{F}_{p^e}^*$ and $a \in \mathbb{F}_{p^m}^*$. For a codeword $\mathbf{c}_a$ of $\mathcal{C}_D$, we denote $N_c = N_c(a)$ to be the number of components $\mathrm{Tr}_e^m(ax)$ of $\mathbf{c}_a$ that are equal to c and n to be the length of $\mathbf{c}_a$. So, we have

$$\begin{aligned} N_c &= \#\{x \in \mathbb{F}_{p^m} : \mathrm{Tr}_e^m(x) = 1, \mathrm{Tr}_e^m(x^2) = 0 \text{ and } \mathrm{Tr}_e^m(ax) = c\} \\ &= \frac{1}{p^{3e}} \sum_{x \in \mathbb{F}_{p^m}} \left(\sum_{y \in \mathbb{F}_{p^e}} \zeta_p^{\mathrm{Tr}_1^e\left(y(\mathrm{Tr}_e^m(x)-1)\right)} \right) \left(\sum_{z \in \mathbb{F}_{p^e}} \zeta_p^{\mathrm{Tr}_1^e(z\mathrm{Tr}_e^m(x^2))} \right) \left(\sum_{w \in \mathbb{F}_{p^e}} \zeta_p^{\mathrm{Tr}_1^e\left(w(\mathrm{Tr}_e^m(ax)-c)\right)} \right) \\ &= \frac{n}{p^e} + p^{-3e} \sum_{x \in \mathbb{F}_{p^m}} \sum_{y \in \mathbb{F}_{p^e}} \zeta_p^{\mathrm{Tr}_1^e\left(y(\mathrm{Tr}_e^m(x)-1)\right)} \sum_{z \in \mathbb{F}_{p^e}} \zeta_p^{\mathrm{Tr}_1^e(z\mathrm{Tr}_e^m(x^2))} \sum_{w \in \mathbb{F}_{p^e}^*} \zeta_p^{\mathrm{Tr}_1^e\left(w(\mathrm{Tr}_e^m(ax)-c)\right)} \\ &= \frac{n}{p^e} + p^{-3e}(\aleph_1 + \aleph_2 + \aleph_3 + \aleph_4), \end{aligned} \tag{6}$$

where

$$\aleph_1 = \sum_{x \in \mathbb{F}_{p^m}} \sum_{w \in \mathbb{F}_{p^e}^*} \zeta_p^{\mathrm{Tr}_1^e\left(w(\mathrm{Tr}_e^m(ax)-c)\right)} = \sum_{w \in \mathbb{F}_{p^e}^*} \overline{\chi}_1(-cw) \sum_{x \in \mathbb{F}_{p^m}} \chi_1(awx) = 0,$$

and $\aleph_2$, $\aleph_3$ and $\aleph_4$ are defined in Lemmas 3.2, 3.3 and 3.4 respectively. In the upcoming theorems, we have determined N_c for few different cases.

Theorem 3.7 *Assume that $c, c_0 \in \mathbb{F}_{p^e}^*$. If $2 \mid s$ and $p \mid s$, then the linear code $\mathcal{C}_D$ defined by (1) has parameters $[p^{m-2e}, s]$, and its complete weight enumerator is given in* Table 1.

Table 1 The complete weight enumerator of the Code $\mathcal{C}_D$ if $2 \mid s$ and $p \mid s$

N_c		Frequency
0		1
p^{m-3e}		$p^{m-e} - p^e$
$p^{m-3e} + (-1)^{\frac{(p-1)^2 m}{8}} p^{\frac{m-4e}{2}}$		$(p^e-1)p^{m-2e}$
N_{c_0} (c_0 is fixed)	$N_c(c \neq c_0)$	Frequency
p^{m-2e}	0	1
$p^{m-3e} - (p^e-1)(-1)^{\frac{(p-1)^2 m}{8}} p^{\frac{m-4e}{2}}$	$p^{m-3e} + (-1)^{\frac{(p-1)^2 m}{8}} p^{\frac{m-4e}{2}}$	$(p^e-1)p^{m-2e}$

Proof From the definition, this code has length $n = \#D$ which follows from Lemma 3.1 and dimension s. From (6), we have $N_c = \frac{n}{p^e} + p^{-3e}(\aleph_2 + \aleph_3 + \aleph_4)$, where $c \in \mathbb{F}_{p^e}^*$. In this case, the length of the code $\mathcal{C}_D$ is $n = p^{m-2e}$.

If $a \in \mathbb{F}_{p^e}^*$, then $\mathrm{Tr}_e^m(a^2) = 0$ and $\mathrm{Tr}_e^m(a) = 0$. Consequently, we have

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_2 + \aleph_3 + \aleph_4) \\ &= \begin{cases} p^{m-3e} + p^{-3e}\left((p^e-1)p^m - (p^e-1)G + (p^e-1)G\right), & \text{if } c = a \\ p^{m-3e} + p^{-3e}\left(-p^m - (p^e-1)G + (p^e-1)G\right), & \text{if } c \neq a \end{cases} \\ &= \begin{cases} p^{m-2e}, & \text{if } c = a, \\ 0, & \text{if } c \neq a. \end{cases} \end{aligned}$$

Each value occurs only once.

Now, suppose that $a \in \mathbb{F}_{p^m}^* \setminus \mathbb{F}_{p^e}^*$. Then $\aleph_2 = 0$. We give the remaining proof in the following cases:

Case 1: If $\mathrm{Tr}_e^m(a^2) = \mathrm{Tr}_e^m(a) = 0$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= p^{m-3e} + p^{-3e}\left(-(p^e-1)G + (p^e-1)G\right) = p^{m-3e}. \end{aligned}$$

By Lemma 3.1, the frequency is $p^{m-2e} + p^{-e}(p^e-1)G - p^e$ as $a \notin \mathbb{F}_{p^e}$.

Case 2: If $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\mathrm{Tr}_e^m(a) = 0$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= p^{m-3e} + p^{-3e}(G - G) = p^{m-3e}. \end{aligned}$$

By Lemma 3.1, the frequency is $(p^e-1)(p^{m-2e} - p^{-e}G)$.

Hence, we conclude from last two cases that $N_c = p^{m-3e}$ occurs $p^{m-e} - p^e$ times.

Case 3: If $\mathrm{Tr}_e^m(a^2) = 0$ and $\mathrm{Tr}_e^m(a) \neq 0$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= p^{m-3e} + p^{-3e}\left(-(p^e-1)G - G\right) = p^{m-3e} - p^{-2e}G. \end{aligned}$$

It follows from Lemma 3.1 that this value occurs $(p^e-1)p^{m-2e}$ times.

Case 4: If $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\mathrm{Tr}_e^m(a) \neq 0$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= \begin{cases} p^{m-3e} + p^{-3e}\left(1 + (p^{2e} - p^e - 1)\right)G, & \text{if } \mathrm{Tr}_e^m(a^2) = 2c\mathrm{Tr}_e^m(a) \\ p^{m-3e} + p^{-3e}\left(1 - (p^e+1)\right)G, & \text{if } \mathrm{Tr}_e^m(a^2) \neq 2c\mathrm{Tr}_e^m(a) \end{cases} \\ &= \begin{cases} p^{m-3e} + p^{-2e}(p^e-1)G, & \text{if } c = c_0, \\ p^{m-3e} - p^{-2e}G, & \text{if } c \neq c_0, \end{cases} \end{aligned}$$

where $c_0 = \frac{\mathrm{Tr}_e^m(a^2)}{2\mathrm{Tr}_e^m(a)} \in \mathbb{F}_{p^e}^*$. By Lemma 3.1, the frequency is $(p^e-1)p^{m-2e}$. This completes the proof of the theorem. □

Table 2 The weight distribution of $\mathcal{C}_D$ if $2 \mid s$ and $p \mid s$

Weight	Frequency
0	1
p^{m-2e}	$p^e - 1$
$(p^e-1)p^{m-3e}$	$p^{m-e} - p^e$
$(p^e-1)\left(p^{m-3e} + (-1)^{\frac{(p-1)^2 m}{8}} p^{\frac{m-4e}{2}}\right)$	$(p^e-1)p^{m-2e}$
$(p^e-1)p^{m-3e} - (-1)^{\frac{(p-1)^2 m}{8}} p^{\frac{m-4e}{2}}$	$(p^e-1)^2 p^{m-2e}$

Corollary 3.8 *If* $2 \mid s$ *and* $p \mid s$*, then the weight distribution of the linear code* $\mathcal{C}_D$ *defined by* (1) *is given in* Table 2.

