CONSTRUCTIONS OF LINEAR CODES WITH SMALL HULLS FROM ASSOCIATION SCHEMES

YE WANG AND RAN TAO*
School of Mathematical Sciences, Zhejiang University
Zhejiang, 310027, China

(Communicated by Sihem Mesnager)

Abstract. The intersection of a linear code and its dual is called the hull of this code. The code is a linear complementary dual (LCD) code if the dimension of its hull is zero. In this paper, we develop a method to construct LCD codes and linear codes with one-dimensional hull by association schemes. One of constructions in this paper generalizes that of linear codes associated with Gauss periods given in [5]. In addition, we present a generalized construction of linear codes, which can provide more LCD codes and linear codes with one-dimensional hull. We also present some examples of LCD MDS, LCD almost MDS codes, and MDS, almost MDS codes with one-dimensional hull from our constructions.

1. Introduction

Let $q$ be a prime power and $\mathbb{F}_q$ denote a finite field of order $q$. An $[n, k, d]$ linear code $C$ over $\mathbb{F}_q$ is a $k$-dimensional subspace of $\mathbb{F}_q^n$ whose minimum Hamming distance is $d$. The dual code $C^\perp$ of $C$ over $\mathbb{F}_q$ is defined as

$$C^\perp = \{ b \in \mathbb{F}_q^n : b \cdot c^T = 0, \forall c \in C \},$$

where $b \cdot c^T$ is the standard inner product of the vectors $b$ and $c$. The hull of the linear code $C$ is defined as

$$\text{Hull}(C) := C \cap C^\perp.$$

The hull plays an important role in determining the complexity of algorithms for checking permutation equivalence of two linear codes and the computation of the automorphism group of a linear code [22, 23], which is always effective when the dimension of the hull is small. The code $C$ is called linear complementary dual (LCD) if the dimension of Hull($C$) is 0, i.e., Hull($C$) = $\{0\}$. For a linear code $C$, the minimum distance $d$ is bounded by the Singleton bound: $d \leq n - k + 1$. If $d = n - k + 1$, then the code $C$ is a maximum distance separable (MDS) code. If $d = n - k$, then the code $C$ is an almost MDS code.

LCD codes are widely applied in data storage, communication systems and consumer electronics and so on. Recently, they have been employed in cryptography. LCD codes were first introduced by Massey [19], and there was a construction of LCD codes whose minimum Hamming distance is at least as great by modifying an arbitrary $[n, k]$ linear code. Carlet and Gailley [4] introduced an application of binary LCD codes against side-channel attacks (SCA) and fault injection attacks.

2020 Mathematics Subject Classification: 94B05, 05E30, 11T24.

Key words and phrases: LCD code, Hull, association scheme, Gauss period, cyclotomic field.

* Corresponding author: Ran Tao.
(FIA). In addition to their practical applications, LCD codes are also interesting objects in the field of algebraic coding. The equivalence of many types of codes with LCD codes has been extensively studied. Carlet et al. [6] showed that any MDS code is equivalent to an LCD code and Jin et al. [13] showed that an algebraic geometry code over \( F_{2^m} \) \((m \geq 7)\) is equivalent to an LCD code. After that, a celebrated result was given in [8], which proved that any linear code over \( F_q \) \((q > 3)\) is equivalent to an LCD code. The study of LCD codes is thus becoming more interesting. Plenty of works have been devoted to the constructions of LCD codes. Liu et al. [18] provided a construction of LCD matrix-product codes with quasi-orthogonal matrices. Li et al. constructed several families of LCD cyclic codes over finite fields in [15]. In [20], Mesnager et al. gave a construction of algebraic geometry LCD codes which could be good candidates to be resistant against SCA. For more discussions about LCD codes, please refer to [7, 8, 17, 21, 24].

What needs to be emphasized is that Carlet et al. [5] employed character sums in semi-primitive case to construct LCD codes and linear codes with one-dimensional hull. Inspired by their results, we notice that there is a close connection between association schemes and LCD codes. We give some constructions of LCD codes and linear codes with one-dimensional hull by association schemes in this work. One of constructions in this paper generalizes that of linear codes associated with Gauss periods given in [5], which will be illustrated in details in Section 3.

This paper is organized as follows. In Section 2, we review some basic facts on algebraic number theory, association schemes and characters. In Section 3, several constructions of LCD codes and linear codes with one-dimensional hull by association schemes are presented. In Section 4, we provide generalized construction to get more LCD codes and linear codes with one-dimensional hull by combining association schemes and matrix extended. Finally, Section 5 concludes this paper.

