Cryptogr. Commun. (2019) 11:609–620
https://doi.org/10.1007/s12095-018-0315-4

Complete weight enumerators of a class of two-weight linear codes

Shudi Yang[1] · **Qin Yue**[2] · **Yansheng Wu**[2] · **Xiangli Kong**[1]

Received: 7 January 2018 / Accepted: 5 June 2018 / Published online: 13 June 2018

Abstract Recently, linear codes constructed from defining sets have been investigated extensively and they have many applications. For an odd prime p, we determine the complete weight enumerator and weight enumerator of a class of p-ary linear codes by choosing a proper defining set. The results show that they have at most two weights and are suitable for applications in secret sharing schemes.

Keywords Linear code · Complete weight enumerator · Weight enumerator · Exponential sum

Mathematics Subject Classification (2010) 94B15 · 11T71

1 Introduction

Throughout this paper, let p be an odd prime and $q = p^e$ for a positive integer e. Denote by $\mathbb{F}_q$ a finite field with q elements. An $[n, \kappa, \delta]$ linear code C over $\mathbb{F}_p$ is a κ-dimensional

✉ Shudi Yang
yangshd3@mail2.sysu.edu.cn

Qin Yue
yueqin@nuaa.edu.cn

Yansheng Wu
wysasd@163.com

Xiangli Kong
kongxiangli@126.com

1 School of Mathematical Sciences, Qufu Normal University, Shandong 273165, People's Republic of China

2 Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, People's Republic of China

subspace of $\mathbb{F}_p^n$ with minimum distance δ (see [20]). Let A_i denote the number of codewords with Hamming weight i in a linear code C of length n. Then $1 + A_1z + A_2z^2 + \cdots + A_nz^n$ is defined to be the weight enumerator of C.

The complete weight enumerator of a code enumerates the codewords according to the number of symbols of each kind contained in each codeword. Let the elements of $\mathbb{F}_p$ be denoted by $w_0 = 0, w_1, \cdots, w_{p-1}$, in some fixed order. Also, let $\mathbb{F}_p^*$ denote $\mathbb{F}_p\backslash\{0\}$. For a codeword $\mathsf{c} = (c_0, c_1, \cdots, c_{n-1}) \in \mathbb{F}_p^n$, let $w[\mathsf{c}]$ be the complete weight enumerator of c, which is defined as

$$w[\mathsf{c}] = w_0^{k_0} w_1^{k_1} \cdots w_{p-1}^{k_{p-1}},$$

where k_j is the number of components of c equal to w_j, $\sum_{j=0}^{p-1} k_j = n$. The complete weight enumerator of the code C is then

$$\mathrm{CWE}(C) = \sum_{\mathsf{c}\in C} w[\mathsf{c}].$$

The weight enumerators of linear codes have been well studied in literature, see, for example, [11, 12, 22, 29, 30] and references therein. The information of the complete weight enumerators of linear codes is of vital use because they not only give the weight enumerators but also show the frequency of each symbol appearing in each codeword. Furthermore the complete weight enumerator has close relation to the deception probabilities of certain authentication codes [7], and is used to compute the Walsh transform of monomial and quadratic bent functions over finite fields [13]. Further research can be found in [2, 3, 8, 15, 16, 25, 26].

The authors of [6, 9, 10] gave the following generic construction of linear codes. Set $D = \{d_1, d_2, \cdots, d_n\} \subseteq \mathbb{F}_q^*$, where $q = p^e$. Denote by Tr the absolute trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. A linear code associated with D is defined by

$$C_D = \{(\mathrm{Tr}(ad_1), \mathrm{Tr}(ad_2), \cdots, \mathrm{Tr}(ad_n)) : a \in \mathbb{F}_q\}.$$

The set D is called the defining set of C_D. This construction technique leads to a new research and was employed to construct linear codes with a few weights, see [1, 14, 17, 18, 23, 24, 27] for more details.

Motivated by the above construction and the idea of [23], we investigate a class of linear codes with defining set. Recall $q = p^e$. Let $d = \gcd(k, e)$ be the greatest common divisor of positive integers k and e. Suppose that e/d is even with $e = 2m$. The code is defined by

$$C_{D_b} = \{(\mathrm{Tr}(ax^{p^k+1}))_{x\in D_b} : a \in \mathbb{F}_{p^d}\}, \tag{1}$$

with defining set

$$D_b = \{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) = b\} \text{ for } b \in \mathbb{F}_p.$$

The remainder of this paper is organized as follows. In Section 2, we describe the main results of this paper, additionally we give some examples. In Section 3, we briefly recall some definitions and results on cyclotomic numbers and exponential sums, then prove the main results. In Section 4, we make a conclusion.

2 Main results

In this section, we only introduce the complete weight enumerator and weight enumerator of C_{D_b} described in Section 1. The main results of this paper are presented below, whose proofs will be given in Section 3.

