SOME CLASSES OF LCD CODES AND SELF-ORTHOGONAL CODES OVER FINITE FIELDS

XIA LI
School of Mathematics, Southwest Jiaotong University
Chengdu 610031, China
and
State Key Laboratory of Cryptology, P. O. Box 5159
Beijing 100878, China

FENG CHENG
School of Mathematics, Southwest Jiaotong University
Chengdu 610031, China

CHUNMING TANG
School of Mathematics and Information, China West Normal University
Nanchong 637002, China

ZHENGCHUN ZHOU
School of Mathematics, Southwest Jiaotong University
Chengdu 610031, China

(Communicated by Sihem Mesnager)

Abstract. Due to their important applications in theory and practice, linear complementary dual (LCD) codes and self-orthogonal codes have received much attention in the last decade. The objective of this paper is to extend a recent construction of binary LCD codes and self-orthogonal codes to the general \( p \)-ary case, where \( p \) is an odd prime. Based on the extended construction, several classes of \( p \)-ary linear codes are obtained. The characterizations of these linear codes to be LCD or self-orthogonal are derived. The duals of these linear codes are also studied. It turns out that the proposed linear codes are optimal in many cases in the sense that their parameters meet certain bounds on linear codes. The weight distributions of these linear codes are settled.

1. Introduction

Let \( q \) be a power of a prime and \( \mathbb{F}_q \) be the finite field with \( q \) elements. Let \( \mathbb{F}_q^n \) denote the vector space over \( \mathbb{F}_q \) with dimension \( n \). In this paper, we always write the elements of \( \mathbb{F}_q^n \) as column vectors unless otherwise stated. We use \( \text{wt}(x) \) to denote the weight of \( x \in \mathbb{F}_q^n \), i.e., the number of nonzero coordinates in \( x = (x_1, x_2, \cdots, x_n)^T \), where \( T \) denotes the transpose of \( x \). For any

\[ 2010 \text{ Mathematics Subject Classification: Primary: 06E75, 94A60, 11T23.} \]
\[ \text{Key words and phrases: Linear codes, self-orthogonal codes, LCD codes, weight distributions, Krawtchouck polynomial.} \]
\[ \ast \text{Corresponding author: Chunming Tang.} \]
\[ \mathbf{x} = (x_1, x_2, \cdots, x_n)^T \] and \( \mathbf{y} = (y_1, y_2, \cdots, y_n)^T \) in \( \mathbb{F}_q^n \), the *Euclidean inner product* of \( \mathbf{x} \) and \( \mathbf{y} \) is defined by
\[
\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i.
\]

An \([n, \kappa, d]\) linear code \( C \) over \( \mathbb{F}_q \) is a \( \kappa \)-dimensional subspace of \( \mathbb{F}_q^n \) with minimum (Hamming) distance \( d \). The *dual* of \( C \) is defined by
\[ C^\perp = \{ \mathbf{w} \in \mathbb{F}_q^n : \mathbf{w} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in C \}. \]

A linear code \( \mathcal{C} \) is called a *linear complementary dual* (LCD) code [27] if \( \mathcal{C} \cap \mathcal{C}^\perp = \{0\} \), and is called a *self-orthogonal code* [17] if \( \mathcal{C} \subseteq \mathcal{C}^\perp \).

Let \( A_i \) denote the number of codewords with Hamming weight \( i \) in a code \( \mathcal{C} \) of length \( n \). The weight enumerator of \( \mathcal{C} \) is defined by
\[ 1 + A_1 z + A_2 z^2 + \cdots + A_n z^n. \]

Accordingly, the sequence \((1, A_1, \cdots, A_n)\) is called the weight distribution of \( \mathcal{C} \). Clearly, the weight distribution gives the minimum distance of the code, and thus the error correcting capability. Moreover, the weight distribution of a code allows the computation of the error probability of error detection and correction with respect to some error detection and error correction algorithms (see [20] for details). Thus the study of the weight distribution of a linear code is important in both theory and applications. A linear code \( \mathcal{C} \) is said to be a \( t \)-weight code if the number of nonzero \( A_i \) in the sequence \((A_1, A_2, \cdots, A_n)\) is equal to \( t \).

Linear codes have wide applications in CD players, high speed modems, cellular phones, and data storage devices. In recent years, linear codes with some special properties have received renewed attentions due to their important role in new applications. Carlet and Guilley found that binary LCD codes could be used in cryptography to resist side-channel attacks and fault non-invasive attacks (see [2] and [5] for more details). Self-orthogonal codes can be used to construct quantum error-correcting codes, which can protect quantum information in quantum computations and quantum communications [3, 15]. Both algebraic and combinatorial constructions of self-orthogonal codes were reported in the literature (see [4, 10, 19] and the references therein).

The study of LCD cyclic codes (under the name of reversible cyclic codes) traces back to the seminal work of Massey [26] where LCD cyclic codes were introduced for data storage applications. Massey made a comparison between LCD codes and non-LCD codes [26], and demonstrated that asymptotically good LCD codes exist [27]. In 1970, Tzeng and Hartmann [33] made a subsequent contribution proving that the minimum distance of a class of LCD cyclic codes is greater than the BCH bound. Esmaeili and Yari [14] studied LCD codes that are quasi-cyclic. For a given length and minimum distance, Dougherty *et al.* [13] established a linear programming bound on the largest possible size of an LCD code. In [21] and [22], Li, Ding and Li gave a well-rounded treatment of LCD cyclic codes and obtained several classes of LCD codes with good parameters. Yan *et al.* [34] studied LCD BCH codes and presented several classes of LCD BCH codes. LCD MDS codes have been constructed from generalized Reed-Solomon codes in [31]. Mesnager *et al.* [28] proposed a construction of algebraic geometry Euclidean LCD codes. In addition, linear codes with Hermitian complementary dual were also studied in the literature [23], [8]. In [7], Carlet *et al.* completely determined all \( q \)-ary \((q > 3)\)
Euclidean LCD codes and all $q^2$-ary ($q > 2$) Hermitian LCD codes for all possible parameters. In a recent paper [9], Euclidean and Hermitian complementary dual were generalized to $\sigma$ complementary dual. Accordingly, Euclidean and Hermitian LCD codes were generalized to $\sigma$-LCD codes. To the best of our knowledge, it is hard to determine the minimal distances of these known LCD codes, not to mention their weight distribution. Very recently, employing a generic construction of linear codes by Ding [12], Zhou et al. [36] obtained several class of LCD codes and self-orthogonal codes which are optimal in many cases in the sense that their parameters meets certain bounds on linear codes. Notably, the weight distributions of some subclasses of these linear codes were completely settled in [36].