Example 3.9 Let $(p, m, s, e) = (3, 12, 6, 2)$. Then, by Theorem 3.7, the code $\mathcal{C}_D$ is a $[6561, 6, 5823]$ linear code. Its complete weight enumerator and weight enumerator are

$$\sum_{i=0}^{8} w_i^{6561} + 59040 \prod_{j=0}^{8} w_j^{729} + 52488 \sum_{i=0}^{8} \left(w_i^{657} \prod_{j \neq i} w_j^{738} \right) (0 \le j \le 8)$$

and $1 + 419904x^{5823} + 59040x^{5832} + 52488x^{5904} + 8x^{6561}$ respectively.

Theorem 3.10 *Assume that* $c \in \mathbb{F}_{p^e}^*$. *If* $2 \mid s$ *and* $p \nmid s$*, then the linear code* $\mathcal{C}_D$ *defined by* (1) *has parameters* $[n, s]$*, where*

$$n = p^{m-2e} - (-1)^{\frac{(p-1)^2 m}{8}} p^{\frac{m-2e}{2}}.$$

Its complete weight enumerator is given in Table 3.

Proof This code has length $n = \#D$ which follows from Lemma 3.1 and dimension s. For $c \in \mathbb{F}_{p^e}^*$, recall from (6) that $N_c = \frac{n}{p^e} + p^{-3e}(\aleph_2 + \aleph_3 + \aleph_4)$. We now consider the case that $2 \mid s$ and $p \nmid s$. In this case the length n of the code $\mathcal{C}_D$ is $p^{m-2e} + p^{-e}G$.

Table 3 The complete weight enumerator of the Code $\mathcal{C}_D$ if $2 \mid s$ and $p \nmid s$

N_c	Frequency	
0	1	
p^{m-3e}	$p^{m-2e} - 1$	
$p^{m-3e} - (-1)^{\frac{(p-1)^2 m}{8}} p^{\frac{m-4e}{2}}$	$\frac{1}{2}(p^e-1)(p^{m-e} + (-1)^{\frac{(p-1)^2 m}{4}} p^{\frac{m}{2}})$	
N_{c_0} ($c_0 \in \mathbb{F}_{p^e}^*$ is fixed)	$N_c (c \neq c_0)$	Frequency
n	0	1
$p^{m-3e} - (-1)^{\frac{(p-1)^2 m}{8}} p^{\frac{m-2e}{2}}$	p^{m-3e}	$p^{m-2e} - 1$
$p^{m-3e} - (p^e-1)(-1)^{\frac{(p-1)^2 m}{8}} p^{\frac{m-4e}{2}}$	$p^{m-3e} + (-1)^{\frac{(p-1)^2 m}{8}} p^{\frac{m-4e}{2}}$	n
$N_{\bar{c}}$ ($\bar{c} = c_0, c_1 \in \mathbb{F}_{p^e}^*$ and $c_0 \neq c_1$)	$N_c (c \neq c_0, c_1)$	Frequency
$p^{m-3e} - (p^e-1)(-1)^{\frac{(p-1)^2 m}{8}} p^{\frac{m-4e}{2}}$	$p^{m-3e} + (-1)^{\frac{(p-1)^2 m}{8}} p^{\frac{m-4e}{2}}$	n

If $a \in \mathbb{F}_{p^e}^*$, then $\mathrm{Tr}_e^m(a^2) = a^2 s \neq 0$ and $\mathrm{Tr}_e^m(a) = as \neq 0$. Consequently, $\nabla = (\mathrm{Tr}_e^m(a))^2 - s\mathrm{Tr}_e^m(a^2) = 0$ and

$$N_c = \frac{n}{p^e} + p^{-3e}(\aleph_2 + \aleph_3 + \aleph_4)$$

$$N_c = \begin{cases} p^{m-3e} + p^{-2e}G + p^{-3e}\left((p^e-1)p^m + G + (p^{2e} - p^e - 1)G\right), & \text{if } c = a \\ p^{m-3e} + p^{-2e}G + p^{-3e}\left(-p^m + G - (p^e+1)G\right), & \text{if } c \neq a \end{cases}$$

$$N_c = \begin{cases} p^{m-2e} + p^{-e}G, & \text{if } c = a, \\ 0, & \text{if } c \neq a. \end{cases}$$

Moreover, each value occurs only once.

Suppose that $a \in \mathbb{F}_{p^m}^* \setminus \mathbb{F}_{p^e}^*$. Under this assumption, we have $\aleph_2 = 0$. We give the remaining proof in the following cases:

Case 1: If $\mathrm{Tr}_e^m(a^2) = \mathrm{Tr}_e^m(a) = 0$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= p^{m-3e} + p^{-2e}G + p^{-3e}\left(-(p^e-1)G - G\right) = p^{m-3e}. \end{aligned}$$

By Lemma 3.1, the frequency is $p^{m-2e} - 1$ as $a \neq 0$.

Case 2: If $\mathrm{Tr}_e^m(a^2) = 0$ and $\mathrm{Tr}_e^m(a) \neq 0$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= \begin{cases} p^{m-3e} + p^{-2e}G + p^{-3e}\left(-(p^e-1)G + (p^{2e} - p^e - 1)G\right), & \text{if } cs = 2\mathrm{Tr}_e^m(a) \\ p^{m-3e} + p^{-2e}G + p^{-3e}\left(-(p^e-1)G - (p^e+1)G\right), & \text{if } cs \neq 2\mathrm{Tr}_e^m(a) \end{cases} \\ &= \begin{cases} p^{m-3e} + p^{-2e}(p^e-1)G, & \text{if } c = c_0, \\ p^{m-3e} - p^{-2e}G, & \text{if } c \neq c_0, \end{cases} \end{aligned}$$

where $c_0 = \frac{2\mathrm{Tr}_e^m(a)}{s} \in \mathbb{F}_{p^e}^*$. By Lemma 3.1, the frequency is $p^{m-2e} + p^{-e}G$.

Case 3: If $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\nabla = 0$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= \begin{cases} p^{m-3e} + p^{-2e}G + p^{-3e}\left(G + (p^{2e} - p^e - 1)G\right), & \text{if } c\mathrm{Tr}_e^m(a) = \mathrm{Tr}_e^m(a^2) \\ p^{m-3e} + p^{-2e}G + p^{-3e}\left(G - (p^e+1)G\right), & \text{if } c\mathrm{Tr}_e^m(a) = \mathrm{Tr}_e^m(a^2) \end{cases} \\ &= \begin{cases} p^{m-3e} + p^{-e}G, & \text{if } c = c_0, \\ p^{m-3e}, & \text{if } c \neq c_0, \end{cases} \end{aligned}$$

where $c_o = \frac{\mathrm{Tr}_e^m(a^2)}{\mathrm{Tr}_e^m(a)} = \frac{\mathrm{Tr}_e^m(a)}{s} \in \mathbb{F}_{p^e}^*$ since $\nabla = 0$. By Lemma 3.1, the frequency is $p^{m-2e} - 1$.

