Des. Codes Cryptogr. (2016) 81:153–168
DOI 10.1007/s10623-015-0136-9

Complete weight enumerators of some linear codes and their applications

Chengju Li[1] · Sunghan Bae[1] · Jaehyun Ahn[2] · Shudi Yang[3,4] · Zheng-An Yao[3]

Received: 11 June 2015 / Revised: 8 September 2015 / Accepted: 10 September 2015 /
Published online: 29 September 2015
© Springer Science+Business Media New York 2015

Abstract Recently, linear codes constructed from defining sets have been extensively studied. It was shown that the linear codes may have a few nonzero weights or be optimal if the defining sets are well chosen. The weight enumerators of these linear codes were also presented. In this paper, we investigate the complete weight enumerators of some linear codes constructed from the defining sets. As applications, we employ the explicit complete weight enumerators of the linear codes to construct constant composition codes and systematic authentication codes. A new class of optimal constant composition codes and three classes of asymptotically optimal systematic authentication codes are presented.

Keywords Complete weight enumerators · Linear codes · Exponential sums · Constant composition codes · Authentication codes

Communicated by C. Ding.

✉ Jaehyun Ahn
jhahn@cnu.ac.kr

Chengju Li
lichengju1987@163.com

Sunghan Bae
shbae@kaist.ac.kr

Shudi Yang
yangshd3@mail2.sysu.edu.cn

Zheng-An Yao
mcsyao@mail.sysu.edu.cn

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

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

3 Department of Mathematics, Sun Yat-sen University, Guangzhou 510275, People's Republic of China

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

Mathematics Subject Classification 94B05 · 11T71 · 11T23 · 94B60 · 94A62

1 Introduction

Let $\mathbb{F}_p$ be the finite field with p elements and let n be a positive integer, where p is an odd prime. 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.

Now we recall the definition of the complete weight enumerator of a code [38,39]. Suppose that the elements of $\mathbb{F}_p$ are $0, 1, \ldots, p-1$. The composition of a vector $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_p^n$ is defined to be $\mathrm{comp}(\mathbf{v}) = (t_0, t_1, \ldots, t_{p-1})$, where each $t_i = t_i(\mathbf{v})$ is the number of components $v_j (0 \le j \le n-1)$ of $\mathbf{v}$ that are equal to i. Clearly, we have

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

Definition 1.1 Let $\mathcal{C}$ be a code over $\mathbb{F}_p$ and let $A(t_0, t_1, \ldots, t_{p-1})$ be the number of codewords $\mathbf{c} \in \mathcal{C}$ with $\mathrm{comp}(\mathbf{c}) = (t_0, t_1, \ldots, t_{p-1})$. Then the complete weight enumerator of $\mathcal{C}$ is the polynomial

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

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

For binary linear codes, the complete weight enumerators are just their Hamming weight enumerators. It is not difficult to see that the Hamming weight enumerators, which have been extensively investigated, can follow from the complete weight enumerators. Constant composition codes whose complete weight enumerators have one term have been intensively studied and some families of optimal constant composition codes were presented [6,9,17]. Moreover, the complete weight enumerators are applied to study the Walsh transform of monomial functions over finite fields [27] and compute the deception probabilities of certain authentication codes constructed from linear codes [16,20]. Hence it is interesting to determine the complete weight enumerators of linear codes.

The complete weight enumerators of Reed-Solomon codes were studied by Blake and Kith [4,29]. Kuzmin and Nechaev [30,31] presented the complete weight enumerators of the generalized Kerdock code and related linear codes over Galois rings. The complete weight enumerators of cyclic codes or linear codes over finite fields were studied in [1,2,17,32,34]. In this paper, we shall employ exponential sums and Galois theory to investigate the complete weight enumerators of linear codes constructed from defining sets.

Let $D = \{d_0, d_1, \ldots, d_{n-1}\} \subset \mathbb{F}_q$, where $q = p^m$ for a positive integer m. Let Tr_m denote the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_p$. Then a linear code of length n over $\mathbb{F}_p$ can be defined by

$$\mathcal{C}_D = \{\mathbf{c}(x) = (\mathrm{Tr}_m(xd_0), \mathrm{Tr}_m(xd_1), \ldots, \mathrm{Tr}_m(xd_{n-1})) : x \in \mathbb{F}_q\}. \tag{1.1}$$

We call D the defining set of the code $\mathcal{C}_D$. By definition, the dimension of $\mathcal{C}_D$ is at most m. In fact, the dimension of the linear code $\mathcal{C}_D$ is equal to the dimension of the $\mathbb{F}_p$-linear subspace of $\mathbb{F}_q$ spanned by D [15].

This construction was proposed by Ding et al. [10–15,21] to present linear codes with a few nonzero weights and optimal codes when the sets D are well chosen. The weight enumerators of these linear codes were also presented. The objective of this paper was to investigate the complete weight enumerators of linear codes $\mathcal{C}_D$ in the following three cases:

(1) D is a skew Hadamard difference set or Paley type partial difference set in $\mathbb{F}_q$;
(2) $D = \{f(x) : x \in \mathbb{F}_q\} \setminus \{0\}$, where $f(x)$ is a quadratic form over $\mathbb{F}_q$;
(3) $D = \{x \in \mathbb{F}_q^* : \mathrm{Tr}_s(x^{p^s+1}) = 0\}$, where $m = 2s$ is an even integer.

It should be remarked that the weight enumerators of $\mathcal{C}_D$ had been determined [12,14] for Cases (1) and (2). In this paper, the complete weight enumerators of the linear codes $\mathcal{C}_D$ can be explicitly presented in these three cases by using exponential sums and Galois theory. Moreover, we employ the complete weight enumerators to construct constant composition codes which are subcodes of the linear codes $\mathcal{C}_D$. Motivated by the original ideas in [16,20], we also present some authentication codes with new parameters. A new class of optimal constant composition codes and three classes of asymptotically optimal systematic authentication codes are presented.

The rest of this paper is organized as follows. In Sect. 2, we present some preliminaries which are very useful to get our results. In Sects. 3, 4, and 5, we investigate the complete weight enumerators of the linear codes in the three cases. In Sect. 6, we employ the complete weight enumerators of the linear codes to construct constant composition codes and systematic authentication codes. In Sect. 7, we conclude this paper.

2 Preliminaries

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

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

where $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a primitive p-th root of unity and Tr_m denotes the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_p$. 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 [33] 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

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

In general, the explicit determination of Gauss sums is a difficult problem. However, they can be explicitly evaluated in a few cases [3,33,45]. We state a result on the quadratic Gauss sums here.

Lemma 2.1 [3,33] *Suppose that $q = p^m$ and η is the quadratic multiplicative 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 $p^* = \left(\frac{-1}{p}\right)p = (-1)^{\frac{p-1}{2}}p$.