2. Preliminaries

2.1. Algebraic number theory. We first introduce some results on algebraic number theory, which can be found in [10] and [12].

Let \( \mathbb{Q} \) be the rational number field and \( K \) be a finite extension over \( \mathbb{Q} \) of degree \( n \). Let \( \mathbb{Z} \) denote the ring of integers, an element \( \alpha \in K \) is called an algebraic integer if there is a polynomial \( f(x) = x^n + r_1x^{n-1} + \cdots + r_n \) where \( r_1, \ldots, r_n \in \mathbb{Z} \), such that \( f(\alpha) = 0 \). The set of all algebraic integers forms a ring denoted by \( \mathbb{O}_K \), which is a Dedekind domain. We call the elements in \( \mathbb{Z} \) rational integers and it is clear that \( \mathbb{Z} \subseteq \mathbb{O}_K \).

Let \( p \) be a prime. Then \( p\mathbb{O}_K \) is the principal ideal generated by \( p \) in \( \mathbb{O}_K \), which can be written uniquely as a product of prime ideals of \( \mathbb{O}_K \). Let \( \mathcal{P} \) be a prime ideal of \( \mathbb{O}_K \) containing \( p\mathbb{O}_K \). If \( p\mathbb{O}_K \subseteq \mathcal{P}^e \) and \( p\mathbb{O}_K \not\subseteq \mathcal{P}^{e+1} \), then we call \( e = \text{ord}_\mathcal{P}(p) \) the ramification index of \( \mathcal{P} \). Since \( \mathbb{O}_K \) is a Dedekind domain, then every prime ideal \( \mathcal{P} \) is maximal and \( \mathbb{O}_K/\mathcal{P} \) is a finite field, which contains \( \mathbb{Z}/p\mathbb{Z} \). Thus the number of elements in \( \mathbb{O}_K/\mathcal{P} \) is \( p^f \), where \( f := [\mathbb{O}_K/\mathcal{P} : \mathbb{Z}/p\mathbb{Z}] \). The number \( f \) is called the degree of \( \mathcal{P} \).

Let \( \mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_g \) be all the prime ideals in \( \mathbb{O}_K \) containing \( p\mathbb{O}_K \). Let \( e_i \) and \( f_i \) be ramification index and degree of \( \mathcal{P}_i \) respectively for each \( i = 1, 2, \ldots, g \). Then

\[
p\mathbb{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\cdots\mathcal{P}_g^{e_g}.
\]
There exists a relation among the numbers $f_i, e_i \ (i = 1, 2, \ldots, g)$ and $n$

$$\sum_{i=1}^{g} e_i f_i = n.$$ 

Let $m$ be an integer with $m \geq 3$ and $m \not\equiv 2 (\text{mod } 4)$. We set $\zeta_m = e^{\frac{2\pi i}{m}}$ to be the $m$-th primitive root of unity. Let $K = \mathbb{Q}(\zeta_m)$ be the cyclotomic field of $m$-th primitive root of unity. Then we have $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$. The following lemma gives the decomposed form of $p\mathcal{O}_K$ in $\mathcal{O}_K$ for a rational prime $p$.

**Lemma 2.1.** [10, Theorem 2.14] Let $K = \mathbb{Q}(\zeta_m)$ be the cyclotomic field defined as above. For each prime $p \in \mathbb{Z}$, we set $m = p^f m' \ (l \geq 0)$ and $p \nmid m'$. Let $f$ be the minimal rational integer such that $p^f \equiv 1 (\text{mod } m')$. Then

$$p\mathcal{O}_K = (\mathcal{P}_1 \mathcal{P}_2 \cdots \mathcal{P}_g)^e,$$

where $e = \varphi(p^f)$, each $\mathcal{P}_i$ has degree $f$ and $g = \frac{\varphi(m')}{f}$. Here $\varphi$ is the Euler function.

### 2.2. Association Schemes

**Definition 2.2.** Let $X$ be a finite set and let $R_i (i = 0, 1, \ldots, d)$ be subsets of $X \times X$ with the properties that

1. $R_0 = \{(x, x) | x \in X\}$;
2. $X \times X = R_0 \cup \ldots \cup R_d$ and $R_i \cap R_j = \emptyset$ if $i \neq j$;
3. $R_i^T = R_{i'}$ for some $i' \in \{0, 1, \ldots, d\}$, where $R_i := \{(x, y) : (y, x) \in R_i\}$. If $i' = i$, $R_i$ is called symmetric;
4. for all $i, j, k$ in $\{0, 1, 2, \ldots, d\}$, there is an integer $p_{ij}^k$ such that, for all $(x, y) \in R_k$,

$$|\{z \in X | (x, z) \in R_i \text{ and } (z, y) \in R_j\}| = p_{ij}^k.$$ 

Such a configuration $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ is called an association scheme with $d$ classes on $X$. Furthermore, an association scheme is said to be symmetric if every $R_i$ is symmetric for $0 \leq i \leq d$ and is called commutative if $p_{ij}^k = p_{ji}^k$ for all $i, j, k$.