Case 4: If $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\overline{\eta}(\nabla) = 1$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= \begin{cases} p^{m-3e} + p^{-2e}G + p^{-3e}\left(G + (p^{2e} - 2p^e - 1)G\right), & \text{if } \phi(c) = 0 \\ p^{m-3e} + p^{-2e}G + p^{-3e}\left(G - (2p^e+1)G\right), & \text{if } \phi(c) \neq 0 \end{cases} \\ &= \begin{cases} p^{m-3e} + p^{-2e}(p^e-1)G, & \text{if } c = c_0, c_1, \\ p^{m-3e} - p^{-2e}G, & \text{if } c \neq c_0, c_1, \end{cases} \end{aligned}$$

where c_0, c_1 are two distinct roots of the equation $\phi(c) = -sc^2 + 2c\mathrm{Tr}_e^m(a) - \mathrm{Tr}_e^m(a^2) = 0$, since $\overline{\eta}(\nabla) = 1$. By Lemmas 3.1 and 3.5, the frequency is $p^{m-2e} + p^{-e}G$.
Case 5: If $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\overline{\eta}(\nabla) = -1$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= p^{m-3e} + p^{-2e}G + p^{-3e}(G - G) \\ &= p^{m-3e} + p^{-2e}G. \end{aligned}$$

By Lemmas 3.1 and 3.5, the frequency is $\frac{1}{2}(p^e - 1)(p^{m-e} - G)$. Thus, the result is established. □

Corollary 3.11 *If* $2 \mid s$ *and* $p \nmid s$*, then the weight distribution of the linear code* $\mathcal{C}_D$ *defined by* (1) *is given in* Table 4.

Example 3.12 Let $(p, m, s, e) = (3, 8, 4, 2)$. Then, by Theorem 3.10, the code $\mathcal{C}_D$ is a $[72, 4, 62]$ linear code. Its complete weight enumerator and weight enumerator are

$$\begin{aligned} &\sum_{i=0}^{8} w_i^{72} + 80\prod_{j=1}^{8} w_j^9 + 3240\prod_{k=0}^{8} w_k^8 + 80w_0^9\sum_{i=1}^{8}\prod_{j\neq i} w_j^9 \ (1 \leq j \leq 8) \\ &+ 72w_0\sum_{j=1}^{8} w_j\left(\prod_{k\neq j} w_k^{10}\right) (1 \leq k \leq 8) \\ &+ 72w_0^{10}\sum_{i=1}^{8} w_i \sum_{j>i} w_j \left(\prod_{k\neq j,i} w_k^{10}\right) (1 \leq j, k \leq 8) \end{aligned}$$

and $1 + 2016x^{62} + 640x^{63} + 3240x^{64} + 576x^{71} + 88x^{72}$ respectively.

Remark 3.13 Consider the linear codes $[81, 6, 48]$ and $[71, 5, 42]$ obtained in [22] and [13] respectively. Then one can see that our code illustrated in the previous example has improved relative minimum distance.

Table 4 The weight distribution of $\mathcal{C}_D$ if $2 \mid s$ and $p \nmid s$

Weight	Frequency
0	1
$(p^e-1)p^{m-3e}$	$p^{m-2e}-1$
$(p^e-1)\left(p^{m-3e}-(-1)^{\frac{(p-1)^2m}{8}}p^{\frac{m-4e}{2}}\right)$	$\frac{1}{2}(p^e-1)\left(p^{m-e}+(-1)^{\frac{(p-1)^2m}{8}}p^{\frac{m}{2}}\right)$
$p^{m-2e}-(-1)^{\frac{(p-1)^2m}{8}}p^{\frac{m-2e}{2}}$	p^e-1
$p^{m-3e}(p^e-1)-(-1)^{\frac{(p-1)^2m}{8}}p^{\frac{m-2e}{2}}$	$(p^e-1)(p^{m-2e}-1)$
$p^{m-3e}(p^e-1)-(-1)^{\frac{(p-1)^2m}{8}}p^{\frac{m-4e}{2}}$	$(p^e-1)(p^{m-2e}-(-1)^{\frac{(p-1)^2m}{8}}p^{\frac{m-2e}{2}})$
$(p^e-1)p^{m-3e}-(p^e+1)(-1)^{\frac{(p-1)^2m}{8}}p^{\frac{m-4e}{2}}$	$\frac{1}{2}(p^e-1)(p^e-2)(p^{m-2e}-(-1)^{\frac{(p-1)^2m}{8}}p^{\frac{m-2e}{2}})$

Theorem 3.14 *Assume that $c \in \mathbb{F}_{p^e}^*$. If $2 \nmid s$ and $p \mid s$, then the linear code $\mathcal{C}_D$ defined by* (1) *has parameters $[p^{m-2e}, s]$. Its complete weight enumerator is given in* Table 5.

Proof Now consider that $2 \nmid s$ and $p \mid s$. In this case the length of the code $\mathcal{C}_D$ is $n = p^{m-2e}$.

If $a \in \mathbb{F}_{p^e}^*$, then $\mathrm{Tr}_e^m(a^2) = 0$ and $\mathrm{Tr}_e^m(a) = 0$. Consequently, by (6), we have

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_2 + \aleph_3 + \aleph_4) \\ &= \begin{cases} p^{m-3e} + p^{-3e}(p^e - 1)p^m, & \text{if } c = a \\ p^{m-3e} + p^{-3e}(-p^m), & \text{if } c \neq a \end{cases} \\ &= \begin{cases} p^{m-2e}, & \text{if } c = a, \\ 0, & \text{if } c \neq a. \end{cases} \end{aligned}$$

Each value occurs only once.

Suppose that $a \in \mathbb{F}_{p^m}^* \setminus \mathbb{F}_{p^e}^*$. Under this assumption, we have $\aleph_2 = 0$. We give the remaining proof in the following cases:

Case 1: If $\mathrm{Tr}_e^m(a^2) = \mathrm{Tr}_e^m(a) = 0$, then

$$N_c = \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) = p^{m-3e}.$$

By Lemma 3.1, the frequency is $p^{m-2e} - p^e$ as $a \notin \mathbb{F}_{p^e}$.

Case 2: If $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\mathrm{Tr}_e^m(a) = 0$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= p^{m-3e} + p^{-3e}(-\overline{\eta}(-\mathrm{Tr}_e^m(a^2)) + \overline{\eta}(-\mathrm{Tr}_e^m(a^2)))G\overline{G} = p^{m-3e}. \end{aligned}$$

By Lemma 3.1, the frequency is $(p^e - 1)p^{m-2e}$.

Hence, we conclude from the last two cases that $N_c = p^{m-3e}$ occurs $p^{m-e} - p^e$ times.

Case 3: If $\mathrm{Tr}_e^m(a^2) = 0$ and $\mathrm{Tr}_e^m(a) \neq 0$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= p^{m-3e} + p^{-2e}\overline{\eta}\left(\frac{c\mathrm{Tr}_e^m(a)}{2}\right)G\overline{G}, \end{aligned}$$

Table 5 The complete weight enumerator of the Code $\mathcal{C}_D$ if $2 \nmid s$ and $p \mid s$

	N_c	Frequency
	0	1
	p^{m-3e}	$p^{m-e} - p^e$
	$p^{m-3e} + \overline{\eta}(c)(-1)^{m+e-2}(-1)^{\frac{(p-1)^2(m+e)}{8}} p^{\frac{m-3e}{2}}$	$\frac{1}{2}(p^e - 1)p^{m-2e}$
	$p^{m-3e} - \overline{\eta}(c)(-1)^{m+e-2}(-1)^{\frac{(p-1)^2(m+e)}{8}} p^{\frac{m-3e}{2}}$	$\frac{1}{2}(p^e - 1)p^{m-2e}$
N_{c_0} ($c_0 \in \mathbb{F}_{p^e}^*$ is fixed)	$N_c(c \neq c_0)$	Frequency
p^{m-2e}	0	1
p^{m-3e}	$p^{m-3e} + \overline{\eta}(c - c_0)(-1)^{m+e-2}(-1)^{\frac{(p-1)^2(m+e)}{8}} p^{\frac{m-3e}{2}}$	$\frac{1}{2}(p^e - 1)p^{m-2e}$
p^{m-3e}	$p^{m-3e} - \overline{\eta}(c - c_0)(-1)^{m+e-2}(-1)^{\frac{(p-1)^2(m+e)}{8}} p^{\frac{m-3e}{2}}$	$\frac{1}{2}(p^e - 1)p^{m-2e}$

from which it follows that $N_c = p^{m-3e} + p^{-2e}\overline{\eta}(c)G\overline{G}$ or $N_c = p^{m-3e} - p^{-2e}\overline{\eta}(c)G\overline{G}$. According to Lemma 3.1, the frequency of each value is $\frac{1}{2}(p^e-1)p^{m-2e}$.