Theorem 1 *If $b = 0$, then the code C_{D_0} of (1) is a $[p^{e-1} - 1, d]$ linear code and the following assertions hold.*

(i) *When $m/d \equiv 1 \mod 2$ and $m/d \not\equiv 0 \mod p$, its weight enumerator is*

$$1 + (p-1)p^{d-1}z^{(p-1)p^{e-2}} + (p^{d-1} - 1)z^{(p-1)(p^{e-2}+p^{m-1})}$$

and its complete weight enumerator is

$$w_0^{p^{e-1}-1} + \frac{p-1}{2}p^{d-1}w_0^{p^{e-2}-1}\left(\prod_{\rho\in\mathbb{F}_p^*} w_\rho^{p^{e-2}-\eta(\rho)p^{m-1}} + \prod_{\rho\in\mathbb{F}_p^*} w_\rho^{p^{e-2}+\eta(\rho)p^{m-1}}\right)$$
$$+(p^{d-1} - 1)w_0^{p^{e-2}-(p-1)p^{m-1}-1} \prod_{\rho\in\mathbb{F}_p^*} w_\rho^{p^{e-2}+p^{m-1}}.$$

(ii) *When $m/d \equiv 1 \mod 2$ and $m/d \equiv 0 \mod p$, the code C_{D_0} has only one non-zero weight $(p-1)(p^{e-2} + p^{m-1})$ and its complete weight enumerator is*

$$w_0^{p^{e-1}-1} + (p^d - 1)w_0^{p^{e-2}-(p-1)p^{m-1}-1} \prod_{\rho\in\mathbb{F}_p^*} w_\rho^{p^{e-2}+p^{m-1}}.$$

(iii) *When $m/d \equiv 0 \mod 2$ and $m/d \not\equiv 0 \mod p$, its weight enumerator is*

$$1 + (p-1)p^{d-1}z^{(p-1)p^{e-2}} + (p^{d-1} - 1)z^{(p-1)(p^{e-2}+p^{m+d-1})}$$

and its complete weight enumerator is

$$w_0^{p^{e-1}-1} + \frac{p-1}{2}p^{d-1}w_0^{p^{e-2}-1}\left(\prod_{\rho\in\mathbb{F}_p^*} w_\rho^{p^{e-2}-\eta(\rho)p^{m+d-1}} + \prod_{\rho\in\mathbb{F}_p^*} w_\rho^{p^{e-2}+\eta(\rho)p^{m+d-1}}\right)$$
$$+(p^{d-1} - 1)w_0^{p^{e-2}-(p-1)p^{m+d-1}-1} \prod_{\rho\in\mathbb{F}_p^*} w_\rho^{p^{e-2}+p^{m+d-1}}.$$

(iv) *When $m/d \equiv 0 \mod 2$ and $m/d \equiv 0 \mod p$, the code C_{D_0} has only one non-zero weight $(p-1)(p^{e-2} + p^{m+d-1})$ and its complete weight enumerator is*

$$w_0^{p^{e-1}-1} + (p^d - 1)w_0^{p^{e-2}-(p-1)p^{m+d-1}-1} \prod_{\rho\in\mathbb{F}_p^*} w_\rho^{p^{e-2}+p^{m+d-1}}.$$

Theorem 2 *If $b \in \mathbb{F}_p^*$, then the code C_{D_b} of (1) is a $[p^{e-1}, d, (p-1)p^{e-2}]$ linear code and the following assertions hold.*

(i) *When $m/d \equiv 1 \mod 2$ and $m/d \not\equiv 0 \mod p$, its weight enumerator is*

$$1 + (p^{d-1} - 1)z^{(p-1)p^{e-2}} + (p-1)p^{d-1}z^{(p-1)p^{e-2}+p^{m-1}}$$

and its complete weight enumerator is

$$w_0^{p^{e-1}} + (p^{d-1} - 1)\prod_{\rho\in\mathbb{F}_p} w_\rho^{p^{e-2}} + p^{d-1}w_0^{p^{e-2}-p^{m-1}} \sum_{\lambda\in\mathbb{F}_p^*}\prod_{\rho\in\mathbb{F}_p^*} w_\rho^{p^{e-2}-\eta(b^2-\rho\lambda)p^{m-1}}.$$

(ii) *When $m/d \equiv 0 \mod 2$ and $m/d \not\equiv 0 \mod p$, its weight enumerator is*

$$1 + (p^{d-1} - 1)z^{(p-1)p^{e-2}} + (p-1)p^{d-1}z^{(p-1)p^{e-2}+p^{m+d-1}}$$

and its complete weight enumerator is

$$w_0^{p^{e-1}}+(p^{d-1}-1)\prod_{\rho\in\mathbb{F}_p} w_\rho^{p^{e-2}}+p^{d-1}w_0^{p^{e-2}-p^{m+d-1}}\sum_{\lambda\in\mathbb{F}_p^*}\prod_{\rho\in\mathbb{F}_p^*} w_\rho^{p^{e-2}-\eta(b^2-\rho\lambda)p^{m+d-1}}.$$

(iii) *When $m/d \equiv 0 \mod p$, the code C_{D_b} has only one non-zero weight $(p-1)p^{e-2}$ and its complete weight enumerator is*

$$w_0^{p^{e-1}}+(p^d-1)\prod_{\rho\in\mathbb{F}_p} w_\rho^{p^{e-2}}.$$

Some concrete examples are provided below to illustrate our results.