A polynomial f over $\mathbb{F}_q$ is called a quadratic form if

$$f(x) = \sum_{i\in I}\sum_{j\in J} a_{ij}x^{p^i+p^j},$$

where $a_{ij} \in \mathbb{F}_q$ and $I, J \subset \{0, 1, 2, \ldots, m-1\}$. The rank of the quadratic form $f(x)$ over $\mathbb{F}_q$ is defined to be the codimension of the $\mathbb{F}_p$-vector space

$$V = \left\{x \in \mathbb{F}_q : f(x+z) - f(x) - f(z) = 0 \text{ for all } z \in \mathbb{F}_q\right\}.$$

That is, $|V| = p^{m-r}$, where r is the rank of $f(x)$.

Lemma 2.2 [23,33] *Let $f(x)$ be a quadratic form of rank r over $\mathbb{F}_q$. Then we have*

$$\sum_{x\in\mathbb{F}_q}\psi(f(x)) = \begin{cases} \pm p^{m-\frac{r}{2}}, & \text{if } p \equiv 1 \pmod 4; \\ \pm(\sqrt{-1})^r p^{m-\frac{r}{2}}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

The following exponential sums will be employed later.

Lemma 2.3 [7] *Let $m = 2s$ be an even integer. Assume that $a \in \mathbb{F}_{p^s}$ and $b \in \mathbb{F}_{p^m}$. Then*

$$\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_s(ax^{p^s+1})+\mathrm{Tr}_m(bx)} = -p^s\zeta_p^{-\mathrm{Tr}_s(\frac{bp^s+1}{a})}.$$

We will also use some well-known results on the Galois group of the cyclotomic field $\mathbb{Q}(\zeta_p)$ [28]. The Galois group of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ is $\{\sigma_j : 1 \leq j \leq p-1\}$, where the automorphism σ_j of $\mathbb{Q}(\zeta_p)$ is defined by

$$\sigma_j(\zeta_p) = \zeta_p^j.$$

Moreover, the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Q}(\sqrt{p^*})$, where $p^* = \left(\frac{-1}{p}\right)p$. By Lemma 2.1, we have

$$\sqrt{p^*} = \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta_p^i.$$

Then

$$\sigma_j(\sqrt{p^*}) = \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta_p^{ij} = \left(\frac{j}{p}\right)\sum_{i=1}^{p-1}\left(\frac{ij}{p}\right)\zeta_p^{ij} = \left(\frac{j}{p}\right)\sqrt{p^*}. \tag{2.1}$$

3 The first case

In this section, we present the complete weight enumerator of the linear code $\mathcal{C}_D$ when D is a skew Hadamard difference set or Paley type partial difference set in $\mathbb{F}_q$.

We assume that the reader is familiar with the basic theory of difference sets. A difference set D in $\mathbb{F}_q$ is called skew Hadamard if $\mathbb{F}_q$ is the disjoint union of D, $-D$, and $\{0\}$, where $-D = \{-d : d \in D\}$. A classical example of skew Hadamard difference sets is the Paley difference set consisting of the nonzero squares of $\mathbb{F}_q$ when $q \equiv 3 \pmod 4$. In fact, if D is a skew Hadamard difference set in $\mathbb{F}_q$, then we must have $q \equiv 3 \pmod 4$. A subset D of $\mathbb{F}_q$, $0 \notin D$, is called a Paley type partial difference sets if D is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ partial difference sets. It is clear that $q \equiv 1 \pmod 4$ if D is a Paley type partial difference sets in $\mathbb{F}_q$. For more details on the skew Hadamard difference sets and the Paley type partial difference sets, we refer the readers to [11,37,43].

There is a well-known lemma in the theory of difference sets [24]. Below we denote $\sum_{d \in D} \psi(d)$ by $\psi(D)$ and $\{xd : d \in D\}$ by xD for simplicity.

Lemma 3.1 [24] *Let D be a subset of $\mathbb{F}_q$ with $|D| = \frac{q-1}{2}$.*

(1) *If $D \bigcap -D = \emptyset$ and $0 \notin D$, then D is a skew Hadamard difference set in $\mathbb{F}_q$ if and only if*

$$\psi_a(D) = \frac{-1 \pm \sqrt{-q}}{2} \text{ for all } a \in \mathbb{F}_q^*.$$

(2) *If $D = -D$ and $0 \notin D$, then D is a Paley type partial difference set in $\mathbb{F}_q$ if and only if*

$$\psi_a(D) = \frac{-1 \pm \sqrt{q}}{2} \text{ for all } a \in \mathbb{F}_q^*.$$

Let $D = \{d_0, d_1, \ldots, d_{n-1}\}$, where $n = \frac{q-1}{2}$. For a codeword $\mathbf{c}(x)$ of $\mathcal{C}_D$, $x \in \mathbb{F}_q^*$, and $c \in \mathbb{F}_p$, let $N_x(c)$ denote the number of components $\mathrm{Tr}_m(xd_i)$ of $\mathbf{c}(x)$ which are equal to c, i.e.,

$$\begin{aligned} N_x(c) &= |\{0 \le i \le n-1 : \mathrm{Tr}_m(xd_i) = c\}| \\ &= |\{0 \le i \le n-1 : \mathrm{Tr}_m(xd_i) - c = 0\}|. \end{aligned}$$

By the orthogonal property of additive characters we have

$$\begin{aligned} N_x(c) &= \sum_{i=0}^{n-1} \frac{1}{p} \sum_{y \in \mathbb{F}_p} \zeta_p^{y(\mathrm{Tr}_m(xd_i)-c)} \\ &= \frac{n}{p} + \frac{1}{p} \sum_{i=0}^{n-1} \sum_{j=1}^{p-1} \sigma_j(\zeta_p^{\mathrm{Tr}_m(xd_i)-c}) \\ &= \frac{n}{p} + \frac{1}{p} \sum_{j=1}^{p-1} \sigma_j(\zeta_p^{-c}) \sum_{i=0}^{n-1} \sigma_j(\zeta_p^{\mathrm{Tr}_m(xd_i)}) \end{aligned}$$

$$= \frac{n}{p} + \frac{1}{p}\sum_{j=1}^{p-1}\sigma_j(\zeta_p^{-c})\sigma_j\left(\sum_{i=0}^{n-1}\zeta_p^{\mathrm{Tr}_m(xd_i)}\right)$$

$$= \frac{n}{p} + \frac{1}{p}\sum_{j=1}^{p-1}\sigma_j(\zeta_p^{-c})\sigma_j(\psi(xD)), \tag{3.1}$$

where $\sigma_j (1 \le j \le p-1)$ is the automorphism of $\mathbb{Q}(\zeta_p)$ defined by $\sigma_j(\zeta_p) = \zeta_p^j$.

