JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **33**, No. 1, February 2020
http://dx.doi.org/10.14403/jcms.2020.33.1.43

WEIGHT ENUMERATORS OF TWO CLASSES OF LINEAR CODES

Jaehyun Ahn* and Yeonseok Ka**

Abstract. Recently, linear codes constructed from defining sets have been studied widely and determined their complete weight enumerators and weight enumerators. In this paper, we obtain complete weight enumerators of linear codes and weight enumerators of linear codes. These codes have at most three weight linear codes. As application, we show that these codes can be used in secret sharing schemes and authentication codes.

1. Introduction

Throughout this paper, let p be an odd prime and $q = p^m$ for a positive integer m. Let $\mathbb{F}_p$ be the finite field with p elements. An $[n, k, d]$ *linear code* $\mathcal{C}$ over $\mathbb{F}_p$ is a k-dimensional subspace of $\mathbb{F}_p^n$ with *minimum distance* d. Let A_i denote the number of codewords with Hamming weight i in the code $\mathcal{C}$ of length n. The weight enumerator of $\mathcal{C}$ is defined by $1 + A_1 z + A_2 z^2 + \cdots + A_n z^n$. The sequence $(1, A_1, A_2, \cdots, A_n)$ is called the *weight distribution* of the code $\mathcal{C}$.

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 $\mathrm{comp}(\mathbf{v})=(t_0, t_1, \ldots, t_{q-1})$, 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.

Received December 10, 2019; Accepted January 13, 2020.
2010 Mathematics Subject Classification: 94B05, 11T23, 11T71.
Key words and phrases: Linear codes, Weight distribution, Gauss sums.
correspondence should be addressed to Yeonseok Ka, dska@cnu.ac.kr.
J. Ahn was supported by a research fund of Chungnam National University.
Y. Ka was supported by Basic Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2018R1D1A1B07048769).

Clearly, we have

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

Let $A(t_0, t_1 \ldots, t_{q-1})$ be the number of codewords $\mathbf{c} \in C$ with $\mathrm{comp}(\mathbf{c})=(t_0, t_1, \ldots, t_{q-1})$. 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 $B_n = \{(t_0, t_1, \ldots, t_{q-1}) : 0 \leqslant t_i \leqslant n, \sum_{i=0}^{q-1} t_i = n\}$.

The weight distribution of linear codes is an interesting subject in coding theory because it estimates the error-correcting capability. But in general it is not easy to determine the weight distribution of linear codes. Recently, linear codes with a few weight have been studied [7, 8, 12, 13, 15, 16, 20, 22, 27–29] by using exponential sums in some cases. They have many applications in authentication codes [10, 11], association schemes [4], strongly regular graphs [5] and secret sharing schemes [6, 14, 23].

In this paper, let $D = \{d_1, d_2, \cdots, d_n\} \subseteq \mathbb{F}_q$ and Tr denote the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. A linear code of length n over $\mathbb{F}_p$ is defined by

$$\mathcal{C}_D = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \cdots, \mathrm{Tr}(xd_n)) : x \in \mathbb{F}_q\}. \tag{1.1}$$

The set D is called the *defining set* of $\mathcal{C}_D$. In [14], the authors presented a class of two-weight and three-weight codes by choosing defining set $D = \{x \in \mathbb{F}_q^* : \mathrm{Tr}(x^2) = 0\}$. And then the authors in [3] gave a generalization of the case [14]. In [21], the authors had constructed a two or three weight linear codes from weakly regular bent functions and presented their weight distribution. Moreover, many linear codes of good parameters are obtained by choosing defining set D properly [1–3, 14, 17, 19, 24–26]. Motivated by the construction given in [21, 26], we define linear codes $\mathcal{C}_{D_i}$ for each $i \in \{0, 1\}$, where

$$D_0 = \{x \in \mathbb{F}_q : \mathrm{Tr}(x^2) \in Sq\}, \tag{1.2}$$

$$D_1 = \{x \in \mathbb{F}_q : \mathrm{Tr}(x^2) \in Nsq\}. \tag{1.3}$$

Here Sq and Nsq denote the set of all squares and non-squares in $\mathbb{F}_p^*$, respectively. And we compute the complete weight enumerators of linear codes.

As an application, we show that our codes are minimal, which can be used to construct secret sharing schemes with an interesting access structure [9, 23]. Also we investigate to construct the systematic authentication codes with new parameters from their the complete weight enumerators. We shall explain it at the end of this paper in detail.

2. Preliminaries

We introduce some basic notations and results of additive characters and exponential sums, and then give some lemmas that will be useful to compute our results.

