Constant Composition Codes as Subcodes of Linear Codes

Long Yu,[*]   Xiusheng Liu

School of Mathematics and Physics, Hubei Polytechnic University,
Huangshi, 435003, China

Abstract

In this paper, on one hand, a class of linear codes with one or two weights is obtained. Based on these linear codes, we construct two classes of constant composition codes, which includes optimal constant composition codes depending on LVFC bound. On the other hand, a class of constant composition codes is derived from known linear codes.

Key Words Linear codes, Gauss sum, Constant composition codes

1   Introduction

Let p be an odd prime and q be a power of p. A linear $[n, k, d]$ code over the finite field $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d. Let A_i denote the number of codewords with Hamming weight i in a linear code $\mathcal{C}$ of length n. The weight enumerator of $\mathcal{C}$ is defined by

$$1 + A_1 X + A_2 X^2 + \cdots + A_n X^n.$$

The sequence $(1, A_1, \cdots, A_n)$ is called the weight distribution of the code $\mathcal{C}$.

---

[*]Corresponding author.
Email addresses: longyu@mails.ccnu.edu.cn (Long Yu), lxs6682@163.com (Xiusheng Liu).

Let $D = \{d_1, d_2, \cdots, d_n\} \subseteq \mathbb{F}_{p^m}^*$, where n, m are positive integers. Let Tr denote the trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. We define a linear code of length n over $\mathbb{F}_p$ by

$$\mathcal{C}_D = \{c(a) = (\text{Tr}(ad_1), \text{Tr}(ad_2), \cdots, \text{Tr}(ad_n)) | a \in \mathbb{F}_{p^m}\}.$$

This construction is generic in the sense that many classes of known codes could be produced by selecting the defining set $D \subseteq \mathbb{F}_{p^m}$. So, this technique could be employed to construct linear codes and cyclic codes in different ways (see [5, 6, 8, 9, 11, 12, 14–21], and references theirin).

Let $S = \{s_0, \cdots, s_{q-1}\}$ be an alphabet of size q. An $[n, M, d, (\omega_0, \omega_1, \cdots, \omega_{q-1})_q]$ constant composition code(CCC) is a subset $C \subset S^n$ of size M, minimal distance d and where the element s_i occurs exactly ω_i times in each codeword in C.

Constant composition codes were studied already in the 1960s. Both algebraic and combinatorial constructions of CCCs have been proposed. For further information, the reader is referred to [1–4, 13].

The objective of this paper is to construct two classes of CCCs. A new constructions CCCs which are subcodes of linear codes (not cyclic codes) is proposed. On one hand, we define a class of linear codes $\mathcal{C}_{D(\alpha)}$ by a set $D(\alpha)$. The corresponding exponential sums have close relationship with Gauss sums. By using the technology of finite field, the parameters of linear codes $\mathcal{C}_{D(\alpha)}$ are obtained for all $\alpha \in \mathbb{F}_p$ (see Theorem 3.2). Furthermore, we select a kind of set S and construct a class of CCCs whose parameters is presented (see Theorem 3.3). Some of these CCCs are optimal in the sense that they meet LFVC bound. On the other hand, a class of CCCs is constructed from known linear codes (see Theorem 4.2).

2 Preliminaries

Throughout this paper, we let $q = p^m$, where m is a positive integer. Let η and $\overline{\eta}$ be the quadratic multiplicative character on $\mathbb{F}_q$ and $\mathbb{F}_p$, respectively. Let $\chi_1(\cdot) = \zeta_p^{\text{Tr}(\cdot)}$ and $\overline{\chi}_1 = \zeta_p^{(\cdot)}$ be the canonical additive characters on $\mathbb{F}_q$ and $\mathbb{F}_p$, respectively. We define $\eta(0) = 0 = \overline{\eta}(0)$, then the quadratic Gaussian sum $G(\eta, \chi_1)$ on $\mathbb{F}_q$ is defined by

$$G(\eta, \chi_1) = \sum_{x \in \mathbb{F}_q} \eta(x)\chi_1(x),$$

and the quadratic Gaussian sum $G(\overline{\eta}, \overline{\chi}_1)$ on $\mathbb{F}_p$ is defined by

$$G(\overline{\eta}, \overline{\chi}_1) = \sum_{x \in \mathbb{F}_p} \overline{\eta}(x)\overline{\chi}_1(x).$$

The following results are well known.