Theorem 3.2 *Let $\mathcal{C}_D$ be the linear code defined by (1.1).*

(1) *Suppose that D is a skew Hadamard difference set in $\mathbb{F}_q$. Then $\mathcal{C}_D$ is a $[\frac{p^m-1}{2}, m]$ linear code and its complete weight enumerator is*

$$z_0^{\frac{p^m-1}{2}} + \frac{p^m-1}{2} z_0^{\frac{p^{m-1}-1}{2}} \prod_{\substack{c\in\mathbb{F}_p^* \\ (\frac{c}{p})=1}} z_c^{\frac{p^{m-1}+p^{\frac{m-1}{2}}}{2}} \prod_{\substack{c\in\mathbb{F}_p^* \\ (\frac{c}{p})=-1}} z_c^{\frac{p^{m-1}-p^{\frac{m-1}{2}}}{2}}$$
$$+ \frac{p^m-1}{2} z_0^{\frac{p^{m-1}-1}{2}} \prod_{\substack{c\in\mathbb{F}_p^* \\ (\frac{c}{p})=1}} z_c^{\frac{p^{m-1}-p^{\frac{m-1}{2}}}{2}} \prod_{\substack{c\in\mathbb{F}_p^* \\ (\frac{c}{p})=-1}} z_c^{\frac{p^{m-1}+p^{\frac{m-1}{2}}}{2}}. \tag{3.2}$$

(2) *Suppose that D is a Paley type partial difference set in $\mathbb{F}_q$. Then $\mathcal{C}_D$ is also a $[\frac{p^m-1}{2}, m]$ linear code. If m is odd, then the complete weight enumerator of $\mathcal{C}_D$ is given by (3.2). If m is even, then the complete weight enumerator of $\mathcal{C}_D$ is*

$$z_0^{\frac{p^m-1}{2}} + \frac{p^m-1}{2} z_0^{\frac{(p^{\frac{m}{2}}-1)(p^{\frac{m}{2}-1}+1)}{2}} (z_1 z_2 \dots z_{p-1})^{\frac{p^{m-1}-p^{\frac{m}{2}-1}}{2}}$$
$$+ \frac{p^m-1}{2} z_0^{\frac{(p^{\frac{m}{2}}+1)(p^{\frac{m}{2}-1}-1)}{2}} (z_1 z_2 \dots z_{p-1})^{\frac{p^{m-1}+p^{\frac{m}{2}-1}}{2}}.$$

Proof (1) If D is a skew Hadamard difference set in $\mathbb{F}_q$, then $q \equiv 3 \pmod 4$. Thus $p \equiv 3 \pmod 4$ and m is odd. By Lemma 3.1, we have

$$\psi(xD) = \frac{-1 \pm (\sqrt{p*})^m}{2} \text{ for all } x \in \mathbb{F}_q^*,$$

where $p^* = \left(\frac{-1}{p}\right)p = -p$. If $c \in \mathbb{F}_p^*$, then

$$N_x(c) = \frac{n}{p} + \frac{1}{p}\sum_{j=1}^{p-1}\sigma_j(\zeta_p^{-c})\sigma_j\left(\frac{-1 \pm (\sqrt{p*})^m}{2}\right)$$
$$= \frac{n}{p} + \frac{1}{p}\sum_{j=1}^{p-1}\zeta_p^{-jc}\frac{-1 \pm (\frac{j}{p})(\sqrt{p*})^m}{2} \qquad \text{(by (2.1))}$$
$$= \frac{n}{p} + \frac{1}{2p}\left(-\sum_{j=1}^{p-1}\zeta_p^{-jc} \pm \sum_{j=1}^{p-1}\zeta_p^{-jc}\left(\frac{j}{p}\right)(\sqrt{p*})^m\right)$$

$$= \frac{n}{p} + \frac{1}{2p}\left(1 \pm (\sqrt{p*})^m \left(\frac{-c}{p}\right)\sqrt{p*}\right) \qquad \text{(by Lemma 2.1)}$$
$$= \frac{p^{m-1} \pm (\frac{c}{p})(-p)^{\frac{m-1}{2}}}{2}.$$

Now we are going to determine the frequency of each composition. Denote

$$n^+ = \left| \left\{ x \in \mathbb{F}_q^* : \psi(xD) = \frac{-1+\sqrt{-q}}{2} \right\} \right|,$$
$$n^- = \left| \left\{ x \in \mathbb{F}_q^* : \psi(xD) = \frac{-1-\sqrt{-q}}{2} \right\} \right|.$$

It is easy to check that

$$\sum_{x \in \mathbb{F}_q^*} \psi(xD) = \sum_{d \in D} \sum_{x \in \mathbb{F}_q^*} \psi(xd) = -|D|.$$

Thus we have

$$n^+ \cdot \frac{-1+\sqrt{-q}}{2} + n^- \cdot \frac{-1-\sqrt{-q}}{2} = -|D|.$$

Note that $n^+ + n^- = q-1$ and $N_x(0) = n - \sum_{c \in \mathbb{F}_p^*} N_x(c)$. Then $n^+ = n^- = \frac{q-1}{2}$ and we get the complete weight enumerator of $\mathcal{C}_D$.

(2) The proof of (2) is very similar to that of (1) and we omit the details. □

It should be remarked that the code $\mathcal{C}_D$ and its weight enumerator had been presented in [12] when D is a skew Hadamard difference set or Paley type partial difference set. By Theorem 3.2, we can also obtain the weight enumerator of the code $\mathcal{C}_D$, which conforms to the results presented in [12].

The complete weight enumerator of the linear code $\mathcal{C}_D$ has been presented if D is a skew Hadamard difference set or Paley type partial difference set. Let α be a primitive element of $\mathbb{F}_q$ and let $\mathcal{C}$ be an irreducible cyclic code with check polynomial $h(x)$, where $h(x)$ is the minimal polynomial of α^{-2} over $\mathbb{F}_p$. In particular, if $D = \langle \alpha^2 \rangle$, then D is a skew Hadamard difference set or Paley type partial difference set. The complete weight enumerators of the linear codes $\mathcal{C}_D$ are the same as those of the irreducible cyclic codes $\mathcal{C}$ which were presented in [2,32]. Thus Theorem 3.2 generalizes the results of [2,32] to some extent.

If D is a multiplicative subgroup in $\mathbb{F}_q^*$, then determining the complete weight enumerators of the linear codes $\mathcal{C}_D$ is equivalent to determining the complete weight enumerators of irreducible cyclic codes which were given in [32], so we will not consider them here. The weight enumerators of the linear codes $\mathcal{C}_D$ were investigated in [10,15,21] for more general D which may not be a multiplicative subgroup of $\mathbb{F}_q^*$.

4 The second case

In this section, we present the complete weight enumerator of the linear code $\mathcal{C}_D$ when $D = \{f(x) : x \in \mathbb{F}_q\} \setminus \{0\}$, where $f(x)$ is a quadratic form over $\mathbb{F}_q$. We always assume that the quadratic form f satisfies the following two conditions:

(I) $f(0) = 0$ and $f(x) \neq 0$ for all $x \in \mathbb{F}_q^*$;

(II) f is e-to-1 on $x \in \mathbb{F}_q^*$, i.e., $f(x) = u$ has either e solutions $x \in \mathbb{F}_q^*$ or no solution for each $u \in \mathbb{F}_q^*$, where e is a positive integer.