Case 4: If $\mathrm{Tr}_e^m(a^2) \neq 0$, $\mathrm{Tr}_e^m(a) \neq 0$ and $\mathrm{Tr}_e^m(a^2) = 2c\mathrm{Tr}_e^m(a)$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= p^{m-3e} + p^{-3e}\left(-\overline{\eta}(-\mathrm{Tr}_e^m(a^2)) + \overline{\eta}(-\mathrm{Tr}_e^m(a^2))\right) G\overline{G} = p^{m-3e}. \end{aligned}$$

Case 5: If $\mathrm{Tr}_e^m(a^2) \neq 0$, $\mathrm{Tr}_e^m(a) \neq 0$ and $\mathrm{Tr}_e^m(a^2) \neq 2c\mathrm{Tr}_e^m(a)$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= p^{m-3e} + p^{-3e}\left(-\overline{\eta}(-\mathrm{Tr}_e^m(a^2)) + \eta\left(2c\mathrm{Tr}_e^m(a) - \mathrm{Tr}_e^m(a^2)\right) p^e + \overline{\eta}(-\mathrm{Tr}_e^m(a^2))\right) G\overline{G}. \end{aligned}$$

So, one can easily combine the last two cases as

$$N_c = \begin{cases} p^{m-3e}, & \text{if } c = c_0, \\ p^{m-3e} + p^{-2e}\overline{\eta}(2\mathrm{Tr}_e^m(a))\overline{\eta}(c-c_0)G\overline{G}, & \text{if } c \neq c_0, \end{cases}$$

where $c_0 = \frac{\mathrm{Tr}_e^m(a^2)}{2\mathrm{Tr}_e^m(a)} \in \mathbb{F}_{p^e}^*$. This concludes that

$$N_c = \begin{cases} p^{m-3e}, & \text{if } c = c_0, \\ p^{m-3e} + p^{-2e}\overline{\eta}(c-c_0)G\overline{G}, & \text{if } c \neq c_0, \end{cases}$$

or

$$N_c = \begin{cases} p^{m-3e}, & \text{if } c = c_0, \\ p^{m-3e} - p^{-2e}\overline{\eta}(c-c_0)G\overline{G}, & \text{if } c \neq c_0. \end{cases}$$

By Lemma 3.1, the frequency is $\frac{1}{2}(p^e-1)p^{m-2e}$. Thus, the result is established. □

Corollary 3.15 *If $2 \nmid s$ and $p \mid s$, then the weight distribution of the linear code $\mathcal{C}_D$ defined by* (1) *is given in the following* Table 6.

Proof The result can be extracted from the complete weight enumerator as shown in the last Theorem 3.14, by observing that

$$\sum_{c\in\mathbb{F}_{p^e}^*} \overline{\eta}(c-c_0) = \sum_{c\in\mathbb{F}_{p^e}} \overline{\eta}(c-c_0) - \overline{\eta}(-c_0) = -\overline{\eta}(-c_0),$$

where $c_0 \in \mathbb{F}_{p^e}^*$. □

Table 6 The weight distribution of $\mathcal{C}_D$ if $2 \nmid s$ and $p \mid s$

Weight	Frequency
0	1
p^{m-2e}	p^e-1
$(p^e-1)p^{m-3e}$	$2p^{m-e} - p^{m-2e} - p^e$
$(p^e-1)p^{m-3e} + p^{\frac{m-3e}{2}}$	$\frac{1}{2}(p^e-1)^2p^{m-2e}$
$(p^e-1)p^{m-3e} - p^{\frac{m-3e}{2}}$	$\frac{1}{2}(p^e-1)^2p^{m-2e}$

Example 3.16 Let $(p, m, s, e) = (3, 6, 3, 2)$. Then, by Theorem 3.14, the code $\mathcal{C}_D$ is a $[9, 3, 7]$ linear code, which is a MDS code. Let $\mathbb{F}_9 = \{w_0, w_1 \ldots, w_8\}$. If w_2, w_4, w_6 and w_8 are square elements in $\mathbb{F}_9^*$, then its complete weight enumerator is

$$\sum_{i=0}^{8} w_i^9 + 72\prod_{j=0}^{8} w_j + 36(w_1w_3w_5w_7)^2w_0 + 36(w_2w_4w_6w_8)^2w_0 + 36(w_2w_4w_6w_8)^2$$
$$\times(w_1 + w_3 + w_5 + w_7)+36(w_1w_3w_5w_7)^2(w_2+w_4+w_6 + w_8) + 36w_2(w_4w_6w_8)^2w_0^2$$
$$+36w_4(w_2w_6w_8)^2w_0^2+36w_6(w_2w_4w_8)^2w_0^2+36w_8(w_2w_4w_6)^2w_0^2+36w_1(w_3w_5w_7)^2w_0^2$$
$$+36w_3(w_1w_5w_7)^2w_0^2 + 36w_5(w_1w_3w_7)^2w_0^2 + 36w_7(w_1w_3w_5)^2w_0^2$$

while its weight enumerator is $1 + 288x^7 + 144x^8 + 296x^9$.

Theorem 3.17 *Assume that $c \in \mathbb{F}_{p^e}^*$. If $2 \nmid s$ and $p \nmid s$, then the linear code $\mathcal{C}_D$ defined by (1) has parameters $[p^{m-2e} - K, s]$, where*

$$K = \overline{\eta}(-s)(-1)^{m+e-2}(-1)^{\frac{(p-1)^2(m+e)}{8}}p^{\frac{m-3e}{2}}.$$

Its complete weight enumerator is given in Table 7, *where ∇ runs through $\mathbb{F}_{p^e}^*$ such that $\overline{\eta}(-\nabla) = -1$.*

Proof Consider the case that $2 \nmid s$ and $p \nmid s$. In this case, the length of the code $\mathcal{C}_D$ is $n = p^{m-2e} - \overline{\eta}(-s)p^{-2e}G\overline{G}$.

If $a \in \mathbb{F}_{p^e}^*$, then $\mathrm{Tr}_e^m(a^2) = a^2s \neq 0$ and $\mathrm{Tr}_e^m(a) = as \neq 0$. Consequently, $\nabla = (\mathrm{Tr}_e^m(a))^2 - s\mathrm{Tr}_e^m(a^2) = 0$ and $\overline{\eta}(-\mathrm{Tr}_e^m(a^2)) = \overline{\eta}(-s)$. Thus

$$N_c = \frac{n}{p^e} + p^{-3e}(\aleph_2 + \aleph_3 + \aleph_4)$$
$$N_c = \begin{cases} p^{-e}n + p^{-3e}\left((p^e-1)p^m - (p^e-1)\overline{\eta}(-s)G\overline{G}\right), & \text{if } c = a \\ p^{-e}n + p^{-3e}\left(-p^m + \overline{\eta}(-s)G\overline{G}\right), & \text{if } c \neq a \end{cases}$$
$$N_c = \begin{cases} n, & \text{if } c = a, \\ 0, & \text{if } c \neq a. \end{cases}$$

Each value occurs only once.