For any $a \in \mathbb{F}_q$, we can define an additive character of the finite field $\mathbb{F}_q$ as follows:

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

where $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a p-th primitive root of unity and Tr denotes the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_p$. For a multiplicative character λ of $\mathbb{F}_q^*$, we define the Gauss sum of λ over $\mathbb{F}_q$ by

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

Suppose that η is the quadratic character of $\mathbb{F}_q^*$ and η_p is the quadratic character of $\mathbb{F}_p^*$. For $z \in \mathbb{F}_p^*$, it is easily checked that

$$\eta(z) = \begin{cases} 1, & \text{if } m \text{ is even,} \\ \eta_p(z), & \text{if } m \text{ is odd.} \end{cases}$$

Lemma 2.1. [18, Lemma 5.15] *Suppose that $q = p^m$ for an odd prime p 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. [18, Lemma 5.33] *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*

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

LEMMA 2.3. [14, Lemma 9] *For each $a \in \mathbb{F}_p$, let*

$$n_a = |\{x \in \mathbb{F}_q : \mathrm{Tr}(x^2) = a\}|.$$

Then

$$n_0 = \begin{cases} p^{m-1} - (-1)^{\frac{p-1}{2}\frac{m}{2}}(p-1)p^{\frac{m-2}{2}}, & \text{if } m \text{ is even,} \\ p^{m-1}, & \text{if } m \text{ is odd.} \end{cases}$$

If $a \neq 0$, then

$$n_a = \begin{cases} p^{m-1} + (-1)^{\frac{p-1}{2}\frac{m}{2}}p^{\frac{m-2}{2}}, & \text{if } m \text{ is even,} \\ p^{m-1} + \eta_p(a)(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{m+1}{2}}p^{\frac{m-1}{2}}, & \text{if } m \text{ is odd.} \end{cases}$$

3. Weight enumerators of the linear codes $\mathcal{C}_{D_i}$

In this section, we present the weight distributions of linear codes $\mathcal{C}_{D_i}$ for each $i \in \{0, 1\}$ defined by (1), (2) and (1), (3), respectively. We start with the weight distributions of the linear codes $\mathcal{C}_{D_i}$ for each $i \in \{0, 1\}$ because we can obtain the complete weight enumerators of $\mathcal{C}_{D_i}$ for each $i \in \{0, 1\}$ from their the weight distributions of $\mathcal{C}_{D_i}$ for each $i \in \{0, 1\}$. We explain the details in Section 4. Clearly, from Lemma 2.3, linear codes $\mathcal{C}_{D_i}$ have the length for each $i \in \{0, 1\}$

$$|D_i| = \begin{cases} \frac{p-1}{2}(p^{m-1} + (-1)^{\frac{m(p-1)}{4}}p^{\frac{m-2}{2}}), & \text{if } m \text{ is even,} \\ \frac{p-1}{2}(p^{m-1} + (-1)^i(-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p-1)(m+1)}{4}}p^{\frac{m-1}{2}}), & \text{if } m \text{ is odd.} \end{cases}$$

For a codeword $\mathbf{c}(a)$ of $\mathcal{C}_{D_i}$ for each $i \in \{0, 1\}$, let $N_{0,i} := N_{0,i}(a)$ be the number of components $\mathrm{Tr}_m(ax)$ of $\mathbf{c}(a)$ which are equal to 0. By the

orthogonal property of additive characters, we have for each $i \in \{0,1\}$

$$\begin{aligned} N_{0,i} &= \sum_{c\in C_i^{(2,p)}} \sum_{x\in\mathbb{F}_q} \left(\frac{1}{p}\sum_{y\in\mathbb{F}_p} \zeta_p^{y(\mathrm{Tr}(x^2)-c)}\right)\left(\frac{1}{p}\sum_{z\in\mathbb{F}_p} \zeta_p^{z\mathrm{Tr}(ax)}\right) \\ &= \frac{1}{p^2}\sum_{c\in C_i^{(2,p)}} \sum_{x\in\mathbb{F}_q} \left(1+\sum_{y\in\mathbb{F}_p^*} \zeta_p^{y(\mathrm{Tr}(x^2)-c)}\right)\left(1+\sum_{z\in\mathbb{F}_p^*} \zeta_p^{z\mathrm{Tr}(ax)}\right) \\ &= \frac{p^m(p-1)}{2p^2} + \frac{1}{p^2}(\Omega_{1,i}+\Omega_{2,i}+\Omega_{3,i}), \end{aligned}$$

where

$$\Omega_{1,i} = \sum_{c\in C_i^{(2,p)}} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(yx^2)},$$

$$\Omega_{2,i} = \sum_{c\in C_i^{(2,p)}} \sum_{z\in\mathbb{F}_p^*} \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(zax)},$$

and

$$\Omega_{3,i} = \sum_{c\in C_i^{(2,p)}} \sum_{y,z\in\mathbb{F}_p^*} \zeta_p^{-yc} \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(yx^2+zax)}.$$