There are some quadratic forms $f(x)$ over $\mathbb{F}_{p^m}$ satisfying Conditions (I) and (II).

Example 4.1 (1) $f(x) = x^{p^l+1}$ is a quadratic form over $\mathbb{F}_{p^m}$, where $l \geq 0$ is an integer. In this case, $e = \gcd(p^l + 1, p^m - 1)$.

(2) $f(x) = x^{10} - ux^6 - u^2x^2$ is a quadratic form over $\mathbb{F}_{3^m}$, where $u \in \mathbb{F}_{3^m}$ and m is odd. In this case, $e = 2$.

Let $D = \{d_0, d_1, \ldots, d_{n-1}\}$, where $n = \frac{q-1}{e}$. For a codeword $\mathbf{c}(x)$ of $\mathcal{C}_D$, $x \in \mathbb{F}_q^*$, and $c \in \mathbb{F}_p^*$, let $N_x(c)$ denote the number of components $\mathrm{Tr}_m(xd_i)$ of $\mathbf{c}(x)$ which are equal to c. By (3.1) we similarly have

$$\begin{aligned} N_x(c) &= \frac{n}{p} + \frac{1}{p}\sum_{j=1}^{p-1} \sigma_j(\zeta_p^{-c})\sigma_j(\psi(xD)) \\ &= \frac{n}{p} + \frac{1}{p}\sum_{j=1}^{p-1} \sigma_j(\zeta_p^{-c})\sigma_j\left(\frac{1}{e}\sum_{z\in\mathbb{F}_q^*} \psi(xf(z))\right) \\ &= \frac{n}{p} + \frac{1}{ep}\sum_{j=1}^{p-1} \sigma_j(\zeta_p^{-c})\sigma_j\left(-1 + \sum_{z\in\mathbb{F}_q} \psi(xf(z))\right), \end{aligned}$$

where $\sigma_j (1 \leq j \leq p-1)$ is the automorphism of $\mathbb{Q}(\zeta_p)$ defined by $\sigma_j(\zeta_p) = \zeta_p^j$.

In general, the dimension k of $\mathcal{C}_D$ is equal to m. When $e \geq \sqrt{q} + 1$, k may be less than m. For example, if m is an even integer and $f(x) = x^{p^{\frac{m}{2}}+1}$, then we have $e = \sqrt{q} + 1$ and the dimension of the linear code $\mathcal{C}_D$ is $\frac{m}{2}$. However, the complete weight enumerator of $\mathcal{C}_D$ can be similarly given by replacing the frequencies. Without loss of generality, we assume that the dimension of $\mathcal{C}_D$ is m in this section.

Theorem 4.2 *Let $\mathcal{C}_D$ be the linear code defined by (1.1) and $D = \{f(x) : x \in \mathbb{F}_q\} \setminus \{0\}$, where $f(x)$ is a quadratic form over $\mathbb{F}_q$ of rank r satisfying Conditions (I) and (II).*

(1) *If r is odd, then the complete weight enumerator of $\mathcal{C}_D$ is*

$$\begin{aligned} &z_0^{\frac{p^m-1}{e}} + \frac{p^m-1}{2} z_0^{\frac{p^{m-1}-1}{e}} \prod_{\substack{c\in\mathbb{F}_p^* \\ (\frac{c}{p})=1}} z_c^{\frac{p^{m-1}+p^{m-\frac{r+1}{2}}}{e}} \prod_{\substack{c\in\mathbb{F}_p^* \\ (\frac{c}{p})=-1}} z_c^{\frac{p^{m-1}-p^{m-\frac{r+1}{2}}}{e}} \\ &\quad + \frac{p^m-1}{2} z_0^{\frac{p^{m-1}-1}{e}} \prod_{\substack{c\in\mathbb{F}_p^* \\ (\frac{c}{p})=1}} z_c^{\frac{p^{m-1}-p^{m-\frac{r+1}{2}}}{e}} \prod_{\substack{c\in\mathbb{F}_p^* \\ (\frac{c}{p})=-1}} z_c^{\frac{p^{m-1}+p^{m-\frac{r+1}{2}}}{e}}. \end{aligned}$$

(2) *If r is even, then the complete weight enumerator of $\mathcal{C}_D$ is*

$$\begin{aligned} &z_0^{\frac{p^m-1}{e}} + \frac{p^m-1}{2} z_0^{\frac{p^{m-1}+p^{m-\frac{r}{2}}-p^{m-1-\frac{r}{2}}-1}{e}} (z_1 z_2 \ldots z_{p-1})^{\frac{p^{m-1}-p^{m-1-\frac{r}{2}}}{e}} \\ &\quad + \frac{p^m-1}{2} z_0^{\frac{p^{m-1}-p^{m-\frac{r}{2}}+p^{m-1-\frac{r}{2}}-1}{e}} (z_1 z_2 \ldots z_{p-1})^{\frac{p^{m-1}+p^{m-1-\frac{r}{2}}}{e}}. \end{aligned}$$

Proof (1) If r is odd, then by Lemma 2.2 we have

$$\sum_{z\in\mathbb{F}_q}\psi(xf(z)) = \pm p^{m-\frac{r+1}{2}}\sqrt{p^*} \text{ for all } x\in\mathbb{F}_q^*,$$

where $p^* = \left(\frac{-1}{p}\right)p$. If $c\in\mathbb{F}_p^*$, then

$$\begin{aligned}
N_x(c) &= \frac{n}{p} + \frac{1}{ep}\sum_{j=1}^{p-1}\sigma_j(\zeta_p^{-c})\sigma_j(-1\pm p^{m-\frac{r+1}{2}}\sqrt{p^*}) \\
&= \frac{n}{p} + \frac{1}{ep}\sum_{j=1}^{p-1}\zeta_p^{-jc}\left(-1\pm p^{m-\frac{r+1}{2}}\left(\frac{j}{p}\right)\sqrt{p^*}\right) \qquad \text{(by (2.1))} \\
&= \frac{n}{p} + \frac{1}{ep}\left(-\sum_{j=1}^{p-1}\zeta_p^{-jc} \pm p^{m-\frac{r+1}{2}}\sqrt{p^*}\sum_{j=1}^{p-1}\zeta_p^{-jc}\left(\frac{j}{p}\right)\right) \\
&= \frac{n}{p} + \frac{1}{ep}\left(1\pm p^{m-\frac{r+1}{2}}\sqrt{p^*}\left(\frac{-c}{p}\right)\sqrt{p^*}\right) \qquad \text{(by Lemma 2.1)} \\
&= \frac{p^{m-1}\pm(\frac{c}{p})p^{m-\frac{r+1}{2}}}{e}.
\end{aligned}$$

Now we are going to determine the frequency of each composition. Denote

$$\begin{aligned}
n^+ &= \left|\left\{x\in\mathbb{F}_q^* : \sum_{z\in\mathbb{F}_q}\psi(xf(z)) = p^{m-\frac{r+1}{2}}\sqrt{p^*}\right\}\right|, \\
n^- &= \left|\left\{x\in\mathbb{F}_q^* : \sum_{z\in\mathbb{F}_q}\psi(xf(z)) = -p^{m-\frac{r+1}{2}}\sqrt{p^*}\right\}\right|.
\end{aligned}$$

By Condition (I) we have

$$\sum_{x\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q}\psi(xf(z)) = q-1+(q-1)\cdot(-1) = 0.$$

Thus

$$n^+\cdot p^{m-\frac{r+1}{2}} - n^-\cdot p^{m-\frac{r+1}{2}} = 0.$$

Note that $n^+ + n^- = q-1$ and $N_x(0) = n - \sum_{c\in\mathbb{F}_p^*}N_x(c)$. Then $n^+ = n^- = \frac{q-1}{2}$ and we get the complete weight enumerator of $\mathcal{C}_D$.