**Definition 2.3.** Let $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ be an association scheme with $d$ classes. For $i \in \{0, 1, \ldots, d\}$, $A_i$ is defined as the adjacency matrix of the relation $R_i$ whose rows and columns are indexed by the elements of $X$ and

$$(A_i)_{xy} = \begin{cases} 
1, & \text{if } (x, y) \in R_i, \\
0, & \text{otherwise}. 
\end{cases}$$

Then the above properties (1)-(4) of the association scheme $\mathcal{X}$ in Definition 2.2 are equivalent to the following properties respectively:

1. $A_0 = I$;
2. $A_0 + A_1 + \ldots + A_d = J$, where $J$ is the all-ones matrix;
3. for each $i$ there is an $i'$ such that $A_i^T = A_{i'}$, where $A_i^T$ expresses the transpose of $A_i$;
4. $A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k$ for all $i, j \in \{0, 1, \ldots, d\}$.

Thus the vector space $(A_0, A_1, \ldots, A_d)_{\mathbb{C}}$ forms an algebra $\mathcal{M}$, which is called the Bose-Mesner algebra. For a commutative association scheme the Bose-Mesner algebra is commutative. In the remaining part of this paper, we just consider the commutative association schemes and all association schemes shown in Section 3 are commutative.
Let $X = (X_i, R_i)_{0 \leq i \leq d}$ be a commutative association scheme with $X = \{x_1, x_2, \ldots, x_n\}$ and $M = \langle A_0, A_1, \ldots, A_d \rangle_{\mathbb{C}}$ be the corresponding commutative algebra. Since $A_i^2 A_j = A_j A_i^T$ by the commutativity of $M$, then $A_i$ is a normal matrix. Thus, the adjacency matrices $A_0, A_1, \ldots, A_d$ are pairwise commutative normal matrices. By linear algebraic theory, they can be diagonalized simultaneously by a unitary matrix over $\mathbb{C}$. There is a decomposition of $V = \mathbb{C}^{|X|} = \mathbb{C}^n$ as

$$V = V_0 \oplus V_1 \oplus \ldots \oplus V_r,$$

where each $V_i$ is a common eigenspace of $A_0, A_1, \ldots, A_d$. We take such a decomposition with $r$ minimal. Then for any $i \neq j$, there is an integer $k$ such that $A_k$ has distinct eigenvalues on $V_i$ and $V_j$. Since the eigenspace of $J = \sum_{i=0}^d A_i$ belonging to the eigenvalue $n$ is the subspace spanned by $(1, 1, ..., 1)$, the one-dimensional subspace $\langle (1, 1, ..., 1) \rangle$ is exactly $V_i$ for some $i$. Then we may choose $i = 0$ such that $\dim V_0 = 1$. Let $p_i(j)$ be the eigenvalue of $A_i$ on $V_j$. In the following part of this subsection, we denote the conjugate of $v$ by $v^c$, the transpose of $v$ by $v^T$, the conjugate and transpose of $v$ by $v^H$ and the conjugate of $p_i(j)$ by $p_i(j)^c$, respectively. If $A_i^2 = A_j$, we take $v \in V_j$ such that $v \neq 0$. Then $v A_i = p_i(j)v$ gives $v A_i v^H = p_i(j)v v^H$. Taking transpose and conjugate, we get $v A_i^T v^H = p_i(j)^c v v^H$. Similarly, $v A_i v = p_i(j)^c v$ gives $v A_i v^H = p_i(j) v v^H$. It follows that $p_i(j) = p_i(j)^c$.