Example 1 Let $(p,m,k)=(5,2,2)$. Then $d=\gcd(2m,k)=2$ and $s=m/d=1$. If $b=0$, the code C_{D_0} has parameters [124, 2, 100], weight enumerator $1+20z^{100}+4z^{120}$ and complete weight enumerator

$$w_0^{124}+10w_0^{24}(w_1w_4)^{20}(w_2w_3)^{30}+10w_0^{24}(w_1w_4)^{30}(w_2w_3)^{20}+4w_0^4(w_1w_2w_3w_4)^{30}.$$

If $b=1$, the code C_{D_1} has parameters [125, 2, 100], weight enumerator $1+4z^{100}+20z^{105}$ and complete weight enumerator

$$w_0^{125}+4\prod_{\rho=0}^{4} w_\rho^{25}+5w_0^{20}\left(w_1^{25}w_2^{20}w_3^{30}w_4^{30}+w_1^{30}w_2^{25}w_3^{30}w_4^{20}+w_1^{20}w_2^{30}w_3^{25}w_4^{30}+w_1^{30}w_2^{30}w_3^{20}w_4^{25}\right).$$

These results are checked by Magma.

Example 2 Let $(p,m,k)=(3,3,1)$. Then $d=\gcd(2m,k)=1$ and $s=m/d=3$. If $b=0$, the code C_{D_0} has parameters [242, 1, 180], weight enumerator $1+2z^{180}$ and complete weight enumerator $w_0^{242}+2w_0^{62}(w_1w_2)^{90}$. If $b=1$, the code C_{D_1} has parameters [243, 1, 162], weight enumerator $1+2z^{162}$ and complete weight enumerator $w_0^{243}+2(w_0w_1w_2)^{81}$. These results are checked by Magma.

3 The proofs of the main results

3.1 Auxiliary results

In order to prove the results proposed in Section 2, we will use several results which are depicted and proved in the sequel. We start with the concepts of cyclotomic numbers and exponential sums over finite fields. Recall that $q=p^e$. Let θ be a primitive element of $\mathbb{F}_q$ and $q=Nh+1$ for integers $N>1$, $h>1$. The *cyclotomic classes* of order N in $\mathbb{F}_q$ are the cosets $C_i^{(N,q)}=\theta^i\langle\theta^N\rangle$ for $i=0,1,\cdots,N-1$, where $\langle\theta^N\rangle$ denotes the subgroup of $\mathbb{F}_q^*$ generated by θ^N. For fixed i and j, we define the *cyclotomic number* $(i,j)^{(N,q)}$ to be the number of solutions of the equation

$$x_i+1=x_j\quad\left(x_i\in C_i^{(N,q)},\ x_j\in C_j^{(N,q)}\right),$$

where $1 = \theta^0$ is the multiplicative unit of $\mathbb{F}_q$. That is, $(i, j)^{(N,q)}$ is the number of ordered pairs (u, v) such that

$$\theta^{Nu+i} + 1 = \theta^{Nv+j} \quad (0 \leqslant u, v \leqslant h - 1).$$

Now we review some results on cyclotomic numbers.

Lemma 1 ([21]) *When $N = 2$, the cyclotomic numbers are given by*

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

Next, let us introduce group characters and exponential sums. For each $b \in \mathbb{F}_q$, an additive character χ_b of $\mathbb{F}_q$ is defined by $\chi_b(x) = \zeta_p^{\mathrm{Tr}(bx)}$ for all $x \in \mathbb{F}_q$, where $\zeta_p = \exp\left(\frac{2\pi\sqrt{-1}}{p}\right)$ and Tr is the simplification of the trace function Tr_1^e from $\mathbb{F}_q$ to $\mathbb{F}_p$. For $b = 1$, χ_1 is called the canonical additive character of $\mathbb{F}_q$.

Let η_e denote the quadratic character of $\mathbb{F}_q$. The quadratic Gauss sum $G(\eta_e, \chi_1)$ is defined by

$$G(\eta_e, \chi_1) = \sum_{x \in \mathbb{F}_q^*} \eta_e(x)\chi_1(x).$$

We denote $G_e = G(\eta_e, \chi_1)$ and $G = G(\eta, \chi_1')$, where η and χ_1' are the quadratic character and canonical additive character of $\mathbb{F}_p$, respectively. Moreover, it is well known that $G_e = (-1)^{e-1}\sqrt{p^*}^e$ and $G = \sqrt{p^*}$, where $p^* = \eta(-1)p$. See [10, 19] for more information.

The following lemmas will be of special use in the sequel.

Lemma 2 (**Theorem 5.33,** [19]) *Let $q = p^e$ be odd and $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$ with $a_2 \neq 0$. Then*

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

where η_e is the quadratic character of $\mathbb{F}_q$.