Table 7 The complete weight enumerator of the Code $\mathcal{C}_D$ if $2 \nmid s$ and $p \nmid s$

N_c		Frequency
0		1
p^{m-3e}		$p^{m-2e} + K(p^e - 1) - 1$
$p^{m-3e} + \overline{\eta}(s^2c^2 - \nabla)K$		$p^{m-2e} - K$
N_{c_0} ($c_0 \in \mathbb{F}_{p^e}^*$ is fixed)	$N_c(c \neq c_0)$	Frequency
$p^{m-2e} - K$	0	1
p^{m-3e}	$p^{m-3e} + \overline{\eta}(c^2 - cc_0)K$	$p^{m-2e} - K$
$p^{m-3e} - K$	p^{m-3e}	$p^{m-2e} + K(p^e - 1) - 1$
$p^{m-3e} - \overline{\eta}(-1)K$	$p^{m-3e} + \overline{\eta}\left(s^2(c-c_0)^2 - \nabla\right)K$	$p^{m-2e} - K$
$N_{\bar{c}}$ ($\bar{c} = c_0, c_1 \in \mathbb{F}_{p^e}^*$ and $c_0 \neq c_1$)	$N_c(c \neq c_0, c_1)$	Frequency
p^{m-3e}	$p^{m-3e} + \overline{\eta}\left((c-c_0)(c-c_1)\right)K$	$p^{m-2e} - K$

Suppose that $a \in \mathbb{F}_{p^m}^* \setminus \mathbb{F}_{p^e}^*$. Under this assumption $\aleph_2 = 0$. The remaining proof is given in the following cases:

Case 1: If $\mathrm{Tr}_e^m(a^2) = \mathrm{Tr}_e^m(a) = 0$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= p^{m-3e} - p^{-3e}\overline{\eta}(-s)G\overline{G} + p^{-3e}\overline{\eta}(-s)G\overline{G} = p^{m-3e}. \end{aligned}$$

By Lemma 3.1, the frequency is $p^{m-2e} + p^{-2e}\overline{\eta}(-s)(p^e-1)G\overline{G} - 1$.

Case 2: If $\mathrm{Tr}_e^m(a^2) = 0$ and $\mathrm{Tr}_e^m(a) \neq 0$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= \begin{cases} p^{m-3e}, & \text{if } cs = 2\mathrm{Tr}_e^m(a) \\ p^{m-3e} + p^{-2e}\overline{\eta}(2c\mathrm{Tr}_e^m(a) - c^2 s)G\overline{G}, & \text{if } cs \neq 2\mathrm{Tr}_e^m(a) \end{cases} \\ &= \begin{cases} p^{m-3e}, & \text{if } c = c_0, \\ p^{m-3e} + p^{-2e}\overline{\eta}(-s)\overline{\eta}(c^2 - cc_0)G\overline{G}, & \text{if } c \neq c_0, \end{cases} \end{aligned}$$

where $c_0 = \frac{2\mathrm{Tr}_e^m(a)}{s} \in \mathbb{F}_{p^e}^*$. By Lemma 3.1, the frequency is n.

Case 3: If $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\nabla = 0$, then $\overline{\eta}(-\mathrm{Tr}_e^m(a^2)) = \overline{\eta}(-s)$. Consequently, we have

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= \begin{cases} p^{-e}n + p^{-3e}\left(-1 - (p^e - 2)\right)\overline{\eta}(-s)G\overline{G}, & \text{if } c\mathrm{Tr}_e^m(a) = \mathrm{Tr}_e^m(a^2) \\ p^{-e}n + p^{-3e}(-1+2)\overline{\eta}(-s)G\overline{G}, & \text{if } c\mathrm{Tr}_e^m(a) \neq \mathrm{Tr}_e^m(a^2) \end{cases} \\ &= \begin{cases} p^{m-3e} - p^{-2e}\overline{\eta}(-s)G\overline{G}, & \text{if } c = c_0, \\ p^{m-3e}, & \text{if } c \neq c_0, \end{cases} \end{aligned}$$

where $c_o = \frac{\mathrm{Tr}_e^m(a)}{s} \in \mathbb{F}_{p^e}^*$ since $\nabla = 0$. One may easily find, by Lemma 3.1, that the frequency is $p^{m-2e} + \overline{\eta}(-s)(p^e-1)p^{-2e}G\overline{G} - 1$.

Case 4: If $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\nabla \neq 0$, then

$$\begin{aligned} N_c &= \frac{n}{p^e} + p^{-3e}(\aleph_3 + \aleph_4) \\ &= \begin{cases} p^{-e}n + p^{-3e}\overline{\eta}(-s)G\overline{G}, & \text{if } \phi(c) = 0 \\ p^{-e}n + p^{-3e}\left(p^e\overline{\eta}(\phi(c)) + \overline{\eta}(-s)\right)G\overline{G}, & \text{if } \phi(c) \neq 0 \end{cases} \\ &= \begin{cases} p^{m-3e}, & \text{if } \phi(c) = 0, \\ p^{m-3e} + p^{-2e}\overline{\eta}(\phi(c))G\overline{G}, & \text{if } \phi(c) \neq 0, \end{cases} \end{aligned}$$

where $\phi(c) = -sc^2 + 2c\mathrm{Tr}_e^m(a) - \mathrm{Tr}_e^m(a^2)$. This case is divided into the following two subcases.

Case 4(a): If $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\overline{\eta}(\nabla) = 1$, then the equation $\phi(c) = 0$ must have two distinct roots. Let c_0 and c_1 be the distinct roots of $\phi(c)$. Then $\phi(c)$ can be represented as $\phi(c) = -s(c - c_0)(c - c_1)$. Therefore, we have

$$N_c = \begin{cases} p^{m-3e}, & \text{if } c = c_0, c_1, \\ p^{m-3e} + p^{-2e}\overline{\eta}(-s)\overline{\eta}(c - c_0)\overline{\eta}(c - c_1)G\overline{G}, & \text{if } c \neq c_0, c_1. \end{cases}$$

By Lemma 3.1, the frequency is n. Moreover, by Lemma 3.5, there are $\frac{1}{2}(p^e-1)(p^e-2)$ such values.

Case 4(b): If $\mathrm{Tr}_e^m(a^2) \neq 0$ and $\overline{\eta}(\nabla) = -1$, then

$$N_c = p^{m-3e} + p^{-2e}\overline{\eta}(\phi(c))G\overline{G}.$$

More precisely, by writing $\phi(c) = -s\left(c - \frac{\mathrm{Tr}_e^m(a)}{s}\right)^2 + \frac{\nabla}{s}$, we deduce that

$$N_c = \begin{cases} p^{m-3e} - p^{-2e}\overline{\eta}(s)G\overline{G}, & \text{if } c = c_0, \\ p^{m-3e} + p^{-2e}\overline{\eta}(-s)\overline{\eta}\left(s^2(c-c_0)^2 - \nabla\right)G\overline{G}, & \text{if } c \neq c_0, \end{cases}$$

where $c_o = \frac{\mathrm{Tr}_e^m(a)}{s}$ and $\mathrm{Tr}_e^m(a) \neq 0$. The number of such values is $\frac{1}{2}(p^e-1)^2$. On the other hand if $\mathrm{Tr}_e^m(a) = 0$, then

$$N_c = p^{m-3e} + p^{-2e}\overline{\eta}(-s)\overline{\eta}(s^2c^2 - \nabla)G\overline{G}.$$

The number of such values is $\frac{1}{2}(p^e-1)$. Again, from Lemma 3.1, each value occurs n times. Thus, we have the desired result. □

Corollary 3.18 *If $2 \nmid s$ and $p \nmid s$, then the weight distribution of the linear code $\mathcal{C}_D$ defined by* (1) *is given in* Table 8, *where*

$$w = (-1)^{m+e-2}(-1)^{\frac{(p-1)^2(m+e)}{8}}p^{\frac{m-3e}{2}},$$

$$f_4 = \begin{cases} \frac{1}{2}(p^e-1)(p^e-2)(p^{m-2e} - \overline{\eta}(-s)w), & \text{if } \overline{\eta}(s) = 1, \\ \frac{1}{2}p^e(p^e-1)(p^{m-2e} - \overline{\eta}(-s)w), & \text{if } \overline{\eta}(s) = -1; \end{cases}$$

$$f_5 = \begin{cases} \frac{1}{2}p^e(p^e-1)(p^{m-2e} - \overline{\eta}(-s)w), & \text{if } \overline{\eta}(s) = 1, \\ \frac{1}{2}(p^e-1)(p^e-2)(p^{m-2e} - \overline{\eta}(-s)w), & \text{if } \overline{\eta}(s) = -1. \end{cases}$$