It’s obvious that $A_0, A_1, \ldots, A_d$ form a basis of $M$. We now introduce another basis of $M$. For each $i = 1, 2, \ldots, r$, let $E_i$ be the orthogonal projection $V \to V_i$ expressed in a matrix form with respect to the basis $\{e_x | x \in X\}$, where $e_x = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{C}^n$ with 1 in the $i$-th place for $x = x_i \in X$. By the properties of orthogonal projection, we have

$$E_0 + E_1 + \ldots + E_r = I, \quad E_0 = \frac{1}{|X|} J, \quad \text{and} \quad E_i E_j = \delta_{ij} E_i,$$

where $\delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases}$

We explore the interplay between $E_i$’s and $A_i$’s. Recall that $p_i(j)$ is the eigenvalue of $A_i$ on $V_j$. It follows that $E_j A_i = p_i(j) E_j$ and then $A_i = (\sum_{j=0}^r E_j) A_i = \sum_{j=0}^r p_i(j) E_j$. It can be proved that $r = d$, please refer to Theorem 3.1 in [1]. Therefore, the set of idempotents $E_0, E_1, \ldots, E_d$ also forms a basis of the algebra $M$. Let $P$ be the matrix of degree $d + 1$ with $p_i(j)$ as the $(j, i)$ entry. In order to make the representations consistent, we will use the index set $\{0, 1, \ldots, d\}$ to label the rows and columns of the matrix $P$. Then we have

$$(A_0, A_1, \ldots, A_d) = (E_0, E_1, \ldots, E_d) P.$$

The matrix $P$ of degree $d + 1$ is called the first eigenmatrix of $X$.

2.3. Characters. A character $\phi$ of a finite abelian group $(G, +)$ of order $|G|$ is a group homomorphism $\phi: G \to \mathbb{C}^\times$, where $\mathbb{C}^\times$ denotes the multiplicative group of nonzero complex numbers; that is, $\phi(g_1 + g_2) = \phi(g_1) \phi(g_2)$ for all $g_1, g_2 \in G$. It is clear that $\phi(0) = 1$ and $\phi(g)^{|G|} = \phi(|G|g) = \phi(0) = 1$ for all $g \in G$. It follows that $\phi(g)$ is a complex $|G|$-th root of unity for all $g \in G$. A character $\phi_0$ is called trivial character of $G$ if $\phi_0(g) = 1$ for all $g \in G$.

Let $\mathbb{F}_q$ be a finite field with $q$ elements, where $q = p^h$, $p$ is a prime and $h$ is a positive integer. An additive character $\phi$ of $\mathbb{F}_q$ is a character of the additive group $(\mathbb{F}_q, +)$. For such a character $\phi$, we have

$$\phi(a + b) = \phi(a) \phi(b) \text{ for any } a, b \in \mathbb{F}_q \text{ and } \phi(0) = 1.$$
Let $\text{Tr}_{q/p}$ denote the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$ defined as

$$\text{Tr}_{q/p}(x) = x + x^p + \ldots + x^{p^{k-1}}$$

for $x \in \mathbb{F}_q$.

Since $\text{Tr}_{q/p}(\cdot)$ is an $\mathbb{F}_p$-linear function, then we can obtain an additive character $\phi_a : (\mathbb{F}_q, +) \rightarrow \mathbb{C}^\times$ for any $a \in \mathbb{F}_q$ by setting

$$\phi_a(x) = \zeta_p^{\text{Tr}_{q/p}(ax)},$$

where $\zeta_p = e^{\frac{2\pi i}{p}}$ is a $p$-th primitive root of unity. The character $\phi_1$ is called the canonical character.

3. Linear codes from association schemes

The following two lemmas provide a complete characterization of LCD codes and a sufficient condition of linear codes with one-dimensional hull, respectively.

**Lemma 3.1.** [19] Let $C$ be an $[n,k]$ linear code over $\mathbb{F}_q$ with generator matrix $G = [I_k, Q]$. Then the code $C$ is LCD if and only if $I_k + QQ^T$ is nonsingular, i.e., $-1$ is not an eigenvalue of the matrix $QQ^T$, where $Q^T$ denotes the transpose of $Q$.

**Lemma 3.2.** [16] Let $C$ be an $[n,k]$ linear code over $\mathbb{F}_q$ with generator matrix $G = [I_k, Q]$. Then the hull of the code $C$ is of dimension one if $-1$ is an eigenvalue of the matrix $QQ^T$ with (algebraic) multiplicity 1, where $Q^T$ denotes the transpose of $Q$.

The main work of this section is to construct the matrix $Q$ that satisfies the condition of Lemma 3.1 and Lemma 3.2 from commutative Bose-Mesner algebra, respectively. Furthermore, we can get the LCD codes and linear codes with one-dimensional hull, respectively. To present our main results, we now unify the notations will be used in this section. Let $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ be a commutative $d$-class association scheme with $|X| = n$ and $\mathcal{M} = \langle A_0, A_1, \ldots, A_d \rangle$ be the corresponding commutative algebra. Then we have the decomposition of $V = V_0 \oplus V_1 \oplus \ldots \oplus V_d$. The following lemma presents an important property of eigenvalues of matrices in the Bose-Mesner algebra $\mathcal{M}$.