The main objective of this paper is to extend the construction of LCD codes and self-orthogonal codes in [36] from binary case to the general $p$-ary case, where $p$ is an odd prime. Specifically, we construct four classes of $p$-ary linear codes using the generic construction in [12]. We give very simple characterizations of these linear codes to be LCD codes or self-orthogonal codes. Using those characterizations, we obtain infinite families of $p$-ary LCD codes and self-orthogonal codes from the proposed linear codes and their duals. To our best knowledge, the self-orthogonal codes constructed in this paper have different parameters from that of those self-orthogonal codes constructed in other literature [30, 32, 35]. Until now, people can only determine the weight distribution of a few class of self-orthogonal codes. We completely determine the weight distributions of the linear codes constructed in this paper. Many LCD codes and self-orthogonal codes presented in this paper are optimal or almost optimal in the sense that they meet certain bounds on general linear codes.

We will compare some of the codes presented in this paper with the tables of best known linear codes (referred to as the Database later) maintained by Markus Grassl at http://www.codetables.de.

2. Some classes of $p$-ary LCD codes and self-orthogonal codes and their duals

Based on a generic construction of linear codes by Ding [12], several classes of binary LCD codes and self-orthogonal codes were constructed in [36]. In this section, we shall extend the results in [36] from the binary case to the general $p$-ary case, where $p$ is an odd prime. Before doing this, we first recall the generic construction of linear codes in [12] from the viewpoint of vector space.

Let $D = \{g_1, g_2, \cdots, g_n\} \subseteq \mathbb{F}_p^m$ and let $G$ be the $m \times n$ matrix formed by the column vectors $g_1, g_2, \cdots, g_n$:
\[
G = [g_1, g_2, \cdots, g_n].
\]

Using $D$, one can obtain a linear code of length $n$ over $\mathbb{F}_p$:
\[
C_D = \{a \cdot g_1, a \cdot g_2, \cdots, a \cdot g_n : a \in \mathbb{F}_p^m\}.
\]

The set $D$ is called the defining set of the code $C_D$. Clearly, $C_D$ is the linear code generated by the row vectors of the matrix $G$. Therefore $C_D$ is an $[n, k]$ linear code with $k = \text{Rank}(G)$, where $\text{Rank}(G)$ denotes the rank of the matrix $G$. In particular, if $k = m$, $G$ is exactly a generator matrix of $C_D$. The following result can be used to determine whether $C_D$ is LCD or self-orthogonal in terms of the ranks of $G$ and $GG^T$. 

Advances in Mathematics of Communications Volume 13, No. 2 (2019), 267–280
Proposition 1. For the linear code $C_D$ of (2), the dimensions of $C_D$ and $C_D \cap C_D^\perp$ are equal to $\text{Rank}(G)$ and $\text{Rank}(G) - \text{Rank}(GG^T)$, respectively.

Proof. It is clear that the dimension of $C_D$ is equal to the rank of the row vectors of $G$. Therefore $C_D$ is an $[n, \kappa]$ linear code with $\kappa = \text{Rank}(G)$. We denote by $c_i$ the $i$-th row of the matrix $G$ for $i \in \{1, 2, \cdots, m\}$. Let $c = \sum_{i=1}^{m} x_i c_i$ be any codeword in $C_D$, where $x_i \in \mathbb{F}_p$. Then, $c \in C_D \cap C_D^\perp$ if and only if 
$$\left( \sum_{i=1}^{m} x_i c_i \right) \cdot c_j = 0 \text{ for any } j \in \{1, 2, \cdots, m\},$$
that is
$$GG^T x = 0,$$
where $x = (x_1, x_2, \cdots, x_m)^T$. Let $K = \{x = (x_1, x_2, \cdots, x_m)^T \in \mathbb{F}_p^m : GG^T x = 0\}$ and let $\sigma$ be the linear transformation from $K$ to $C_D \cap C_D^\perp$ defined by
$$\sigma(x) = x^T G, \ \forall x \in K.$$Then, the dimension of $K$ is $m - \text{Rank}(GG^T)$ and the kernel of $\sigma$ is $m - \text{Rank}(G)$. Note that $\sigma$ is surjective. Thus, the dimension of $C_D \cap C_D^\perp$ equals $\text{Rank}(G) - \text{Rank}(GG^T)$. This completes the proof. $\square$

From Proposition 1, we immediately get the condition on the code $C_D$ to be LCD or self-orthogonal.

Corollary 1. Let $C_D$ be the linear code of (2). Then $C_D$ is LCD (resp. self-orthogonal) if and only if $\text{Rank}(GG^T) = \text{Rank}(G)$ (resp. $GG^T = 0$).

Note that the matrix $G$ of (1) is formed by all elements in the set $D$. Therefore, in order to construct LCD or self-orthogonal codes using the generic method introduced above, the key point is to choose an appropriate defining set $D$. This will be the focus of the next sections.

3. $p$-ary LCD codes and self-orthogonal codes from the generic construction

In this section, we shall construct four classes of linear codes from the generic construction mentioned above using the following four types of defining sets. It will be shown that the proposed linear codes contain infinite families of LCD codes and self-orthogonal codes. We follow the notation in Section 2.

