Des. Codes Cryptogr. (2017) 83:83–99
DOI 10.1007/s10623-016-0205-8

Complete weight enumerators of a class of linear codes

Jaehyun Ahn[1] · **Dongseok Ka**[1] · **Chengju Li**[2,3]

Received: 3 January 2016 / Revised: 25 March 2016 / Accepted: 30 March 2016 /
Published online: 13 April 2016

Abstract Let $\mathbb{F}_q$ be the finite field with $q = p^m$ elements, where p is an odd prime and m is a positive integer. For a positive integer t, let $D \subset \mathbb{F}_q^t$ and let Tr_m be the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_p$. In this paper, let $D = \{(x_1, x_2, \ldots, x_t) \in \mathbb{F}_q^t \setminus \{(0, 0, \ldots, 0)\} : \mathrm{Tr}_m(x_1 + x_2 + \cdots + x_t) = 0\}$, we define a p-ary linear code $\mathcal{C}_D$ by

$$\mathcal{C}_D = \{\mathbf{c}(a_1, a_2, \ldots, a_t) : (a_1, a_2, \ldots, a_t) \in \mathbb{F}_q^t\},$$

where

$$\mathbf{c}(a_1, a_2, \ldots, a_t) = (\mathrm{Tr}_m(a_1 x_1^2 + a_2 x_2^2 + \cdots + a_t x_t^2))_{(x_1, x_2, \ldots, x_t) \in D}.$$

We shall present the complete weight enumerators of the linear codes $\mathcal{C}_D$ and give several classes of linear codes with a few weights. This paper generalizes the results of Yang and Yao (Des Codes Cryptogr, 2016).

Keywords Linear codes · Weight distribution · Gauss sums

Mathematics Subject Classification 94B05 · 11T23 · 11T71

Communicated by T. Helleseth.

✉ Dongseok Ka
dska@cnu.ac.kr

Jaehyun Ahn
jhahn@cnu.ac.kr

Chengju Li
lichengju1987@163.com

1 Department of Mathematics, Chungnam National University, Daejeon 305-764, Korea

2 School of Computer Science and Software Engineering, East China Normal University, Shanghai 200062, China

3 Department of Mathematics, KAIST, Daejeon 305-701, Korea

1 Introduction

Let $\mathbb{F}_p$ be the finite field with p elements where p is an odd prime. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_p$ is k-dimensional subspace of $\mathbb{F}_p^n$ with minimum distance d. We recall the definition of the complete weight enumerator of linear code [14]. Suppose that the elements of $\mathbb{F}_q$ are $w_0 = 0, w_1, \ldots, w_{q-1}$, which are listed in some fixed order. The composition of a vector $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_q^n$ is defined to be comp($\mathbf{v}$)=$(t_0, t_1, \ldots, t_{q-1})$, where each $t_i = t_i(\mathbf{v})$ is the number of components $v_j (0 \leqslant j \leqslant n-1)$ of $\mathbf{v}$ that equal to w_i. Clearly, we have

$$\sum_{i=0}^{q-1} t_i = n.$$

Definition 1.1 Let C be an $[n, k]$ linear code over $\mathbb{F}_q$ and let $A(t_0, t_1 \ldots, t_{q-1})$ be the number of codewords $\mathbf{c} \in C$ with comp($\mathbf{c}$)=$(t_0, t_1, \ldots, t_{q-1})$. Then the complete weight enumerator of C is defined to be the polynomial

$$\begin{aligned} W_C &= \sum_{\mathbf{c} \in C} z_0^{t_0} z_1^{t_1} \cdots z_{q-1}^{t_{q-1}} \\ &= \sum_{(t_0, t_1, \ldots, t_{q-1}) \in B_n} A(t_0, t_1, \ldots, t_{q-1}) z_0^{t_0} z_1^{t_1} \cdots z_{q-1}^{t_{q-1}}, \end{aligned}$$

where $B_n = \{(t_0, t_1, \ldots, t_{q-1}) : 0 \leqslant t_i \leqslant n, \sum_{i=0}^{q-1} t_i = n\}$.

Recently, linear codes with a few weights have been investigated [1,6–10,13,16,19] by using exponential sums in some cases. They may have many applications in association schemes [3], strongly regular graphs [4], and secret sharing schemes [5,18]. In addition, the complete weight enumerators of linear codes over finite fields can be applied to compute the deception probabilities of certain authentication codes constructed from linear codes [11,12]. We begin to recall a class of two-weight and three-weight linear codes which were proposed by Ding and Ding [9]. Let $D = \{x \in \mathbb{F}_q^* : \mathrm{Tr}_m(x^2) = 0\}$, where Tr_m is the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_p$. Then a linear code of length $n = |D|$ over $\mathbb{F}_p$ can be defined by

$$\mathcal{C}_D = \{\mathbf{c}(a) = (\mathrm{Tr}_m(ax))_{\in D} : a \in \mathbb{F}_q\}.$$

It was proved that $\mathcal{C}_D$ is a two-weight code if m is even and a three-weight code if m is odd. Motivated by the results given in [9], Bae et al. gave a generalization of Ding and Ding's case [1]. Let $D = \{(x_1, x_2, \ldots, x_t) \in \mathbb{F}_q^t \setminus \{(0, 0, \ldots, 0)\} : \mathrm{Tr}_m(x_1^2 + x_2^2 + \cdots + x_t^2) = 0\}$. They define a p-ary linear code $\mathcal{C}_D$ by

$$\mathcal{C}_D = \{\mathbf{c}(a_1, a_2, \ldots, a_t) : a_1, a_2, \ldots, a_t \in \mathbb{F}_{p^m}\},$$

where

$$\mathbf{c}(a_1, a_2, \ldots, a_t) = (\mathrm{Tr}_m(a_1x_1 + a_2x_2 + \cdots + a_tx_t))_{(x_1, x_2, \ldots, x_t) \in D}.$$

It was also shown that $\mathcal{C}_D$ is two-weight if tm is even and three-weight if tm is odd. If $D = \{x \in \mathbb{F}_q^* : \mathrm{Tr}_m(x) = 0\}$ and $\mathcal{C}_D = \{\mathrm{Tr}_m(ax^2)_{x \in D} : a \in \mathbb{F}_q\}$, Yang and Yao [17] determined the complete weight enumerators of $\mathcal{C}_D$. In this paper, let $D = \{(x_1, x_2, \ldots, x_t) \in \mathbb{F}_q^t \setminus \{(0, 0, \ldots, 0)\} : \mathrm{Tr}_m(x_1 + x_2 + \cdots + x_t) = 0\}$. We define a p-ary linear code $\mathcal{C}_D$ by

$$\mathcal{C}_D = \{\mathbf{c}(a_1, a_2, \ldots, a_t) : (a_1, a_2, \ldots, a_t) \in \mathbb{F}_q^t\}, \quad (1)$$

where

$$\mathbf{c}(a_1, a_2, \ldots, a_t) = (\mathrm{Tr}_m(a_1x_1^2 + a_2x_2^2 + \cdots + a_tx_t^2))_{(x_1,x_2,\ldots,x_t)\in D}. \quad (2)$$

We shall present the complete weight enumerators of this class of linear codes and get several linear codes with a few weights. In addition, this paper generalizes the results of Yang and Yao [17].