First of all, we easily compute $\Omega_{1,i}$ for each $i \in \{0,1\}$.

$$\Omega_{1,i} = \sum_{c\in C_0^{(2,p)}} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(yx^2)} = \begin{cases} -\frac{p-1}{2}G(\eta), & \text{if } m \text{ is even,} \\ \frac{p-1}{2}(-1)^i(-1)^{\frac{p-1}{2}}G(\eta)G(\eta_p), & \text{if } m \text{ is odd.} \end{cases}$$

The last equality follows from Lemma 2.2. For each $i \in \{0,1\}$,

$$\Omega_{2,i} = \sum_{c\in C_i^{(2,p)}} \sum_{z\in\mathbb{F}_p^*} \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(zax)} = 0$$

Therefore, we need to compute $\Omega_{3,i}$ for each $i \in \{0,1\}$.

Lemma 3.1. *For $i \in \{0,1\}$,*
(1) *If m is even, then*

$$\Omega_{3,i} = \begin{cases} -\frac{(p-1)^2}{2}G(\eta), & \text{if } \mathrm{Tr}(a^2)=0, \\ \frac{p-1}{2}\big((-1)^i G(\eta)G(\eta_p)^2\eta_p(\mathrm{Tr}(a^2)) + G(\eta)\big), & \text{if } \mathrm{Tr}(a^2)\neq 0. \end{cases}$$

(2) *If m is odd, then*

$$\Omega_{3,i} = \begin{cases} \frac{(p-1)^2}{2}(-1)^i(-1)^{\frac{p-1}{2}}G(\eta)G(\eta_p), & \text{if } \mathrm{Tr}(a^2)=0, \\ -\frac{p-1}{2}\big(G(\eta)G(\eta_p)\eta_p(-\mathrm{Tr}(a^2)) + (-1)^i(-1)^{\frac{p-1}{2}}G(\eta)G(\eta_p)\big), & \text{if } \mathrm{Tr}(a^2)\neq 0. \end{cases}$$

Proof. By Lemma 2.2, we have

$$\Omega_{3,i} = \sum_{c\in C_i^{(2,p)}} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-z^2(4y)^{-1}\mathrm{Tr}(a^2)} \eta(y) G(\eta). \tag{3.1}$$

Because the case of even m is similar, we only consider the case of odd m. If $\mathrm{Tr}(a^2) = 0$, then from (4) we have

$$\Omega_{3,i} = \frac{(p-1)^2}{2} G(\eta) G(\eta_p) \eta_p(-c).$$

If $\mathrm{Tr}(a^2) \neq 0$, then it follows from (3) and Lemma 2.2 that

$$\begin{aligned}
\Omega_{3,i} &= G(\eta) \sum_{c\in C_i^{(2,p)}} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \eta_p(y) \left(\sum_{z\in\mathbb{F}_p^*} \zeta_p^{-z^2(4y)^{-1}\mathrm{Tr}(a^2)} - 1 \right) \\
&= G(\eta) \sum_{c\in C_i^{(2,p)}} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \eta_p(y) \big(\eta_p(-(4y)^{-1}\mathrm{Tr}(a^2)) G(\eta_p) - 1 \big) \\
&= G(\eta) G(\eta_p) \eta_p(-\mathrm{Tr}(a^2)) \sum_{c\in C_i^{(2,p)}} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} - \sum_{c\in C_i^{(2,p)}} G(\eta) \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \eta_p(y) \\
&= \frac{(p-1)}{2} \big(- G(\eta) G(\eta_p) \eta_p(-\mathrm{Tr}(a^2)) - G(\eta) G(\eta_p) \eta_p(-c) \big).
\end{aligned}$$

This completes the proof. □

THEOREM 3.2. *Let m be even, the code $\mathcal{C}_{D_0}$ and $\mathcal{C}_{D_1}$ are defined in* (1), (2) *and* (1) (3), *then the code $\mathcal{C}_{D_0}$ and $\mathcal{C}_{D_1}$ are an $[\frac{p-1}{2}(p^{m-1} + (-1)^{\frac{m(p-1)}{4}} p^{\frac{m-2}{2}}), m]$ two-weight linear code with the weight distribution in Table* 1.