For $\alpha, \beta \in \mathbb{F}_q$ and any integer k, the exponential sum $S(\alpha, \beta)$ is defined by

$$S(\alpha, \beta) = \sum_{x \in \mathbb{F}_q} \chi_1(\alpha x^{p^k+1} + \beta x).$$

We recall some results of $S(\alpha, \beta)$ for $\alpha \neq 0$ and q odd.

Lemma 3 (**Theorem 2,** [4]) *Let $d = \gcd(k, e)$ and e/d be even with $e = 2m$. Then*

$$S(\alpha, 0) = \begin{cases} (-1)^s p^m & \text{if } \alpha^{(q-1)/(p^d+1)} \neq (-1)^s, \\ (-1)^{s+1} p^{m+d} & \text{if } \alpha^{(q-1)/(p^d+1)} = (-1)^s, \end{cases}$$

where $s = m/d$.

Lemma 4 (**Theorem 4.7,** [5]) *Let $\beta \neq 0$ and e/d be even with $e = 2m$. Set $f_\alpha(X) = \alpha^{p^k} X^{p^{2k}} + \alpha X$. Then $S(\alpha, \beta) = 0$ unless the equation $f_\alpha(X) = -\beta^{p^k}$ is solvable. There are two possibilities.*

(i) *If* $\alpha^{(q-1)/(p^d+1)} \neq (-1)^s$, *then for any choice of* $\beta \in \mathbb{F}_q$, *the equation has a unique solution* x_0 *and*

$$S(\alpha, \beta) = (-1)^s p^m \chi_1(-\alpha x_0^{p^k+1}).$$

(ii) *If* $\alpha^{(q-1)/(p^d+1)} = (-1)^s$ *and the equation is solvable with some solution* x_0 *say, then*

$$S(\alpha, \beta) = (-1)^{s+1} p^{m+d} \chi_1(-\alpha x_0^{p^k+1}).$$

Lemma 5 (Theorem 4.1, [4]**)** *For* $e = 2m$ *the equation* $\alpha^{p^k} X^{p^{2k}} + \alpha X = 0$ *is solvable for* $X \in \mathbb{F}_q^*$ *if and only if* e/d *is even and*

$$\alpha^{(q-1)/(p^d+1)} = (-1)^s.$$

In such cases there are $p^{2d} - 1$ *non-zero solutions.*

3.2 The proofs of the theorems in Section 2

In this subsection, we will prove of our main results presented in Section 2. Recall that $q = p^e$, $d = \gcd(k, e)$, e/d is even with $e = 2m$. The code C_{D_b} with $b \in \mathbb{F}_p$, is defined by

$$C_{D_b} = \{(\mathrm{Tr}(ax^{p^k+1}))_{x \in D_b} : a \in \mathbb{F}_{p^d}\},$$

where $D_b = \{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) = b\}$. It is trivial that C_{D_b} has length $n_0 = p^{e-1} - 1$ if $b = 0$ and $n_b = p^{e-1}$ otherwise.

Observe that $a = 0$ gives the zero codeword and the contribution to the complete weight enumerator is w_0^n. This value occurs only once. Hence, we may assume that $a \in \mathbb{F}_{p^d}^*$ in the rest of this subsection.

For a codeword $\mathsf{c}_a = (\mathrm{Tr}(ax^{p^k+1}))_{x \in D_b}$ of C_{D_b} and $\rho \in \mathbb{F}_p$, let $n_a(b, \rho)$ denote the number of components of c_a that are equal to ρ, i.e.,

$$n_a(b, \rho) = \#\{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) = b \text{ and } \mathrm{Tr}(ax^{p^k+1}) = \rho\}.$$

For convenience, we compute

$$N_a(b, \rho) = \#\{x \in \mathbb{F}_q : \mathrm{Tr}(x) = b \text{ and } \mathrm{Tr}(ax^{p^k+1}) = \rho\}.$$

Then we have

$$N_a(b, 0) = p^{e-1} - \sum_{\rho \in \mathbb{F}_p^*} N_a(b, \rho). \tag{2}$$

Also it is easy to obtain the Hamming weight of c_a, that is

$$wt(\mathsf{c}_a) = \sum_{\rho \in \mathbb{F}_p^*} N_a(b, \rho) = p^{e-1} - N_a(b, 0).$$

So we only consider $\rho \in \mathbb{F}_p^*$ and $a \in \mathbb{F}_{p^d}^*$ in the sequel.