Lemma 2.1. *[7] Let the notations be given as above, we have*

$$G(\eta, \chi_1) = (-1)^{m-1}\sqrt{-1}^{(\frac{p-1}{2})^2 m}\sqrt{q}$$

and

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

Lemma 2.2. *[7] Let χ be a nontrivial additive character of $\mathbb{F}_q$, and let $f(x) = a_2 x^2 + a_1 x + a_0 \in \mathbb{F}_q[x]$ with $a_2 \neq 0$. Then*

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

The conclusions of the following two lemmas are easy to obtain.

Lemma 2.3. *If m is odd, then $\eta(a) = \overline{\eta}(a)$ for any $a \in \mathbb{F}_p$. If m is even, then $\eta(a) = 1$ for any $a \in \mathbb{F}_p^*$.*

Lemma 2.4. *For each $\alpha \in \mathbb{F}_p$, we let*

$$N_\alpha = \#\{x \in \mathbb{F}_{p^m} | \mathrm{Tr}(x) = \alpha\}.$$

Then $N_\alpha = p^{m-1}$.

We will need the following lemma.

Lemma 2.5. *[6] With the notations given as above. For each $\alpha \in \mathbb{F}_p$, let*

$$N_\alpha = \#\{x \in \mathbb{F}_{p^m} | \mathrm{Tr}(x^2) = \alpha\}.$$

Then

$$N_\alpha = \begin{cases} p^{m-1}, & \text{if } m \text{ is odd and } \alpha = 0; \\ p^{m-1} - (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}}(p-1)p^{\frac{m-2}{2}}, & \text{if } m \text{ is even and } \alpha = 0; \\ p^{m-1} + \overline{\eta}(-\alpha)(-1)^{(\frac{p-1}{2})^2(\frac{m+1}{2})}p^{\frac{m-1}{2}}, & \text{if } m \text{ is odd and } \alpha \neq 0; \\ p^{m-1} + (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}}p^{\frac{m-2}{2}}, & \text{if } m \text{ is even and } \alpha \neq 0. \end{cases}$$

At the end of this section, we give the LFVC bound of constant composition code.

Proposition 2.6. *[10] Assume $nd - n^2 + \omega_0^2 + \omega_1^2 + \cdots + \omega_{p-1}^2 > 0$. Then, an $[n, M, d, (\omega_\beta)_{\beta \in \mathbb{F}_p}]$ CCC satisfies the following inequality*

$$M \leq nd/\left(nd - n^2 + \omega_0^2 + \omega_1^2 + \cdots + \omega_{p-1}^2\right).$$

If

$$M = nd/\left(nd - n^2 + \omega_0^2 + \omega_1^2 + \cdots + \omega_{p-1}^2\right),$$

then we call CCC is optimal.

3   The first construction

In this section, we will define a CCC as a subcode of linear code $\mathcal{C}_{D(\alpha)}$ defined by (3.1). Throughout this section, we always assume that m is a positive integer. The defining set $D(\alpha)$ is given by

$$D(\alpha) = \{d \in \mathbb{F}_{p^m}^* | \mathrm{Tr}(d) = \alpha\},$$

where $\alpha \in \mathbb{F}_p$. Let n_α be the length of linear code $\mathcal{C}_{D(\alpha)}$, where

$$\mathcal{C}_{D(\alpha)} = \{c(a) = (\mathrm{Tr}(ad_1), \mathrm{Tr}(ad_2), \cdots, \mathrm{Tr}(ad_{n_\alpha}) | a \in \mathbb{F}_{p^m}\}. \tag{3.1}$$

Then by Lemma 2.4, we have the following result.

Lemma 3.1. *With the notations given as above, we have*

$$n_\alpha = \begin{cases} p^{m-1} - 1, & \alpha = 0; \\ p^{m-1}, & \text{otherwise.} \end{cases}$$

Theorem 3.2. *Let the notations be given as above.*

- *When $\alpha = 0$, $\mathcal{C}_{D(0)}$ defined by (3.1) is a $[p^{m-1} - 1, m - 1]$ code over $\mathbb{F}_p$ with the weight distribution as follows.*

weight	frequency
0	1
$p^{m-2}(p-1)$	$p^{m-1} - 1$

- *When $\alpha \in \mathbb{F}_p^*$, $\mathcal{C}_{D(\alpha)}$ defined by (3.1) is a $[p^{m-1}, m]$ code over $\mathbb{F}_p$ with the weight distribution as follows.*

weight	frequency
0	1
p^{m-1}	$p - 1$
$p^{m-2}(p-1)$	$p^m - p$

Proof. For $a \neq 0$, the Hamming weight of codeword $c(a)$ is equal to

$$wt(c(a)) = n_\alpha - \frac{1}{p} \sum_{x \in D(\alpha)} \sum_{u \in \mathbb{F}_p} \zeta_p^{u\mathrm{Tr}(ax)}$$