For any positive integers $m, t$ with $1 \leq t \leq m - 1$, let $D_t$ be the set of vectors in $\mathbb{F}_p^m$ with weight $t$, where $p$ is an odd prime, that is
$$D_t = \{g \in \mathbb{F}_p^m : \text{wt}(g) = t\}.$$Let $D_{\leq t}$ be the set of nonzero vectors in $\mathbb{F}_p^m$ with weight no more than $t$, that is
$$D_{\leq t} = \{g \in \mathbb{F}_p^m : 1 \leq \text{wt}(g) \leq t\}.$$Define
$$\overline{D}_t = D_t \cup D_m,$$
and
$$\overline{D}_{\leq t} = D_{\leq t} \cup D_m.$$
3.1. LCD and self-orthogonal codes from $D_t$ and their duals. From now on, we always suppose that $n_t = \#D_t$. Then, $n_t = (p - 1)^t \binom{m}{t}$ according to the definition of $D_t$. Let $D_t = \{g_1, g_2, \cdots, g_{n_t}\}$ and $G_t = [g_1, g_2, \cdots, g_{n_t}]$.

**Lemma 3.1.** \(\text{Rank}(G_t) = m\) for any \(1 \leq t \leq m\).

**Lemma 3.2.** Let \(1 \leq t \leq m, p = 3, M = (m_{i,j})_{m \times m} = G_tG_t^T\). Then, \(m_{i,i} \equiv 2^t \binom{m-1}{t-1} \text{ (mod 3)}\) for \(i \in \{1, 2, \cdots, m\}\) and \(m_{i,j} \equiv 0 \text{ (mod 3)}\) for \(i \neq j\).

**Proof.** The conclusion of the case \(t = 1\) follows directly from the definition of $G_t$. We now prove the case \(t \geq 2\). Let \(c_i\) be the \(i\)-th row vector of $G_t$. Then,

\[
m_{i,i} = c_i c_i^T = c_i \cdot c_i = 2^{t-1} \binom{m-1}{t-1} (1 + 4) \equiv 2^t \binom{m-1}{t-1} \text{ (mod 3)}
\]

for \(i \in \{1, 2, \cdots, m\}\), and

\[
m_{i,j} = c_i c_j^T = c_i \cdot c_j = 2^{t-2} \binom{m-2}{t-2} (1 + 2 + 2 + 4) \equiv 0 \text{ (mod 3)}
\]

for \(i \neq j\). This completes the proof. $\square$

**Lemma 3.3.** Let \(p > 3, M = (m_{i,j})_{m \times m} = G_tG_t^T\). Then, \(M = 0\).

**Proof.** The proof is divided into the following two cases.

- **Case 1:** when \(t = 1\). In this case,

\[
M = (1 + 2^2 + \cdots + (p - 1)^2)E = \frac{(p - 1)p(2p - 1)}{6}E,
\]

where $E$ denotes the identity matrix of size \(m\).

If \(6 \mid (p - 1)\), then \(M \equiv 0 \text{ (mod p)}\);

If \(6 \nmid (p - 1)\), due to \(2 \mid (p - 1)\), so, \(3 \mid (p - 1)\), \(p \equiv 2 \text{ (mod 3)}\). For any positive integer \(k\), we have \(p = 3k + 2\). Hence, \(3 \mid (2p - 1)\). So, \(M \equiv 0 \text{ (mod p)}\).

- **Case 2:** when \(2 \leq t \leq m\). Let \(c_i\) be the \(i\)-th row vector of $G_t$. Then,

\[
m_{i,i} = c_i c_i^T = (p - 1)^{t-1} \binom{m-1}{t-1} (1 + 2^2 + \cdots + (p - 1)^2)
\]

\[
= \frac{(m-1)(p-1)^t p(2p-1)}{6} \equiv 0 \text{ (mod p)}
\]

for \(i \in \{1, 2, \cdots, m\}\), and

\[
m_{i,j} = c_i c_j^T
\]

\[
= (p - 1)^{t-2} \binom{m-2}{t-2} (1 \cdot (1 + 2 + \cdots + p - 1) + \cdots + (p - 1) \cdot (1 + 2 + \cdots + p - 1))
\]

\[
= \frac{(p - 1)^t p^2 \binom{m-2}{t-2}}{4}
\]

\[
\equiv 0 \text{ (mod p)}
\]

for \(i \neq j\). This completes the proof. $\square$
Lemma 3.4. Let \( t \) be a positive integer with \( 1 \leq t \leq m \). Then,
- when \( p = 3 \),
  \[
  \mathrm{Rank}(G_t^T G_t) = \begin{cases} 
  0, & \text{if } \binom{m-1}{t-1} \equiv 0 \pmod{3}, \\
  m, & \text{if } \binom{m-1}{t-1} \equiv 1 \text{ or } 2 \pmod{3}.
  \end{cases}
  \]
- when \( p > 3 \), \( \mathrm{Rank}(G_t^T G_t) = 0 \).

Proof. The conclusion directly follows from Lemmas 3.2 and 3.3. \( \square \)

Proposition 2. Let \( t \) be a positive integer with \( 1 \leq t \leq m \). Then,
- when \( p = 3 \),
  \[
  \dim_{F_3}(C_{D_t} \cap C_{D_t}^\perp) = \begin{cases} 
  \dim_{F_3}(C_{D_t}), & \text{if } \binom{m-1}{t-1} \equiv 0 \pmod{3}, \\
  0, & \text{if } \binom{m-1}{t-1} \equiv 1 \text{ or } 2 \pmod{3}.
  \end{cases}
  \]
- when \( p > 3 \), \( \dim_{F_p}(C_{D_t} \cap C_{D_t}^\perp) = \dim_{F_p}(C_{D_t}) \).