**Lemma 3.3.** Let $\chi_i(B)$ denote the eigenvalue of $B$ on $V_t$ for $B = \sum_{i=0}^{d} b_i A_i \in \mathcal{M}$ and $t \in \{0, 1, \ldots, d\}$. For each $t$, we have $\chi_i(B) = \sum_{i=0}^{d} b_i p_i(t)$ and $\chi_i(BC) = \chi_i(B) \chi_i(C)$ for any $B = \sum_{i=0}^{d} b_i A_i$, $C = \sum_{i=0}^{d} c_i A_i \in \mathcal{M}$.

**Proof.** For any $t \in \{0, 1, \ldots, d\}$, taking any $0 \neq v \in V_t$, we have $vB = \sum_{i=0}^{d} b_i v A_i = \sum_{i=0}^{d} b_i p_i(t)v$ and so we deduce that $\chi_i(B) = \sum_{i=0}^{d} b_i p_i(t)$. By the expression of $B$, $C$, $\chi_i(B)$ and $\chi_i(C)$, we just need to show that $\chi_i(A_i A_j) = \chi_i(A_i) \chi_i(A_j)$ for any $i, j \in \{0, 1, \ldots, d\}$. For any $0 \neq v \in V_t$, we have

$$v \chi_i(A_i A_j) = v(A_i A_j) = (v A_i) A_j = \chi_i(A_i)(v A_j) = v \chi_i(A_i) \chi_i(A_j).$$

Therefore, the proof is completed. 

In the following part of this paper, we always set $p_0$ to be a prime, $u$ to be a positive integer and $\mathbb{F}_{p_0^u}$ to be the finite field with $p_0^u$ elements. For any $n_0 \in \mathbb{Z}$, we define $\overline{n_0} = n_0 \mod p_0$, and then we have $\overline{n_0} \in \mathbb{F}_{p_0}$. Let $M_n(\mathbb{Z})$ denote the set of square matrix of order $n$ whose entries are elements in $\mathbb{Z}$. Taking

(1) \quad $Q = \sum_{i=0}^{d} c_i A_i \in \mathcal{M}$ with $c_i \in \mathbb{Z}$, for $0 \leq i \leq d$. 

For such a matrix $Q = (q_{ij}) \in M \cap M_n(\mathbb{Z})$, we define
\begin{equation}
\overline{Q} = (\overline{q}_{ij}) \in M_n(\mathbb{F}_{p_0}) \text{ with } \overline{q}_{ij} = q_{ij} \pmod{p_0}.
\end{equation}

For each $t \in \{0, 1, \ldots, d\}$, we define $T'_t = \chi_t(QQ^T)$ to be the eigenvalue of $QQ^T$ on $V_t$. By the definition of $QQ^T$ and Lemma 3.3, we have
\begin{equation}
T'_t = \left( \sum_{i=0}^{d} c_i p_i(t) \right),
\end{equation}
where $A^T_i = A'_i$ for some $i' \in \{0, 1, \ldots, d\}$. In particular, if the association scheme is symmetric, then we have
\begin{equation}
T'_t = \left( \sum_{i=0}^{d} c_i p_i(t) \right)^2
\end{equation}
for each $t \in \{0, 1, \ldots, d\}$.

With the notations mentioned as above, we are ready to present our main results as follows.

**Theorem 3.4.** Let $C$ be a $[2n, n]$ linear code over $\mathbb{F}_{p_0}$ with generator matrix $G = [I_n, \overline{Q}]$, where $Q$ is given by Eq. (1). For each $t \in \{0, 1, \ldots, d\}$, let $T'_t$ be defined by Eq. (3) as the eigenvalue of $QQ^T$ on $V_t$ and $T_t = T'_t + 1$. If all $T'_t$'s are rational numbers, then we have the following.

1. The code $C$ is LCD if and only if $\Pi_{t=0}^d T_t \not\equiv 0 \pmod{p_0}$;
2. The code $C$ has one-dimensional hull if $T_0 \equiv 0 \pmod{p_0}$ and $T_t \not\equiv 0 \pmod{p_0}$ for $t = 1, 2, \ldots, d$.