$$= n_\alpha - \frac{1}{p^2} \sum_{x\in\mathbb{F}_{p^m}^*} \sum_{u\in\mathbb{F}_p} \zeta_p^{u\mathrm{Tr}(ax)} \sum_{v\in\mathbb{F}_p} \zeta_p^{v(\mathrm{Tr}(x)-\alpha)}$$

$$= n_\alpha - \frac{1}{p^2} \sum_{x\in\mathbb{F}_{p^m}^*} (1+\sum_{u\in\mathbb{F}_p^*} \zeta_p^{u\mathrm{Tr}(ax)})(1+\sum_{v\in\mathbb{F}_p^*} \zeta_p^{v(\mathrm{Tr}(x)-\alpha)})$$

$$= n_\alpha - \frac{1}{p^2}(p^m-1) - \frac{1}{p^2} \sum_{x\in\mathbb{F}_{p^m}^*} \sum_{v\in\mathbb{F}_p^*} \zeta_p^{v(\mathrm{Tr}(x)-\alpha)} - \frac{1}{p^2} \sum_{x\in\mathbb{F}_{p^m}^*} \sum_{u\in\mathbb{F}_p^*} \zeta_p^{u\mathrm{Tr}(ax)}$$

$$- \frac{1}{p^2} \sum_{x\in\mathbb{F}_{p^m}^*} \sum_{u\in\mathbb{F}_p^*} \zeta_p^{u\mathrm{Tr}(ax)} \sum_{v\in\mathbb{F}_p^*} \zeta_p^{v(\mathrm{Tr}(x)-\alpha)}$$

$$= n_\alpha - \frac{1}{p^2}(p^m-1) + \frac{1}{p^2} \sum_{v\in\mathbb{F}_p^*} \zeta_p^{-v\alpha} + \frac{1}{p^2}(p-1)$$

$$- \frac{1}{p^2} \sum_{u\in\mathbb{F}_p^*} \sum_{v\in\mathbb{F}_p^*} \zeta_p^{-v\alpha}(\sum_{x\in\mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}((au+v)x)} - 1). \tag{3.2}$$

1) If $\alpha = 0$, from (3.2) and Lemma 3.1, we have

$$wt(c(a)) = n_0 - \frac{1}{p^2}(p^m-1) + \frac{2}{p^2}(p-1) - \frac{1}{p^2} \sum_{u\in\mathbb{F}_p^*} \sum_{v\in\mathbb{F}_p^*} (\sum_{x\in\mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}((au+v)x)} - 1)$$

$$= n_0 - p^{m-2} + 1 - \frac{1}{p^2} \sum_{u\in\mathbb{F}_p^*} \sum_{v\in\mathbb{F}_p^*} \sum_{x\in\mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}((au+v)x)}$$

$$= n_0 - p^{m-2} + 1 - p^{m-2}\#\{u,v\in\mathbb{F}_p^* | au+v=0\}$$

$$= \begin{cases} 0, & \text{if } a\in\mathbb{F}_p^*; \\ p^{m-2}(p-1), & \text{otherwise.} \end{cases}$$

Note that when $a\in\mathbb{F}_p$, we have $wt(c(a)) = 0$. This implies that the dimension of linear code $\mathcal{C}_{D(0)}$ is $m-1$.

2) If $\alpha \neq 0$, then

$$\sum_{v\in\mathbb{F}_p^*} \zeta_p^{-v\alpha} = -1 \quad \text{and} \quad \sum_{u\in\mathbb{F}_p^*} \sum_{v\in\mathbb{F}_p^*} \zeta_p^{-v\alpha} = -(p-1).$$

From (3.2) and Lemma 3.1, we get

$$wt(c(a)) = n_\alpha - p^{m-2} - \frac{1}{p^2} \sum_{u\in\mathbb{F}_p^*} \sum_{v\in\mathbb{F}_p^*} \zeta_p^{-v\alpha} \sum_{x\in\mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}((au+v)x)}$$

5

$$= \begin{cases} n_\alpha - p^{m-2} - p^{m-2} \displaystyle\sum_{\{u,v \in \mathbb{F}_p^* \mid au+v=0\}} \zeta_p^{-v\alpha}, & \text{if } a \in \mathbb{F}_p^*; \\ p^{m-2}(p-1), & \text{otherwise.} \end{cases}$$

$$= \begin{cases} n_\alpha - p^{m-2} - p^{m-2} \displaystyle\sum_{v \in \mathbb{F}_p^*} \zeta_p^{-v\alpha}, & \text{if } a \in \mathbb{F}_p^*; \\ p^{m-2}(p-1), & \text{otherwise.} \end{cases}$$

$$= \begin{cases} p^{m-1}, & \text{if } a \in \mathbb{F}_p^*; \\ p^{m-2}(p-1), & \text{otherwise.} \end{cases}$$

Note that when $a \in \mathbb{F}_{p^m}^*$, we have $wt(c(a)) > 0$. This implies that the dimension of linear code $\mathcal{C}_{D(\alpha)}$ is m.