Proof. By Proposition 1, \( \dim_{F_p}(C_{D_t} \cap C_{D_t}^\perp) = \mathrm{Rank}(G_t) - \mathrm{Rank}(G_t^T G_t) \). The conclusion then follows from Lemmas 3.1 and 3.4. \( \square \)

Theorem 3.5. Let \( t \) be a positive integer with \( 1 \leq t \leq m \). Then, \( C_{D_t} \) is an \([n, \kappa]\) linear code with \( n = (p-1)\binom{m}{t} \) and \( \kappa = m \). Furthermore,
- when \( p = 3 \),
  1. \( C_{D_t} \) is self-orthogonal if and only if \( \binom{m-1}{t-1} \equiv 0 \pmod{3} \); and
  2. \( C_{D_t} \) is LCD, if and only if \( \binom{m-1}{t-1} \equiv 1 \text{ or } 2 \pmod{3} \).
- when \( p > 3 \), \( C_{D_t} \) is self-orthogonal.

Proof. Recall the definitions of LCD codes and self-orthogonal codes. The desired conclusions follow from Propositions 1 and 2. \( \square \)

Theorem 3.6. Let \( n = (p-1)\binom{m}{t} \) and \( C_{D_t} \) be the linear code in Theorem 3.5. Then \( C_{D_t}^\perp \) is a \( p \)-ary \([n, n-m, 2]\) linear code.

Example 1. Let \( p = 3 \), \( m = 4 \) and \( t = 2 \). Then \( C_{D_t} \) is a ternary self-orthogonal code with parameters \([24,4,12]\). The dual of \( C_{D_t} \) is a ternary linear code with parameters \([24,20,2]\), which is almost optimal according to the Database.

Example 2. Let \( p = 3 \), \( m = 5 \) and \( t = 2 \). Then \( C_{D_t} \) is a ternary LCD code with parameters \([40,5,16]\). The dual of \( C_{D_t} \) is a ternary LCD code with parameters \([40,35,2]\), which is almost optimal according to the Database.

Example 3. Let \( p = 5 \), \( m = 3 \) and \( t = 2 \). Then \( C_{D_t} \) is a 5-ary self-orthogonal code with parameters \([48,3,32]\). The dual of \( C_{D_t} \) is a 5-ary linear code with parameters \([48,45,2]\), which is optimal according to the Database.

3.2. LCD and self-orthogonal codes from \( \overline{D_t} \) and their duals. Recall that \( \overline{D_t} = D_t \cup D_m \). Let \( G_t = [g_1, \ldots, g_n, G_m] \) be the matrix formed by all the elements of \( \overline{D_t} \). Note that
\[
G_t G_t^T = G_t G_t^T + G_m G_m^T.
\]
Let \( p = 3 \), by Lemma 3.2, one has
\[
\mathrm{Rank}(G_t G_t^T) = \begin{cases} 
  0, & \text{if } \binom{m-1}{t-1} \equiv (-1)^{m-t+1} \pmod{3}, \\
  m, & \text{if } \binom{m-1}{t-1} \not\equiv (-1)^{m-t+1} \pmod{3}.
  \end{cases}
\]
This together with Proposition 1 yields
\[ \dim_{\mathbb{F}_q}(C_{D_t} \cap C_{D_t}^T) = \begin{cases} \dim_{\mathbb{F}_q}(C_{D_t}^T), & \text{if } (\frac{m-1}{t-1}) \equiv (-1)^{m-t+1} \pmod{3}, \\ 0, & \text{if } (\frac{m-1}{t-1}) \not\equiv (-1)^{m-t+1} \pmod{3}. \end{cases} \]

Let \( p > 3 \), by Lemma 3.3, one has \( \text{Rank}(G_t G_t^T) = 0 \). Combining this and Proposition 1 gives \( \dim_{\mathbb{F}_q}(C_{D_t} \cap C_{D_t}^T) = \dim_{\mathbb{F}_q}(C_{D_t}^T) \). Thus, we obtain the following.

**Theorem 3.7.** Let \( t \) be a positive integer with \( 1 \leq t \leq m - 1 \). Then, \( C_{D_t} \) is an \([n, \kappa] \) linear code with \( n = (p-1)^t \binom{m}{t} + (p-1)^m \) and \( \kappa = m \). Furthermore,

- when \( p = 3 \),
  1. \( C_{D_t} \) is self-orthogonal if and only if \( (\frac{m-1}{t-1}) \equiv (-1)^{m-t+1} \pmod{3} \); and
  2. \( C_{D_t} \) is LCD, if and only if \( (\frac{m-1}{t-1}) \not\equiv (-1)^{m-t+1} \pmod{3} \).
- when \( p > 3 \), \( C_{D_t}^T \) is self-orthogonal.

**Theorem 3.8.** Let \( n = (p-1)^t \binom{m}{t} + (p-1)^m \) and \( C_{D_t} \) be the linear code in Theorem 3.7. Then \( C_{D_t}^T \) is a \( p \)-ary \([n, n-m, 2] \) linear code.

**Example 4.** Let \( p = 3 \), \( m = 3 \) and \( t = 2 \). Then \( C_{D_3} \) is a ternary LCD code with parameters \([20, 3, 12]\) which is almost optimal according to the Database. The dual of \( C_{D_3} \) is a ternary LCD code with parameters \([20, 17, 2]\), which is almost optimal according to the Database.

**Example 5.** Let \( p = 3 \), \( m = 5 \) and \( t = 2 \). Then \( C_{D_3} \) is a ternary self-orthogonal code with parameters \([72, 5, 42]\). The dual of \( C_{D_3} \) is a ternary linear code with parameters \([72, 67, 2]\), which is almost optimal according to the Database.

**Example 6.** Let \( p = 5 \), \( m = 3 \) and \( t = 1 \). Then \( C_{D_3} \) is a 5-ary self-orthogonal code with parameters \([76, 3, 56]\). The dual of \( C_{D_3} \) is a 5-ary linear code with parameters \([76, 73, 2]\), which is optimal according to the Database.

### 3.3. LCD and self-orthogonal codes from \( D_{\leq t} \) and their duals.

In this subsection, we study the linear codes from the defining set \( D_{\leq t} \), where \( 1 \leq t \leq m \).

