Constant composition codes derived from linear codes

Long Yu∗, Xiusheng Liu

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

Abstract

In this paper, we propose a class of linear codes and obtain their weight distribution. Some of these codes are almost optimal. Moreover, several classes of constant composition codes (CCC) are constructed as subcodes of 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 \( D = \{d_1, d_2, \cdots, d_n\} \subseteq \mathbb{F}_q^* \), where \( n \) is a positive integer. Let \( \text{Tr} \) denote the trace function from \( \mathbb{F}_q \) to \( \mathbb{F}_p \). We define a linear code of length \( n \) over \( \mathbb{F}_p \) by

\[
C_D = \{c(a) = (\text{Tr}(ad_1), \text{Tr}(ad_2), \cdots, \text{Tr}(ad_n)) | a \in \mathbb{F}_q \}.
\]

(1.1)

Let \( A_i \) denote the number of codewords with Hamming weight \( i \) in a linear code \( C \) of length \( n \). The weight enumerator of \( C \) is defined by

\[
1 + A_1X + A_2X^2 + \cdots + A_nX^n.
\]

∗Corresponding author.
Email addresses: longyu@mails.ccnu.edu.cn (Long Yu), lxs6682@163.com (Xiusheng Liu).
The sequence \((1, A_1, \ldots, A_n)\) is called the weight distribution of the code \(C\).

The construction of linear code defined by (1.1) is generic in the sense that many classes of known codes could be produced by selecting the suitable defining set \(D \subseteq \mathbb{F}_q\). So, the corresponding exponential sums can be computed by some technologies of finite field. Therefore, the weight distributions of a large number of linear codes (cyclic codes) were obtained (see [5, 6, 8, 9, 11, 12, 14, 15, 17–22], and references therein).

Let \(S = \{s_0, \ldots, s_{q-1}\}\) be an alphabet of size \(q\). An \([n, M, d, (\omega_0, \omega_1, \ldots, \omega_{q-1})]\) constant composition code (CCC) is a subset \(C \subseteq S^n\) of size \(M\), minimal distance \(d\) and where the element \(s_i\) occurs exactly \(\omega_i\) 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 aim of this paper is to construct CCCs from linear codes. Luo and Helleseth [13] proposed a new way to obtain CCCs from some known cyclic codes. Recently, Yu and Liu [16] construct several classes of CCCs from linear codes. Following this line, we define a class of linear codes \(C_{D(\alpha)}\) by the set \(D(\alpha)\). When \(\alpha = 0\), Ding and Ding [6] have already studied this kind of linear codes. So, for \(\alpha \neq 0\), we investigate the weight distribution of \(C_{D(\alpha)}\) (see Theorem 3.3). Furthermore, we choose a kind of set \(S_{\gamma}\) and obtain several classes of CCCs (see Theorem 4.1).

## 2 Preliminaries

Throughout this paper, we let \(q = p^m\), where \(m\) is a positive integer. Let \(\eta\) 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. [3] Let the notations be given as above, we have
\[ G(\eta, \chi_1) = (-1)^{m-1} \sqrt{-1}^{(\frac{m-1}{2})^2 m} \sqrt{q} \]
and
\[ G(\overline{\eta}, \chi_1) = \sqrt{-1}^{(\frac{m-1}{2})^2} \sqrt{p}. \]

Lemma 2.2. [3] Let \( \chi \) be a nontrivial additive character of \( \mathbb{F}_q \), and let \( f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x] \) with \( a_2 \neq 0 \). Then
\[ \sum_{x \in \mathbb{F}_q} \chi(f(x)) = \chi(a_0 - a_1^2/(4a_2))\eta(a_2)G(\eta, \chi). \]

The conclusion of the following lemma is 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 \( a \in \mathbb{F}_p^\ast \).

We will need the following lemma.