Now it comes to determine the value of $N_a(b,\rho)$ for $\rho \in \mathbb{F}_p^*$. By definition, we have

$$\begin{aligned} N_a(b,\rho) &= p^{-2}\sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_p}\zeta_p^{y\mathrm{Tr}(x)-by}\sum_{z\in\mathbb{F}_p}\zeta_p^{z\mathrm{Tr}(ax^{p^k+1})-\rho z} \\ &= p^{e-2}+p^{-2}\sum_{z\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q}\zeta_p^{z\mathrm{Tr}(ax^{p^k+1})-\rho z}+p^{-2}\sum_{y\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q}\zeta_p^{y\mathrm{Tr}(x)-by} \\ &\quad +p^{-2}\sum_{y\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}(azx^{p^k+1}+yx)-by-\rho z} \\ &= p^{e-2}+p^{-2}A_a(\rho)+p^{-2}B_a(b,\rho), \end{aligned} \tag{3}$$

where

$$A_a(\rho) := \sum_{z\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q}\zeta_p^{z\mathrm{Tr}(ax^{p^k+1})-\rho z}, \tag{4}$$

$$B_a(b,\rho) := \sum_{y\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}(azx^{p^k+1}+yx)-by-\rho z}. \tag{5}$$

The following lemmas state the evaluations of $A_a(\rho)$ and $B_a(b,\rho)$.

Lemma 6 *Let $a \in \mathbb{F}_{p^d}^*$ and $\rho \in \mathbb{F}_p^*$. Denote $s = m/d$. Then*

$$A_a(\rho) = \begin{cases} p^m & \text{if } s \text{ is odd,} \\ p^{m+d} & \text{if } s \text{ is even.} \end{cases}$$

Proof By (4),

$$A_a(\rho) = \sum_{z\in\mathbb{F}_p^*}\zeta_p^{-\rho z}S(az,0).$$

A straightforward calculation gives that $(az)^{(q-1)/(p^d+1)} = 1$ for $z \in \mathbb{F}_p^*$ and $a \in \mathbb{F}_{p^d}^*$. Then the desired conclusion follows from Lemma 3. □

For the later use, we set $f_a(X) = aX^{p^{2k}} + aX \in \mathbb{F}_q[X]$ for $a \in \mathbb{F}_{p^d}^*$.

Lemma 7 *Let $b \in \mathbb{F}_p$ and $\rho \in \mathbb{F}_p^*$. Suppose that e/d is even with $e = 2m$ and $s = m/d$. Then for each $a \in \mathbb{F}_{p^d}^*$, the equation $f_a(X) = -1$ has a solution $\gamma = -1/(2a)$ and so $B_a(b,\rho) \neq 0$. Denote $\lambda := \mathrm{Tr}(a^{-1})$. The evaluation of $B_a(b,\rho) \neq 0$ partitions into the following two cases.*

(*i*) *If $b = 0$, then*

$$B_a(0,\rho) = \begin{cases} (p-1)p^m & \text{if } s \text{ is odd and } \lambda = 0, \\ -(p\eta(-\rho\lambda)+1)\,p^m & \text{if } s \text{ is odd and } \lambda \neq 0, \\ (p-1)p^{m+d} & \text{if } s \text{ is even and } \lambda = 0, \\ -(p\eta(-\rho\lambda)+1)\,p^{m+d} & \text{if } s \text{ is even and } \lambda \neq 0. \end{cases}$$

(*ii*) *If* $b \neq 0$, *then*

$$B_a(b,\rho) = \begin{cases} -p^m & \text{if } s \text{ is odd and } \lambda = 0, \\ -\left(p\eta(b^2-\rho\lambda)+1\right)p^m & \text{if } s \text{ is odd and } \lambda \neq 0, \\ -p^{m+d} & \text{if } s \text{ is even and } \lambda = 0, \\ -\left(p\eta(b^2-\rho\lambda)+1\right)p^{m+d} & \text{if } s \text{ is even and } \lambda \neq 0. \end{cases}$$

Proof Let e/d be even. By (5),

$$B_a(b,\rho) = \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-by} \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-\rho z} S(az,y). \tag{6}$$

For $y, z \in \mathbb{F}_p^*$, it follows from Lemma 4 that $S(az,y) = 0$ unless the equation $f_{az}(X) = -y^{p^k}$ is solvable. But for each $a \in \mathbb{F}_{p^d}^*$, we can verify that $\gamma = -1/(2a)$ is a solution of $f_a(X) = aX^{p^{2k}} + aX = -1$ and so $z^{-1}\gamma y$ is a solution of $f_{az}(X) = (az)X^{p^{2k}} + (az)X = -y^{p^k}$. This implies that $B_a(b,\rho) \neq 0$.

For the evaluation of $B_a(b,\rho) \neq 0$, we first consider the case that s is odd. In this case $f_{az}(X) = -y^{p^k}$ has a unique solution $z^{-1}\gamma y$ because $f_a(X) = aX^{p^{2k}} + aX$ is a permutation polynomial over $\mathbb{F}_q$ by Lemma 5 and γ is the unique solution of $f_a(X) = -1$. Thus we have from Lemma 4 that

$$S(az,y) = -p^m \chi_1(-az(z^{-1}\gamma y)^{p^k+1}).$$

Plugging this into $B_a(b,\rho)$ of (6) gives that

$$\begin{aligned} B_a(b,\rho) &= -p^m \sum_{y\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_p^*} \zeta_p^{-by-\rho z}\chi_1(-az(z^{-1}\gamma y)^{p^k+1}) \\ &= -p^m \sum_{y\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_p^*} \zeta_p^{-by-\rho z}\zeta_p^{-\frac{\lambda y^2}{4z}}, \end{aligned}$$

where $\lambda = \mathrm{Tr}(a^{-1})$.