$\square$

The Code $\mathcal{C}_\alpha'$ is defied by

$$\mathcal{C}_\alpha' = \{c(a) \mid a \in \mathbb{F}_{p^m} \setminus \mathbb{F}_p\}. \tag{3.3}$$

Denote the size of code $\mathcal{C}_\alpha'$ by M_α. It is easy to check

$$M_\alpha = \begin{cases} p^{m-1} - 1, & \text{if } \alpha = 0; \\ p^m - p, & \text{otherwise.} \end{cases}$$

Theorem 3.3. *The code $\mathcal{C}_\alpha'$ defined by (3.3) is an $[n_\alpha, M_\alpha, d, (\omega_\beta)_{\beta \in \mathbb{F}_p}]$ CCC, where*
1) in the case $\alpha = 0$:

$$\begin{aligned} n_0 &= p^{m-1} - 1; \\ M_0 &= p^{m-1} - 1; \\ \omega_0 &= p^{m-2} - 1; \\ \omega_\beta &= p^{m-2} \quad \text{for any} \quad \beta \in \mathbb{F}_p^*; \\ d &= p^{m-2}(p-1); \end{aligned}$$

2) in the case $\alpha \neq 0$:

$$\begin{aligned} n_\alpha &= p^{m-1}; \\ M_\alpha &= p^m - p; \\ \omega_\beta &= p^{m-2} \quad \text{for any} \quad \beta \in \mathbb{F}_p; \\ d &= p^{m-2}(p-1). \end{aligned}$$

6

Proof. 1) Note that $a \neq 0$. If $\alpha = 0$, for any $\beta \in \mathbb{F}_p^*$, we have

$$
\begin{aligned}
\omega_\beta &= \frac{1}{p} \sum_{x \in D(\alpha)} \sum_{u \in \mathbb{F}_p} \zeta_p^{u(\mathrm{Tr}(ax)-\beta)} \\
&= \frac{1}{p^2} \sum_{x \in \mathbb{F}_{p^m}^*} \sum_{u \in \mathbb{F}_p} \zeta_p^{u(\mathrm{Tr}(ax)-\beta)} \sum_{v \in \mathbb{F}_p} \zeta_p^{v\mathrm{Tr}(x)} \\
&= \frac{1}{p^2} \sum_{x \in \mathbb{F}_{p^m}} \sum_{u \in \mathbb{F}_p} \zeta_p^{u(\mathrm{Tr}(ax)-\beta)} \sum_{v \in \mathbb{F}_p} \zeta_p^{v\mathrm{Tr}(x)} \\
&= \frac{1}{p^2} \sum_{u \in \mathbb{F}_p} \sum_{v \in \mathbb{F}_p} \zeta_p^{-u\beta} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}((au+v)x)} \\
&= p^{m-2} + \frac{1}{p^2} \sum_{u \in \mathbb{F}_p^*} \zeta_p^{-u\beta} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}(aux)} + \frac{1}{p^2} \sum_{v \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}(vx)} \\
&\quad + \frac{1}{p^2} \sum_{u \in \mathbb{F}_p^*} \sum_{v \in \mathbb{F}_p^*} \zeta_p^{-u\beta} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}((au+v)x)} \\
&= p^{m-2} + \frac{1}{p^2} \sum_{u \in \mathbb{F}_p^*} \sum_{v \in \mathbb{F}_p^*} \zeta_p^{-u\beta} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}((au+v)x)}.
\end{aligned}
$$

Note that $a \in \mathbb{F}_{p^m} \setminus \mathbb{F}_p$, then $au + v \neq 0$ for any $u, v \in \mathbb{F}_p^*$. This implies that

$$
\sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}((au+v)x)} = 0.
$$

Thus, we have $\omega_\beta = p^{m-2}$, for any $\beta \neq 0$. Recall $n_0 = p^{m-1} - 1$, then $\omega_0 = p^{m-2} - 1$.