Lemma 2.4. [6] With the notations given as above. For each \( \alpha \in \mathbb{F}_p \), let
\[ N_\alpha = \# \{ x \in \mathbb{F}_p^m | \text{Tr}(x^2) = \alpha \}. \]

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

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

Proposition 2.5. [10] Assume \( nd - n^2 + \omega^2_0 + \omega^2_1 + \cdots + \omega^2_{p-1} > 0 \). Then, an \( [n, M, d, (\omega_\beta)_{\beta \in \mathbb{F}_p}] \) CCC satisfies the following inequality
\[ M \leq nd/ (nd - n^2 + \omega^2_0 + \omega^2_1 + \cdots + \omega^2_{p-1}). \]

If
\[ M = nd/ (nd - n^2 + \omega^2_0 + \omega^2_1 + \cdots + \omega^2_{p-1}), \]
then we call CCC is optimal.
3 A class of linear code

In this section, for a fixed \( \alpha \in \mathbb{F}_p \), we define set
\[
D(\alpha) = \{ d \in \mathbb{F}^*_p | \text{Tr}(d^2) = \alpha \}.
\]
The corresponding linear code is given as
\[
C_{D(\alpha)} = \{ c(a) = (\text{Tr}(ad_1), \text{Tr}(ad_2), \ldots, \text{Tr}(ad_n)) | a \in \mathbb{F}_p^m \}, \tag{3.1}
\]
where \( n_\alpha \) is the length of \( C_{D(\alpha)} \). In particular, when \( \alpha = 0 \), Ding and Ding \cite{6} investigated the weight distribution of linear code \( C_{D(0)} \). Furthermore, Yu and Liu constructed a class of CCCs from code \( C_{D(0)} \). Here, we calculate the weight distribution of linear code \( C_{D(\alpha)} \) for \( \alpha \neq 0 \) and construct CCCs from \( C_{D(\alpha)} \).

Let \( \epsilon = (-1)^{(p-1)/2} \frac{m+1}{2} \) for odd \( m \) and \( \tau = (-1)^{(p-1)/2} \frac{m}{2} \) for even \( m \), we have the following result.

Lemma 3.1. With the notations given as above. Then
\[
\sum_{u \in \mathbb{F}^*_p} \zeta_p^{-ua} \sum_{v \in \mathbb{F}^*_p} \sum_{x \in \mathbb{F}_p^m} \zeta_p^{\text{Tr}(avx + ux^2)} = \begin{cases} 
\epsilon \eta(-\alpha)(p-1)p^{\frac{m+1}{2}}, & \text{if } m \text{ is odd and } \text{Tr}(a^2) = 0; \\
\tau (p-1)p^{\frac{m}{2}}, & \text{if } m \text{ is even and } \text{Tr}(a^2) = 0; \\
-\epsilon p^{\frac{m+1}{2}} (\eta(\text{Tr}(-a^2)) + \eta(-\alpha)), & \text{if } m \text{ is odd and } \text{Tr}(a^2) \neq 0; \\
-\tau p^{\frac{m}{2}} ((-1)^{(p-1)/2} \eta(\alpha \text{Tr}(a^2)))p + 1), & \text{if } m \text{ is even and } \text{Tr}(a^2) \neq 0.
\end{cases}
\]

Proof. By Lemma \ref{2.2} we have
\[
\sum_{u \in \mathbb{F}^*_p} \zeta_p^{-ua} \sum_{v \in \mathbb{F}^*_p} \sum_{x \in \mathbb{F}_p^m} \zeta_p^{\text{Tr}(avx + ux^2)} = G(\eta, \chi_1) \sum_{u \in \mathbb{F}^*_p} \zeta_p^{-ua} \sum_{v \in \mathbb{F}^*_p} \eta(u)\zeta_p^{-\text{Tr}(\frac{u^2}{4n})} = G(\eta, \chi_1) \sum_{u \in \mathbb{F}^*_p} \eta(u)\zeta_p^{-ua} \sum_{v \in \mathbb{F}^*_p} \zeta_p^{\frac{u^2}{4n}} \text{Tr}(\frac{a^2}{4n}) \tag{3.2}
\]