**Proof.** Since $Q \in M_n(\mathbb{Z})$, then all eigenvalues $T'_t$ ($0 \leq t \leq d$) of $QQ^T$ are algebraic integer. Thus, all $T'_t$'s are rational numbers if and only if all $T'_t$'s are integers so that we can define $\overline{T'_t} = T'_t \pmod{p_0}$ for $t \in \{0, 1, \ldots, d\}$. We claim that $\overline{T'_t}$ is an eigenvalue of $QQ^T$ if and only if $\overline{T'_t}$ is an eigenvalue of $QQ^T$ for each $t = 0, 1, \ldots, d$. It’s known that $T'_t$ is an eigenvalue of $QQ^T$ if and only if $T'_t$ is a root of the polynomial
\begin{equation}
g(x) = \det(xI - QQ^T) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x],
\end{equation}
which is equivalent to saying that $\overline{T'_t}$ is a root of the polynomial
\begin{equation}
\overline{g}(x) = x^n + \overline{a}_{n-1}x^{n-1} + \cdots + \overline{a}_1x + \overline{a}_0 \in \mathbb{Z}_{p_0}[x].
\end{equation}
Thus, the claim follows.

1. By Lemma 3.1 and above arguments, we have that the code $C$ is LCD if and only if $\Pi_{t=0}^d T_t \not\equiv 0 \pmod{p_0}$;
2. If $T_0 \equiv 0 \pmod{p_0}$ and $T_t \not\equiv 0 \pmod{p_0}$ for $t = 1, 2, \ldots, d$, then $-1$ is an eigenvalue of $QQ^T$ on $V_0$, but not on $V_t$ for $i \neq 0$ by above arguments. As we mentioned in Section 2, $V_0$ is the one-dimensional subspace spanned by $(1, 1, \ldots, 1)$, thus the multiplicity of $-1 = \chi_0(QQ^T)$ is 1. The second assertion follows from Lemma 3.2 and Lemma 3.3.

Based on Theorem 3.4, we shall give some constructions of LCD codes and linear codes with one-dimensional hull by several types of association schemes.
3.1. Linear codes associated with cyclotomic association schemes. For a \( d \)-class association scheme \( \mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d}) \), we say that \((X, \{S_i\}_{0 \leq i \leq d})\) is a fusion of the association scheme \((X, \{R_i\}_{0 \leq i \leq d})\) if \( S_0 = R_0 \) and \( S_i \) is the union of some of the relations \( R_i \), for all \( i \). If an association scheme has the property that any of its fusions is also an association scheme, then we call the association scheme \textit{amorphic}. For more details about amorphic association schemes, please refer to [25]. A typical example of amorphic association schemes is the cyclotomic association scheme over a finite field in semi-primitive case, which we will introduce below.

Let \( q = p^h \), where \( p \) is a prime and \( h \) is a positive integer. Let \( \alpha \) be a fixed primitive element of \( \mathbb{F}_q \) and \( N|(q - 1) \) with \( N > 1 \). Let \( C_0 = \langle \alpha^N \rangle \), and

\[
C_i = \alpha^i C_0 \text{ for } 1 \leq i \leq N - 1.
\]

Assume that \(-1 \in C_0\). Define \( R_0 = \{(x, x) \mid x \in \mathbb{F}_q\} \), and for \( i \in \{1, 2, \ldots, N\} \), define \( R_i = \{(x, y) \mid x, y \in \mathbb{F}_q, x - y \in C_i - 1\} \). Then \((\mathbb{F}_q, \{R_i\}_{0 \leq i \leq N})\) is an association scheme, which is called cyclotomic association scheme of class \( N \) over \( \mathbb{F}_q \). If there exists an integer \( j_0 \) such that \( p^{j_0} \equiv -1 (mod \, N) \), then we say that the cyclotomic association scheme is in the semi-primitive case. For \( N > 2 \), the cyclotomic association scheme is amorphic if and only if it is in the semi-primitive case. This conclusion has been proved in [2].

The first eigenmatrix \( P \) of the cyclotomic association scheme of class \( N \) is as following

\[
P = \begin{pmatrix}
1 & \frac{q-1}{N} & \frac{q-1}{N} & \cdots & \frac{q-1}{N} \\
1 & \eta_0 & \eta_1 & \eta_2 & \cdots & \eta_{N-1} \\
1 & \eta_1 & \eta_2 & \eta_3 & \cdots & \eta_0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \eta_{N-1} & \eta_0 & \eta_1 & \cdots & \eta_{N-2}
\end{pmatrix},
\]

where the \( \eta_i \)'s \((0 \leq i \leq N - 1)\) are Gauss periods of order \( N \) defined by

\[
\eta_i = \sum_{x \in C_i} \phi_1(x).
\]

Here \( \phi_1 \) is the canonical additive character of \( \mathbb{F}_q \) introduced in Section 2. The following lemma gives Gauss periods in the semi-primitive case.

**Lemma 3.5.** [9] Let \( N \geq 3 \) be an integer. Assume that there exists the smallest positive integer \( j_0 \) such that \( p^{j_0} \equiv -1 (mod \, N) \). Let \( q = p^{2j_0\gamma} \) for some positive integer \( \gamma \).