If $\lambda = 0$, then $B_a(b,\rho) = -p^m \sum_{y\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_p^*} \zeta_p^{-by-\rho z}$ and the corresponding result then follows.

Now suppose that $\lambda \neq 0$ and we consider the following cases separately.

(*i*) If $b = 0$, we have from Lemma 4 that

$$\begin{aligned} B_a(0,\rho) &= -p^m \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-\rho z} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-\frac{\lambda y^2}{4z}} \\ &= -p^m \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-\rho z} \left(\sum_{y\in\mathbb{F}_p} \zeta_p^{-\frac{\lambda y^2}{4z}} - 1 \right) \\ &= -p^m \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-\rho z} \eta\left(-\frac{\lambda}{z}\right) G - p^m \\ &= -p^m \eta(\rho\lambda) G^2 - p^m = -\left(p\eta(-\rho\lambda)+1\right)p^m. \end{aligned}$$

(ii) If $b \neq 0$, then it follows from Lemma 4 again that

$$\begin{aligned} B_a(b,\rho) &= -p^m \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-\rho z} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-\frac{\lambda y^2}{4z}-by} \\ &= -p^m \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-\rho z}\zeta_p^{\frac{b^2}{\lambda}z}\eta\left(-\frac{\lambda}{z}\right)G - p^m \\ &= -p^m \sum_{z\in\mathbb{F}_p^*} \zeta_p^{(\frac{b^2}{\lambda}-\rho)z}\eta\left(-\frac{\lambda}{z}\right)G - p^m \\ &= \begin{cases} -p^m & \text{if } b^2=\rho\lambda, \\ -(p\eta(b^2-\rho\lambda)+1)p^m & \text{if } b^2\neq\rho\lambda. \end{cases} \end{aligned}$$

Therefore we conclude that $B_a(b,\rho) = -(p\eta(b^2-\rho\lambda)+1)p^m$ for $b \neq 0$.

We now study the case that s is even. Since $z^{-1}\gamma y$ is a solution to $f_{az}(X) = -y^{p^k}$, we have from Lemma 4 that

$$S(az, y) = -p^{m+d}\chi_1(-az(z^{-1}\gamma y)^{p^k+1}).$$

By a similar argument as above, we obtain the desired conclusions and complete the whole proof of this lemma. □

3.2.1 *The first case that* $b = 0$

In this subsection, we assume that $b = 0$. Recall that $s = m/d$ and $\lambda = \mathrm{Tr}(a^{-1})$ for $a \in \mathbb{F}_{p^d}^*$. By (2), (3), Lemmas 6 and 7, we have the following two lemmas.

Lemma 8 *Let* $a \in \mathbb{F}_{p^d}^*$, *then*

$$N_a(0,0) = \begin{cases} p^{e-2} - (p-1)p^{m-1} & \text{if } s \text{ is odd and } \lambda = 0, \\ p^{e-2} & \text{if } s \text{ is odd and } \lambda \neq 0, \\ p^{e-2} - (p-1)p^{m+d-1} & \text{if } s \text{ is even and } \lambda = 0, \\ p^{e-2} & \text{if } s \text{ is even and } \lambda \neq 0. \end{cases}$$

Lemma 9 *Let* $a \in \mathbb{F}_{p^d}^*$ *and* $\rho \in \mathbb{F}_p^*$, *we have*

$$N_a(0,\rho) = \begin{cases} p^{e-2} + p^{m-1} & \text{if } s \text{ is odd and } \lambda = 0, \\ p^{e-2} - \eta(-\rho\lambda)p^{m-1} & \text{if } s \text{ is odd and } \lambda \neq 0, \\ p^{e-2} + p^{m+d-1} & \text{if } s \text{ is even and } \lambda = 0, \\ p^{e-2} - \eta(-\rho\lambda)p^{m+d-1} & \text{if } s \text{ is even and } \lambda \neq 0. \end{cases}$$

Now we are in a position to prove Theorem 1.

Proof Denote

$$\begin{aligned} w_1 &= (p-1)(p^{e-2}+p^{m-1}), \\ w_2 &= (p-1)p^{e-2}, \\ w_3 &= (p-1)(p^{e-2}+p^{m+d-1}). \end{aligned}$$

The code C_{D_0} has length $n_0 = p^{e-1} - 1$ and dimension d, since $wt(\mathsf{c}_a) > 0$ for each $a \in \mathbb{F}_{p^d}^*$. Observe that $\lambda = \mathrm{Tr}(a^{-1}) = \mathrm{Tr}_d^e\left(\mathrm{Tr}_1^d(a^{-1})\right) = 2s\mathrm{Tr}_1^d(a^{-1})$, where Tr_d^e is the trace function from $\mathbb{F}_{p^e}$ to $\mathbb{F}_{p^d}$. Therefore the calculation can be divided into four cases according to the values of p and s. We only give the proof of two cases and the other two can be similarly treated.