If \( \text{Tr}(a^2) = 0 \), by Lemma \ref{2.3} one has
\[
G(\eta, \chi_1) \sum_{u \in \mathbb{F}^*_p} \eta(u)\zeta_p^{-ua} \sum_{v \in \mathbb{F}^*_p} \zeta_p^{\frac{u^2}{4n}} \text{Tr}(\frac{a^2}{4n})
\]
\[
G(\eta, \chi_1)(p - 1) \sum_{u \in \mathbb{F}_p^*} \eta(u) \zeta_p^{-\alpha} \\
= G(\eta, \chi_1)(p - 1) \eta(-\alpha) \sum_{u \in \mathbb{F}_p^*} \eta(u) \zeta_p^u \\
= \begin{cases} 
G(\eta, \chi_1)(p - 1) \eta(-\alpha) \sum_{u \in \mathbb{F}_p^*} \bar{\eta}(u) \zeta_p^u, & \text{if } m \text{ is odd;} \\
G(\eta, \chi_1)(p - 1) \eta(-\alpha) \sum_{u \in \mathbb{F}_p^*} \zeta_p^u, & \text{if } m \text{ is even.}
\end{cases}
\]

If \( \text{Tr}(a^2) \neq 0 \), by Lemmas 2.2 and 2.3, then (3.2) is equal to

\[
G(\eta, \chi_1) \sum_{u \in \mathbb{F}_p^*} \eta(u) \zeta_p^{-\alpha} \sum_{v \in \mathbb{F}_p^*} \zeta_p^{v^2 \text{Tr}(\frac{a^2}{4u})} - 1
\]

\[
= G(\eta, \chi_1) \left( \sum_{u \in \mathbb{F}_p^*} \eta(u) \zeta_p^{-\alpha} \bar{\eta}(\text{Tr}(\frac{a^2}{4u})) G(\eta, \chi_1) - \sum_{u \in \mathbb{F}_p^*} \eta(u) \zeta_p^{-\alpha} \right)
\]

\[
= \begin{cases} 
G(\eta, \chi_1) \left( G(\eta, \chi_1) \eta(\text{Tr}(\frac{-a^2}{4u})) \sum_{u \in \mathbb{F}_p^*} \zeta_p^{-\alpha} - \eta(-\alpha) \sum_{u \in \mathbb{F}_p^*} \bar{\eta}(u) \zeta_p^u \right), & \text{if } m \text{ is odd;} \\
G(\eta, \chi_1) \left( G(\eta, \chi_1) \eta(\alpha \text{Tr}(a^2)) \sum_{u \in \mathbb{F}_p^*} \bar{\eta}(u) \zeta_p^{-\alpha} - \sum_{u \in \mathbb{F}_p^*} \zeta_p^u \right), & \text{if } m \text{ is even.}
\end{cases}
\]

The desired conclusions then follow from Lemma 2.1.

The following lemma will be employed later.

**Lemma 3.2.** For \( a \in \mathbb{F}_{p^m}^* \) and \( \alpha \in \mathbb{F}_p \), let

\[
N(a) = |x \in \mathbb{F}_{p^m} | \text{Tr}(x^2) = \alpha \text{ and } \text{Tr}(ax) = 0|
\]
Then

\[
N(a) = \begin{cases} 
p^{m-2} + \epsilon \eta (-\alpha) p^{m-1}, & \text{if } m \text{ is odd and } \text{Tr}(a^2) = 0; 
p^{m-2} + \tau p^{m-1}, & \text{if } m \text{ is even and } \text{Tr}(a^2) = 0; 
p^{m-2} - \epsilon \eta (\text{Tr}(a^2)) p^{m-3}, & \text{if } m \text{ is odd and } \text{Tr}(a^2) \neq 0; 
p^{m-2} - (-1)^{(m+1)/2} \eta(\alpha \text{Tr}(a^2)) p^{m-1}, & \text{if } m \text{ is even and } \text{Tr}(a^2) \neq 0.
\end{cases}
\]