(2) If r is even, then by Lemma 2.2 we have

$$\sum_{z\in\mathbb{F}_q}\psi(xf(z)) = \pm p^{m-\frac{r}{2}} \in \mathbb{Q} \text{ for all } x\in\mathbb{F}_q^*.$$

Thus $\sigma_j(\sum_{z\in\mathbb{F}_q}\psi(xf(z))) = \pm p^{m-\frac{r}{2}}$ for all $j = 1,2,\ldots,p-1$. The remainder of the proof is very similar to that of (1) and we omit it here. □

We remark that the weight enumerator of $\mathcal{C}_D$ has been presented in [12]. By Theorem 4.2, we can also obtain the weight enumerator of the code $\mathcal{C}_D$, which conforms to the results presented in [12].

5 The third case

In this section, we present the complete weight enumerator of the linear code $\mathcal{C}_D$ when $D = \{z \in \mathbb{F}_{p^m}^* : \mathrm{Tr}_s(z^{p^s+1}) = 0\}$, where m is even and $m = 2s$.

We begin to determine the length of the linear code $\mathcal{C}_D$. By the orthogonal property of additive characters we have

$$\begin{aligned} n &= |\{z \in \mathbb{F}_q^* : \mathrm{Tr}_s(z^{p^s+1}) = 0\}| \\ &= \sum_{z\in\mathbb{F}_q^*} \frac{1}{p} \sum_{y\in\mathbb{F}_p} \zeta_p^{y\mathrm{Tr}_s(z^{p^s+1})} \\ &= \frac{q-1}{p} - \frac{p-1}{p} + \frac{1}{p} \sum_{y\in\mathbb{F}_p^*} \sum_{z\in\mathbb{F}_q} \zeta_p^{y\mathrm{Tr}_s(z^{p^s+1})} \\ &= \frac{q-p}{p} + \frac{1}{p} \sum_{j=1}^{p-1} \sigma_j \left(\sum_{z\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_s(z^{p^s+1})} \right) \\ &= \frac{q-p}{p} + \frac{1}{p} \sum_{j=1}^{p-1} \sigma_j(-p^s) \qquad \text{(by Lemma 2.3)} \\ &= (p^s+1)(p^{s-1}-1), \end{aligned} \tag{5.1}$$

where $\sigma_j (1 \le j \le p-1)$ is the automorphism of $\mathbb{Q}(\zeta_p)$ defined by $\sigma_j(\zeta_p) = \zeta_p^j$.

For a codeword $\mathbf{c}(x)$ of $\mathcal{C}_D$, $x \in \mathbb{F}_q^*$, and $c \in \mathbb{F}_p^*$, let $N_x(c)$ denote the number of components $\mathrm{Tr}_m(xd)$ of $\mathbf{c}(x)$ which are equal to c when d runs over D. Then

$$\begin{aligned} N_x(c) &= |\{z \in \mathbb{F}_q^* : \mathrm{Tr}_s(z^{p^s+1}) = 0 \text{ and } \mathrm{Tr}_m(xz) = c\}| \\ &= \sum_{z\in\mathbb{F}_q^*} \left(\frac{1}{p} \sum_{y_1\in\mathbb{F}_p} \zeta_p^{y_1 \mathrm{Tr}_s(z^{p^s+1})} \right) \left(\frac{1}{p} \sum_{y_2\in\mathbb{F}_p} \zeta_p^{y_2(\mathrm{Tr}_m(xz)-c)} \right) \\ &= \frac{q-1}{p^2} + \frac{1}{p^2} \sum_{y_1\in\mathbb{F}_p^*} \sum_{z\in\mathbb{F}_q^*} \zeta_p^{y_1\mathrm{Tr}_s(z^{p^s+1})} + \frac{1}{p^2} \sum_{y_2\in\mathbb{F}_p^*} \sum_{z\in\mathbb{F}_q^*} \zeta_p^{y_2(\mathrm{Tr}_m(xz)-c)} \\ &\quad + \frac{1}{p^2} \sum_{y_1\in\mathbb{F}_p^*} \sum_{y_2\in\mathbb{F}_p^*} \sum_{z\in\mathbb{F}_q^*} \zeta_p^{y_1\mathrm{Tr}_s(z^{p^s+1})+y_2(\mathrm{Tr}_m(xz)-c)}. \end{aligned} \tag{5.2}$$

Theorem 5.1 *Let $\mathcal{C}_D$ be the linear code defined by (1.1) and $D = \{z \in \mathbb{F}_{p^m}^* : \mathrm{Tr}_s(z^{p^s+1}) = 0\}$, where m is even and $m = 2s$ for an integer $s > 1$. Then $\mathcal{C}_D$ is a $[(p^s+1)(p^{s-1}-1), m]$ linear code and its complete weight enumerator is*

$$\begin{aligned} &z_0^{(p^s+1)(p^{s-1}-1)} + (p^s+1)(p^{s-1}-1) z_0^{p^{m-2}-p^s+p^{s-1}-1} (z_1 z_2 \dots z_{p-1})^{p^{m-2}} \\ &\quad + (p^s+1)(p^s-p^{s-1}) z_0^{p^{m-2}-1} (z_1 z_2 \dots z_{p-1})^{p^{m-2}-p^{s-1}}. \end{aligned}$$

Proof Note that $n = (p^s+1)(p^{s-1}-1) > p^s+1$. Then the dimension of $\mathcal{C}_D$ is m. By (5.1) we have

$$\sum_{y_1\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_q^*}\zeta_p^{y_1\mathrm{Tr}_s(z^{p^s+1})} = -(p-1)(p^s+1).$$

It is easily checked that

$$\sum_{y_2\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_q^*}\zeta_p^{y_2(\mathrm{Tr}_m(xz)-c)} = \sum_{j=1}^{p-1}\zeta_p^{-jc}\sigma_j\left(\sum_{z\in\mathbb{F}_q^*}\zeta_p^{\mathrm{Tr}_m(xz)}\right) = 1.$$

We are now ready to compute the third sum of (5.2).