2) If $\alpha \neq 0$, for any $\beta \in \mathbb{F}_p^*$ and $a \neq 0$, then

$$
\begin{aligned}
\omega_\beta &= \frac{1}{p} \sum_{x \in D(\alpha)} \sum_{u \in \mathbb{F}_p} \zeta_p^{u(\mathrm{Tr}(ax)-\beta)} \\
&= \frac{1}{p^2} \sum_{x \in \mathbb{F}_{p^m}^*} \sum_{u \in \mathbb{F}_p} \zeta_p^{u(\mathrm{Tr}(ax)-\beta)} \sum_{v \in \mathbb{F}_p} \zeta_p^{v(\mathrm{Tr}(x)-\alpha)} \\
&= \frac{1}{p^2} \sum_{x \in \mathbb{F}_{p^m}} \sum_{u \in \mathbb{F}_p} \zeta_p^{u(\mathrm{Tr}(ax)-\beta)} \sum_{v \in \mathbb{F}_p} \zeta_p^{v(\mathrm{Tr}(x)-\alpha)} \\
&= \frac{1}{p^2} \sum_{u \in \mathbb{F}_p} \sum_{v \in \mathbb{F}_p} \zeta_p^{-u\beta} \zeta_p^{-v\alpha} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}((au+v)x)}
\end{aligned}
$$

7

$$= p^{m-2} + \frac{1}{p^2} \sum_{u \in \mathbb{F}_p^*} \zeta_p^{-u\beta} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}(aux)} + \frac{1}{p^2} \sum_{v \in \mathbb{F}_p^*} \zeta_p^{-v\alpha} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}(vx)}$$

$$+ \frac{1}{p^2} \sum_{u \in \mathbb{F}_p^*} \sum_{v \in \mathbb{F}_p^*} \zeta_p^{-u\beta} \zeta_p^{-v\alpha} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}((au+v)x)}$$

$$= p^{m-2} + \frac{1}{p^2} \sum_{u \in \mathbb{F}_p^*} \sum_{v \in \mathbb{F}_p^*} \zeta_p^{-u\beta} \zeta_p^{-v\alpha} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}((au+v)x)}.$$

Note that $a \in \mathbb{F}_{p^m} \setminus \mathbb{F}_p$, then $au + v \neq 0$ for any $u, v \in \mathbb{F}_p^*$. This leads to

$$\sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}((au+v)x)} = 0, \quad u, v \in \mathbb{F}_p^*.$$

Therefore, $\omega_\beta = p^{m-2}$ for any $\beta \in \mathbb{F}_p^*$. Recall $n_\alpha = p^{m-1}$, then $\omega_0 = p^{m-1} - p^{m-2}(p - 1) = p^{m-2}$.

Denote by $d_H(c(a_1), c(a_2))$ the Hamming distance of $c(a_1)$ and (a_2). For any $\alpha \in \mathbb{F}_p$, when a_1 and a_2 run through $\mathbb{F}_{p^m} \setminus \mathbb{F}_p$ with $a_1 \neq a_2$, then $a_1 - a_2$ runs through $\mathbb{F}_{p^m}^*$. Therefore, the minimal distance of $\mathcal{C}'$ is the same as that of $\mathcal{C}$, which is obtained by Theorem 3.2. This completes the proof. $\square$

Remark 3.4. *When $\alpha = 0$, the parameters of code $\mathcal{C}_0'$ in above Theorem satisfy*

$$n_0 d / (n_0 d - n_0^2 + \omega_0^2 + \omega_1^2 + \cdots + \omega_{p-1}^2) = M_0.$$

Thus, we obtain a class of optimal CCCs. However, if $\alpha \in \mathbb{F}_p^*$, the parameters of code $\mathcal{C}_\alpha'$ satisfy

$$n_\alpha d - n_\alpha^2 + \omega_0^2 + \omega_1^2 + \cdots + \omega_{p-1}^2 = 0.$$

Therefore, the LFVC bound cannot be applied to measure the optimality of these CCCs. Note that for large m, code $\mathcal{C}_\alpha'$ has the same minimal distance d and length n_α. In this sense, compared to $\mathcal{C}_0'$ which is optimal, $\mathcal{C}_\alpha'$ has more codewords with same minimal distance d for $\alpha \in \mathbb{F}_p^*$. This implies that $\mathcal{C}_\alpha'$ are excellent.