**Proof.** By definition, we have

\[
p^2 N(a) = \sum_{x \in \mathbb{F}_p} \left( \sum_{u \in \mathbb{F}_p} \zeta_p^{u \text{Tr}(x^2) - \alpha} \right) \left( \sum_{v \in \mathbb{F}_p} \zeta_p^{v \text{Tr}(ax)} \right)
= \sum_{v \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_p} \zeta_p^{v \text{Tr}(ax)} + \sum_{u \in \mathbb{F}_p} \sum_{v \in \mathbb{F}_p^*} \zeta_p^{u \text{Tr}(x^2) - \alpha}
+ \sum_{u \in \mathbb{F}_p^*} \sum_{v \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_p} \zeta_p^{v \text{Tr}(ux + x^2)}
= \pm \alpha + \sum_{u \in \mathbb{F}_p^*} \sum_{v \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_p} \zeta_p^{v \text{Tr}(ux + x^2)}.
\]

The desired conclusions then follow from Lemmas 2.4 and 3.1.

Now, we give the main result in this section.

**Theorem 3.3.** Let the notations be given as above.

- For odd \(m\), \(C_{D(\alpha)}\) defined by (3.1) is a \([p^{m-1} + \epsilon \eta (-\alpha) p^{m-1}, m]\) code with weight distribution in Table 1. where \(\epsilon = (-1)^{(m+1)/2} p^{m+1}/2\).

| weight |
|--------|
| \((p - 1)p^{m-2}\) |
| \((p - 1)p^{m-2} + \epsilon(\eta(-1) + p\eta(-\alpha))p^{m-3}\) |
| \((p - 1)p^{m-2} + \epsilon(-\eta(-1) + p\eta(-\alpha))p^{m-3}\) |

| frequency |
|-----------|
| \(1\) |
| \(p^{m-1} - 1\) |
| \(p^{m-1} - \eta(-1)p^{m-1}/2\) |
| \(p^{m-1} - \eta(-1)p^{m-1}/2\) |
Table 2: For even $m$, the weight distribution of $C_{D(\alpha)}$

| Weight          | Frequency                  |
|-----------------|----------------------------|
| $(p - 1)p^{m-2}$ | $\frac{p+1}{2} p^{m-1} - \frac{1}{2} (p^2 - 1)^2 + 1$ |
| $(p - 1)p^{m-2} + 2\tau p^{m-1}$ | $\frac{p-1}{2} (p^{m-1} + \tau p^{m-1})$ |

• For even $m$, $C_{D(\alpha)}$ defined by (3.1) is an \([p^{m-1} + \tau p^{m-2}, m]\) code with weight distribution in Table 2, where $\tau = (-1)^{(\frac{p\pm 1}{2})^2 m} / 2$.

Proof. It is easy to obtain $n_\alpha$ from Lemma 2.4. If $m$ is odd, for $a \neq 0$, then

$$wt(c(a)) = n_\alpha - N(a)$$

$$= \begin{cases} 
(p - 1)p^{m-2}, & \text{if } Tr(a^2) = 0; \\
(p - 1)p^{m-2} + \epsilon (\eta(Tr(-a^2)) + \eta(-\alpha)) p^{m-3}, & \text{if } Tr(a^2) \neq 0.
\end{cases}$$

Note that $Tr(a^2) \in F^*_p$ is a square element, then, by Lemma 2.4, we have the number of $a$ is

$$(p - 1)\left(p^{m-1} + \eta(-1)\epsilon p^{m-1}\right).$$

Note that $Tr(a^2) \in F^*_p$ is a non-square element, then, by Lemma 2.4, we get the number of $a$ is

$$(p - 1)\left(p^{m-1} - \eta(-1)\epsilon p^{m-1}\right).$$

If $m$ is even, then

$$wt(c(a)) = n_\alpha - N(a)$$

$$= \begin{cases} 
(p - 1)p^{m-2}, & \text{if } Tr(a^2) = 0; \\
(p - 1)p^{m-2} + \tau \left(1 + (-1)^{(\frac{p\pm 1}{2})^2 \eta(\alpha)}\right) p^{m-1}, & \text{if } Tr(a^2) \text{ is square}; \\
(p - 1)p^{m-2} + \tau \left(1 - (-1)^{(\frac{p\pm 1}{2})^2 \eta(\alpha)}\right) p^{m-1}, & \text{if } Tr(a^2) \text{ is non-square}.
\end{cases}$$

Note that when $a \in F^*_p$, we have $wt(c(a)) > 0$ for any $m$. This implies that the dimension of linear code $C_{D(\alpha)}$ is $m$.