2 Preliminaries

Let p be an odd prime and $q = p^m$ for a positive integer m. For any $a \in \mathbb{F}_q$, we can define an additive character of the finite field $\mathbb{F}_q$ as follows:

$$\psi_a : \mathbb{F}_q \longrightarrow \mathbb{C}^*, \psi_a(x) = \zeta_p^{\mathrm{Tr}_m(ax)},$$

where $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a p-th primitive root of unity. It is clear that $\psi_0(x) = 1$ for all $x \in \mathbb{F}_q$. Then ψ_0 is called the trivial additive character of $\mathbb{F}_q$. If $a = 1$, we call $\psi := \psi_1$ the canonical additive character of $\mathbb{F}_q$. It is easy to see that $\psi_a(x) = \psi(ax)$ for all $a, x \in \mathbb{F}_q$. The orthogonal property of additive characters which can be found in [14] is given by

$$\sum_{x\in\mathbb{F}_q} \psi_a(x) = \begin{cases} q, & \text{if } a = 0, \\ 0, & \text{if } a \in \mathbb{F}_q^*. \end{cases}$$

Let $\lambda : \mathbb{F}_q^* \to \mathbb{C}^*$ be a multiplicative character of $\mathbb{F}_q^*$. Now we define the Gauss sum over $\mathbb{F}_q$ by

$$G(\lambda) = \sum_{x\in\mathbb{F}_q^*} \lambda(x)\psi(x).$$

Let $q - 1 = sN$ for two positive integers $s > 1$, $N > 1$ and α be a fixed primitive element of $\mathbb{F}_q$. Let $\langle\alpha^N\rangle$ denote the subgroup of $\mathbb{F}_q^*$ generated by α^N. The *cyclotomic classes* of order N in $\mathbb{F}_q$ are the cosets $C_i^{(N,q)} = \alpha^i\langle\alpha^N\rangle$ for $i = 0, 1, \ldots, N-1$. We know that $|C_i^{(N,q)}| = \frac{q-1}{N}$. The Gaussian periods of order N are defined by

$$\eta_i^{(N,q)} = \sum_{x\in C_i^{(N,q)}} \psi(x).$$

Lemma 2.1 [2,14] *Suppose that $q = p^m$ and η is the quadratic character of $\mathbb{F}_q^*$ where p is an odd prime and $m \geq 1$. Then*

$$G(\eta) = (-1)^{m-1}\sqrt{(p^*)^m} = \begin{cases} (-1)^{m-1}\sqrt{q}, & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{m-1}(\sqrt{-1})^m\sqrt{q}, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where $p^* = \left(\frac{-1}{p}\right)p = (-1)^{\frac{p-1}{2}}p$.

Lemma 2.2 [14] *If q is odd and $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$ with $a_2 \neq 0$, then*

$$\sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_m(f(x))} = \zeta_p^{\mathrm{Tr}_m(a_0 - a_1^2(4a_2)^{-1})}\eta(a_2)G(\eta),$$

where η is the quadratic character of $\mathbb{F}_q^*$.

Lemma 2.3 [15] *When $N = 2$, the Gaussian periods are given by*

$$\eta_0^{(2,q)} = \begin{cases} \frac{-1+(-1)^{m-1}}{2}\sqrt{q}, & \text{if } p \equiv 1 \pmod 4, \\ \frac{-1+(-1)^{m-1}(\sqrt{-1})^m\sqrt{q}}{2}, & \text{if} p \equiv 3 \pmod 4, \end{cases}$$

and $\eta_1^{(2,q)} = -1 - \eta_0^{(2,q)}$.

3 Complete weight enumerators

In this section, we will investigate the complete weight enumerators of the linear codes $\mathcal{C}_D$ defined by (1) and (2), where

$$D = \{(x_1, x_2, \ldots, x_t) \in \mathbb{F}_q^t \setminus \{(0, 0, \ldots, 0)\} : \mathrm{Tr}_m(x_1 + x_2 + \cdots + x_t) = 0\}.$$

Let η_p be the quadratic character of $\mathbb{F}_p^*$ and let $G(\eta_p)$ denote the quadratic Gauss sum over $\mathbb{F}_p$. For $z \in \mathbb{F}_p^*$, it is easily checked that $\eta(z) = \eta_p(z)$ if m is odd and $\eta(z) = 1$ if m is even, where η is the quadratic character of $\mathbb{F}_q^*$ (see [9]). Since the trace function is balanced, we have the following lemma.

Lemma 3.1 *Denote $n_c = |\{(x_1, x_2, \ldots, x_t) \in \mathbb{F}_q^t : \mathrm{Tr}_m(x_1 + x_2 + \cdots + x_t) = c\}|$ for each $c \in \mathbb{F}_p$, then $n_c = p^{tm-1}$.*

By Lemma 3.1 it is easy to see that the length of $\mathcal{C}_D$ is $n = n_0 - 1 = p^{tm-1} - 1$. For a codeword $\mathbf{c}(a_1, a_2, \ldots, a_t)$ of $\mathcal{C}_D$ and $\rho \in \mathbb{F}_p^*$, let $N_\rho := N_\rho(a_1, a_2, \ldots, a_t)$ be the number of components $\mathrm{Tr}_m(a_1x_1^2 + \cdots + a_tx_t^2)$ of $\mathbf{c}(a_1, \ldots, a_t)$ which are equal to ρ. Then

$$\begin{aligned} N_\rho &= \sum_{\substack{x_1,x_2,\ldots,x_t \in \mathbb{F}_q \\ (x_1,x_2,\ldots,x_t)\neq(0,0,\ldots,0)}} \left(\frac{1}{p}\sum_{y\in\mathbb{F}_p} \zeta_p^{y\mathrm{Tr}_m(x_1+x_2+\cdots+x_t)}\right)\left(\frac{1}{p}\sum_{z\in\mathbb{F}_p} \zeta_p^{z\mathrm{Tr}_m(a_1x_1^2+\cdots+a_tx_t^2)-z\rho}\right) \\ &= \frac{1}{p^2}\sum_{x_1,x_2,\ldots,x_t\in\mathbb{F}_q}\left(1+\sum_{y\in\mathbb{F}_p^*}\zeta_p^{y\mathrm{Tr}_m(x_1+x_2+\cdots+x_t)}\right)\left(1+\sum_{z\in\mathbb{F}_p^*}\zeta_p^{z\mathrm{Tr}_m(a_1x_1^2+\cdots+a_tx_t^2)-z\rho}\right) \\ &= p^{tm-2} + \frac{1}{p^2}(\Omega_1 + \Omega_2 + \Omega_3), \end{aligned} \tag{3}$$

where

$$\Omega_1 = \sum_{y\in\mathbb{F}_p^*}\sum_{x_1\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_m(yx_1)}\sum_{x_2\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_m(yx_2)}\cdots\sum_{x_t\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_m(yx_t)} = 0,$$

$$\Omega_2 = \sum_{z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\sum_{x_1\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_m(za_1x_1^2)}\sum_{x_2\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_m(za_2x_2^2)}\cdots\sum_{x_t\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_m(za_tx_t^2)},$$

and

$$\Omega_3 = \sum_{y,z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\sum_{x_1\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_m(za_1x_1^2+yx_1)}\sum_{x_2\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_m(za_2x_2^2+yx_2)}\cdots\sum_{x_t\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_m(za_tx_t^2+yx_t)}.$$

Lemma 3.2 *Suppose that there are exactly k elements $a_{i_1}, \ldots, a_{i_k} \neq 0$ among $a_1, \ldots, a_t$ for $1 \leq k \leq t$.*

(1) *If m is even, then*

$$\Omega_2 = -q^{t-k}\eta(a_{i_1}\cdots a_{i_k})G(\eta)^k.$$

(2) *If m is odd, then*

$$\Omega_2 = \begin{cases} -q^{t-k}\eta(a_{i_1}\cdots a_{i_k})G(\eta)^k, & k \text{ is even}, \\ q^{t-k}\eta(a_{i_1}\cdots a_{i_k})G(\eta)^k G(\eta_p)\eta_p(-\rho), & k \text{ is odd}. \end{cases}$$

Proof If $a_1 = a_2 = \cdots = a_t = 0$, then it is easy to see that $\Omega_2 = -q^t$. Otherwise by Lemma 2.2, we get

$$\begin{aligned}\Omega_2 &= q^{t-k}\sum_{z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\eta(za_{i_1})G(\eta)\eta(za_{i_2})G(\eta)\cdots\eta(za_{i_k})G(\eta)\\ &= q^{t-k}\eta(a_{i_1}a_{i_2}\cdots a_{i_k})G(\eta)^k\sum_{z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\eta(z)^k.\end{aligned}$$

If m is even or if m is odd and k is even, then $\eta(z)^k = 1$. Thus, we get the result.

If m is odd and k is odd, then $\eta_p(z)^k = \eta_p(z)$ and $\sum_{z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\eta_p(z) = G(\eta_p)\eta_p(-\rho)$. Thus, we get the result. □

To simplify formulas, we denote $A = a_1\cdots a_t$ and $B = a_1^{-1}+\cdots+a_t^{-1}$ throughout this paper.