4   The second construction

In this section, we let $\tau = (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}}$, where m is even. The defining set E is given by

$$E = \{d \in \mathbb{F}_{p^m}^* | \mathrm{Tr}(d^2) = 0\}.$$

The linear code $\mathcal{C}_E$ is defined as

$$\mathcal{C}_E = \{c(a) = (\mathrm{Tr}(ad_1), \mathrm{Tr}(ad_2), \cdots, \mathrm{Tr}(ad_n)) | a \in \mathbb{F}_{p^m}\}. \tag{4.1}$$

Lemma 4.1. *[6] Then the code $\mathcal{C}_E$ defined by (4.1) over $\mathbb{F}_p$ has parameters $[p^{m-1} - \tau(p-1)p^{\frac{m}{2}-1} - 1, m]$ and weight distribution in the following.*

weight	frequency
0	1
$(p-1)p^{m-2}$	$p^{m-1} - \tau(p-1)p^{\frac{m}{2}-1} - 1$
$(p-1)(p^{m-2} - \tau p^{\frac{m}{2}-1})$	$(p-1)\left(p^{m-1} + \tau p^{\frac{m}{2}-1}\right)$

Define set

$$S = \{a \in \mathbb{F}_{q^m} | \mathrm{Tr}(a^2) \neq 0\}$$

and code

$$\mathcal{C}'_E = \{c(a) \mid a \in S\}. \tag{4.2}$$

By Lemma 2.5, we obtain the size of S is $p^m - p^{m-1} + \tau(p-1)p^{\frac{m}{2}-1}$. In the following, we give our main result.

Theorem 4.2. *The code $\mathcal{C}'_E$ defined by (4.2) is a CCC with parameters $[n, M, d, (\omega_\beta)_{\beta \in \mathbb{F}_p}]$ where*

$$
\begin{aligned}
n &= p^{m-1} - \tau(p-1)p^{\frac{m}{2}-1} - 1; \\
M &= p^m - p^{m-1} + \tau(p-1)p^{\frac{m}{2}-1}; \\
\omega_0 &= p^{m-2} - 1; \\
\omega_\beta &= p^{m-2} - \tau p^{\frac{m}{2}-1} \quad for \quad any \quad \beta \in \mathbb{F}_p^*; \\
d &= \begin{cases} (p-1)p^{m-2}, & \tau = -1; \\ (p-1)(p^{m-2} - p^{\frac{m}{2}-1}), & \tau = 1. \end{cases}
\end{aligned}
$$

Proof. It is easy to see

$$n = p^{m-1} - \tau(p-1)p^{\frac{m}{2}-1} - 1$$

and

$$M = p^m - p^{m-1} + \tau(p-1)p^{\frac{m}{2}-1}.$$

For any $\beta \in \mathbb{F}_p^*$, we have

$$
\begin{aligned}
\omega_\beta &= \frac{1}{p} \sum_{x \in E} \sum_{u \in \mathbb{F}_p} \zeta_p^{u(\mathrm{Tr}(ax) - \beta)} \\
&= \frac{1}{p^2} \sum_{x \in \mathbb{F}_{p^m}^*} \sum_{u \in \mathbb{F}_p} \zeta_p^{u(\mathrm{Tr}(ax) - \beta)} \sum_{v \in \mathbb{F}_p} \zeta_p^{v\mathrm{Tr}(x^2)}
\end{aligned}
$$

$$
\begin{aligned}
&= \ \frac{1}{p^2} \sum_{x \in \mathbb{F}_{p^m}} \sum_{u \in \mathbb{F}_p} \zeta_p^{u(\mathrm{Tr}(ax)-\beta)} \sum_{v \in \mathbb{F}_p} \zeta_p^{v \mathrm{Tr}(x^2)} \\
&= \ \frac{1}{p^2} \sum_{u \in \mathbb{F}_p} \sum_{v \in \mathbb{F}_p} \zeta_p^{-u\beta} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}(aux+vx^2)} \\
&= \ p^{m-2} + \frac{1}{p^2} \sum_{u \in \mathbb{F}_p^*} \zeta_p^{-u\beta} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}(aux)} + \frac{1}{p^2} \sum_{v \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}(vx^2)} \\
&\quad + \frac{1}{p^2} \sum_{u \in \mathbb{F}_p^*} \sum_{v \in \mathbb{F}_p^*} \zeta_p^{-u\beta} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}(aux+vx^2)}. \tag{4.3}
\end{aligned}
$$

Since $a \cdot u \neq 0$, then
$$
\sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}(aux)} = 0.
$$