Weight	*Frequency*
0	1
$\frac{p-1}{2}(p^{m-1} - p^{m-2})$	$\frac{1}{2}\big(p^m + p^{m-1} - (-1)^{\frac{m(p-1)}{4}}(p-1)p^{\frac{m-2}{2}}\big) - 1$
$\frac{p-1}{2}(p^{m-1} - p^{m-2} + 2(-1)^{\frac{m(p-1)}{4}} p^{\frac{m-2}{2}})$	$\frac{p-1}{2}\big(p^{m-1} + (-1)^{\frac{m(p-1)}{4}} p^{\frac{m-2}{2}}\big)$

TABLE 1. The weight distribution of C_{D_0} and C_{D_1} for even m

THEOREM 3.3. *Let m be odd and the code $\mathcal{C}_{D_0}$ be defined in* (1) *and* (2), *then the code $\mathcal{C}_{D_0}$ is an $[\frac{(p-1)}{2}(p^{m-1} + (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p-1)(m+1)}{4}} p^{\frac{m-1}{2}}), m]$ three-weight linear code with the weight distribution in Table* 2.

Weight	*Frequency*
0	1
$\frac{p-1}{2}(p^{m-1}-p^{m-2})$	$p^{m-1}-1$
$\frac{p-1}{2}\big(p^{m-1}-p^{m-2}+(-1)^{\frac{(m+1)(p-1)}{4}}p^{\frac{m-3}{2}}\big((-1)^{\frac{p-1}{2}}p+1\big)\big)$	$\frac{p-1}{2}(p^{m-1}+(-1)^{\frac{(m+1)(p-1)}{4}}p^{\frac{m-1}{2}})$
$\frac{p-1}{2}\big(p^{m-1}-p^{m-2}+(-1)^{\frac{(m+1)(p-1)}{4}}p^{\frac{m-3}{2}}\big((-1)^{\frac{p-1}{2}}p-1\big)\big)$	$\frac{p-1}{2}(p^{m-1}-(-1)^{\frac{(m+1)(p-1)}{4}}p^{\frac{m-1}{2}})$

TABLE 2. The weight distribution of C_{D_0} for odd m

THEOREM 3.4. *Let m be odd and the code $\mathcal{C}_{D_1}$ be defined in* (1) *and* (3)*, then the code $\mathcal{C}_{D_1}$ is an $[\frac{(p-1)}{2}(p^{m-1}-(-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p-1)(m+1)}{4}}p^{\frac{m-1}{2}}), m]$ three-weight linear code with the weight distribution in Table* 3.

Weight	*Frequency*
0	1
$\frac{p-1}{2}(p^{m-1}-p^{m-2})$	$p^{m-1}-1$
$\frac{p-1}{2}\big(p^{m-1}-p^{m-2}-(-1)^{\frac{(m+1)(p-1)}{4}}p^{\frac{m-3}{2}}\big((-1)^{\frac{p-1}{2}}p-1\big)\big)$	$\frac{p-1}{2}(p^{m-1}+(-1)^{\frac{(m+1)(p-1)}{4}}p^{\frac{m-1}{2}})$
$\frac{p-1}{2}\big(p^{m-1}-p^{m-2}-(-1)^{\frac{(m+1)(p-1)}{4}}p^{\frac{m-3}{2}}\big((-1)^{\frac{p-1}{2}}p+1\big)\big)$	$\frac{p-1}{2}(p^{m-1}-(-1)^{\frac{(m+1)(p-1)}{4}}p^{\frac{m-1}{2}})$

TABLE 3. The weight distribution of C_{D_1} for odd m

Proof. Since the proofs are similar, we are going to prove theorems 3.1, 3.2 and 3.3 together. Recall that $N_{0,i}=\frac{p^m(p-1)}{2p^2}+\frac{1}{p^2}(\Omega_{1,i}+\Omega_{2,i}+\Omega_{3,i})$ for each $i\in\{0,1\}$. First of all, we employ Lemma 3.1 to compute $N_{0,0}$. The case of even m can be proved in the same way as the case of odd m. Suppose that m is odd. If $\mathrm{Tr}(a^2)=0$, then we obtain

$$\begin{aligned}N_{0,0}&=\frac{p^m(p-1)}{2p^2}+\frac{(p-1)}{2p^2}\Big(G(\eta)G(\eta_p)\eta_p(-1)+(p-1)G(\eta)G(\eta_p)\eta_p(-1)\Big)\\&=\frac{(p-1)}{2p^2}\Big(p^m+pG(\eta)G(\eta_p)\eta_p(-1)\Big).\end{aligned}$$