Lemma 3.3 *If $a_1a_2\cdots a_t = 0$, then $\Omega_3 = 0$. Assume that $a_1a_2\cdots a_t \neq 0$.*

(1) *If tm is even, then*

$$\Omega_3 = \begin{cases} -(p-1)G(\eta)^t\eta(A), & \text{if } \mathrm{Tr}_m(B)=0, \\ G(\eta)^t\eta(A)\big(p\eta_p(-\mathrm{Tr}_m(B))\eta_p(\rho)+1\big), & \text{if } \mathrm{Tr}_m(B)\neq 0. \end{cases}$$

(2) *If tm is odd, then*

$$\Omega_3 = \begin{cases} (p-1)G(\eta)^t\eta(A)G(\eta_p)\eta_p(-\rho), & \text{if } \mathrm{Tr}_m(B)=0, \\ -G(\eta)^t\eta(A)G(\eta_p)\big(\eta_p(-\mathrm{Tr}_m(B))+\eta(-\rho)\big), & \text{if } \mathrm{Tr}_m(B)\neq 0. \end{cases}$$

Proof By Lemma 2.2 we have

$$\begin{aligned}\Omega_3 &= \sum_{y,z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\left(\zeta_p^{\mathrm{Tr}_m(-y^2(4a_1z)^{-1})}\eta(za_1)G(\eta)\right)\cdots\left(\zeta_p^{\mathrm{Tr}_m(-y^2(4a_tz)^{-1})}\eta(za_t)G(\eta)\right)\\ &= \sum_{y,z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\zeta_p^{\mathrm{Tr}_m(-y^2((4a_1z)^{-1})+\cdots+(4a_tz)^{-1}))}\eta(za_1)\cdots\eta(za_1)G(\eta)^t\\ &=G(\eta)^t\eta(A)\sum_{z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\eta(z)^t\sum_{y\in\mathbb{F}_p^*}\zeta_p^{-y^2(4z)^{-1}\mathrm{Tr}_m(B)} \qquad (4)\\ &=G(\eta)^t\eta(A)\sum_{z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\eta(z)^t\left(\sum_{y\in\mathbb{F}_p}\zeta_p^{-y^2(4z)^{-1}\mathrm{Tr}_m(B)}-1\right). \qquad (5)\end{aligned}$$

Now, we consider the case that tm is even. If $\mathrm{Tr}_m(B) = 0$, then from (4) we have

$$\Omega_3 = -(p-1)G(\eta)^t \eta(A).$$

If $\mathrm{Tr}_m(B) \neq 0$, then from Lemma 2.2 and (5) we have

$$\begin{aligned}\Omega_3 &= G(\eta)^t \eta(A)\eta_p(\mathrm{Tr}_m(B))G(\eta_p) \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-z\rho}\eta_p(-(4z)^{-1}) + G(\eta)^t\eta(A) \\ &= G(\eta)^t \eta(A)\eta_p(\mathrm{Tr}_m(B))G(\eta_p) \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-z\rho}\eta_p(-z) + G(\eta)^t\eta(A).\end{aligned}$$

Thus, we get the result.

Now, assume that tm is odd. If $\mathrm{Tr}_m(B) = 0$, then it follows from (4) that

$$\Omega_3 = (p-1)G(\eta)^t \eta(A)G(\eta_p)\eta_p(-\rho).$$

Also, if $\mathrm{Tr}_m(B) \neq 0$, then it follows from Lemma 2.2 and (5) that

$$\begin{aligned}\Omega_3 &= G(\eta)^t \eta(A) \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-z\rho}\eta_p(z)\Big(\eta_p(-(4z)^{-1})\eta_p(\mathrm{Tr}_m(B))G(\eta_p) - 1\Big) \\ &= G(\eta)^t \eta(A) \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-z\rho}\Big(\eta_p(-1)\eta_p(\mathrm{Tr}_m(B))G(\eta_p) - \eta_p(z)\Big).\end{aligned}$$

Thus, we get the results. □

By the Lemmas 3.2 and 3.3, we obtain the values of N_ρ. To get the frequency of each composition, we need the following lemmas.

Lemma 3.4 *For $c \in \mathbb{F}_p$, let*

$$n_c^{'} = |\{(a_1, \ldots, a_t) \in (\mathbb{F}_q^*)^t : \mathrm{Tr}_m(B) = c\}|.$$

Then we have

$$n_c^{'} = \begin{cases} \frac{1}{p}\{(p^m-1)^t + (-1)^t(p-1)\}, & \text{if } c = 0, \\ \frac{1}{p}\{(p^m-1)^t - (-1)^t\}, & \text{if } c \neq 0. \end{cases}$$

Proof By the orthogonal property of additive characters we get

$$\begin{aligned}n_c^{'} &= \sum_{a_1,\ldots,a_t\in\mathbb{F}_q^*} \frac{1}{p}\sum_{y\in\mathbb{F}_p} \zeta_p^{y(\mathrm{Tr}_m(B)-c)} \\ &= \frac{(q-1)^t}{p} + \frac{1}{p}\left(\sum_{y\in\mathbb{F}_p^*}\zeta_p^{-yc}\sum_{a_1,\ldots,a_t\in\mathbb{F}_q^*}\zeta_p^{\mathrm{Tr}_m(y(B)-yc)}\right) \\ &= \frac{(q-1)^t}{p} + \frac{1}{p}\sum_{y\in\mathbb{F}_p^*}\zeta_p^{-yc}\left(\sum_{a_1\in\mathbb{F}_q^*}\zeta_p^{\mathrm{Tr}_m(ya_1^{-1})}\cdots\sum_{a_t\in\mathbb{F}_q^*}\zeta_p^{\mathrm{Tr}_m(ya_t^{-1})}\right) \\ &= \frac{(q-1)^t}{p} + \frac{1}{p}\left(\sum_{y\in\mathbb{F}_p^*}\zeta_p^{-yc}(-1)^t\right).\end{aligned}$$

Thus, we get the desired results. □

Lemma 3.5 *For* $i \in \{-1, 1\}$, *let*

$$n_i = |\{(a_1, \ldots, a_t) \in (\mathbb{F}_q^*)^t : \eta(A) = i \text{ and } \mathrm{Tr}_m(B) = 0\}|$$

(1) *If* m *is even, then*

$$n_1 = \frac{1}{2p}\big((p^m - 1)^t + (p-1)\big((-1)^t + G(\eta)^t\big)\big)$$

$$n_{-1} = \frac{1}{2p}\big((p^m - 1)^t + (p-1)\big((-1)^t - G(\eta)^t\big)\big).$$

(2) *If* m *is odd, then*

$$n_1 = \begin{cases} \frac{1}{2p}\big((p^m-1)^t + (p-1)\big((-1)^t + G(\eta)^t\big)\big), & \text{if } t \text{ is even,} \\ \frac{1}{2p}\big((p^m-1)^t + (p-1)(-1)^t\big), & \text{if } t \text{ is odd.} \end{cases}$$

$$n_{-1} = \begin{cases} \frac{1}{2p}\big((p^m-1)^t + (p-1)\big((-1)^t - G(\eta)^t\big)\big), & \text{if } t \text{ is even,} \\ \frac{1}{2p}\big((p^m-1)^t + (p-1)(-1)^t\big), & \text{if } t \text{ is odd.} \end{cases}$$

Proof It follows from Lemma 3.4 that $n_{-1} = n_0^{'} - n_1$. Thus, we only need to compute n_1. Let α be a primitive element of $\mathbb{F}_q$. Then $\mathbb{F}_p^* = \langle \alpha^{\frac{q-1}{p-1}} \rangle$. Note that $\eta(A) = 1$ if and only if $A \in C_0^{(2,q)} = \langle \alpha^2 \rangle$.