By Lemmas 2.2 and 2.3, together with $a \in S$, we have (4.3) is equal to

$$
\begin{aligned}
\omega_\beta &= \ p^{m-2} + \frac{p-1}{p^2} G(\eta, \chi_1) + \frac{1}{p^2} \sum_{u \in \mathbb{F}_p^*} \sum_{v \in \mathbb{F}_p^*} \zeta_p^{-u\beta} \zeta_p^{\mathrm{Tr}(-\frac{a^2 u^2}{4v})} G(\eta, \chi_1) \\
&= \ p^{m-2} + \frac{p-1}{p^2} G(\eta, \chi_1) + \frac{1}{p^2} G(\eta, \chi_1) \sum_{v \in \mathbb{F}_p^*} \Big(\sum_{u \in \mathbb{F}_p} \zeta_p^{-\beta u - \frac{\mathrm{Tr}(a^2)}{4v} u^2} - 1 \Big) \\
&= \ p^{m-2} + \frac{1}{p^2} G(\eta, \chi_1) \sum_{v \in \mathbb{F}_p^*} \sum_{u \in \mathbb{F}_p} \zeta_p^{-\beta u - \frac{\mathrm{Tr}(a^2)}{4v} u^2} \\
&= \ p^{m-2} + \frac{1}{p^2} G(\eta, \chi_1) \sum_{v \in \mathbb{F}_p^*} \overline{\eta}\Big(-\frac{\mathrm{Tr}(a^2)}{4v}\Big) \zeta_p^{\frac{\beta^2 v}{\mathrm{Tr}(a^2)}} G(\overline{\eta}, \overline{\chi}_1) \\
&= \ p^{m-2} + \frac{1}{p^2} G(\eta, \chi_1) G(\overline{\eta}, \overline{\chi}_1) \sum_{v \in \mathbb{F}_p^*} \overline{\eta}(-1) \overline{\eta}\Big(\frac{\beta^2 v}{\mathrm{Tr}(a^2)}\Big) \zeta_p^{\frac{\beta^2 v}{\mathrm{Tr}(a^2)}} \\
&= \ p^{m-2} + \frac{1}{p^2} G(\eta, \chi_1) G(\overline{\eta}, \overline{\chi}_1) \overline{\eta}(-1) \sum_{v \in \mathbb{F}_p^*} \overline{\eta}(v) \zeta_p^{v} \\
&= \ p^{m-2} + \frac{1}{p^2} G(\eta, \chi_1) G^2(\overline{\eta}, \overline{\chi}_1) \overline{\eta}(-1) \\
&= \ p^{m-2} - (-1)^{(\frac{p-1}{2})^2} \overline{\eta}(-1) \tau p^{\frac{m}{2}-1} \\
&= \ p^{m-2} - (-1)^{(\frac{p-1}{2})^2} (-1)^{(\frac{p-1}{2})} \tau p^{\frac{m}{2}-1} \\
&= \ p^{m-2} - \tau p^{\frac{m}{2}-1}.
\end{aligned}
$$

Note that $n = p^{m-1} - \tau(p-1)p^{\frac{m}{2}-1} - 1$, then

$$\omega_0 = p^{m-2} - 1.$$

Denote by $d_H(c(a_1), c(a_2))$ the Hamming distance of $c(a_1)$ and (a_2). When a_1 and a_2 run through S with $a_1 \neq a_2$, then $a_1 - a_2$ runs through $\mathbb{F}_{p^m}^*$. Therefore, the minimal distance of $\mathcal{C}'_E$ is the same as that of $\mathcal{C}_E$. By Lemma 4.1, we finish the proof. □

Remark 4.3. *We can check that $nd - n^2 + \omega_0^2 + \omega_1^2 + \cdots + \omega_{p-1}^2 < 0$ for $\tau = \pm 1$. Therefore, the LFVC bound cannot be applied to measure the optimality of these CCCs.*

In a similar way, we can prove that $\{c(a)|a \in \mathbb{F}_{p^m}^* \setminus S\}$ is a CCC. However, this code has only $p^{m-1} - \tau(p-1)p^{\frac{m-2}{2}} - 1$ codewords which is fewer in comparison with $\mathcal{C}'_E$.

Corollary 4.4. *The code $\{c(a)|a \in \mathbb{F}_{p^m}^* \setminus S\}$ is a CCC with parameters $[n, M', d, (\omega_\beta)_{\beta \in \mathbb{F}_p}]$ where*

$$
\begin{aligned}
n &= p^{m-1} - \tau(p-1)p^{\frac{m}{2}-1} - 1; \\
M' &= p^{m-1} - \tau(p-1)p^{\frac{m}{2}-1} - 1; \\
\omega_0 &= p^{m-2} - \tau(p-1)p^{\frac{m}{2}-1} - 1; \\
\omega_\beta &= p^{m-2} \quad for \ any \ \beta \in \mathbb{F}_p^*; \\
d &= \begin{cases} (p-1)p^{m-2}, & \tau = -1; \\ (p-1)(p^{m-2} - p^{\frac{m}{2}-1}), & \tau = 1. \end{cases}
\end{aligned}
$$

5 Conclusion

In this paper, we obtained several classes of CCCs with exact parameters. One of them is optimal based on LFVC bound. However, the other CCCs cannot be measured by LFVC bound. The optimality of these CCCs is not clear. At the end, we mention that CCCs over $\mathbb{F}_p$ obtained in this paper can be generalized to the case of CCCs over $\mathbb{F}_q$.