$$\begin{aligned}
&\sum_{y_1\in\mathbb{F}_p^*}\sum_{y_2\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_q^*}\zeta_p^{y_1\mathrm{Tr}_s(z^{p^s+1})+y_2(\mathrm{Tr}_m(xz)-c)}\\
&= \sum_{y_2\in\mathbb{F}_p^*}\zeta_p^{-y_2c}\sum_{y_1\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_q^*}\zeta_p^{\mathrm{Tr}_s(y_1z^{p^s+1})+\mathrm{Tr}_m(y_2xz)}\\
&= \sum_{y_2\in\mathbb{F}_p^*}\zeta_p^{-y_2c}\sum_{y_1\in\mathbb{F}_p^*}\left(-1+\sum_{z\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_s(y_1z^{p^s+1})+\mathrm{Tr}_m(y_2xz)}\right)\\
&= \sum_{y_2\in\mathbb{F}_p^*}\zeta_p^{-y_2c}\left(-(p-1)-p^s\sum_{y_1\in\mathbb{F}_p^*}\zeta_p^{-\mathrm{Tr}_s(\frac{(y_2x)^{p^s+1}}{y_1})}\right) \qquad \text{(by Lemma 2.3)}\\
&= -(p-1)\sum_{y_2\in\mathbb{F}_p^*}\zeta_p^{-y_2c} - p^s\sum_{y_2\in\mathbb{F}_p^*}\zeta_p^{-y_2c}\sum_{y_1\in\mathbb{F}_p^*}\zeta_p^{-y_1y_2^2\mathrm{Tr}_s(x^{p^s+1})}\\
&= \begin{cases} p-1-p^s(p-1)\sum\limits_{y_2\in\mathbb{F}_p^*}\zeta_p^{-y_2c} = (p-1)(p^s+1), & \text{if } \mathrm{Tr}_s(x^{p^s+1})=0;\\ p-1+p^s\sum\limits_{y_2\in\mathbb{F}_p^*}\zeta_p^{-y_2c} = p-1-p^s, & \text{if } \mathrm{Tr}_s(x^{p^s+1})\neq 0. \end{cases}
\end{aligned}$$

Then, for $c\in\mathbb{F}_p^*$, by (5.2) we have

$$N_x(c) = \begin{cases} p^{m-2}, & \text{if } \mathrm{Tr}_s(x^{p^s+1})=0;\\ p^{m-2}-p^{s-1}, & \text{if } \mathrm{Tr}_s(x^{p^s+1})\neq 0. \end{cases}$$

Now we are going to determine the frequency of each composition. It is well-known that the norm function $N:\mathbb{F}_{p^{2s}}\to\mathbb{F}_{p^s}$ defined by $N(x)=x^{p^s+1}$ is (p^s+1)-to-1 except for $N(0)=0$ and $\mathrm{Tr}_s:\mathbb{F}_{p^s}\to\mathbb{F}_p$ is p^{s-1}-to-1. Then

$$|\{x\in\mathbb{F}_{p^m}^* : \mathrm{Tr}_s(x^{p^s+1})=0\}| = (p^s+1)|\{x\in\mathbb{F}_{p^s}^* : \mathrm{Tr}_s(x)=0\}| = (p^s+1)(p^{s-1}-1)$$

and

$$\left|\left\{x\in\mathbb{F}_{p^m}^* : \mathrm{Tr}_s(x^{p^s+1})\neq 0\right\}\right| = (p^s+1)(p^s-p^{s-1}).$$

Therefore, we can get the complete weight enumerator of $\mathcal{C}_D$ and this completes the proof. □

From Theorem 5.1, we can see that the values of $N_x(c)$ are independent of $c\in\mathbb{F}_p^*$. In addition, the weight enumerator of $\mathcal{C}_D$ can be determined and $\mathcal{C}_D$ is a two-weight linear code.

It is clear that Lemma 2.3 plays a key role in the proof of Theorem 5.1. In fact, the exponential sums determined by Coulter [7] are more general. It will be nice if the complete weight enumerators of more linear codes $\mathcal{C}_D$ can be given by using the general exponential sums.

6 Applications

In this section, we employ the complete weight enumerators of the linear codes $\mathcal{C}_D$ to construct constant composition codes and systematic authentication codes.

6.1 Constant composition codes

Let $S = \{s_0, s_1, \ldots, s_{p-1}\}$ be an alphabet of size p, where p is a positive integer (not necessarily a prime). An $(n, M, d, (t_0, t_1, \ldots, t_{p-1}), p)$ constant composition code over S is a subset $\mathcal{C} \subset S^n$ of size M and minimum Hamming distance d such that each codeword has the same composition $(t_0, t_1, \ldots, t_{p-1})$. Thus the complete weight enumerator of the constant composition code has only one term.

The constant composition codes have many applications in communications engineering [6,40]. Many elegant methods are proposed to construct constant composition codes with excellent parameters in recent years [5,6,8,9,16,18,19,22,25,26,34–36,44]. The LFVC bound of constant composition codes is described in the following lemma.

Lemma 6.1 *[36] If* $nd - n^2 + (t_0^2 + t_1^2 + \cdots + t_{p-1}^2) > 0$, *then*

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

Now we begin to construct several constant composition codes which are subcodes of the linear codes $\mathcal{C}_D$. A new class of optimal constant composition codes with respect to the LFVC bound are presented. In fact, every term of the complete weight enumerators gives a constant composition code.

Let $\mathcal{C}_D$ be a linear code defined by (1.1) and $D = \{f(x) : x \in \mathbb{F}_q\} \setminus \{0\}$, where $f(x)$ is a quadratic form of rank r over $\mathbb{F}_q$ satisfying Conditions (I) and (II). By Theorem 4.2, we can get the following constant composition codes $\mathcal{C}$ over $\mathbb{F}_p$ which contain a new class of optimal constant composition codes with respect to the LFVC bound.

Theorem 6.2 *Let p be an odd prime and m a positive integer. There exist the following $(n, M, d, (t_0, t_1, \ldots, t_{p-1}), p)$ constant composition codes $\mathcal{C}$.*

(1) $n = \frac{p^m-1}{e}$, $M = \frac{p^m-1}{2}$, $d = \frac{(p-1)p^{m-1}}{e}$, $t_0 = \frac{p^{m-1}-1}{e}$, $t_c = \frac{p^{m-1}+p^{\frac{m-1}{2}}}{e}$ *for* $\left(\frac{c}{p}\right) = 1$, *and* $t_c = \frac{p^{m-1}-p^{\frac{m-1}{2}}}{e}$ *for* $\left(\frac{c}{p}\right) = -1$, *where m is odd. This is an optimal constant composition code with respect to the LFVC bound.*

(2) $n = \frac{p^m-1}{e}$, $M = \frac{p^m-1}{2}$, $d = \frac{(p-1)(p^{m-1}-p^{m-1-\frac{r}{2}})}{e}$, $t_0 = \frac{p^{m-1}+p^{m-\frac{r}{2}}-p^{m-1-\frac{r}{2}}-1}{e}$, *and* $t_c = \frac{p^{m-1}-p^{m-1-\frac{r}{2}}}{e}$ *for $c \neq 0$, where r is even.*