$$\begin{aligned}
n_1 &= \sum_{A \in C_0^{(2,q)}} \frac{1}{p} \sum_{y \in \mathbb{F}_p} \zeta_p^{y\mathrm{Tr_m}(B)} \\
&= \sum_{A \in C_0^{(2,q)}} \frac{1}{p} \left(\sum_{y \in \mathbb{F}_p^*} \zeta_p^{y\mathrm{Tr_m}(B)} + 1 \right) \\
&= \frac{1}{p}\frac{(q-1)^t}{2} + \frac{1}{p} \sum_{A \in C_0^{(2,q)}} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{y\mathrm{Tr_m}(B)} \\
&= \frac{1}{p}\frac{(q-1)^t}{2} + \frac{1}{p} \sum_{y \in \mathbb{F}_p^*} \left(\sum_{j=0}^{[\frac{t}{2}]} \sum_{\substack{a_{i_1}, \ldots, a_{i_{2j}} \in C_1^{(2,q)} \\ a_1, \ldots, a_t \setminus \{a_{i_1}, \ldots, a_{i_{2j}}\} \in C_0^{(2,q)}}} \zeta_p^{\mathrm{Tr_m}(y a_1^{-1})} \cdots \zeta_p^{\mathrm{Tr_m}(y a_t^{-1})} \right) \\
&= \frac{1}{p}\frac{(q-1)^t}{2} + \frac{1}{p} \sum_{y \in \mathbb{F}_p^*} \left(\sum_{j=0}^{[\frac{t}{2}]} \binom{t}{2j} \sum_{\substack{a_{i_1}, \ldots, a_{2j} \in C_1^{(2,q)} \\ a_{2j+1}, \ldots, a_t \in C_0^{(2,q)}}} \zeta_p^{\mathrm{Tr_m}(y a_1^{-1})} \cdots \zeta_p^{\mathrm{Tr_m}(y a_t^{-1})} \right).
\end{aligned} \tag{6}$$

Assume that m is even, then 2 divides $\frac{q-1}{p-1}$ and so $\mathbb{F}_p^* \subseteq C_0^{(2,q)}$. By (6) we can get

$$n_1 = \frac{1}{p}\frac{(q-1)^t}{2} + \frac{1}{p}(p-1)\left(\sum_{j=0}^{[\frac{t}{2}]} \binom{t}{2j} (\eta_0^{(2,q)})^{t-2j} (\eta_1^{(2,q)})^{2j} \right)$$

Note that $\eta_1^{(2,q)}+\eta_0^{(2,q)}=-1$ and $\eta_0^{(2,q)}-\eta_1^{(2,q)}=G(\eta)$. Thus, we get the result. Now suppose that m is odd, then $|\mathbb{F}_p^*\cap C_0^{(2,q)}|=|\mathbb{F}_p^*\cap C_1^{(2,q)}|=\frac{p-1}{2}$. By (6) we have

$$\begin{aligned} n_1 =& \frac{1}{p}\frac{(q-1)^t}{2}+\frac{1}{p}\left(\frac{p-1}{2}\sum_{j=0}^{[\frac{t}{2}]}\binom{t}{2j}(\eta_0^{(2,q)})^{t-2j}(\eta_1^{(2,q)})^{2j}\right.\\ &\left.+\frac{p-1}{2}\sum_{j=0}^{[\frac{t}{2}]}\binom{t}{2j}(\eta_1^{(2,q)})^{t-2j}(\eta_0^{(2,q)})^{2j}\right)\\ =&\frac{1}{p}\frac{(p^m-1)^t}{2}+\frac{p-1}{2p}\left(\frac{1}{2}\left((\eta_0^{(2,q)}-\eta_1^{(2,q)})^t+(\eta_1^{(2,q)}-\eta_0^{(2,q)})^t\right)+(-1)^t\right). \end{aligned}$$

Note that $n_{-1}=n^{'}-n_1$ and this completes the proof. □

Recall that α is a fixed primitive element of $\mathbb{F}_q$.

Lemma 3.6 *For* $0\le k\le[t/2]$ *and* $c\in C_0^{(2,p)}$, *let* $n_{2k,c}=|\{a_1,\dots,a_t\in\mathbb{F}_q^*:\mathrm{Tr}_m(\alpha a_1^2+\cdots+\alpha a_{2k}^2+a_{2k+1}^2+\cdots+a_t^2)=c\}|$.

(1) *If m is even, then*

$$n_{2k,c}=\frac{(p^m-1)^t}{p}-\frac{1}{p}(G(\eta)+1)^{2k}(G(\eta)-1)^{t-2k}.$$

(2) *If m is odd and* $k<t/4$, *then*

$$n_{2k,c}=\begin{cases}\frac{(p^m-1)^t}{p}-\frac{1}{p}(G(\eta)^2-1)^{2k}\left(\sum_{i=0}^{\frac{t-4k}{2}}\binom{t-4k}{2i}G(\eta)^{2i}\right.\\ \left.+\eta_p(-c)\sum_{i=0}^{\frac{t-4k}{2}-1}\binom{t-4k}{2i+1}G(\eta)^{2i+1}G(\eta_p)\right), & \text{if } t \text{ is even},\\ \frac{(p^m-1)^t}{p}+\frac{1}{p}(G(\eta)^2-1)^{2k}\left(\sum_{i=0}^{\frac{t-4k-1}{2}}\binom{t-4k}{2i}G(\eta)^{2i}\right.\\ \left.+\eta_p(-c)\sum_{i=0}^{\frac{t-4k-1}{2}}\binom{t-4k}{2i+1}G(\eta)^{2i+1}G(\eta_p)\right), & \text{if } t \text{ is odd}.\end{cases}$$

(3) *If m is odd and $k > t/4$, then*

$$n_{2k,c} = \begin{cases} \frac{(p^m-1)^t}{p} + \frac{1}{p}(G(\eta)^2-1)^{t-2k}\left(-\sum_{i=0}^{\frac{4k-t}{2}}\binom{4k-t}{2i}G(\eta)^{2i} \right. \\ \left. +\eta_p(-c)\sum_{i=0}^{\frac{4k-t}{2}-1}\binom{4k-t}{2i+1}G(\eta)^{2i+1}G(\eta_p)\right), & \text{if } t \text{ is even}, \\ \frac{(p^m-1)^t}{p} + \frac{1}{p}(G(\eta)^2-1)^{t-2k}\left(-\sum_{i=0}^{\frac{4k-t-1}{2}}\binom{4k-t}{2i}G(\eta)^{2i} \right. \\ \left. +\eta_p(-c)\sum_{i=0}^{\frac{4k-t-1}{2}}\binom{4k-t}{2i+1}G(\eta)^{2i+1}G(\eta_p)\right), & \text{if } t \text{ is odd}. \end{cases}$$

(4) *If m is odd, $t \equiv 0 \pmod 4$ and $k = t/4$, then*

$$n_{2k,c} = n_{\frac{t}{2},c} = \frac{(p^m-1)^t}{p} - \frac{1}{p}(G(\eta)^2-1)^{\frac{t}{2}}.$$

Proof By the orthogonal property of additive characters, we have

$$\begin{aligned} n_{2k,c} &= \sum_{a_1,\ldots,a_t\in\mathbb{F}_q^*}\frac{1}{p}\sum_{y\in\mathbb{F}_p}\zeta_p^{y(\mathrm{Tr}_m(\alpha a_1^2+\alpha a_2^2+\cdots+\alpha a_{2k}^2+a_{2k+1}^2+\cdots+a_t^2)-c)} \\ &= \sum_{a_1,\ldots,a_t\in\mathbb{F}_q^*}\frac{1}{p}\left(\sum_{y\in\mathbb{F}_p^*}\zeta_p^{y(\mathrm{Tr}_m(\alpha a_1^2+\alpha a_2^2+\cdots+\alpha a_{2k}^2+a_{2k+1}^2+\cdots+a_t^t)-c)}+1\right) \\ &= \frac{(q-1)^t}{p}+\frac{1}{p}\sum_{y\in\mathbb{F}_p^*}\zeta_p^{-yc}\sum_{a_1,\ldots,a_t\in\mathbb{F}_q^*}\zeta_p^{\mathrm{Tr}_m(y\alpha a_1^2)}\cdots\zeta_p^{\mathrm{Tr}_m(y\alpha a_{2k}^2)}\zeta_p^{\mathrm{Tr}_m(ya_{2k+1}^2)}\cdots\zeta_p^{\mathrm{Tr}_m(ya_t^2)} \\ &= \frac{(q-1)^t}{p}+\frac{1}{p}\left(\sum_{y\in\mathbb{F}_p^*}\zeta_p^{-yc}\left(\sum_{a_1\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_m(y\alpha a_1^2)}-1\right)\cdots\left(\sum_{a_{2k}\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_m(y\alpha a_{2k}^2)}-1\right)\right. \\ &\quad \left.\times\left(\sum_{a_{2k+1}\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_m(ya_{2k+1}^2)}-1\right)\cdots\left(\sum_{a_t\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_m(ya_t^2)}-1\right)\right). \end{aligned}$$