If $\mathrm{Tr}(a^2)\neq 0$, then we obtain

$$\begin{aligned}N_{0,0}&=\frac{p^m(p-1)}{2p^2}+\frac{(p-1)}{2p^2}\Big(G(\eta)G(\eta_p)\eta_p(-1)-G(\eta)G(\eta_p)\eta_p(-1)-G(\eta)G(\eta_p)\eta_p(-\mathrm{Tr}(a^2))\Big)\\&=\begin{cases}\frac{(p-1)}{2p^2}\big(p^m-G(\eta)G(\eta_p)\big), & \text{if } \eta_p(-\mathrm{Tr}(a^2))=1,\\ \frac{(p-1)}{2p^2}\big(p^m+G(\eta)G(\eta_p)\big), & \text{if } \eta_p(-\mathrm{Tr}(a^2))=-1.\end{cases}\end{aligned}$$

Since the case of $N_{0,1}$ for even m can be similarly calculated, we only consider the case of odd m.
If $\mathrm{Tr}(a^2) = 0$, then we obtain

$$\begin{aligned} N_{0,1} &= \frac{p^m(p-1)}{2p^2} - \frac{(p-1)}{2p^2}\big(G(\eta)G(\eta_p)\eta_p(-1) + (p-1)G(\eta)G(\eta_p)\eta_p(-1)\big) \\ &= \frac{(p-1)}{2p^2}\big(p^m - pG(\eta)G(\eta_p)\eta_p(-1)\big). \end{aligned}$$

If $\mathrm{Tr}(a^2) \neq 0$, then we obtain

$$\begin{aligned} N_{0,1} &= \frac{p^m(p-1)}{2p^2} + \frac{(p-1)}{2p^2}\Big(- G(\eta)G(\eta_p)\eta_p(-1) + G(\eta)G(\eta_p)\eta_p(-1) - G(\eta)G(\eta_p)\eta_p(-\mathrm{Tr}(a^2))\Big) \\ &= \begin{cases} \frac{(p-1)}{2p^2}\big(p^m - G(\eta)G(\eta_p)\big), & \text{if } \eta_p(-\mathrm{Tr}(a^2)) = 1, \\ \frac{(p-1)}{2p^2}\big(p^m + G(\eta)G(\eta_p)\big), & \text{if } \eta_p(-\mathrm{Tr}(a^2)) = -1. \end{cases} \end{aligned}$$

By Lemma 2.3, we immediately obtain the frequency of each weight. Since the Hamming weight of $\mathbf{c}(a)$ is equal to $W_H(\mathbf{c}(a)) = |D_i| - N_{0,i}$ for each $i \in \{0,1\}$, we get the desired results. □

4. Complete weight enumerators of linear codes $\mathcal{C}_{D_i}$

In this section, we investigate the complete weight enumerators of linear codes $\mathcal{C}_{D_0}$ defined by (1) and (2). Since the case of $\mathcal{C}_{D_1}$ is similar, we only consider the case of $\mathcal{C}_{D_0}$. For a codeword $\mathbf{c}(a)$ of $\mathcal{C}_{D_0}$ and $\rho \in \mathbb{F}_p^*$, let $N_{\rho,0} := N_{\rho,0}(a)$ be the number of components $\mathrm{Tr}(ax)$ of $\mathbf{c}(a)$ which are equal to ρ. Then

$$N_{\rho,0} = \sum_{c \in C_0^{(2,p)}} \sum_{x \in \mathbb{F}_q} \left(\frac{1}{p} \sum_{y \in \mathbb{F}_p} \zeta_p^{y(\mathrm{Tr}(x^2)-c)} \right) \left(\frac{1}{p} \sum_{z \in \mathbb{F}_p} \zeta_p^{z(\mathrm{Tr}(ax)-\rho)} \right)$$

$$= \frac{1}{p^2} \sum_{c \in C_0^{(2,p)}} \sum_{x \in \mathbb{F}_q} \left(1 + \sum_{y \in \mathbb{F}_p^*} \zeta_p^{y(\mathrm{Tr}(x^2)-c)} \right) \left(1 + \sum_{z \in \mathbb{F}_p^*} \zeta_p^{z(\mathrm{Tr}(ax)-\rho)} \right)$$

$$= \frac{p^m(p-1)}{2p^2} + \frac{1}{p^2}(\Omega_1' + \Omega_2' + \Omega_3'),$$

where

$$\Omega_{1,0}^{'} = \sum_{c\in C_0^{(2,p)}} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(yx^2)},$$
$$\Omega_{2,0}^{'} = \sum_{c\in C_0^{(2,p)}} \sum_{z\in\mathbb{F}_p^*} \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(zax)},$$
and
$$\Omega_{3,0}^{'} = \sum_{c\in C_0^{(2,p)}} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-z\rho} \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(yx^2+zax)}.$$