(3) $n = \frac{p^m-1}{e}$, $M = \frac{p^m-1}{2}$, $d = \frac{(p-1)(p^{m-1}-p^{m-1-\frac{r}{2}})}{e}$, $t_0 = \frac{p^{m-1}-p^{m-\frac{r}{2}}+p^{m-1-\frac{r}{2}}-1}{e}$, *and* $t_c = \frac{p^{m-1}+p^{m-1-\frac{r}{2}}}{e}$ *for $c \neq 0$, where r is even.*

Proof We can immediately get (2) and (3), so we only need to prove (1). If r is odd, by Theorem 4.2, an $(n, M, d, (t_0, t_1, \ldots, t_{p-1}), p)$ constant composition code $\mathcal{C}$ over $\mathbb{F}_p$ can be given, where $n = \frac{p^m-1}{e}$, $M = \frac{p^m-1}{2}$, $d = \frac{(p-1)p^{m-1}}{e}$, $t_0 = \frac{p^{m-1}-1}{e}$, $t_c = \frac{p^{m-1}+p^{\frac{m-r+1}{2}}}{e}$ for $\left(\frac{c}{p}\right) = 1$, and $t_c = \frac{p^{m-1}-p^{\frac{m-r+1}{2}}}{e}$ for $\left(\frac{c}{p}\right) = -1$. In this case, we have $nd - n^2 + (t_0^2 + t_1^2 + \cdots + t_{p-1}^2) > 0$ and

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

Then

$$M = \frac{p^m - 1}{2} \leq \frac{p^m - 1}{p^{m-r} + 1}$$

by Lemma 6.1, so $p^{m-r} + 1 \leq 2$ and this leads to $m = r$. Thus we can get the desired conclusions and this completes the proof. □

By the proof of Theorem 6.2, if r is odd, then $m = r$ and the complete weight enumerator of the linear code $\mathcal{C}_D$ presented in Theorem 4.2 is

$$z_0^{\frac{p^m-1}{e}} + \frac{p^m-1}{2} z_0^{\frac{p^{m-1}-1}{e}} \prod_{\substack{c\in\mathbb{F}_p^* \\ (\frac{c}{p})=1}} z_c^{\frac{p^{m-1}+p^{\frac{m-1}{2}}}{e}} \prod_{\substack{c\in\mathbb{F}_p^* \\ (\frac{c}{p})=-1}} z_c^{\frac{p^{m-1}-p^{\frac{m-1}{2}}}{e}}$$
$$+ \frac{p^m-1}{2} z_0^{\frac{p^{m-1}-1}{e}} \prod_{\substack{c\in\mathbb{F}_p^* \\ (\frac{c}{p})=1}} z_c^{\frac{p^{m-1}-p^{\frac{m-1}{2}}}{e}} \prod_{\substack{c\in\mathbb{F}_p^* \\ (\frac{c}{p})=-1}} z_c^{\frac{p^{m-1}+p^{\frac{m-1}{2}}}{e}}.$$

Ding and Yin [17] presented a class of optimal constant composition codes with following parameters: $n = \frac{p^m-1}{2}$, $M = \frac{p^m-1}{2}$, $d = \frac{(p-1)p^{m-1}}{2}$, $t_0 = \frac{p^{m-1}-1}{2}$, $t_c = \frac{p^{m-1}+p^{\frac{m-1}{2}}}{2}$ for $\left(\frac{c}{p}\right) = 1$, and $t_c = \frac{p^{m-1}-p^{\frac{m-1}{2}}}{2}$ for $\left(\frac{c}{p}\right) = -1$, where m is odd. In addition, the known optimal constant composition codes were shown in a table [22]. Therefore, Theorem 6.2 generalizes the results of [17] and gives a new class of optimal constant composition codes.

If D is a skew Hadamard difference set or Paley type partial difference set in $\mathbb{F}_q$ and $\mathcal{C}_D$ is a linear code defined by (1.1), then the constant composition codes $\mathcal{C}$ over $\mathbb{F}_p$ which are subcodes of $\mathcal{C}_D$ can also be given by Theorem 3.2. In fact, the parameters of these codes are contained in Theorem 6.2 and we omit them here.

6.2 Systematic authentication codes

A systematic authentication code is a four-tuple $(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_\kappa : \kappa \in \mathcal{K}\})$, 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 $E_\kappa : \mathcal{S} \to \mathcal{T}$ is called an encoding rule. For more details on the authentication codes, we refer the readers to [16,20,42]. Below 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 bonds on P_I and P_S [16,41]:

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

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

Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_p$ and let $\mathbf{c}_i = (c_{i,0}, c_{i,1}, \ldots, c_{i,n-1})$ be a codeword of $\mathcal{C}$, $0 \le i \le p^k - 1$. Define a systematic authentication code as follows:

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_\kappa : \kappa \in \mathcal{K}\}) = (\mathbb{Z}_{p^k}, \mathbb{F}_p, \mathbb{Z}_n \times \mathbb{F}_p, \{E_\kappa : \kappa \in \mathcal{K}\}), \tag{6.1}$$

where $E_\kappa(s) = c_{s,\kappa_1} + \kappa_2$ for any $s \in \mathcal{S}$ and $\kappa = (\kappa_1, \kappa_2) \in \mathcal{K}$.

Lemma 6.3 [20] *For the authentication code of* (6.1)*, we have*

$$P_I = \frac{1}{p} \text{ and } P_S = \max_{0 \neq \mathbf{c} \in \mathcal{C}} \max_{u \in \mathbb{F}_p} \frac{N_{\mathbf{c}}(u)}{n},$$

where $N_{\mathbf{c}}(u)$ denotes the number of components of $\mathbf{c}$ that are equal to u.

It is clear that the values of P_I and P_S are closely related to the complete weight enumerators of linear codes. There are three classes of authentication codes which are obtained from Theorems 3.2, 4.2, and 5.1 directly. By Lemma 6.3, we easily get the following result.

Theorem 6.4 *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, 4.2, and 5.1. Therefore, these authentication codes are asymptotically optimal.*

7 Concluding remarks

In this paper, we used exponential sums and Galois theory to investigate the complete weight enumerators of the linear codes constructed from the defining sets D in the three cases. Furthermore, the explicit complete weight enumerators of the linear codes were employed to construct constant composition codes and systematic authentication codes. We obtained a new class of optimal constant composition codes and three classes of asymptotically optimal systematic authentication codes.

Acknowledgments The authors are very grateful to the editor and the anonymous reviewers for their valuable comments and suggestions that improved the quality of this paper. This paper is supported by the National Research Foundation of Korea (NRF) Grant funded by the Korea Government (MSIP) (ASARC, NRF-2007-0056093), the National Natural Science Foundation of China (Nos. 11171150, 11271381, 11431015, and 61472457), the Fundamental Research Funds for the Central Universities (No. 56XZA15002), the 973 Program of China (Grant No. 2011CB808000), and the Natural Science Foundation of Guangdong (Grant No. 2014A030313161).