It follows from Lemma 2.2 that

$$n_{2k,c} = \frac{(q-1)^t}{p}+\frac{1}{p}\sum_{y\in\mathbb{F}_p^*}\zeta_p^{-yc}(\eta(\alpha y)G(\eta)-1)^{2k}(\eta(y)G(\eta)-1)^{t-2k}. \tag{7}$$

Now, if m is even, then we have

$$n_{2k,c} = \frac{(p^m-1)^t}{p} - \frac{1}{p}(G(\eta)+1)^{2k}(G(\eta)-1)^{t-2k}.$$

Suppose that m is odd and $k < t/4$. Then by (7) we have

$$n_{2k,c} = \frac{(q-1)^t}{p} + \frac{1}{p}(G(\eta)^2-1)^{2k} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \left(\sum_{i=0}^{t-4k} \binom{t-4k}{i} \eta_p(y)^i G(\eta)^i (-1)^{t-4k-i} \right). \tag{8}$$

If t is even, then it follows from (8) that

$$\begin{aligned} n_{2k,c} =& \frac{(q-1)^t}{p} + \frac{1}{p}(G(\eta)^2-1)^{2k} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \left(\sum_{i=0}^{\frac{t-4k}{2}} \binom{t-4k}{2i} G(\eta)^{2i} \right. \\ &\left. + \sum_{i=0}^{\frac{t-4k}{2}-1} \binom{t-4k}{2i+1} \eta_p(y) G(\eta)^{2i+1}(-1) \right) \\ =& \frac{(q-1)^t}{p} + \frac{1}{p}(G(\eta)^2-1)^{2k} \left((-1) \sum_{i=0}^{\frac{t-4k}{2}} \binom{t-4k}{2i} G(\eta)^{2i} \right. \\ &\left. +(-1) \sum_{i=0}^{\frac{t-4k}{2}-1} \binom{t-4k}{2i+1} G(\eta)^{2i+1} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \eta_p(y) \right). \end{aligned}$$

Thus, we get the desired result.

It is similar to give the proof when t is odd or m is odd for $k > t/4$. Finally, if m is odd, $t \equiv 0 \pmod 4$ and $k = t/4$, it follows from (7) that

$$n_{2k,c} = n_{\frac{t}{2},c} = \frac{(q-1)^t}{p} + \frac{1}{p}(G(\eta)^2-1)^{\frac{t}{2}} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} = \frac{(p^m-1)^t}{p} - \frac{1}{p}(G(\eta)^2-1)^{\frac{t}{2}}.$$

□

Lemma 3.7 *For $i, j \in \{-1, 1\}$, let*

$$n_{i,j} = |\{a_1, \ldots, a_t \in \mathbb{F}_q^* : \eta(A) = i \text{ and } \eta_p(-\mathrm{Tr}_m(B)) = j\}|$$

Then we have

$$n_{1,1} = \frac{1}{2^t} \frac{p-1}{2} \sum_{i=0}^{[\frac{t}{2}]} \binom{t}{2i} n_{2i,-1} \text{ and } n_{1,-1} = \frac{1}{2^t} \frac{p-1}{2} \sum_{i=0}^{[\frac{t}{2}]} \binom{t}{2i} n_{2i,-\beta},$$

where $\beta = \alpha^{\frac{q-1}{p-1}}$. Moreover, if tm is even, then $n_{1,1} = n_{1,-1}$.

Proof For $j \in \{-1, 1\}$, we have

$$\begin{aligned}
n_{1,j} =& |\{a_1, \dots, a_t \in \mathbb{F}_q^* : \eta(A) = 1 \text{ and } \eta_p(-\mathrm{Tr}_m(B)) = j\}| \\
=& |\{a_1, \dots, a_t \in \mathbb{F}_q^* : A \in C_0^{(2,q)},\ \eta_p(-\mathrm{Tr}_m(B)) = j\}| \\
=& \sum_{i=0}^{[\frac{t}{2}]} \binom{t}{2i} |\{a_1, \dots, a_{2i} \in C_1^{(2,q)}, a_{2i+1}, \dots, a_t \in C_0^{(2,q)} :\ \eta_p(-\mathrm{Tr}_m(B)) = j\}| \\
=& \frac{1}{2^t} \sum_{i=0}^{[\frac{t}{2}]} \binom{t}{2i} |\{b_1, \dots, b_t \in \mathbb{F}_q^* :\ \eta_p(-\mathrm{Tr}_m(\alpha b_1^2 + \alpha b_2^2 + \cdots + \alpha b_{2[\frac{t}{2}]}^2 \\
&+ b_{2[\frac{t}{2}]+1}^2 + \cdots + b_t^2) = j\}|.
\end{aligned}$$

By Lemma 3.6 we have

$$n_{1,1} = \frac{1}{2^t} \sum_{i=0}^{[\frac{t}{2}]} \binom{t}{2i} \sum_{c \in C_0^{(2,p)}} n_{2i,-c} = \frac{1}{2^t} \sum_{i=0}^{[\frac{t}{2}]} \binom{t}{2i} \frac{p-1}{2} n_{2i,-1}.$$

and

$$n_{1,-1} = \frac{1}{2^t} \sum_{i=0}^{[\frac{t}{2}]} \binom{t}{2i} \sum_{c \in C_0^{(2,p)}} n_{2i,-\beta}$$

If m is even, from Lemma 3.6, then it is easy to see that $n_{2k,c}$ are independent of $c \in \mathbb{F}_p^*$. Thus $n_{2k,-1} = n_{2k,-\beta}$ and so $n_{1,1} = n_{1,-1}$.

Next assume that m is odd and $t \equiv 2 \pmod 4$. By Lemma 3.6 we have

$$\begin{aligned}
n_{1,1} =& \frac{1}{2^t} \frac{p-1}{2} \left(\sum_{k=0}^{[\frac{t}{4}]} \binom{t}{2k} n'_{2k,-1} + \sum_{k=[\frac{t}{4}]+1}^{\frac{t}{2}} \binom{t}{2k} n'_{2k,-1} \right) \\
=& \frac{1}{2^t} \frac{p-1}{2} \left(\sum_{k=0}^{[\frac{t}{4}]} \binom{t}{2k} \left\{ \frac{(p^m-1)^t}{p} - \frac{1}{p} (G(\eta)^2 - 1)^{2k} \right.\right. \\
& \times \left.\left(\sum_{i=0}^{\frac{t-4k}{2}} \binom{t-4k}{2i} G(\eta)^{2i} + G(\eta_p \right) \sum_{i=0}^{\frac{t-4k}{2}-1} \binom{t-4k}{2i+1} G(\eta)^{2i+1}) \right\} \\
& + \sum_{k=[\frac{t}{4}]+1}^{\frac{t}{2}} \binom{t}{2k} \left\{ \frac{(p^m-1)^t}{p} - \frac{1}{p} (G(\eta)^2 - 1)^{t-2k} \right. \\
& \times \left.\left.\left(\sum_{i=0}^{\frac{4k-t}{2}} \binom{4k-t}{2i} G(\eta)^{2i} - G(\eta_p) \sum_{i=0}^{\frac{4k-t}{2}-1} \binom{4k-t}{2i+1} G(\eta)^{2i+1} \right) \right\} \right).
\end{aligned}$$