Let \( G_{\leq t} = [G_1 \vert G_2 \vert \cdots \vert G_t] \) be the matrix formed by the elements of \( D_{\leq t} \). By Lemma 3.1, \( \text{Rank}(G_{\leq t}) = m \).

\[
G_{\leq t} G_{\leq t}^T = [G_1 \vert G_2 \vert \cdots \vert G_t] [G_1 \vert G_2 \vert \cdots \vert G_t]^T
= \sum_{i=1}^{t} G_i G_i^T
\]

Let \( p = 3 \), by Lemma 3.2, one has
\[
\text{Rank}(G_{\leq t} G_{\leq t}^T) = \begin{cases} 0, & \text{if } \sum_{i=1}^{t} 2^i (\frac{m-1}{i-1}) \equiv 0 \pmod{3}, \\ m, & \text{if } \sum_{i=1}^{t} 2^i (\frac{m-1}{i-1}) \equiv 1 \text{ or } 2 \pmod{3}. \end{cases}
\]

Let \( p > 3 \), by Lemma 3.3, one has \( \text{Rank}(G_{\leq t} G_{\leq t}^T) = 0 \). Therefore, we arrive at the following.

**Theorem 3.9.** Let \( t \) be a positive integer with \( 1 \leq t \leq m \). Then, \( C_{D_{\leq t}} \) is an \([n, \kappa] \) linear code with \( n = \sum_{i=1}^{t} (p-1)^i \binom{m}{i} \) and \( \kappa = m \). Furthermore,
Example 10. Let \( C_n \) be a linear code with parameters \([124, 3, 36]\). Then \( C_n \) is self-orthogonal if and only if \( \sum_{i=1}^{t} 2^i (m-1) \equiv 0 \pmod{3} \); and

\[
(2) \quad C_n \text{ is LCD, if and only if } \sum_{i=1}^{t} 2^i (m-1) \equiv 1 \text{ or } 2 \pmod{3}.
\]

Example 11. Let \( \mathcal{C}_{D_n} \) be the linear code in Theorem 3.10. Then \( \mathcal{C}_{D_n} \) is a ternary self-orthogonal code with parameters \([82, 3, 36]\). The dual of \( \mathcal{C}_{D_n} \) is a ternary self-orthogonal code with parameters \([50, 5, 18]\). The dual of \( \mathcal{C}_{D_n} \) is a ternary linear code with parameters \([60, 5, 2]\), which is optimal according to the Database.

Example 12. Let \( \mathcal{C}_{D_n} \) be the ternary LCD code with parameters \([77, 3, 36]\) when \( p = 3 \), \( m = 3 \) and \( t = 2 \). Then \( \mathcal{C}_{D_n} \) is a ternary LCD code with parameters \([18, 15, 2]\), which is almost optimal according to the Database. The dual of \( \mathcal{C}_{D_n} \) is a 5-ary self-orthogonal code with parameters \([60, 5, 2]\), which is optimal according to the Database.

3.4. LCD AND SELF-ORTHOGONAL CODES FROM \( \text{D}_{\leq t} \) AND THEIR DUALS. Note that \( \text{D}_{\leq t} = D_{\leq t} \cup D_m \). We state the following results on \( \mathcal{C}_{\text{D}_{\leq t}} \), without proof since the proofs are similar to the case of \( \mathcal{C}_{D_n} \).

Theorem 3.11. Let \( t \) be a positive integer with \( 1 \leq t \leq m \). Then, \( \mathcal{C}_{\text{D}_{\leq t}} \) is an \([n, \kappa] \) linear code with \( n = \sum_{i=1}^{t} (p-1)^i (m)_i + (p-1)^m \) and \( \kappa = m \). Furthermore,

\[
\bullet \text{ when } p = 3,
\quad
(1) \quad \mathcal{C}_{\text{D}_{\leq t}} \text{ is self-orthogonal if and only if } \sum_{i=1}^{t} 2^i (m-1) + 2^m \equiv 0 \pmod{3};
\quad
\text{and}
\quad
(2) \quad \mathcal{C}_{\text{D}_{\leq t}} \text{ is LCD, if and only if } \sum_{i=1}^{t} 2^i (m-1) + 2^m \equiv 1 \text{ or } 2 \pmod{3}.
\]

\[
\bullet \text{ when } p > 3, \quad \mathcal{C}_{\text{D}_{\leq t}} \text{ is self-orthogonal.}
\]

Theorem 3.12. Let \( n = \sum_{i=1}^{t} (p-1)^i (m)_i + (p-1)^m \) and \( \mathcal{C}_{\text{D}_{\leq t}} \) be the linear code in Theorem 3.11. Then \( \mathcal{C}_{\text{D}_{\leq t}} \) is a \( p \)-ary \([n, n-m, 2]\) linear code.

Example 10. Let \( p = 3 \), \( m = 5 \) and \( t = 2 \). Then \( \mathcal{C}_{\text{D}_{\leq t}} \) is a ternary LCD code with parameters \([82, 5, 46]\). The dual of \( \mathcal{C}_{\text{D}_{\leq t}} \) is a ternary LCD code with parameters \([82, 77, 2]\), which is almost optimal according to the Database.

Example 11. Let \( p = 3 \), \( m = 3 \) and \( t = 2 \). Then \( \mathcal{C}_{\text{D}_{\leq t}} \) is a ternary self-orthogonal code with parameters \([26, 3, 18]\) which is optimal according to the Database. The dual of \( \mathcal{C}_{\text{D}_{\leq t}} \) is a ternary linear code with parameters \([26, 23, 2]\), which is optimal according to the Database.

Example 12. Let \( p = 5 \), \( m = 3 \) and \( t = 2 \). Then \( \mathcal{C}_{\text{D}_{\leq t}} \) is a 5-ary self-orthogonal code with parameters \([124, 3, 100]\) which is optimal according to the Database.
dual of $C_{D, t}$ is a 5-ary linear code with parameters $[124, 121, 2]$, which is optimal according to the Database.