1. If \( p, \gamma \) and \( \frac{p^{j_0+1}}{N} \) are all odd, then

\[
\eta_{N/2} = \frac{(N-1)\sqrt{q} - 1}{N}, \quad \eta_i = -\sqrt{q} + 1 \text{ for } i \neq N/2;
\]

2. In any other case,

\[
\eta_0 = \frac{(-1)^{\gamma+1}(N-1)\sqrt{q} - 1}{N}, \quad \eta_i = \frac{(-1)^\gamma \sqrt{q} - 1}{N} \text{ for } i \neq 0.
\]

**Theorem 3.6.** Let \( \mathcal{X} = (\mathbb{F}_q, \{R_i\}_{0 \leq i \leq N}) \) be the cyclotomic association scheme of class \( N \) and \( A_0, A_1, \ldots, A_N \) be the corresponding adjacency matrices. As the same notations referenced in Theorem 3.4, taking \( Q \) and \( \overline{Q} \) to be defined in Eqs. (1) and (2). Let \( C \) be a \([2q, q]\) linear code over \( \mathbb{F}_{p^h} \) with generator matrix \([I_q, \overline{Q}]\).
1. If \( p, \gamma \) and \( \frac{p^{\gamma}+1}{2} \) are all odd, we set \( L_0 = (c_0 + \frac{q-1}{N} \sum_{i=1}^{N} c_i)^2 + 1 \) and \( L_j = (c_0 + c_j \eta_{N/2} + \eta_0 \sum_{i=1, i \neq j}^{N} c_i)^2 + 1 \) for \( j = 1, 2, \ldots, N \). Then \( \mathcal{C} \) is a \([2q, q]\) LCD code over \( \mathbb{F}_{p^0} \) if and only if

\[
\prod_{j=0}^{N} L_j \not\equiv 0 (\text{mod } p_0).
\]

and \( \mathcal{C} \) is a \([2q, q]\) linear code with one-dimensional hull if

\[
L_0 \equiv 0 (\text{mod } p_0), \quad L_j \not\equiv 0 (\text{mod } p_0) \quad \text{for } j = 1, 2, \ldots, N.
\]

2. In any other case, we set \( L_0 = (c_0 + \frac{q-1}{N} \sum_{i=1}^{N} c_i)^2 + 1 \), and \( L_j = (c_0 + c_j \eta_0 + \eta_1 \sum_{i=1, i \neq j}^{N} c_i)^2 + 1 \) for \( j = 1, 2, \ldots, N \). Then \( \mathcal{C} \) is a \([2q, q]\) LCD code over \( \mathbb{F}_{p^0} \) if and only if

\[
\prod_{j=0}^{N} L_j \not\equiv 0 (\text{mod } p_0).
\]

and \( \mathcal{C} \) is a \([2q, q]\) linear code with one-dimensional hull if

\[
L_0 \equiv 0 (\text{mod } p_0), \quad L_j \not\equiv 0 (\text{mod } p_0) \quad \text{for } j = 1, 2, \ldots, N.
\]

Proof. It is easy to check that the cyclotomic association scheme is symmetric since \(-1 \in C_0\) and then \( Q^T = Q \) for \( Q = \sum_{i=0}^{N} c_i A_i \) with \( c_i \in \mathbb{Z} \). By Eq. (3) and the symmetric property of \( Q \), we have that all eigenvalues of \( QQ^T \) are

\[
T'_t = \left( \sum_{i=0}^{N} c_i p_i(t) \right)^2,
\]

where \( t = 0, 1, \ldots, N \). Applying Lemma 3.5, we can compute and conclude that:

1. If \( p, \gamma \) and \( \frac{p^{\gamma}+1}{N} \) are all odd, then \( \eta_i = \eta_0 \) for \( i \in \{0, 1, \ldots, N-1\} \setminus \{N/2\} \). It means that, except the first row of \( P \), \( \eta_{N/2} \) appears one time and \( \eta_0 \) appears \( N - 1 \) times in each row of \( P \). Then, it is easy to compute that \( L_j - 1, 0 \leq j \leq d \) are exactly the eigenvalues of \( QQ^T \) and \( L_0 = T'_0 + 1 \) by Eq. (9).

Since all \( \eta_i \)’s are rational numbers, we employ Theorem 3.4 and deduce the first assertion holds.

2. In any other case, \( \eta_i = \eta_1 \) for \( i \in \{1, \ldots, N-1\} \). By the same argument as the first case, it can be computed that \( L_j - 1, 0 \leq j \leq d \) are exactly the eigenvalues of \( QQ^T \) and \( L_0 = T'_0 + 1 \) by Eq. (9) in this case. By Theorem 3.4, the second assertion follows.