By changing k with $\frac{t}{2}-k$ in the second summation we have

$$n_{1,1}=\frac{1}{2^t}\frac{p-1}{2}\left(\sum_{k=0}^{[\frac{t}{4}]}\binom{t}{2k}\left\{\frac{(p^m-1)^t}{p}-\frac{1}{p}(G(\eta)^2-1)^{2k}\right.\right.$$
$$\times\left(\sum_{i=0}^{\frac{t-4k}{2}}\binom{t-4k}{2i}G(\eta)^{2i}+G(\eta_p)\sum_{i=0}^{\frac{t-4k}{2}-1}\binom{t-4k}{2i+1}G(\eta)^{2i+1}\right)\Bigg\}$$
$$+\sum_{k=0}^{[\frac{t}{4}]}\binom{t}{2k}\left\{\frac{(p^m-1)^t}{p}-\frac{1}{p}(G(\eta)^2-1)^{2k}\right.$$
$$\left.\left.\times\left(\sum_{i=0}^{\frac{t-4k}{2}}\binom{4k-t}{2i}G(\eta)^{2i}-G(\eta_p)\sum_{i=0}^{\frac{t-4k}{2}-1}\binom{t-4k}{2i+1}G(\eta)^{2i+1}\right)\right\}\right)$$
$$=\frac{p-1}{2^t}\left(\sum_{k=0}^{[\frac{t}{4}]}\binom{t}{2k}\left\{\frac{(p^m-1)^t}{p}-\frac{1}{p}(G(\eta)^2-1)^{2k}\sum_{i=0}^{\frac{t-4k}{2}}\binom{t-4k}{2i}G(\eta)^{2i}\right\}\right).$$

For $n_{1,-1}$, we similarly have

$$n_{1,-1}=\frac{1}{2^t}\frac{p-1}{2}\left(\sum_{k=0}^{[\frac{t}{4}]}\binom{t}{2k}\left\{\frac{(q-1)^t}{p}-\frac{1}{p}(G(\eta)^2-1)^{2k}\right.\right.$$
$$\times\left(\sum_{i=0}^{\frac{t-4k}{2}}\binom{t-4k}{2i}G(\eta)^{2i}-G(\eta_p)\sum_{i=0}^{\frac{t-4k}{2}-1}\binom{t-4k}{2i+1}G(\eta)^{2i+1}\right)\Bigg\}$$
$$+\sum_{k=[\frac{t}{4}]+1}^{\frac{t}{2}}\binom{t}{2k}\left\{\frac{(q-1)^t}{p}-\frac{1}{p}(G(\eta)^2-1)^{t-2k}\right.$$
$$\left.\left.\times\left(\sum_{i=0}^{\frac{4k-t}{2}}\binom{4k-t}{2i}G(\eta)^{2i}+G(\eta_p)\sum_{i=0}^{\frac{4k-t}{2}-1}\binom{4k-t}{2i+1}G(\eta)^{2i+1}\right)\right\}\right).$$

By changing k with $\frac{t}{2}-k$ in the second summation we have

$$n_{1,-1}=\frac{p-1}{2^t}\left(\sum_{k=0}^{[\frac{t}{4}]}\binom{t}{2k}\left\{\frac{(p^m-1)^t}{p}-\frac{1}{p}(G(\eta)^2-1)^{2k}\sum_{i=0}^{\frac{t-4k}{2}}\binom{t-4k}{2i}G(\eta)^{2i}\right\}\right).$$

Thus, $n_{1,1}=n_{1,-1}$. It is similar to get the desired results when m is odd and $t\equiv 0 \pmod 4$. This completes the proof. □

Lemma 3.8 *For $i\in\{-1,1\}$, let*

$$s_i=|\{a_1,\ldots,a_t\in\mathbb{F}_q^*:\eta(A)\eta_p(-\mathrm{Tr}_m(B))=i\}|$$

(1) *If tm is even, then we have*

$$s_1 = s_{-1} = \frac{p-1}{2p}\big((p^m-1)^t - (-1)^t\big).$$

(2) *If tm is odd, then we have*

$$\begin{aligned} s_{\pm 1} = \pm \frac{p-1}{2^t} \Bigg(& \sum_{k=0}^{[\frac{t}{4}]} \binom{t}{2k} \left\{ \frac{1}{p}(G(\eta)^2-1)^{2k} \sum_{i=0}^{\frac{t-4k-1}{2}} \binom{t-4k}{2i+1} G(\eta)^{2i+1} G(\eta_p) \right\} \\ & + \sum_{k=[\frac{t}{4}]+1}^{\frac{t-1}{2}} \binom{t}{2k} \left\{ \frac{1}{p}(G(\eta)^2-1)^{t-2k} \sum_{i=0}^{\frac{4k-t-1}{2}} \binom{4k-t}{2i+1} G(\eta)^{2i+1} G(\eta_p) \right\} \Bigg) \\ & + \frac{p-1}{2p}\big((p^m-1)^t - (-1)^t\big). \end{aligned}$$

Proof It is easy to see that $s_1 = n_{1,1} + n_{-1,-1} = n_{1,1} + T - n_{1,-1}$, where $T = |\{a_1, \ldots, a_t \in \mathbb{F}_q^* : \eta_p(-\mathrm{Tr}_m(B)) = -1\}|$. By Lemma 3.4 we have

$$\begin{aligned} T &= |\{a_1, \ldots, a_t \in \mathbb{F}_q^* : -\mathrm{Tr}_m(B) \in C_1^{(2,p)}\}| \\ &= \sum_{c \in C_1^{(2,p)}} n'_{-c} = \frac{p-1}{2p}\big((p^m-1)^t - (-1)^t\big). \end{aligned}$$

Similarly, we have $s_{-1} = n_{1,-1} + T - n_{1,1}$. If tm is even, then by Lemma 3.7, we get the desired result.
Next, if tm is odd, then by Lemmas 3.6 and 3.7 we have

$$\begin{aligned} n_{1,1} = & \frac{1}{2^t}\frac{p-1}{2} \Bigg(\sum_{k=0}^{[\frac{t}{4}]} \binom{t}{2k} \Bigg\{ \frac{(p^m-1)^t}{p} + \frac{1}{p}(G(\eta)^2-1)^{2k} \\ & \times \left(\sum_{i=0}^{\frac{t-4k-1}{2}} \binom{t-4k}{2i} G(\eta)^{2i} + G(\eta_p) \sum_{i=0}^{\frac{t-4k-1}{2}} \binom{t-4k}{2i+1} G(\eta)^{2i+1} \right) \Bigg\} \\ & + \sum_{k=[\frac{t}{4}]+1}^{\frac{t-1}{2}} \binom{t}{2k} \Bigg\{ \frac{(p^m-1)^t}{p} + \frac{1}{p}(G(\eta)^2-1)^{t-2k} \\ & \times \left(- \sum_{i=0}^{\frac{4k-t-1}{2}} \binom{4k-t}{2i} G(\eta)^{2i} + G(\eta_p) \sum_{i=0}^{\frac{4k-t-1}{2}} \binom{4k-t}{2i+1} G(\eta)^{2i+1} \right) \Bigg\} \Bigg), \end{aligned}$$

$$\begin{aligned} n_{1,-1} = & \frac{1}{2^t}\frac{p-1}{2} \Bigg(\sum_{k=0}^{[\frac{t}{4}]} \binom{t}{2k} \Bigg\{ \frac{(p^m-1)^t}{p} + \frac{1}{p}(G(\eta)^2-1)^{2k} \\ & \times \left(\sum_{i=0}^{\frac{t-4k-1}{2}} \binom{t-4k}{2i} G(\eta)^{2i} - G(\eta_p) \sum_{i=0}^{\frac{t-4k-1}{2}} \binom{t-4k}{2i+1} G(\eta)^{2i+1} \right) \Bigg\} \Bigg) \end{aligned}$$

$$+\sum_{k=[\frac{t}{4}]+1}^{\frac{t-1}{2}}\binom{t}{2k}\left\{\frac{(p^m-1)^t}{p}-\frac{1}{p}(G(\eta)^2-1)^{t-2k}\right.$$
$$\left.\times\left(\sum_{i=0}^{\frac{4k-t-1}{2}}\binom{4k-t}{2i}G(\eta)^{2i}+G(\eta_p)\sum_{i=0}^{\frac{4k-t-1}{2}}\binom{4k-t}{2i+1}G(\eta)^{2i+1}\right)\right\}\Bigg).$$