Proof For $a \in \mathbb{F}_{p^m}^*$, define $N_0 = \#\{x \in \mathbb{F}_{p^m} : \mathrm{Tr}_e^m(x) = 1, \mathrm{Tr}_e^m(x^2) = 0 \text{ and } \mathrm{Tr}_e^m(ax) = 0\}$. For given n the length of $\mathcal{C}_D$, the Hamming weight of a codeword $\mathbf{c}_a$ is given by

$$\mathrm{wt}(\mathbf{c}_a) = n - N_0, \tag{7}$$

In the same manner, as in (6), we can find that

$$N_0 = \frac{n}{p^e} + p^{-3e}(\overline{\aleph}_1 + \overline{\aleph}_2 + \overline{\aleph}_3 + \overline{\aleph}_4), \tag{8}$$

Table 8 The weight distribution of $\mathcal{C}_D$ if $2 \nmid s$ and $p \nmid s$

Weight	Frequency
0	1
$(p^e-1)p^{m-3e}$	$p^{m-2e} + \overline{\eta}(-s)(p^e-1)w - 1$
$p^{m-2e} - \overline{\eta}(-s)w$	$p^e - 1$
$p^{m-3e}(p^e-1) - \overline{\eta}(-s)w$	$(p^e-1)\left(2p^{m-2e} + \overline{\eta}(-s)(p^e-2)w - 1\right)$
$p^{m-3e}(p^e-1) - (\overline{\eta}(-1) + \overline{\eta}(-s))w$	f_4
$p^{m-3e}(p^e-1) + (\overline{\eta}(-1) - \overline{\eta}(-s))w$	f_5

where

$$\overline{\aleph}_1 = \sum_{x\in\mathbb{F}_{p^m}}\sum_{w\in\mathbb{F}_{p^e}^*}\zeta_p^{\mathrm{Tr}_1^e(w\mathrm{Tr}_e^m(ax))} = \sum_{w\in\mathbb{F}_{p^e}^*}\sum_{x\in\mathbb{F}_{p^m}}\zeta_p^{\mathrm{Tr}_1^m(awx)} = 0,$$

$$\overline{\aleph}_2 = \sum_{x\in\mathbb{F}_{p^m}}\sum_{y\in\mathbb{F}_{p^e}^*}\zeta_p^{\mathrm{Tr}_1^e\left(y(\mathrm{Tr}_e^m(x)-1)\right)}\sum_{w\in\mathbb{F}_{p^e}^*}\zeta_p^{\mathrm{Tr}_1^e(w\mathrm{Tr}_e^m(ax))},$$

$$\overline{\aleph}_3 = \sum_{x\in\mathbb{F}_{p^m}}\sum_{z\in\mathbb{F}_{p^e}^*}\zeta_p^{\mathrm{Tr}_1^e(z\mathrm{Tr}_e^m(x^2))}\sum_{w\in\mathbb{F}_{p^e}^*}\zeta_p^{\mathrm{Tr}_1^e(w\mathrm{Tr}_e^m(ax))},$$

$$\overline{\aleph}_4 = \sum_{x\in\mathbb{F}_{p^m}}\sum_{y\in\mathbb{F}_{p^e}^*}\zeta_p^{\mathrm{Tr}_1^e\left(y(\mathrm{Tr}_e^m(x)-1)\right)}\sum_{z\in\mathbb{F}_{p^e}^*}\zeta_p^{\mathrm{Tr}_1^e(z\mathrm{Tr}_e^m(x^2))}\sum_{w\in\mathbb{F}_{p^e}^*}\zeta_p^{\mathrm{Tr}_1^e(w\mathrm{Tr}_e^m(ax))}.$$

Let $2 \nmid s$ and $p \nmid s$. Then, by following the arguments similar to the arguments used in the proofs of Lemmas 3.2, 3.3 and 3.4, one may easily get that

$$\overline{\aleph}_2 = \begin{cases} -p^m, & \text{if } a \in \mathbb{F}_{p^e}^*, \\ 0, & \text{otherwise;} \end{cases}$$

$$\overline{\aleph}_3 = \begin{cases} 0, & \text{if } \mathrm{Tr}_e^m(a^2) = 0, \\ (p^e-1)\overline{\eta}(-\mathrm{Tr}_e^m(a^2))G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) \neq 0; \end{cases}$$

$$\overline{\aleph}_4 = \begin{cases} -(p^e-1)\overline{\eta}(-s)G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) = 0 \text{ and } \mathrm{Tr}_e^m(a) = 0, \\ \overline{\eta}(-s)G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) = 0 \text{ and } \mathrm{Tr}_e^m(a) \neq 0, \\ -(p^e-2)\overline{\eta}(-s)G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) \neq 0 \text{ and } \nabla = 0, \\ \left(\overline{\eta}(-\mathrm{Tr}_e^m(a^2)) + \overline{\eta}(-s)\right)G\overline{G}, & \text{if } \mathrm{Tr}_e^m(a^2) \neq 0 \text{ and } \nabla \neq 0. \end{cases}$$

The result is directly follows from (7), (8) and Lemmas 3.1 and 3.6. □

Remark 3.19 If $b \in \mathbb{F}_{p^e}^*$ is fixed and $D_b = \{x \in \mathbb{F}_{p^m} : \mathrm{Tr}_e^m(x) = b \text{ and } \mathrm{Tr}_e^m(x^2) = 0\}$, then we get the code $\mathcal{C}_{D_b}$ of the form (1). Now, define a mapping $f_b : D_1 \to D_b$ by

$$f_b(x) = bx.$$

This implies that the code $\mathcal{C}_{D_b}$ is equal to $\mathcal{C}_{D_1}$. So, Theorems 3.7, 3.10, 3.14 and 3.17 actually demonstrate the complete weight enumerators of $\mathcal{C}_{D_b}$ for all $b \in \mathbb{F}_{p^e}^*$.

Corollary 3.20 *Let $\mathcal{C}_D$ be the linear code defined by* (1). *Then $\mathcal{C}_D$ is optimal with respect to the Griesmer bound only if $s = 3$. If $s = p = 3$, then it is MDS and it has parameters* $[3^e, 3, 3^e - 2]$. *Moreover, for $s = 3$ and $p > 3$, it has parameters $[p^e + 1, 3, p^e - 1]$ if $\overline{\eta}(-3) = -1$ and $[p^e - 1, 3, p^e - 3]$ if $\overline{\eta}(-3) = 1$.*

Proof If $2 \nmid s$ and $p \mid s$, then it directly follows from Corollary 3.15 that $\mathcal{C}_D$ has parameters $[p^{m-2e}, s, (p^e-1)p^{m-3e} - p^{\frac{m-3e}{2}}]$. Suppose that $s = 2s' + 1$, where $s = \frac{m}{e}$ and $s' \geq 1$. Then we have

$$\sum_{i=0}^{s-1}\left\lceil \frac{d}{p^{ei}} \right\rceil = p^{e(2s'-1)} - p^{e(s'-1)} + 1 - \frac{p^{e(s'-1)} - 1}{p^e - 1}.$$

Table 9 Characterization of the linear codes obtained in [22]

Variables	Parameters	$\delta(\mathcal{C})$	$\delta(\mathcal{C})$+$\mathcal{R}(\mathcal{C})$
$(p, m) = (3, 6)$	[81, 6, 48]	0.5802	0.6543
$(p, m) = (5, 4)$	[20, 4, 14]	0.65	0.85
$(p, m) = (5, 3)$	[6, 3, 4](MDS Code)	0.5	1
$(p, m) = (3, 3)$	[3, 3, 1](MDS Code)	0	1

By the equation

$$p^{e(2s'-1)} - p^{e(s'-1)} + 1 - \frac{p^{e(s'-1)} - 1}{p^e - 1} = p^{e(2s'-1)},$$

we have $s' = 1$ whence $s = 3$. Since $p \mid s$, we must have $p = 3$. Thus, for $p = s = 3$, the code $\mathcal{C}_D$ is MDS with parameters $[3^e, 3, 3^e - 2]$.