4. The weight distributions of these linear codes

In this section we follow the notation in Section 3. In general it is difficult to determine the minimal distance of the aforementioned four classes of linear codes although we determined the minimal distance of their duals. However, this can be done in some special cases. Actually, we can establish the weight distribution of these linear codes we have constructed. Our main mathematical tool is the Krawtchouk polynomials which are closely related to coding theory [16] and cryptography.

4.1. Krawtchouck polynomials. For any prime power $q$ and positive integers $x, m$, the Krawtchouk polynomial $K_{q,i}(x, m)$ of degree $i$ is defined as

$$K_{q,i}(x, m) = \sum_{j=0}^{i} (-1)^j (q - 1)^{i-j} \binom{x}{j} \binom{m-x}{i-j}, \quad 0 \leq i \leq m.$$ 

In 1957, Lloyd [24], in his work on perfect codes, was the first to use the Krawtchouk polynomial in connection with coding theory. Krawtchouk polynomials have applications in computing the weight distribution of codes. Let $C$ be an $[n, k]$ code over $\mathbb{F}_q$ with weight distribution $\{1, A_1, \cdots, A_n\}$, and let the weight distribution of the dual code $C^\perp$ be $\{1, A_1^+, \cdots, A_n^+\}$. Then we have the following set of equations involving Krawtchouk polynomials,

$$q^k A_j^+ = \sum_{i=0}^{n} A_i K_{q,i}(i, n), \quad 0 \leq j \leq n,$$

which is equivalent to the MacWilliams equations.

Now let us focus on the case of $q = p$. We write

$$K_i(k, m) := K_{p,i}(k, m) = \sum_{j=0}^{i} (-1)^j (p - 1)^{i-j} \binom{k}{j} \binom{m-k}{i-j}.$$ 

The following properties of the Krawtchouk polynomial will be needed later.

**Lemma 4.1** (Lemma 1, [6]). Let $m, k, r$ be integers such that $m, k \geq 1$ and $0 \leq r \leq m$. Then we have

$$\sum_{i=0}^{r} K_i(k, m) = K_r(k-1, m-1).$$ 

**Lemma 4.2** (Lemma 2.6.2, [17]). For any fixed vector $w \in \mathbb{F}_p^m$ with $\text{wt}(w) = k$, we have

$$\sum_{x \in \mathbb{F}_p^m, \text{wt}(x) = i} \zeta_p^{w \cdot x} = \sum_{j=0}^{i} (-1)^j (p - 1)^{i-j} \binom{k}{j} \binom{m-k}{i-j} = K_i(k, m),$$

where $\zeta_p = \exp\left(\frac{2\pi \sqrt{-1}}{p}\right)$ is the primitive $p$-th root of unity in the field of complex numbers.
4.2. The Weight Distribution of $C_{D_t}$.

**Theorem 4.3.** Let $C_{D_t}$ be the linear codes in Theorem 3.5 with $1 \leq t \leq m$, and $n = (p - 1)^t \binom{m}{t}$. Then $C_{D_t}$ is an $[n, m]$ linear code with the weight distribution given in Table 1.

| Weight | Multiplicity |
|--------|--------------|
| 0      | 1 time       |
| $(p-1)^{t-k}K_t(k, m)$ for $k = 1, 2, \ldots, m - 1$ | $(p-1)^t \binom{m}{k}$ times |
| $(p-1)^t(p-1)^t + (p-1)^{t+1}$ | $(p-1)^m$ times |

**Proof.** The length and dimension of $C_{D_t}$ follow from Theorem 3.5. Therefore, we only need to calculate its weight distribution. Let $c_a = (a \cdot g_1, a \cdot g_2, \ldots, a \cdot g_n)$ be any codeword in $C_{D_t}$, where $a \in \mathbb{F}_p^m$. Then the weight of $c_a$ is equal to $n - N_a$, where $N_a = |\{ x \in \mathbb{F}_p^m : \text{wt}(x) = t \text{ and } a \cdot x = 0 \}|$.

Let $\text{wt}(a) = k$, where $k$ is an integer with $0 \leq k \leq m$. Clearly there are $(p-1)^k \binom{m}{k}$ vectors $a$ in $\mathbb{F}_p^m$ with $\text{wt}(a) = k$. In terms of exponential sums, the weight of $c_a$ can be calculated as follows:

\[
\text{wt}(c_a) = n - N_a = n - \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{x \in D_t} \zeta_p^{y(a \cdot x)} = n - \frac{1}{p} \left( n + \sum_{x \in D_t} \zeta_p^{a \cdot x} + \sum_{x \in D_t} \zeta_p^{2a \cdot x} + \cdots + \sum_{x \in D_t} \zeta_p^{(p-1)a \cdot x} \right)
\]

\[
= n - \frac{1}{p} \left( n + (p-1)K_t(k, m) \right)
\]

\[
= \frac{(p-1)n - (p-1)K_t(k, m)}{p}.
\]

**Example 13.** Let $p = 3, m = 3$. Then the weight enumerator of $C_{D_2}$ is $1 + 8z^6 + 6z^8 + 12z^{10}$.

**Example 14.** Let $p = 3, m = 4$. Then the weight enumerator of $C_{D_2}$ is $1 + 24z^{12} + 56z^{18}$.

**Example 15.** Let $p = 5, m = 3$. Then the weight enumerator of $C_{D_2}$ is $1 + 12z^{32} + 64z^{36} + 48z^{44}$.

4.3. The Weight Distribution of $C_{D_{\leq t}}$. In this subsection, we establish the weight distribution of the linear codes $C_{D_{\leq t}}$. We have the following results.