Now, it is easy to get s_1 and s_{-1}. This completes the proof. □

Theorem 3.9 *Let $\mathcal{C}_D$ be the linear code defined by* (1) *and* (2), *where $D=\{(x_1,x_2,\ldots,x_t)\in\mathbb{F}_q^t\setminus\{(0,0,\ldots,0)\}:\mathrm{Tr}_m(x_1+x_2+\cdots+x_t)=0\}$ and $\rho\in\mathbb{F}_p^*$. Then $\mathcal{C}_D$ is a $[p^{tm-1}-1,tm]$ linear code.*

(1) *If m is even, then the complete weight enumerator of $\mathcal{C}_D$ is given as follows:*

$N_\rho=0$ occurs 1 time,

$N_\rho=p^{tm-2}\pm p^{m(t-\frac{k}{2})-2}$ $(0<k<t)$ occurs $\binom{t}{k}\frac{(p^m-1)^k}{2}$ times,

$N_\rho=p^{tm-2}\pm p^{\frac{tm-2}{2}}$ occurs $\frac{1}{2p}\big((p^m-1)^t+(p-1)\big((-1)^t\mp p^{\frac{tm}{2}}\big)\big)$ times,

$N_\rho=p^{tm-2}\pm p^{\frac{tm-2}{2}}\eta_p(\rho)$ occurs $\frac{p-1}{2p}\big((p^m-1)^t-(-1)^t\big)$ times.

(2) *If m is odd and t is even, then the complete weight enumerator of $\mathcal{C}_D$ is given as follows:*

$N_\rho=0$ occurs 1 time,

$N_\rho=p^{tm-2}\pm p^{m(t-\frac{k}{2})-2}$ $(0<k<t$ and k is even) occurs $\binom{t}{k}\frac{(p^m-1)^k}{2}$ times,

$N_\rho=p^{tm-2}\pm p^{m(t-\frac{k}{2})-\frac{3}{2}}\eta_p(\rho)$ $(0<k<t$ and k is odd) occurs $\binom{t}{k}\frac{(p^m-1)^k}{2}$ times,

$N_\rho=p^{tm-2}\pm p^{\frac{tm-2}{2}}$ occurs $\frac{1}{2p}\big((p^m-1)^t+(p-1)\big((-1)^t\mp p^{\frac{tm}{2}}\big)\big)$ times,

$N_\rho=p^{tm-2}\pm p^{\frac{tm-2}{2}}\eta_p(\rho)$ occurs $\frac{p-1}{2p}\big((p^m-1)^t-(-1)^t\big)$ times.

(3) *If m is odd and t is odd, then the complete weight enumerator of $\mathcal{C}_D$ is given as follows:*

$N_\rho=0$ occurs 1 time,

$N_\rho=p^{tm-2}\pm p^{m(t-\frac{k}{2})-2}$ $(0<k<t$ and k is even) occurs $\binom{t}{k}\frac{(p^m-1)^k}{2}$ times,

$N_\rho=p^{tm-2}\pm p^{m(t-\frac{k}{2})-\frac{3}{2}}\eta_p(\rho)$ $(0<k<t$ and k is odd) occurs $\binom{t}{k}\frac{(p^m-1)^k}{2}$ times,

$N_\rho=p^{tm-2}\pm p^{\frac{tm-1}{2}}\eta_p(\rho)$ occurs $\frac{1}{2p}\big((p^m-1)^t+(p-1)(-1)^t\big)$ times,

$N_\rho=p^{tm-2}\pm(-1)^{\frac{(tm+1)(p-1)}{4}}p^{\frac{tm-3}{2}}$ occurs

$$\mp\frac{p-1}{2^t}\left(\sum_{k=0}^{[\frac{t}{4}]}\binom{t}{2k}\left\{\frac{1}{p}\big((-1)^{\frac{m(p-1)}{2}}p^m-1\big)^{2k}\sum_{i=0}^{\frac{t-4k-1}{2}}\binom{t-4k}{2i+1}(-1)^{\frac{((2i+1)m+1)(p-1)}{4}}p^{\frac{(2i+1)m+1}{2}}\right\}\right.$$

$$+\sum_{k=[\frac{t}{4}]+1}^{\frac{t-1}{2}}\binom{t}{2k}\left\{\frac{1}{p}\left((-1)^{\frac{m(p-1)}{2}}p^m-1\right)^{t-2k}\sum_{i=0}^{\frac{4k-t-1}{2}}\binom{4k-t}{2i+1}(-1)^{\frac{((2i+1)m+1)(p-1)}{4}}p^{\frac{(2i+1)m+1}{2}}\right\}\Bigg)$$
$$+\frac{p-1}{2p}\left((p^m-1)^t-(-1)^t\right) \text{ times.}$$

Proof Recall that $N_\rho = p^{tm-2}+\frac{1}{p^2}(\Omega_1+\Omega_2+\Omega_3)$. We employ Lemmas 3.2 and 3.3 to compute N_ρ. As computations for frequencies are done by Lemmas 3.4, 3.5, 3.6, 3.7 and 3.8 it is sufficient to give a proof for even m.

Suppose that there are exactly k elements $a_{i_1},\ldots,a_{i_k}\neq 0$ among $a_1,\ldots,a_t$ for $1\leq k\leq t$. If $1\leq k\leq t-1$, then we obtain

$$N_\rho=\begin{cases} p^{tm-2}-\frac{1}{p^2}q^{t-k}G(\eta)^k, & \text{if } a_{i_1}\cdots a_{i_k}\in C_0^{(2,q)},\\ p^{tm-2}+\frac{1}{p^2}q^{t-k}G(\eta)^k, & \text{if } a_{i_1}\cdots a_{i_k}\in C_1^{(2,q)}.\end{cases}$$

In this case, the frequencies are both $\binom{t}{k}\frac{(q-1)^k}{2}$.

If $k=t$ and $\mathrm{Tr}_m(B)=0$, then

$$\begin{aligned} N_\rho &= p^{tm-2}+\frac{1}{p^2}\left(-\eta(A)G(\eta)^t-(p-1)\eta(A)G(\eta)^t\right)\\ &= p^{tm-2}-\frac{1}{p}\eta(a_1\cdots a_t)G(\eta)^t. \end{aligned}$$

Thus,

$$N_\rho=\begin{cases} p^{tm-2}-\frac{1}{p}G(\eta)^t, & \text{if } \eta(A)=1 \text{ and } \mathrm{Tr}_m(B)=0,\\ p^{tm-2}+\frac{1}{p}G(\eta)^t, & \text{if } \eta(A)=-1 \text{ and } \mathrm{Tr}_m(B)=0.\end{cases}$$

Now the frequencies follow from Lemma 3.5.

If $k=t$ and $\mathrm{Tr}_m(B)\neq 0$, then

$$\begin{aligned} N_\rho &= p^{tm-2}+\frac{1}{p^2}\left(-\eta(A)G(\eta)^t+G(\eta)^t\eta(A)\left(p\eta_p(-\mathrm{Tr}_m(B))\eta_p(\rho)+1\right)\right)\\ &= p^{tm-2}+\frac{1}{p}\eta(A)G(\eta)^t\eta_p(-\mathrm{Tr}_m(B))\eta_p(\rho). \end{aligned}$$

Thus,

$$N_\rho=\begin{cases} p^{tm-2}+\frac{1}{p}G(\eta)^t\eta_p(\rho), & \text{if } \eta(A)\eta_p(-\mathrm{Tr}_m(B))=1\\ & \text{and } \mathrm{Tr}_m(B)\neq 0,\\ p^{tm-2}-\frac{1}{p}G(\eta)^t\eta_p(\rho), & \text{if } \eta(A)\eta_p(-\mathrm{Tr}_m(B))=-1\\ & \text{and } \mathrm{Tr}_m(B)\neq 0.\end{cases}$$

Now the frequencies follow from Lemma 3.7. □

In fact, when $t=1$, the complete weight enumerators of $\mathcal{C}_D$ were given by [17]. Thus Theorem 3.9 can be viewed as a generalization of the results in [17]. From Theorem 3.9 we can also get the weight enumerators of $\mathcal{C}_D$ directly.