Now, we suppose that $2 \nmid s$, $p \nmid s$ and $\overline{\eta}(-s)^{m+e-2}(-1)^{\frac{(p-1)^2(m+e)}{8}} = -1$. From Corollary 3.18, the code $\mathcal{C}_D$ has parameters $[p^{m-2e} + p^{\frac{m-3e}{2}}, s, (p^e - 1)p^{m-3e}]$. Thus

$$\sum_{i=0}^{s-1} \left\lceil \frac{d}{p^{ei}} \right\rceil = p^{e(s-2)} + 1.$$

Hence, the equation $p^{e(s-2)} + 1 = p^{e(s-2)} + p^{\frac{e(s-3)}{2}}$ gives that $s = 3$. Consequently, we have $\overline{\eta}(-3) = -1$. Therefore, the code $\mathcal{C}_D$ is MDS with parameters $[p^e + 1, 3, p^e - 1]$.

Further, consider that $2 \nmid s$, $p \nmid s$ and $\overline{\eta}(-s)^{m+e-2}(-1)^{\frac{(p-1)^2(m+e)}{8}} = 1$. In the same manner, we can show that $\mathcal{C}_D$ is MDS with parameters $[p^e - 1, 3, p^e - 3]$ when $s = 3$ and $\overline{\eta}(-3) = 1$. Other cases may similarly be verified.

Thus, it follows from Lemma 2.6 that the code $\mathcal{C}_D$ is optimal achieving the Griesmer bound provided that $s = 3$. □

It is well known that error-correcting capability of a linear code $\mathcal{C} = [n, k, d]$ depends on the relative minimun distance $\delta(\mathcal{C})$(see [15]). A linear code $\mathcal{C}$ is MDS if and only if $\delta(\mathcal{C}) + \mathcal{R}(\mathcal{C}) = 1$, where $\mathcal{R}(\mathcal{C})$ is the transmission rate of $\mathcal{C}$. The Remark 3.21 and Tables 9 and 10 conclude that codes determined in this paper have improved error-correcting capability and more close to MDS codes than the codes in [22].

Table 10 Characterization of the linear codes obtained in the present paper

Variables	Parameters	$\delta(\mathcal{C})$	$\delta(\mathcal{C})$+$\mathcal{R}(\mathcal{C})$
$(p, m, s, e) = (3, 12, 6, 2)$	[6561, 6, 5823]	0.8873	0.8882
$(p, m, s, e) = (3, 8, 4, 2)$	[72, 4, 62]	0.8472	0.9027
$(p, m, s, e) = (3, 6, 3, 2)$	[9, 3, 7](MDS Code)	0.6666	1
$(p, m, s, e) = (5, 8, 4, 2)$	[600, 4, 574]*	0.9566	0.9633

In the Table 10, $*$ shows that the complete weight enumerator of the code is not inlcluded in the present paper due to large presentation.

Remark 3.21 The MDS code [3, 3, 1], which is unique, obtained in [22] has zero relative minimum distance while our MDS codes $[3^e, 3, 3^e - 2]$ have nonzero relative minimum distance for every $e \geq 2$. In addition, it can easily be checked that

$$\frac{p^e-2}{p^e+1} > \frac{p-2}{p+1} \text{ and } \frac{p^e-4}{p^e-1} > \frac{p-4}{p-1} \text{ for all } e \geq 2.$$

Hence, one can conclude that our MDS codes have better error-correcting capability than the MDS codes in Corollary 2 of [22].

3.2 The dual code of the code $\mathcal{C}_D$

In this subsection, we study the dual code of the code $\mathcal{C}_D$. In the following theorem, we have determined bounds on the minimum distance of the dual code.

Theorem 3.22 *Let the symbols have the same meanings as before, and let $d^{\perp}$ denote the minimum distance of the dual code $\mathcal{C}_D^{\perp}$ of the code $\mathcal{C}_D$ defined in (1). Then*

1. *if $2 \mid s$ and $p \mid s$, we have $3 \leq d^{\perp} \leq 4$.*
2. *if $2 \mid s$, $p \nmid s$ and $e \geq 2$, we have $3 \leq d^{\perp} \leq 4$.*
3. *if $2 \nmid s$ and $e \geq 2$, we have $3 \leq d^{\perp} \leq 4$. In particular, $d^{\perp} = 4$ if $m = 3e$.*

Proof We only give the proof of first part since the proofs of other parts are similar to the proof of first part. It can easily be checked that $\mathcal{C}_D^{\perp}$ has no codeword of weight 1. Next, suppose to the contrary that there exists a codeword $c \in \mathcal{C}_D^{\perp}$ such that wt(c)=2. Then, for all $a \in \mathbb{F}_{p^m}$, we have

$$\begin{aligned} & c_i \mathrm{Tr}_e^m(ad_i) + c_j \mathrm{Tr}_e^m(ad_i) = 0 \text{ for some } c_i, c_j \in \mathbb{F}_{p^e}^* \text{ and } d_i, d_j \in D \\ \iff\; & \mathrm{Tr}_m^e\left(a(c_i d_i + c_j d_j)\right) = 0 \iff c_i d_i + c_j d_j = 0 \text{ since } \mathrm{Tr}_e^m \text{ is onto} \\ \implies\; & c_i \mathrm{Tr}_e^m(d_i) + c_j \mathrm{Tr}_e^m(d_j) = 0 \implies c_i = -c_j. \end{aligned}$$

Consequently, we have that $c_i(d_i - d_j) = 0$. This is contradictory to the facts that $c_i \neq 0$ and $d_i \neq d_j$. Hence, we do not have any vector $c \in \mathcal{C}_D^{\perp}$ of weight 2. The upper bound is directly follows from the sphere-packing (or Hamming) bound. Thus, the result is established. □

Example 3.23 Let $(p, m, s, e) = (5, 6, 3, 2)$. Then the code $\mathcal{C}_D^{\perp}$ has parameters [24, 21, 4], and it is optimal with respect to the Griesmer bound. In addition, it is MDS code.

Example 3.24 Let $(p, m, s, e) = (3, 9, 3, 3)$. Then the code $\mathcal{C}_D^{\perp}$ has parameters [27, 24, 4], and it is optimal with respect to the Griesmer bound. In fact, it is MDS code.

4 Application to constant composition codes

In this section, we construct some optimal constant composition codes employing the complete weight enumerators of the linear code $\mathcal{C}_D$. The code $\mathcal{C}_D$ can be found in Theorems 3.7, 3.10, 3.14 and 3.17.

It is well known that one can easily construct constant composition codes from the complete weight enumerators of the linear codes. Let r be a positive interger, and let $A = \{a_0, a_1, \ldots, a_{r-1}\}$ be a code alphabet. Any subset $C \subset S^n$ of size M and minimum distance d such that each codeword has the same composition $(t_0, t_1, \ldots, t_{r-1})$ is known as $(n, M, d, (t_0, t_1, \ldots, t_{r-1}))$ constant composition code over S. There are many applications of constant composition codes in communications engineering [3, 19]. The following LFVC bound of constant composition codes is given in [17].

Lemma 4.1 *Let $(n, M, d, (t_0, t_1, \ldots, t_{r-1}))$ be a constant composition code over S with $nd - n^2 + (t_0^2 + t_1^2 + \cdots + t_{r-1}^2) > 0$. Then*

$$M \geq \frac{nd}{nd - n^2 + (t_0^2 + t_1^2 + \cdots + t_{r-1}^2)}.$$

A constant composition code which meets the LFVC bound is known as optimal constant composition code. We construct some optimal constant composition codes from the complete weight enumerators of $\mathcal{C}_D$ in the following theorems:

Theorem 4.2 *Consider the CWE of the Theorem 3.10. If $m = 4e$, then there exists an $(n, M, d, (t_0, t_1, \ldots, t_{p^e-1}))$ optimal constant composition code $\tilde{\mathcal{C}}$ over $\mathbb{F}_{p^e}$, where $n = p^{m-2e} - p^{\frac{m-2e}{2}}$, $M = p^{\frac{m-2e}{2}} - 1$, $d = p^{m-2e} - p^{m-3e}$, $t_0 = p^{m-3e} - p^{\frac{m-2e}{2}}$, $t_i = p^{m-3e}$ for $i \neq 0$.*

Proof Since, we have $p^{m-2e} - 1$ codewords of desired parameters n, t_0 and $t_i (1 \leq i \leq p^e - 1)$. So, any codeword can be re-arranged as

$$(\underbrace{w_1, w_1, \ldots, w_1}_{p^{m-3e} \text{ symbols}}, \underbrace{w_2, w_2, \ldots, w_2}_{p^{m-3e} \text{ symbols}}, \ldots, \underbrace{w_{p^e-1}, w_{p^e-1}, \ldots, w_{p^e-1}}_{p^{m-3e} \text{ symbols}}, \underbrace{0, 0, \ldots, 0}_{t_0 \text{ symbols}}).$$

Fix all zero symbols, and consider all same symbols as a single symbol. Now, we take $p^e - 1$ cycles of the nonzero symbols of the above re-arranged codeword. Define $\tilde{\mathcal{C}}$ as the collection of all constructed cycles. It is obvious that the minimum distance of the code $\tilde{\mathcal{C}}$ is $p^{m-2e} - p^{m-3e}$.