**Theorem 4.4.** Let $C_{D_{\leq t}}$ be the linear codes in Theorem 3.9 with $1 \leq t \leq m$, and $n = \sum_{i=1}^{t} (p - 1)^i \binom{m}{i}$. Then $C_{D_{\leq t}}$ is an $[n, m]$ linear code with the weight distribution given in Table 2.
Table 2. The weight distribution of $C_{D_i}$ for $1 \leq t \leq m$

| Weight | Multiplicity |
|--------|--------------|
| 0      | 1 time       |
| $\frac{1}{i} \binom{m}{i} - \frac{1}{i} \binom{m-1}{i} + p - 1$ | $(p-1)m$ times |
| $\frac{1}{i} \binom{p-1}{i} \binom{m-1}{i} + (p-1)^k \binom{m}{i}$ | $(p-1)^k \binom{m}{i}$ times |

Proof. The length and dimension of $C_{D_i}$ follow from Theorem 3.9. Therefore, we only need to calculate its weight distribution. Let $c_a = (a \cdot g_1, a \cdot g_2, \ldots, a \cdot g_n)$ be any codeword in $C_{D_i}$, where $a \in \mathbb{F}_p^m$. Then the weight of $c_a$ is equal to $n - N_a$, where

$$N_a = |\{x \in \mathbb{F}_p^m : \text{wt}(x) \leq t \text{ and } a \cdot x = 0\}|.$$ 

Let $\text{wt}(a) = k$, where $k$ is an integer with $0 \leq k \leq m$. Clearly there are $(p-1)^k \binom{m}{k}$ vectors $a$ in $\mathbb{F}_p^m$ with $\text{wt}(a) = k$. In terms of exponential sums, the weight of $c_a$ can be calculated as follows:

$$\text{wt}(c_a) = n - N_a$$

$$= n - \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{x \in D_{\leq t}} \zeta_p^{y(a \cdot x)}$$

$$= n - \frac{1}{p} (n + \sum_{x \in D_{\leq t}} \zeta_p^{a \cdot x} + \sum_{x \in D_{\leq t}} \zeta_p^{2a \cdot x} + \cdots + \sum_{x \in D_{\leq t}} \zeta_p^{(p-1)a \cdot x})$$

$$= n - \frac{1}{p} (n + (p-1)K_1(k, m) + (p-1)K_2(k, m) + \cdots + (p-1)K_t(k, m))$$

$$= n - \frac{1}{p} (n + (p-1)K_t(k-1, m-1) - (p-1)).$$

$$= \frac{(p-1)n - (p-1)K_t(k-1, m-1) + (p-1)}{p}$$

Example 16. Let $p = 3$, $m = 3$. Then the weight enumerator of $C_{D_{\leq 2}}$ is $1 + 6z^{10} + 8z^{12} + 12z^{14}$.

Example 17. Let $p = 3$, $m = 4$. Then the weight enumerator of $C_{D_{\leq 2}}$ is $1 + 8z^{14} + 16z^{20} + 24z^{22} + 32z^{24}$.

Example 18. Let $p = 5$, $m = 3$. Then the weight enumerator of $C_{D_{\leq 2}}$ is $1 + 12z^{36} + 64z^{48} + 48z^{52}$.

4.4. The weight distributions of $C_{D_{\leq t}}$ and $C_{D_{\leq t}}$. Using a discussion that is completely similar with Subsections 4.2 and 4.3, we can obtain the weight distributions of the linear codes $C_{D_{\leq t}}$ and $C_{D_{\leq t}}$.

Theorem 4.5. Let $C_{D_{\leq t}}$ be the linear codes in Theorem 3.7 with $1 \leq t \leq m$, and $n = (p-1)^t \binom{m}{t} + (p-1)^m$. Then $C_{D_{\leq t}}$ is an $[n, m]$ linear code with the weight distribution given in Table 3.

For the linear codes $C_{D_{\leq t}}$, their weight distribution is presented in the following theorem.
Table 3. The weight distribution of $C_{D_t}$ for $1 \leq t \leq m$

| Weight | Multiplicity |
|--------|--------------|
| 0      | 1 time       |
| $\frac{(p-1)n-(p-1)K_t(k,m)+K_m(k,m)}{p}$ for $k = 1, 2, \cdots, m-1$ | $(p-1)^{k} \binom{m}{k}$ times |
| $\frac{(p-1)(p-1)^{t}+(p-1)^{t+1}}{p}$ | $(p-1)^{m}$ times |

Theorem 4.6. Let $C_{D_{\leq t}}$ be the linear codes in Theorem 3.11 with $1 \leq t \leq m$, and $n = \sum_{i=1}^{t} (p-1)^{i} \binom{m}{i} + (p-1)^{m}$. Then $C_{D_{\leq t}}$ is an $[n, m]$ linear code with the weight distribution given in Table 4.

Table 4. The weight distribution of $C_{D_t}$ for $1 \leq t \leq m$

| Weight | Multiplicity |
|--------|--------------|
| 0      | 1 time       |
| $\frac{p(p-1)^{m} + \sum_{i=1}^{t} (p-1)^{i+1} \binom{m}{i} - (p-1)^{t+1} \binom{m-1}{t-1} + p-1}{p}$ | $(p-1)^{m}$ times |
| $\frac{(p-1)n-(p-1)K_t(k-1,m-1)+K_m(k,m)-1}{p}$ | $(p-1)^{k} \binom{m}{k}$ times |

5. Conclusion

In this paper, several classes of $p$-ary linear codes were constructed by generalizing a previous construction of binary ones. Their parameters were studied and their properties to be LCD or self-orthogonal were also characterized. The duals of these codes were also given. Some of these codes are optimal or almost optimal. The weight distributions of these linear codes were established as well.

6. Acknowledgments

The authors are very grateful to the reviewers and the Editor, Prof. Sihem Mesnager, for their valuable comments and suggestions that improved the presentation and quality of this paper. The work of X. Li and Z. Zhou was supported by National Cryptography Development Fund under Grant MMJJ20180103. The work of C. Tang was supported by NSFC under Grant 11871058.