Example 3.4. Let $p = 5$, $m = 3$ and $\alpha$ is square. By Magma, we have $C_{D(\alpha)}$ is a \([30, 3, 20]\) code, which confirms the results in Table 1.

Let $p = 7$, $m = 3$ and $\alpha$ is non-square. By Magma, we have $C_{D(\alpha)}$ is a \([56, 3, 42]\) code, which agrees with the results in Table 1.
Let $p = 3$, $m = 6$. By Magma, we have $C_{D(\alpha)}$ is a $[234, 6, 144]$ code, which agrees with the results in Table 2.

Let $p = 3$, $m = 4$. By Theorem 3.3, we have $C_{D(\alpha)}$ is a $[30, 4, 18]$ code, which confirms the results in Table 2. As we known, for $n = 30$, $k = 4$, the best code has parameters $[30, 4, 19]$. This implies that $C_{D(\alpha)}$ is almost optimal.

\[\square\]

4 Constant composition codes

In this section, we will construct a class of CCCs as subcodes of linear code $C_{D(\alpha)}$ defined by (3.1). For each $\gamma \in \mathbb{F}_p$, we let

\[S_\gamma = \{a \in \mathbb{F}_{p^m}^* | \text{Tr}(a^2) = \gamma\} \]

Let $\alpha \in \mathbb{F}_p^*$. Define

\[C_{D(\alpha)}^\gamma = \{c(a) | a \in S_\gamma\} \]

**Theorem 4.1.** Let $m$ be even and $\tau = (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}}$. The code $C_{D(\alpha)}^\gamma$ is a CCC with parameters $(n_\alpha, M, d, [\omega_\beta]_{\beta \in \mathbb{F}_p})$, where

1) in the case of $\gamma = 0$:

\[
\begin{align*}
    n_\alpha & = p^{m-1} + \tau p^{\frac{m-2}{2}} \\
    M & = p^{m-1} - (p-1)\tau p^{\frac{m-2}{2}} - 1 \\
    \omega_\beta & = \begin{cases} 
        p^{m-2} + \tau p^{\frac{m}{2}-1}, & \beta = 0; \\
        p^{m-2}, & \beta \neq 0.
    \end{cases} \\
    d & = \begin{cases} 
        (p-1)p^{m-2} - 2p^{\frac{m-2}{2}}, & \tau = -1; \\
        (p-1)p^{m-2}, & \tau = 1.
    \end{cases}
\end{align*}
\]

2) in the case of square $\alpha \gamma$:

\[
\begin{align*}
    n_\alpha & = p^{m-1} + \tau p^{\frac{m-2}{2}}; \\
    M & = p^{m-1} + \tau p^{\frac{m-2}{2}}; \\
    \omega_\beta & = \begin{cases} 
        p^{m-2} + (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}} \tau p^{\frac{m}{2}-1}, & \beta = 0; \\
        p^{m-2}, & \beta = \pm \sqrt{\alpha \gamma}; \\
        p^{m-2} + (-1)^{(\frac{p-1}{2})^2 \frac{m}{2}} \tau \eta(\alpha \gamma - \beta^2)p^{\frac{m}{2}-1}, & \text{otherwise.}
    \end{cases} \\
    d & = \begin{cases} 
        (p-1)p^{m-2} - 2p^{\frac{m-2}{2}}, & \tau = -1; \\
        (p-1)p^{m-2}, & \tau = 1.
    \end{cases}
\end{align*}
\]
3) in the case of non-square $\alpha \gamma$:

$$n_\alpha = p^{m-1} + \tau p^{m-2};$$

$$M = p^{m-1} + \tau p^{m-2};$$

$$\omega_\beta = \begin{cases} 
  p^{m-2} - (-1)^{(m-1)/2} \tau p^{\frac{m-2}{2}}, & \beta = 0; \\
  p^{m-2} + (-1)^{(m-1)/2} \tau p^{\frac{m-2}{2}}, & \text{otherwise.}
\end{cases}$$

$$d = \begin{cases} 
  (p-1)p^{m-1} - 2p^{m-2}, & \tau = -1; \\
  (p-1)p^{m-1}, & \tau = 1.
\end{cases}$$