One can easily check that $nd - n^2 + (t_0^2 + t_1^2 + \cdots + t_{p^e-1}^2) = P^{\frac{3m-6e}{2}} - P^{\frac{3m-8e}{2}} > 0$ and $nd = (p^{m-2e} - p^{\frac{m-2e}{2}})(p^{m-2e} - p^{m-3e})$. Then we have

$$\frac{nd}{nd - n^2 + (t_0^2 + t_1^2 + \cdots + t_{p^e-1}^2)} = \frac{(p^{m-2e} - p^{\frac{m-2e}{2}})(p^{m-2e} - p^{m-3e})}{p^{\frac{m-2e}{2}}(p^{m-2e} - p^{m-3e})} = M.$$

Hence, by Lemma 4.1, $\tilde{\mathcal{C}}$ is an optimal constant composition code. Thus, the result is established. □

Theorem 4.3 *Consider the CWE of the Theorem 3.17. If $m = 3e$ and $\overline{\eta}(-3) = 1$, then there exists an $(n, M, d, (t_0, t_1, \ldots, t_{p^e-1}))$ optimal constant composition code $\tilde{\mathcal{C}}$ over $\mathbb{F}_{p^e}$, where $n = p^{m-2e} - p^{\frac{m-3e}{2}}$, $M = p^{\frac{m-e}{2}} - 1$, $d = p^{m-2e} - p^{m-3e}$, $t_0 = p^{m-3e} - p^{\frac{m-3e}{2}}$, $t_i = p^{m-3e}$ for $i \neq 0$.*

Proof Following the arguments used in the proof of previous theorem, we can construct $p^{\frac{m-e}{2}} - 1$ codewords of desired parameters $(n, M, d, (t_0, t_1, \ldots, t_{p^e-1}))$.

One can easily check that $nd - n^2 + (t_0^2 + t_1^2 + \cdots + t_{p^e-1}^2) = P^{\frac{3m-7e}{2}} - P^{\frac{3m-9e}{2}} > 0$ and $nd = (p^{m-2e} - p^{\frac{m-3e}{2}})(p^{m-2e} - p^{m-3e})$. Then, we have

$$\frac{nd}{nd - n^2 + (t_0^2 + t_1^2 + \cdots + t_{p^e-1}^2)} = \frac{(p^{m-2e} - p^{\frac{m-3e}{2}})(p^{m-2e} - p^{m-3e})}{p^{\frac{m-3e}{2}}(p^{m-2e} - p^{m-3e})} = M.$$

By Lemma 4.1, $\tilde{\mathcal{C}}$ is an optimal constant composition code. This completes the proof. □

5 Concluding remarks

In this paper, a class of linear codes over arbitrary finite fields with their complete weight enumerators by giving two restrictions in the defining set has been presented. In addition, the weight distributions of the codes are also determined. The codes presented in this paper have improved relative minimum distance as we have shown in Table 10 which improves error-correcting capability. In Corollary 3.20, we have found a MDS code $[3^e, 3, 3^e - 2]$ for any positive integer e. Furthermore, in Sections 3.2 and 4, we have found some optimal dual codes and constant composition codes respectively. Lastly the work presented in the paper may further be extended to find more applicable codes.

Acknowledgements The authors would like to thank the reviewers and the Editor for their valuable comments that considerably helped to improve the presentation and quality of the paper. The present research is supported by University Grants Commission, New Delhi, India, under JRF in Science, Humanities & Social Sciences scheme, with Grant number 11-04-2016-413564.

References

1. Ahn, J., Ka, D., Li, C.: Complete weight enumerators of a class of linear codes. Des. Codes Cryptogr. **83**(1), 83–99 (2017)
2. Calderbank, A.R., Goethals, J.M.: Three-weight codes and association schemes. Philips J. Res. **39**(4-5), 143–152 (1984)
3. Chu, W., Colbourn, C.J., Dukes, P.: On constant composition codes. Discrete Appl. Math. **154**(6), 912–929 (2006)
4. Ding, C.: Optimal constant composition codes from zero-difference balanced functions. IEEE Trans. Inf. Theory **54**(12), 5766–5770 (2008)
5. Ding, K., Ding, C.: Binary linear codes with three-weights. IEEE Commun. Lett. **18**(11), 1879–1882 (2014)
6. Ding, K., Ding, C.: A class of two-weight and three-weight codes and their applications in secret sharing. IEEE Trans. Inform. Theory **61**(11), 5835–5842 (2015)
7. Ding, C., Helleseth, T., Kløve, T., Wang, X.: A generic construction of Cartesian authentication codes. IEEE Trans. Inf. Theory **53**(6), 2229–2235 (2007)
8. Ding, C., Wang, X.: A coding theory construction of new systematic authentication codes. Theoret. Comput. Sci. **330**(1), 81–99 (2005)
9. Ding, C., Yin, J.: A construction of optimal constant composition codes. Des. Codes Cryptogr. **40**(2), 157–165 (2006)
10. Griesmer, J.H.: A bound for error-correcting codes. IBM J. Res. Develop. **4**(5), 532–542 (1960)
11. Heng, Z., Yue, Q.: Two classes of two-weight linear codes. Finite Fields Appl. **38**, 72–92 (2016)
12. Li, C., Bae, S., Ahn, J., Yang, S., Yao, Z.: Complete weight enumerators of some linear codes and their applications. Des. Codes Cryptogr. **81**(1), 153–168 (2016)

13. Li, F., Wang, Q., Lin, D.: A class of three-weight and five-weight linear codes. Discrete Appl. Math. **241**, 25–38 (2018)
14. Lidl, R., Niederreiter, H.: Finite fields. Cambridge University Press, New York (1997)
15. Ling, S., Xing, C.P.: Coding theory. A first course. Cambridge University Press, Cambridge (2004)
16. Liu, Y., Liu, Z.: Complete weight enumerators of a new class of linear codes. Discrete Math. **341**(7), 1959–1972 (2018)
17. Luo, Y., Fu, F., Vinck, A.J.H., Chen, W.: On constant-composition codes over $\mathbb{Z}_q$. IEEE Trans. Inf. Theory **49**(11), 3010–3016 (2003)
18. MacWilliams, F.J., Slone, N.J.A.: The theory of error-correcting codes. North-Holland Publishing, Amsterdam (1977)
19. Milenkovic, O., Kashyap, N.: On the design of codes for DNA computing lecture notes in computer science, vol. 3969. Springer, Berlin (2006)
20. Storer, T.: Cyclotomy and difference sets. Markham Publishing Company, Markham, Chicago (1967)
21. Wang, Q., Li, F., Lin, D.: Complete weight enumerators of two classes of linear codes. Discrete Math. **340**(4), 467–480 (2017)
22. Yang, S., Kong, X., Tang, C.: A construction of linear codes and their complete weight enumerators. Finite Fields Appl. **48**, 196–226 (2017)
23. Yang, S., Yao, Z.: Complete weight enumerators of a family of three-weight linear codes. Des. Codes Cryptogr. **82**(3), 663–674 (2017)
24. Yang, S., Yao, Z., Zhao, C.: A class of three-weight linear codes and their complete weight enumerators. Cryptogr. Common. **9**(1), 133–149 (2017)