- (i) When s is odd and $p \nmid s$, we have from the above two lemmas that $wt(\mathsf{c}_a)$ takes two non-zero values w_1 and w_2 with frequencies $A_{w_1} = p^{d-1} - 1$ and $A_{w_2} = (p-1)p^{d-1}$, respectively. Hence we get the weight enumerator of C_{D_0}. Note that for $\lambda \neq 0$, $\eta(-\rho\lambda) = \eta(\rho)$ if $-\lambda \in C_0^{(2,p)}$ and $\eta(-\rho\lambda) = -\eta(\rho)$ otherwise, so it is not hard to determine its complete weight enumerator from Lemma 9.
- (ii) When s is odd and $p \mid s$, we have $\lambda = 0$ for all $a \in \mathbb{F}_{p^d}^*$ and so all codewords c_a, except the zero codeword, have the same weight w_1 and the frequency is $A_{w_1} = p^d - 1$. Hence C_{D_0} has only one non-zero weight and its complete weight enumerator then follows from Lemma 9.

□

3.2.2 The second case that $b \neq 0$

In this subsection, we assume that $b \neq 0$. By (3), Lemmas 6 and 7 again, it is easy to get the value of $N_a(b,\rho)$ for $\rho \neq 0$.

Lemma 10 *For $a \in \mathbb{F}_{p^d}^*$, b and $\rho \in \mathbb{F}_p^*$, we have*

$$N_a(b,\rho) = \begin{cases} p^{e-2} & \text{if } s \text{ is odd and } \lambda = 0, \\ p^{e-2} - \eta(b^2 - \rho\lambda)p^{m-1} & \text{if } s \text{ is odd and } \lambda \neq 0, \\ p^{e-2} & \text{if } s \text{ is even and } \lambda = 0, \\ p^{e-2} - \eta(b^2 - \rho\lambda)p^{m+d-1} & \text{if } s \text{ is even and } \lambda \neq 0. \end{cases}$$

In order to evaluate $N_a(b,0)$, we need one more lemma given below.

Lemma 11 *Let b and $\lambda \in \mathbb{F}_p^*$. Then*

$$\sum_{\rho \in \mathbb{F}_p^*} \eta(b^2 - \rho\lambda) = -1.$$

Proof Write $p = 2h+1$ with a positive integer h. For fixed $\lambda \in \mathbb{F}_p^*$,

$$\eta(b^2 - \rho\lambda) = \begin{cases} 0 & \text{if } b^2 - \rho\lambda = 0, \\ 1 & \text{if } b^2 - \rho\lambda \in C_0^{(2,p)}, \\ -1 & \text{if } b^2 - \rho\lambda \in C_1^{(2,p)}. \end{cases}$$

Let $d = b^2 - \rho\lambda$. Then $\rho\lambda/d + 1 = b^2/d$. According to Lemma 1, the number of $\rho \in \mathbb{F}_p^*$ satisfying $d \in C_0^{(2,p)}$ is

$$(0,0)^{(2,p)} + (1,0)^{(2,p)} = h - 1.$$

Similarly, the number of $\rho \in \mathbb{F}_p^*$ satisfying $d \in C_1^{(2,p)}$ is

$$(0,1)^{(2,p)} + (1,1)^{(2,p)} = h.$$

It then follows that

$$\sum_{\rho \in \mathbb{F}_p^*} \eta(b^2 - \rho\lambda) = (h-1) \cdot 1 + h \cdot (-1) = -1,$$

giving the desired conclusion. □

The following lemma follows from (2), Lemmas 10 and 11.

Lemma 12 *For $a \in \mathbb{F}_{p^d}^*$ and $b \in \mathbb{F}_p^*$, we have*

$$N_a(b, 0) = \begin{cases} p^{e-2} & \text{if } s \text{ is odd and } \lambda = 0, \\ p^{e-2} - p^{m-1} & \text{if } s \text{ is odd and } \lambda \neq 0, \\ p^{e-2} & \text{if } s \text{ is even and } \lambda = 0, \\ p^{e-2} - p^{m+d-1} & \text{if } s \text{ is even and } \lambda \neq 0. \end{cases}$$

Now we begin to prove Theorem 2.

Proof Suppose that $b \neq 0$. By Lemmas 10 and 12, the proof is similar to that of Theorem 1 and so is omitted here. □

4 Concluding remarks

In this paper, we employed exponential sums to present the complete weight enumerators and weight enumerators of the linear codes C_{D_b} in the two cases $b = 0$ and $b \neq 0$. As introduced in [28], any linear code over $\mathbb{F}_p$ can be employed to construct secret sharing schemes with interesting access structures provided that

$$\frac{w_{min}}{w_{max}} > \frac{p-1}{p},$$

where w_{min} and w_{max} denote the minimum and maximum non-zero weights in C_D, respectively. Assume that $p \nmid s$. It can be verified that the linear codes in Theorems 1 and 2 satisfy the property $w_{min}/w_{max} > (p-1)/p$ if $m > 1$ and $s \equiv 1 \mod 2$, or if $m > d+1$ and $s \equiv 0 \mod 2$. We remark that the dimensions of the codes in this paper are small compared with their lengths and this makes them suitable for applications in secret sharing schemes with interesting access structures.