References

1. Bae S., Li C., Yue Q.: On the complete weight enumerator of some reducible cyclic codes. Discret. Math. **338**, 2275–2287 (2015).
2. Baumert L.D., McEliece R.J.: Weights of irreducible cyclic codes. Inf. Control **20**(2), 158–175 (1972).
3. Berndt B., Evans R., Williams K.: Gauss and Jacobi Sums. Wiley, New York (1997).
4. Blake I.F., Kith K.: On the complete weight enumerator of Reed-Solomon codes. SIAM J. Discret. Math. **4**(2), 164–171 (1991).
5. Cai H., Zeng X., Helleseth T., Tang X., Yang Y.: A new construction of zero-difference balanced functions and its applications. IEEE Trans. Inf. Theory **59**(8), 5008–5015 (2013).
6. Chu W., Colbourn C.J., Dukes P.: On constant composition codes. Discret. Appl. Math. **154**, 912–929 (2006).
7. Coulter R.S.: Further evaluation of some Weil sums. Acta Arith. **86**, 217–226 (1998).

8. Ding Y.: A construction for constant-composition codes. IEEE Trans. Inf. Theory **54**(8), 3738–3741 (2008).
9. Ding C.: Optimal constant composition codes from zero-difference balanced functions. IEEE Trans. Inf. Theory **54**(12), 5766–5770 (2008).
10. Ding C.: A class of three-weight and four-weight codes. In: Xing C., et al. (eds.) Proceedings of the Second International Workshop on Coding Theory and Cryptography. Lecture Notes in Computer Science, vol. 5557, pp. 34–42. Springer, Berlin (2009).
11. Ding C.: Codes from Difference Sets. World Scientific, Singapore (2014).
12. Ding C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265–3275 (2015).
13. Ding K., Ding C.: Binary linear codes with three weights. IEEE Commun. Lett. **18**(11), 1879–1882 (2014).
14. Ding K., Ding C.: A class of two-weight and three-weight codes and their applications in secret sharing. IEEE Trans. Inf. Theory (2015). doi:10.1109/TIT.2015.2473861.
15. Ding C., Niederreiter H.: Cyclotomic linear codes of order 3. IEEE Trans. Inf. Theory **53**(6), 2274–2277 (2007).
16. Ding C., Wang X.: A coding theory construction of new systematic authentication codes. Theor. Comput. Sci. **330**(1), 81–99 (2005).
17. Ding C., Yin J.: Algebraic constructions of constant composition codes. IEEE Trans. Inf. Theory **51**(4), 1585–1589 (2005).
18. Ding C., Yuan J.: A family of optimal constant-composition codes. IEEE Trans. Inf. Theory **51**(10), 3668–3671 (2005).
19. Ding C., Fu F.W., Kløve T., Wei V.W.K.: Constructions of permutation arrays. IEEE Trans. Inf. Theory **48**(4), 977–980 (2002).
20. Ding C., Helleseth T., Kløve T., Wang X.: A general construction of authentication codes. IEEE Trans. Inf. Theory **53**(6), 2229–2235 (2007).
21. Ding C., Luo J., Niederreiter H.: Two-weight codes punctured from 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).
22. Ding C., Wang Q., Xiong M.: Three new classes of zero-difference balanced functions with applications. IEEE Trans. Inf. Theory **60**(4), 2407–2413 (2014).
23. Feng K., Luo J.: Weight distribution of some reducible cyclic codes. Finite Fields Appl. **14**, 390–409 (2008).
24. Feng T., Momihara K., Xiang Q.: Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes. Combinatorica **35**(4), 413–434 (2015).
25. Fu F.W., Kløve T.: Two constructions of permutation arrays. IEEE Trans. Inf. Theory **50**(5), 881–883 (2004).
26. Gao F., Ge G.: Optimal ternary constant composition codes of weight four and distance five. IEEE Trans. Inf. Theory **57**(6), 3742–3757 (2011).
27. 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).
28. Ireland K., Rosen M.: A Classical Introduction to Modern Number Theory, 2nd edn. GTM 84, Springer, Berlin (1990).
29. Kith K.: Complete weight enumeration of Reed-Solomon codes. Master's Thesis, Department of Electrical and Computing Engineering, University of Waterloo, Waterloo, Ontario, Canada (1989).
30. Kuzmin A.S., Nechaev A.A.: Complete weight enumerators of generalized Kerdock code and linear recursive codes over Galois rings. In: Proceedings of the WCC99 Workshop on Coding and Cryptography, pp. 332–336, Paris, France, 11–14 January (1999)
31. Kuzmin A.S., Nechaev A.A.: Complete weight enumerators of generalized Kerdock code and related linear codes over Galois rings. Discret. Appl. Math. **111**, 117–137 (2001).
32. Li C., Yue Q., Fu F.W.: Complete weight enumerators of some cyclic codes. Des. Codes Cryptogr. (2015). doi:10.1007/s10623-015-0091-5.
33. Lidl R., Niederreiter H.: Finite Fields. Addison-Wesley, London (1983).
34. Luo J., Helleseth T.: Constant composition codes as subcodes of cyclic codes. IEEE Trans. Inf. Theory **57**(11), 7482–7488 (2011).
35. Luo J., Tang Y.: A new class of constant composition codes. In Proceedings of International Workshop on Signal Design and Its Applications, Fukuoka, Japan, pp. 138–140 (2009).
36. Luo Y., Fu F.W., Vinck A.J.H., Chen W.: On constant composition codes over $\mathbb{Z}_q$. IEEE Trans. Inf. Theory **49**(11), 3010–3016 (2003).
37. Ma S.L.: A survey of partial difference sets. Des. Codes Cryptogr. **4**, 221–261 (1994).

38. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977).
39. MacWilliams F.J., Mallows C.L., Sloane N.J.A.: Generalizations of Gleason's theorem on weight enumerators of self-dual codes. IEEE Trans. Inf. Theory **18**(6), 794–805 (1972).
40. Milenkovic O., Kashyap N.: On the Design of Codes for DNA Computing. Lecture Notes in Computer Science, vol. 3969. Springer, Berlin (2006).
41. Rees R.S., Stinson D.R.: Combinatorial Characterizations of Authentication Codes. Des. Codes Cryptogr. **7**, 239–259 (1996).
42. Simmons G.J.: Authentication Theory/Coding Theory. In: Advances in Cryptology—CRYPTO'84. Lecture Notes in Computer Science, vol. 196, pp. 411–431. Springer, Berlin (1984).
43. Xiang Q.: Recent progress in algebraic design theory. Finite Fields Appl. **11**, 622–653 (2005).
44. Yan J., Yin J.: A class of optimal constant composition codes from GDRP. Des. Codes Cryptogr. **50**, 61–76 (2009).
45. Yang J., Xia L.: Complete solving of the explicit evaluation of Gauss sums in the index 2 case. Sci. China Math. **53**(9), 2525–2542 (2010).