References

[1] E. R. Berlekamp, *Algebraic Coding Theory*, Revised edition. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2015.
[2] J. Bringer, C. Carlet, H. Chabanee, S. Guilley and H. Maghrebi, Orthogonal direct sum masking, a smartcard friendly computation paradigm in a code, with builtin protection against side-channel and fault attacks, Proceedings of WISTP 2014. *Lecture Notes in Computer Science, 8501* (2014), 40–56.
[3] A. K. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction and orthogonal geometry, *Phys. Rev. Lett.*, 78 (1997), 405–408.
[4] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Inform. Theory, 44* (1998), 1369–1387.
[5] C. Carlet and S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, In: E. R. Pinto et al. (eds.), *Coding Theory and Applications, CIM Series in Mathematical Sciences, 3* (2014), 97–105, Springer Verlag.
Some classes of LCD codes and self-orthogonal codes

[6] C. Carlet, X. Zeng, C. Li and L. Hu, Further properties of several classes of boolean functions with optimum algebraic immunity, Des. Codes Cryptogr., 52 (2009), 303–338.

[7] C. Carlet, S. Mesnager, C. Tang, Y. Qi and R. Pellikaan, Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$, IEEE Trans. Inform. Theory, 64 (2018), 3010–3017.

[8] C. Carlet, S. Mesnager, C. Tang and Y. Qi, Euclidean and Hermitian LCD MDS codes, Designs, Codes Cryptogr., 86 (2018), 2605–2618.

[9] C. Carlet, S. Mesnager, C. Tang and Y. Qi, On $\sigma$-LCD codes, IEEE Trans. Inform. Theory, accepted for publication.

[10] H. Chen, S. Ling and C. Xing, Quantum codes from concatenated algebraic-geometric codes, IEEE Trans. Inform. Theory, 51 (2005), 2915–2920.

[11] D. K. Dalai, S. Maitra and S. Sarkar, Basic theory in construction of boolean functions with maximum possible annihilator immunity, Des. Codes Cryptogr., 40 (2006), 41–58.

[12] C. Ding, Linear codes from some 2-designs, IEEE Trans. Inform. Theory, 61 (2015), 3265–3275.

[13] S. T. Dougherty, J.-L. Kim, B. Özkaya, L. Sok and P. Solé, The combinatorics of LCD codes: Linear Programming bound and orthogonal matrices, International Journal of Information and Coding Theory, 4 (2017), 116–128.

[14] M. Esmaili and S. Yari, On complementary-dual quasi-cyclic codes, Finite Fields Appl., 15 (2009), 375–386.

[15] D. Gottesman, A class of quantum error-correcting codes saturating the quantum Hamming bounds, Phys. Rev. A, 54 (1996), 1862–1868.

[16] Z. Heng, C. Ding and Z. Zhou, Minimal linear codes over finite fields, Finite Fields and Their Applications, 54 (2018), 176–196.

[17] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge university press, 2003.

[18] L. Jin, Construction of MDS codes with complementary duals, IEEE Trans. Inform. Theory, 63 (2017), 2843–2847.

[19] L. Jin and C. Xing, Euclidean and Hermitian self-orthogonal algebraic geometry codes and their application to quantum codes, IEEE Trans. Inform. Theory, 58 (2012), 5484–5489.

[20] T. Kløve, Codes for Error Detection, World Scientific, 2007.

[21] C. Li, C. Ding and S. X. Li, LCD cyclic codes over finite fields, IEEE Trans. Inform. Theory, 63 (2017), 4344–4356.

[22] S. Li, C. Li, C. Ding and H. Liu, Two families of LCD BCH codes, IEEE Trans. Inform. Theory, 63 (2017), 5699–5717.

[23] C. Li, Hermitian LCD codes from cyclic codes, Des. Codes Cryptogr., 86 (2018), 2261–2278.

[24] S. Lloyd, Binary block coding, Bell Labs Technical Journal, 36 (1957), 517–535.

[25] E. Lucas, Sur les congruences des nombres euleriens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier, Bull. Soc. Math. (France), 6 (1878), 49–54.

[26] J. L. Massey, Reversible codes, Information and Control, 7 (1964), 369–380.

[27] J. L. Massey, Linear codes with complementary duals, Discrete Math., 106/107 (1992), 337–342.

[28] S. Mesnager, C. Tang and Y. Qi, Complementary dual algebraic geometry codes, IEEE Trans. Inform. Theory, 64 (2018), 2390–2397.

[29] N. Sendrier, Linear codes with complementary duals meet the Gilbert–Varshamov bound, Discrete Math., 285 (2004), 345–347.

[30] A. Sharma, Self-dual and self-orthogonal negacyclic codes of length $2^mp^n$ over a finite field, Discrete Mathematics, 338 (2015), 576–592.

[31] X. Shi, Q. Yue and S. Yang, New LCD MDS codes constructed from generalized Reed–Solomon codes, Cryptogr. Commun., 10 (2018), 1165–1182.

[32] R. Townsend and E. Weldon, Self-orthogonal quasi-cyclic codes, IEEE Transactions on Information Theory, 13 (1967), 183–195.

[33] K. K. Tzeng and C. R. P. Hartmann, On the minimum distance of certain reversible cyclic codes, IEEE Trans. Inform. Theory, 16 (1970), 644–646.

[34] H. Yan, H. Liu, C. Li and S. Yang, Parameters of LCD BCH codes with two lengths, Advances in Mathematics of Communications, 12 (2018), 579–594.

[35] T. Zhang and G. Ge, Quantum codes derived from certain classes of polynomials, IEEE Transactions on Information Theory, 62 (2016), 6638–6643.
[36] Z. Zhou, C. Tang, X. Li and C. Ding, Binary LCD Codes and Self-orthogonal Codes from a Generic Construction, IEEE Trans. Inform. Theory, 65 (2019), 16–27.

Received March 2018; revised September 2018.

E-mail address: lixia@my.swjtu.edu.cn
E-mail address: chengfeng2013@swjtu.edu.cn
E-mail address: tangchunmingmath@163.com
E-mail address: zzc@swjtu.edu.cn