Acknowledgements The work is partially supported by the National Natural Science Foundation of China (11701317, 61772015, 61472457, 11571380), China Postdoctoral Science Foundation Funded Project (2017M611801) and Jiangsu Planned Projects for Postdoctoral Research Funds (1701104C). This work is also partially supported by Guangzhou Science and Technology Program (201607010144) and the Natural Science Foundation of Shandong Province of China (ZR2016AM04).

References

1. Ahn, J., Ka, D., Li, C.: Complete weight enumerators of a class of linear codes. Des. Codes Crypt. **83**, 83–99 (2017)
2. Bae, S., Li, C., Yue, Q.: On the complete weight enumerators of some reducible cyclic codes. Discret. Math. **338**(12), 2275–2287 (2015)
3. Blake, I.F., Kith, K.: On the complete weight enumerator of Reed-Solomon codes. SIAM J. Discret. Math. **4**(2), 164–171 (1991)

4. Coulter, R.S.: Explicit evaluations of some Weil sums. Acta Arithmetica **83**(3), 241–251 (1998)
5. Coulter, R.S.: The number of rational points of a class of artincschreier curves. Finite Fields Appl. **8**, 397–413 (2002)
6. Ding, C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265–3275 (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. Theor. Comput. Sci. **330**, 81–99 (2005)
9. Ding, K., Ding, C.: Binary linear codes with three weights. IEEE Commun. Lett. **18**(11), 1879–1882 (2014)
10. 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)
11. Dinh, H.Q., Li, C., Yue, Q.: Recent progress on weight distributions of cyclic codes over finite fields. J. Algebra Comb. Discret. Struct. Appl. **2**(1), 39–63 (2015)
12. Feng, K., Luo, J.: Weight distribution of some reducible cyclic codes. Finite Fields Appl. **14**(2), 390–409 (2008)
13. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**(5), 2018–2032 (2006)
14. Heng, Z., Yue, Q.: Complete weight distributions of two classes of cyclic codes. Cryptogr. Commun. **9**(3), 323–343 (2017)
15. Kith, K.: Complete weight enumeration of Reed-Solomon codes. Master's thesis, Department of Electrical and Computing Engineering, University of Waterloo (1989)
16. Kuzmin, A., Nechaev, A.: Complete weight enumerators of generalized Kerdock code and linear recursive codes over Galois ring. In: Workshop on Coding and Cryptography, pp. 332–336 (1999)
17. Li, C., Bae, S., Ahn, J., Yang, S., Yao, Z.: Complete weight enumerators of some linear codes and their applications. Des. Codes Crypt. **81**, 153–168 (2016)
18. Li, C., Yue, Q., Fu, F.W.: Complete weight enumerators of some cyclic codes. Des. Codes Crypt. **80**, 295–315 (2016)
19. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and its Applications, p. 20. Addison-Wesley, Reading (1983)
20. MacWilliams, F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes, vol. 16. North-Holland Publishing, Amsterdam (1977)
21. Storer, T.: Cyclotomy and Difference Sets. Markham Publishing Company, Markham (1967)
22. Vega, G.: The weight distribution of an extended class of reducible cyclic codes. IEEE Trans. Inf. Theory **58**(7), 4862–4869 (2012)
23. Wang, Q., Li, F., Ding, K., Lin, D.: Complete weight enumerators of two classes of linear codes. Discret. Math. **340**, 467–480 (2017)
24. Yang, S., Kong, X., Tang, C.: A construction of linear codes and their complete weight enumerators. Finite Fields Appl. **48**, 196–226 (2017)
25. Yang, S., Yao, Z., Zhao, C.: The weight enumerator of the duals of a class of cyclic codes with three zeros. Applic. Algebra Eng. Commun. Comput. **26**(4), 347–367 (2015)
26. Yang, S., Yao, Z., Zhao, C.: The weight distributions of two classes of p-ary cyclic codes with few weights. Finite Fields Appl. **44**, 76–91 (2017)
27. Yang, S., Yao, Z.: Complete weight enumerators of a class of linear codes. Discret. Math. **340**, 729–739 (2017)
28. Yuan, J., Ding, C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory **52**(1), 206–212 (2006)
29. Zheng, D., Wang, X., Yu, L., Liu, H.: The weight enumerators of several classes of p-ary cyclic codes. Discret. Math. **338**(7), 1264–1276 (2015)
30. Zhou, Z., Ding, C., Luo, J., Zhang, A.: A family of five-weight cyclic codes and their weight enumerators. IEEE Trans. Inf. Theory **59**(10), 6674–6682 (2013)