**Proof.** Note that $\alpha \neq 0$, for any $\beta \in F_p$, by Lemmas 2.2 and 2.3, we have

$$\omega_\beta = \frac{1}{p} \sum_{x \in D(\alpha)} \sum_{u \in F_p} \zeta_{p}(\text{Tr}(ax) - \beta)$$

$$= \frac{1}{p^2} \sum_{x \in F_p^m} \sum_{u \in F_p} \zeta_{p}(\text{Tr}(ax) - \beta) \sum_{v \in F_p} \zeta_{p}(\text{Tr}(x^2) - \alpha)$$

$$= \frac{1}{p^2} \sum_{u \in F_p} \sum_{v \in F_p} \zeta_{p}^{-u\beta} \zeta_{p}^{-v\alpha} \sum_{x \in F_p^m} \zeta_{p}(\text{Tr}(ax+ux^2))$$

$$= \frac{1}{p^2} \sum_{u \in F_p} \sum_{v \in F_p} \zeta_{p}^{-u\beta} \zeta_{p}^{-v\alpha} \sum_{x \in F_p^m} \zeta_{p}(\text{Tr}(ux^2))$$

$$+ \frac{1}{p^2} \sum_{u \in F_p} \sum_{v \in F_p} \zeta_{p}^{-u\beta} \zeta_{p}^{-v\alpha} \sum_{x \in F_p^m} \zeta_{p}(\text{Tr}(ux+ux^2))$$

$$= \frac{1}{p^2} G(\eta, \chi_1) + \frac{1}{p^2} \sum_{u \in F_p} \sum_{v \in F_p} \zeta_{p}^{-u\beta} \zeta_{p}^{-v\alpha} \zeta_{p}(\text{Tr}(\frac{-a^2}{4v}u^2)) G(\eta, \chi_1)$$

$$= \frac{1}{p^2} G(\eta, \chi_1) + \frac{1}{p^2} G(\eta, \chi_1) \sum_{v \in F_p} \zeta_{p}^{-v\alpha} \sum_{u \in F_p} \zeta_{p}^{-\beta u - \frac{\text{Tr}(a^2)}{4v}u^2} - 1$$

$$= \frac{1}{p^2} G(\eta, \chi_1) \sum_{v \in F_p} \zeta_{p}^{-v\alpha} \sum_{u \in F_p} \zeta_{p}^{-\beta u - \frac{\text{Tr}(a^2)}{4v}u^2}. \quad (4.1)$$

If $\text{Tr}(a^2) = 0$, i.e. $\gamma = 0$, then (4.1) is equal to

$$\omega_\beta = \frac{1}{p^2} G(\eta, \chi_1) \sum_{v \in F_p} \zeta_{p}^{-v\alpha} \sum_{u \in F_p} \zeta_{p}^{-\beta u}$$

$$= \begin{cases} 
  p^{m-2} - \frac{1}{p} G(\eta, \chi_1), & \beta = 0; \\
  p^{m-2}, & \beta \neq 0.
\end{cases}$$
If $\text{Tr}(a^2) \neq 0$, i.e. $\gamma \neq 0$, then (4.1) is equal to

$$\omega_\beta = p^{m-2} + \frac{1}{p^2} G(\eta, \chi_1)G(\overline{\eta}, \overline{\chi}_1) \sum_{v \in \mathbb{F}_p^*} \zeta_p v \overline{\eta}( - \frac{\text{Tr}(a^2)}{4v} ) \zeta_p^\frac{\beta^2 v}{\text{Tr}(a^2)}$$

$$= p^{m-2} + \frac{1}{p^2} G(\eta, \chi_1)G(\overline{\eta}, \overline{\chi}_1) \overline{\eta}( - \text{Tr}(a^2) ) \sum_{v \in \mathbb{F}_p} \overline{\eta}(v) \zeta_p^{(-\alpha + \frac{\beta^2}{\text{Tr}(a^2)}) v}.$$  