Now, we show that $N_{\rho,0}$ of $\mathcal{C}_{D_0}$ is independent of $\rho \in \mathbb{F}_p^*$. Then, we easily obtain the complete weight enumerators of the linear codes $\mathcal{C}_{D_0}$. We easily check that both $\Omega_{1,0}^{'}$ and $\Omega_{2,0}^{'}$ are independent of $\rho \in \mathbb{F}_p^*$. Thus, we only focus on $\Omega_{3,0}^{'}$.

$$\begin{aligned}\Omega_{3,0}^{'} &= \sum_{c\in C_0^{(2,p)}} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-z\rho} \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(yx^2+zax)} \\ &= \sum_{c\in C_0^{(2,p)}} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-z\rho} \sum_{x\in\mathbb{F}_q} \zeta_p^{-z^2(4y)^{-1}\mathrm{Tr}(a^2)} \eta(y) G(\eta) \\ &= G(\eta) \sum_{c\in C_0^{(2,p)}} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-\mathrm{Tr}(a^2)(4y)^{-1}z^2-z\rho}. \qquad (4.1)\end{aligned}$$

Suppose that m is even. If $\mathrm{Tr}(a^2) = 0$, then it follows from (5) that

$$\Omega_{3,0}^{'} = G(\eta) \sum_{c\in C_0^{(2,p)}} \sum_{y\in\mathbb{F}_p^*} \zeta_p^{-yc} \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-z\rho} = G(\eta) \sum_{c\in C_0^{(2,p)}} 1.$$

Thus, $\Omega_{3,0}^{'}$ is independent of $\rho \in \mathbb{F}_p^*$.
If $\mathrm{Tr}(a^2) \neq 0$, then it follows from (5) and Lemma 2.2 that

$$\begin{aligned}\Omega_{3,0}^{'} &= G(\eta) \sum_{c \in C_0^{(2,p)}} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{-yc} \left(\sum_{z \in \mathbb{F}_p} \zeta_p^{-\mathrm{Tr}(a^2)(4y)^{-1}z^2 - \rho z} - 1 \right) \\ &= G(\eta) \sum_{c \in C_0^{(2,p)}} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{-yc} \left(\sum_{z \in \mathbb{F}_p} \zeta_p^{\rho^2 (4\mathrm{Tr}(a^2))^{-1}((4y)^{-1})^{-1}} \eta_p(-\mathrm{Tr}(a^2)(4y)^{-1}) G(\eta) - 1 \right) \\ &= G(\eta) G(\eta_p) \sum_{c \in C_0^{(2,p)}} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{(\frac{\rho^2}{\mathrm{Tr}(a^2)} - c)y} \eta_p(-\mathrm{Tr}(a^2)y) + \frac{p-1}{2} G(\eta). \end{aligned} \tag{4.2}$$

We only consider the case $\mathrm{Tr}(a^2)$ is a square because the case $\mathrm{Tr}(a^2)$ is a non-square is similar. From (6) we obtain

$$\begin{aligned}\Omega_{3,0}^{'} &= G(\eta) G(\eta_p) \left(\sum_{\substack{c \in C_0^{(2,p)} \\ c \neq \frac{\rho^2}{\mathrm{Tr}_m(a^2)}}} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{(\frac{\rho^2}{\mathrm{Tr}(a^2)} - c)y} \eta_p(-\mathrm{Tr}(a^2)y) + \sum_{y \in \mathbb{F}_p^*} \eta_p(-\mathrm{Tr}(a^2)y) \right) \\ &\quad + \frac{p-1}{2} G(\eta) \\ &= G(\eta) G(\eta_p)^2 \sum_{\substack{c \in C_0^{(2,p)} \\ c \neq \frac{\rho^2}{\mathrm{Tr}(a^2)}}} \eta_p(c\mathrm{Tr}(a^2) - \rho^2) + \frac{p-1}{2} G(\eta). \end{aligned}$$

Note that when c runs through $C_0^{(2,p)}$, $c\rho^2$ also runs through $C_0^{(2,p)}$.
Thus we have

$$\begin{aligned}\sum_{\substack{c \in C_0^{(2,p)} \\ c \neq \frac{\rho^2}{\mathrm{Tr}(a^2)}}} \eta_p(c\mathrm{Tr}(a^2) - \rho^2) &= \sum_{\substack{c \in C_0^{(2,p)} \\ c \neq \frac{1}{\mathrm{Tr}(a^2)}}} \eta_p(c\rho^2\mathrm{Tr}(a^2) - \rho^2) \\ &= \sum_{\substack{c \in C_0^{(2,p)} \\ c \neq \frac{1}{\mathrm{Tr}(a^2)}}} \eta_p(c\mathrm{Tr}(a^2) - 1). \end{aligned}$$

Therefore, $\Omega_{3,0}^{'}$ is independent of $\rho \in \mathbb{F}_p^*$. For odd m, we can show that $\Omega_{3,0}^{'}$ is independent of $\rho \in \mathbb{F}_p^*$ similarly. The case of $N_{\rho,1}$ can be similarly

checked. Therefore, $N_{\rho,i}$ are independent of $\rho \in \mathbb{F}_p^*$ for $i \in \{0,1\}$. Thus for each $i \in \{0,1\}$,

$$N_{\rho,i} = \frac{(|D| - N_{0,i})}{p-1} \text{ for all } \rho \in \mathbb{F}_p^*.$$

We easily get the complete weight distribution.