References

[1] W. Chu, C.J.Colbourn and P. Dukes, "Constructions for permutation codes in powerline communnications," Designs Codes, Crypt., **32**, 51–64, 2004.

[2] C. Ding, "Optimal constant composition codes from zero-difference balanced functions," *IEEE Trans. Inf. Theory*, **54**(12), 5766–5770, 2008.

[3] C. Ding and J. Yin, "Algebraic constructions of constant composition codes," *IEEE Trans. Inf. Theory*, **51**(4), 1585–1589, 2005.

[4] C. Ding and J. Yuan, "A family of optimal constant-composition codes," *IEEE Trans. Inf. Theory*, **51**(10), 3668–3671, 2005.

[5] C. Ding and H. Niederreiter, "Cyclotomic linear codes of order 3", *IEEE Trans. Inf. Theory*, **53**(6), 2274–2277, 2007.

[6] K. Ding and C. Ding. "A Class of Two-Weight and Three-Weight Codes and Their Applications in Secret Sharing." *IEEE Trans. Inf. Theory*, **61**(11), 5835–5842, 2015.

[7] R. Lidl and H. Niederreiter, "Finite Fields," Cambridge, U.K.: Cambridge Univ. Press, 1997.

[8] C. Li, Q. Yue and F. Li, "Hamming weights of the duals of cyclic codes with two zeros", *IEEE Trans. Inform. Theory*, **60**(7), 3895–3902, 2014.

[9] C. Li and Q. Yue, "Weight distributions of two classes of cyclic codes with respect to two distinct order elements", *IEEE Trans. Inform. Theory*, **60**(1), 296–303, 2014.

[10] Y. Luo, F. Fu, A. Vinck and W. Chen, "On constantcomposition codes over $\mathbb{Z}_q$," *IEEE Trans. Inform. Theory*, **49**, 3010–3016, 2003.

[11] J. Luo and K. Feng, "Cyclic codes and sequences from generalized Coulter-Matthews function," *IEEE Trans. Inform. Theory*, **54**(12), 5345–5353, 2008.

[12] J. Luo and K. Feng, "On the weight distributions of two classes of cyclic codes," *IEEE Trans. Inform. Theory*, **54**(12), 5332–5344, 2008.

[13] J. Luo and T. Helleseth, "Constant Composition Codes as Subcodes of Cyclic Codes", *IEEE Trans. Inf. Theory*, **57**(11), 2011.

[14] L. Yu and H. Liu, "A class of p-ary cyclic codes and their weight enumerators", *Adv. Math. Commun.*, **10**(2), 437–457, 2016.

[15] L. Yu and H. Liu, "The weight distribution of a family of p-ary cyclic codes", *Des. Codes Cryptogr.* **78**, 731–745, 2016.

[16] X. Zeng, J. Shan and L. Hu, "A triple-error-correcting cyclic code from the Gold and Kasami-Welch APN power functions," *Finite Fields Appl.* **18**(1), 70-92(2012).

[17] X. Zeng, L. Hu, W. Jiang, Q. Yue and X. Cao, "The weight distribution of a class of p-ary cyclic codes", *Finite Fields Appl.* **16**(1), 56–73, 2010.

[18] D. Zheng, X. Wang, X. Zeng and L. Hu, "The weight distribution of a family of p-ary cyclic codes," *Des. Codes Cryptogr.* **75**(2), 1–13, 2015.

[19] D. Zheng, X. Wang, L. Yu and H. Liu, "The weight distributions of several classes of p-ary cyclic codes", *Discrete Mathematics*, **338**, 1264–1276, 2015.

[20] Z. Zhou and C. Ding, "A class of three-weight cyclic codes", *Finite Fields Appl.* **25**, 79–93, 2014.

[21] Z. Zhou , N. Li, C. Fan and T. Helleseth, "Linear codes with two or three weights from quadratic bent functions", *Des Codes Cryptogr*, 81(2), 283–295, 2016.