Case I: if $\alpha \gamma$ is a square element, then we have

$$\omega_\beta = \begin{cases} 
  p^{m-2}, & \beta = \pm \sqrt{\alpha \gamma}; \\
  p^{m-2} + \frac{1}{p^2} G(\eta, \chi_1)G(\overline{\eta}, \overline{\chi}_1) \overline{\eta}( - \text{Tr}(a^2) ) \overline{\eta}( -\alpha + \frac{\beta^2}{\text{Tr}(a^2)} ) \sum_{v \in \mathbb{F}_p} \overline{\eta}(v) \zeta_p^v, & \text{otherwise.}
\end{cases}$$

Case II: if $\alpha \gamma$ is a non-square element, then we have

$$\omega_\beta = \begin{cases} 
  p^{m-2}, & \beta = \pm \sqrt{\alpha \gamma}; \\
  p^{m-2} + \frac{1}{p^2} G(\eta, \chi_1)G^2(\overline{\eta}, \overline{\chi}_1) \overline{\eta}( -\alpha \text{Tr}(a^2) - \beta^2 ) \sum_{v \in \mathbb{F}_p} \overline{\eta}(v) \zeta_p^v, & \text{otherwise.}
\end{cases}$$

$n_\alpha$ is the length of linear code $C_{D(\alpha)}$. Note that $M$ is the size of $S_\gamma$, which can be obtained from Lemma 2.4. Denote by $d_H(c(a_1), c(a_2))$ the Hamming distance of $c(a_1)$ and $c(a_2)$. When $a_1$ and $a_2$ run through $S_\gamma$ with $a_1 \neq a_2$, then $a_1 - a_2$ runs through $\mathbb{F}_p^*$. Therefore, the minimal distance of $C_{D(\alpha)}$ is the same as that of $C_{D(\alpha)}$.

The desired conclusions then follow from Lemmas 2.1 and 3.3.

**Corollary 4.2.** Let $t \in \mathbb{F}_p^*$, then

$$\sum_{x \in \mathbb{F}_p} \overline{\eta}(t - x^2) = (-1)^{(p-1)^2}.$$

**Proof.** Note that

$$\sum_{\beta \in \mathbb{F}_p} \omega_\beta = n_\alpha.$$

By Theorem 4.1, we finish the proof.

Therefore, from Theorem 4.1 and Corollary 4.2, we have the following result.
Proposition 4.3. For $\gamma \neq 0$, then
\[
\sum_{\beta \in \mathbb{F}_p} \omega_{\beta}^2 = p^{2m-3} + p^{m-1} + 2\tau p^{\frac{3m}{2} - 3}.
\]

Remark 4.4. By Proposition 4.3 and Theorem 4.1, we can check that
\[
n_{\alpha}d - n_{\alpha}^2 + \omega_{0}^2 + \omega_{1}^2 + \cdots + \omega_{p-1}^2 \leq 0, \quad \text{for} \quad \tau = \pm 1.
\]
Therefore, the LFVC bound cannot be applied to measure the optimality of these CCCs.

Acknowledgment

The authors would like to thank the referees for their comments that improved the readability of the paper. The work of L. Yu was supported by research funds of HBPU (Grant No. 17xjz04R).

References

[1] W. Chu, C.J. Colbourn and P. Dukes, “Constructions for permutation codes in powerline communications,” Des. Codes Cryptogr., 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 constant composition 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), 7482–7488, 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] L. Yu and X. Liu, “Constant Composition Codes as Subcodes of Linear Codes,” [arXiv:1706.06997](https://arxiv.org/abs/1706.06997).

[17] 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).

[18] 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.

[19] 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.

[20] 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.

[21] Z. Zhou and C. Ding, “A class of three-weight cyclic codes,” *Finite Fields Appl.* 25, 79–93, 2014.
[22] 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.