EXAMPLE 4.1. *(1) Let $p = 5$ and $m = 3$. Then $q = 125$ and $n = 60$. The code C_{D_0} is a $[60, 3, 40]$ linear code. Its complete weight enumerator is*

$$z_0^8 + 24z_0^{20}(z_1z_2z_3z_4)^{10} + 40(z_0z_1z_2z_3z_4)^{12} + 60z_0^8(z_1z_2z_3z_4)^{13},$$

and its weight enumerator is

$$1 + 24x^{40} + 40x^{48} + 60x^{52},$$

which are checked by Magma.

Let $p = 5$ and $m = 3$. Then $q = 125$ and $n = 40$. The code C_{D_1} is a $[40, 3, 28]$ linear code. Its complete weight enumerator is

$$z_0^{40} + 40z_0^{12}(z_1z_2z_3z_4)^7 + 60(z_0z_1z_2z_3z_4)^8 + 24(z_1z_2z_3z_4)^{10},$$

and its weight enumerator is

$$1 + 40x^{28} + 60x^{32} + 24x^{40},$$

which are checked by Magma.

(2) Let $p = 5$ and $m = 4$. Then $q = 625$ and $n = 260$. The code C_{D_0} and C_{D_1} is a $[260, 4, 200]$ linear code. Its complete weight enumerator is

$$z_0^8 + 260z_0^{40}(z_1z_2z_3z_4)^{55} + 364z_0^{60}(z_1z_2z_3z_4)^{50},$$

and its weight enumerator is

$$1 + 364x^{200} + 260x^{220},$$

which are checked by Magma.

5. Concluding remarks

In this section, we employ the complete weight enumerators of the linear codes C_{D_i} for each $i \in \{0,1\}$ to get secret sharing schemes with interesting access structures. And we construct a systematic authentication codes.

(1) **Secret Sharing Schemes from the linear codes C_{D_i}**

Let w_{min} and w_{max} be the minimum and maximum nonzero weight of linear code C_{D_i}, respectively. We recall that if $w_{min}/w_{max} > p-1/p$, then all nonzero codewords of code C_D are minimal (see [23]). We easily check that the linear codes in this paper are minimal for $m \geq 4$ and can be used to get secret sharing schemes with interesting access structures.

(2) **Systematic Authentication codes**

A systematic authentication codes is a four-tuple $(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\})$, where $\mathcal{S}$ is the source state space associated with a probability distribution, $\mathcal{T}$ is the tag space, $\mathcal{K}$ is the key space, and $E_k : \mathcal{S} \to \mathcal{T}$ is called an encoding rule. For more information, see [10, 11, 15] about the authentication codes. We denote the maximum success probability of the impersonation attack and the substitution attack by P_I and P_S, respectively. For the systematic authentication codes, there are two lower bounds on P_I and P_S [10, 11]:

$$P_I \geq \frac{1}{|\mathcal{T}|} \text{ and } P_S \geq \frac{1}{|\mathcal{T}|.}$$

It is desired that P_I and P_S must be as small as possible.

We mention that the complete weight enumerators, presented by Theorems 3.2, 3.3 and 3.4 can be applied to compute the deception probabilities of certain authentication codes constructed from our linear codes as in [10]. Moreover, if p^m is large enough, then we have $P_I = \frac{1}{p}$ and $P_S \approx \frac{1}{p}$ for all authentication codes obtained from Theorems 3.2, 3.3 and 3.4. Therefore, these authentication codes are asymptotically optimal.

References

[1] J. Ahn, D. Ka, and C. Li, *Complete weight enumerators of a class of linear codes*, Des. Codes Cryptogr., **83** (2017), 83-99.

[2] J. Ahn and D. Ka, *Weight enumerators of a class of linear codes,* Appl Algebra Engrg Comm Comput., **29** (2018), 59-76.

[3] S. Bae, C. Li, and Q. Yue, *Some results on two-weight and three-weight linear codes,* preprint (2015).