Corollary 3.10 *Let $\mathcal{C}_D$ be a linear code defined by* (1) *and* (2), *where* $D=\{(x_1,x_2,\ldots,x_t)\in\mathbb{F}_q^t\setminus\{(0,0,\ldots,0)\}:\mathrm{Tr}_m(x_1+x_2+\cdots+x_t)=0\}$.

Table 1 The weight distribution of C_D for even m

Weight	Frequency
0	1
$(p-1)\big(p^{tm-2} \pm p^{m(t-\frac{k}{2})-2}\big)$	$\binom{t}{k}\frac{(p^m-1)^k}{2}$ for $0 < k < t$
$(p-1)\big(p^{tm-2} \pm p^{\frac{tm-2}{2}}\big)$	$\frac{1}{2p}\big((p^m-1)^t + (p-1)\big((-1)^t \mp p^{\frac{tm}{2}}\big)\big)$
$(p-1)p^{tm-2}$	$\frac{p-1}{p}\big((p^m-1)^t - (-1)^t\big)$

Table 2 The weight distribution of C_D for odd m and even t

Weight	Frequency
0	1
$(p-1)\big(p^{tm-2} \pm p^{m(t-\frac{k}{2})-2}\big)$	$\binom{t}{k}\frac{(p^m-1)^k}{2}$ for even k with $0 < k < t$
$(p-1)\big(p^{tm-2} \pm p^{\frac{tm-2}{2}}\big)$	$\frac{1}{2p}\big((p^m-1)^t + (p-1)\big((-1)^t \mp p^{\frac{tm}{2}}\big)\big)$
$(p-1)p^{tm-2}$	$\frac{p-1}{p}\big((p^m-1)^t - 1\big) + \frac{p^{tm}-(2-p^m)^t}{2}$

Table 3 The weight distribution of C_D for odd m and odd t, where $s_{\pm 1}$ is given by Lemma 3.8(2)

Weight	Frequency
0	1
$(p-1)\big(p^{tm-2} \pm p^{m(t-\frac{k}{2})-2}\big)$	$\binom{t}{k}\frac{(p^m-1)^k}{2}$ for even k with $0 < k < t$
$(p-1)\big(p^{tm-2} \pm (-1)^{\frac{(tm+1)(p-1)}{4}} p^{\frac{tm-3}{2}}\big)$	$s_{\mp 1}$
$(p-1)p^{tm-2}$	$\frac{1}{p}\big((p^m-1)^t - (p-1)\big) + \frac{p^{tm}-(2-p^m)^t}{2} - (p^m-1)^t$

(1) *If m is even, then the weight distribution of $\mathcal{C}_D$ is given by Table 1.*
(2) *If m is odd and t is even, then the weight distribution of $\mathcal{C}_D$ is given by Table 2.*
(3) *If m is odd and t is odd, then the weight distribution of $\mathcal{C}_D$ is given by Table 3.*

Remark 3.11 By Corollary 3.10, we easily get several linear codes with a few weights. For example, we obtain 3-weight linear codes for $m = 2$ and $t = 2$, and 5-weight linear codes for even $m \geq 4$, $t = 2$ and $m = 2$, $t = 3$. We also have 3-weight linear codes for odd m, $t = 2$, and 5-weight linear codes for odd m, $t = 3, 4$.

Example 3.12 (1) Let $p = 3$, $m = 2$, and $t = 3$. Then $q = 9$ and $n = 242$. By Theorem 3.9, the code C_D is a [242, 6, 108] linear code. Its complete weight enumerator is

$$z_0^{242} + 12z_0^{134}(z_1z_2)^{54} + 190z_0^{98}(z_1z_2)^{72} + 171z_0^{80}z_1^{72}z_2^{90} + 171z_0^{80}z_1^{90}z_2^{72} + 172z_0^{62}(z_1z_2)^{90} + 12z_0^{26}(z_1z_2)^{108},$$

and its weight enumerator is

$$1+12x^{108}+190x^{144}+342x^{162}+172x^{180}+12x^{216},$$

which are checked by Magma.

(2) Let $p=3$, $m=3$, and $t=3$. Then $q=27$ and $n=6560$. By Theorem 3.9, the code C_D is a [6560, 9, 4212] linear code. Its complete weight enumerator is

$$z_0^{6560}+1014z_0^{2348}(z_1z_2)^{2106}+5940z_0^{2240}(z_1z_2)^{2160}+39z_0^{2186}z_1^{1458}z_2^{2916}$$
$$+39z_0^{2186}z_1^{2916}z_2^{1458}+2929z_0^{2186}z_1^{2106}z_2^{2268}+2929z_0^{2186}z_1^{2268}z_2^{2106}$$
$$+5778z_0^{2132}(z_1z_2)^{2214}+1014z_0^{2024}(z_1z_2)^{2268},$$

and its weight enumerator is

$$1+1014x^{4212}+5940x^{4320}+5936x^{4374}+5778x^{4428}+1014x^{4536},$$

which are checked by Magma.

Acknowledgements The authors would like to express deepest thanks to the editor and the anonymous reviewers for their invaluable comments and suggestions to improve the quality of this paper. Without their careful reading and sophisticated advice, the paper would have never been developed like this.

References

1. Bae S., Li C., Yue Q.: Some results on two-weight and three-weight linear codes, preprint (2015).
2. Berndt B., Evans R., Williams K.: Gauss and Jacobi Sums. Wiley, New York (1997).
3. Calderbank A.R., Goethals J.M.: Three-weight codes and association schemes. Philips J. Res. **39**, 143–152 (1984).
4. Calderbank A.R., Kantor W.M.: The geometry of two-weight codes. Bull. Lond. Math. Soc. **18**, 97–122 (1986).
5. Carlet C., Ding C., Yuan J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Trans. Inf. Theory **51**(6), 2089–2102 (2005).
6. Ding C.: Codes from Difference Sets. World Scientific, Singapore (2014).
7. Ding C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265–3275 (2015).
8. Ding K., Ding C.: Binary linear codes with three weights. IEEE Commun. Lett. **18**(11), 1879–1882 (2014).
9. Ding K., Ding C.: A class of two-weight and three-weight codes and their applications in secret sharing. IEEE Trans. Inf. Theory **61**(11), 5835–5842 (2015).
10. Ding C., Niederreiter H.: Cyclotomic linear codes of order 3. IEEE Trans. Inf. Theory **53**(6), 2274–2277 (2007).
11. Ding C., Wang X.: A coding theory construction of new systematic authentication codes. Theor. Comput. Sci. **330**(1), 81–99 (2005).
12. Ding C., Helleseth T., Kløve T., Wang X.: A general construction of authentication codes. IEEE Trans. Inf. Theory **53**(6), 2229–2235 (2007).
13. Ding C., Luo J., Niederreiter H.: Two-weight codes puncturedfrom irreducible cyclic codes. In: Li Y, et al. (eds.) Proceedings of the First Worshop on Coding and Cryptography, pp. 119–124. World Scientific, Singapore (2008).
14. Lidl R., Niederreiter H.: Finite Fields. Addison-Wesley, Reading (1983).
15. Myerson G.: Period polynomials and gauss sums for finite fields. Acta Arith. **39**(3), 251–264 (1981).
16. Tang C., Li N., Qi Y., Zhou Z., Helleseth T.: Linear codes with two or three weights from weakly regular bent functions. IEEE Trans. Inf. Theory **62**(3), 1166–1176 (2016).
17. Yang S., Yao Z.: Complete weight enumerators of a family of three-weight liner codes. Des. Codes Cryptogr. (2016). doi:10.1007/s10623-016-0191-x.
18. Yuan J., Ding C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory **52**(1), 206–212 (2006).
19. Zhou Z., Li N., Fan C., Helleseth T.: Linear codes with two or three weights from quadratic Bent functions. Des. Codes Cryptogr. (2015). doi:10.1007/s10623-015-0144-9.