[4] A.R. Calderbank and J.M. Goethals, *Three-weight codes and association schemes,* Philips J Res., **39** (1984), 143-152.

[5] A.R. Calderbank and W.M. Kantor, *The geometry of two-weight codes,* Bull. London Math Soc., **18** (1986), 97-122.

[6] C. Carlet, C. Ding, and J. Yuan, *Linear codes from perfect nonlinear mappings and their secret sharing schemes,* IEEE Trans. Inf. Theory., **51** (2005), no. 6, 2089-2102.
[7] C. Ding, *Linear codes from some* 2*-designs,* IEEE Trans. Inf. Theory. **61** (2015), no. 6, 3265-3275.
[8] C. Ding, C. Li, N. Li, and Z. Zhou, *Three-weight cyclic codes and their weight distribution,* Discret. Math., **339** (2016), no. 2, 415-427.
[9] C. Ding and J. Yuan, *Covering and secret sharing with linear codes*, Discrete Mathematics and Theoretical Computer Science, **2731**, Berlin, Germany: Springer-Verlag, (2003), 11-25.
[10] C. Ding and X. Wang, *A coding theory construction of new systematic authentication codes,* Theor. Comput. Sci., **330** (2005), no. 1, 81-99.
[11] C. Ding, T. Helleseth, and X. Wang, *A generic construction of cartesian authentication codes,* IEEE Trans. Inf. Theory., **53** (2007), no. 6, 2229-2235.
[12] C. Ding and J. Yang, *Hamming weights in irreducible cyclic codes,* Discret. Math., **313** (2013), no, 4, 434-446.
[13] K. Ding and C. Ding, *Binary linear codes with three weight,* IEEE Commun. Lett., **18** (2014), no. 11, 1879-1882.
[14] K. Ding and C. Ding, *A class of two-weight and three-weight codes and their applications in secret sharing,* IEEE Trans. Inf. Theory., **81** (2015), no. 11, 5835-5842.
[15] C. Li, S. Bae, J. Ahn, S. Yang, and Z. Yao, *Complete weight enumerators some linear codes and their application,* Des. Codes Cryptogr., **81** (2016), 153-168.
[16] C. Li and Q. Yue, *Weight distribution of two classes of cyclic codes with respect to two distinct order elements,* IEEE Trans. Inf. Theory., **60** (2014), no. 1, 296-303.
[17] C. Li, Q. Yue, and F.Fu, *A construction of several classes of two-weight and three-weight linear codes,* Appl Algebra Engrg Comm Comput., **28** (2017), 11-30.
[18] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983.
[19] F. Li, Q. Wang, and D. Lin, *A class of three-weight and five-weight linear codes,* Discret. Appl Math., http://dx.doi.org/j.dam.2016.11.005
[20] Z. Shi and F. Fu, *Complete weight enumerators of some irreducible cyclic codes,* Discret. Appl Math., **219** (2017), 182-192.
[21] C. Tang, N. Li, Y. Qi, Z. Zhou, and T. Helleseth, *Linear codes with two or three weight from weakly regular bent functions,* IEEE Trans. Inf. Theory., **62** (2016), no. 3, 1166-1176.
[22] Q. Wang, K. Ding, and R. Xue, *Binary linear codes with two weights,* IEEE Commun. Lett., **19** (2015), no. 7, 1097-1100.
[23] J. Yuan and C. Ding, *Secret sharing schemes from three classes of linear codes,* IEEE Trans. Inf. Theory., **52** (2006), no. 1, 206-212.
[24] S. Yang and Z. Yao, *Complete weight enumerators of a family of three-weight liner codes,* Des. Codes Cryptogr., **82** (2017), 663-674.
[25] S. Yang and Z. Yao, *Complete weight enumerators of a class of linear codes,* Discret. Math., **340** (2017), 729-739.
[26] S. Yang, Z. Yao, and C. Zhao, *A class of three-weight linear codes ans their complete weight enumerators,* Cryptogr. Commun., **9** (2017), 133-149.

[27] Z. Zhou and C. Ding, *A class of three-weight cyclic codes,* Finite Fields Appl., **25** (2014), no. 11, 79-93.
[28] Z. Heng and Q. Yue, *A class of binary codes with at most three weights,* IEEE Commun. Lett., **19** (2015), no. 9, 1488-1491.
[29] Z. Heng and Q. Yue, *Two classes of two-weight linear codes,* Finite Fields Appl., **38** (2016), 72-92.

Department of Mathematics
Chungnam National University
Daejon 305-764, Republic of Korea
E-mail: jhahn@cnu.ac.kr

Department of Mathematics
Chungnam University
Daejeon 305-764, Republic of Korea
E-mail: dska@cnu.ac.kr