\( \square \)

Remark 1. We remark that Theorem 3 and Theorem 4 in [5] are special cases of Theorem 3.6 of this paper. In particular, we take \( Q = A_1 \) in Theorem 3.6. Then we can get the same conclusions as Theorem 3 and Theorem 4 in [5] respectively. Therefore, the way of considering cyclotomic association schemes can provide more possible constructions of LCD codes and linear codes with one-dimensional hull by changing the coefficients \( c_i \)’s of matrix \( Q \).

Two examples of Theorem 3.6 are given as follows.
Example 1. Let \( p = 3, \gamma = 1, N = 4 \). Then we have \( j_0 = 1 \) and \( q = 9 \) by the assumption of Lemma 3.5. By Eq. (6) and Lemma 3.5, the first eigenmatrix \( P \) is given by

\[
P = \begin{pmatrix}
1 & 2 & 2 & 2 \\
1 & -1 & -1 & 2 \\
1 & -1 & 2 & -1 \\
1 & -1 & -1 & -1 \\
1 & -1 & -1 & 2
\end{pmatrix}
\]

(10)

Let \( C \) be a linear code over \( \mathbb{F}_{p_0} \) with generator matrix \([I_q, Q]\), where \( Q = 3A_0 + A_1 + 4A_2 + 2A_3 + 5A_4 \). Since \( p, \gamma, p^{j_0+1} \) are all odd, we employ the first case in Theorem 3.6 and compute that \( L_0 = 730, L_1 = 10, L_2 = 10, L_3 = 37, L_4 = 37 \) and \( \prod_{j=0}^4 L_j = 2^3 \cdot 5^3 \cdot 37^2 \cdot 73 \). If \( p_0 \neq 2, 5, 37, 73 \), then \( C \) is an \([18,9] \) LCD code. In particular, when \( p_0 = 19, 43, 47, 53, 61, 71, 79, 83, 89, 97 \), \( C \) is an \([18,9,9] \) LCD almost MDS code; If \( p_0 = 73 \), then \( C \) is an \([18,9,9] \) almost MDS linear code with one-dimensional hull.

Example 2. Let \( p = 2, \gamma = 1, N = 3 \). Then we have \( j_0 = 1 \) and \( q = 4 \) by the assumption of Lemma 3.5. By Eq. (6) and Lemma 3.5, the first eigenmatrix \( P \) is given by

\[
P = \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 \\
1 & -1 & 1 & -1
\end{pmatrix}
\]

(11)

Let \( C \) be a linear code over \( \mathbb{F}_{p_0} \) with generator matrix \([I_q, Q]\), where \( Q = 8A_0 + A_1 + 7A_2 + 6A_3 \). Since \( \gamma \) and \( p^{j_0+1} \) are not odd, we employ the second case of Theorem 3.6 and compute that \( L_0 = 485, L_1 = 17, L_2 = 65, L_3 = 37 \) and \( \prod_{j=0}^3 L_j = 5^2 \cdot 13 \cdot 17 \cdot 37 \cdot 97 \). If \( p_0 \neq 5, 13, 17, 37, 97 \), then \( C \) is an \([8,4] \) LCD code; In particular, if \( p_0 = 19, 29, 31, 43, 47, 53, 59, 61, 71, 73, 79, 83, 101, 103, 107, 109, 113, 127, 137 \), then \( C \) is an \([8,4,5] \) LCD MDS code. If \( p_0 = 97 \), then \( C \) is an \([8,4,5] \) MDS linear code with one-dimensional hull.

3.2. Linear codes associated with three-class association schemes.

Three-class association scheme is an important type of association scheme. In [11], the authors give some constructions of symmetric three-class association schemes as the fusion schemes of the cyclotomic association schemes. Now we will employ one of these three-class association schemes to construct LCD codes and linear codes with one-dimensional hull by Theorem 3.4.

Let \( s \) be a positive integer and \( E = \mathbb{F}_{2^s} \), \( F = \mathbb{F}_{2^{2s}} \) denote the finite field with \( 2^s \), \( 2^{2s} \) elements respectively. Set \( \omega \) to be a primitive element of \( F \). Let \( N = \frac{2^s - 1}{2^i - 1} \) and \( C_i = \omega^i \langle \omega^N \rangle, 0 \leq i \leq N - 1 \), be the cyclotomic classes of order \( N \) in \( F \). Clearly \( C_0 \) is equal to \( E^* \), which is the multiplicative group of \( E \).

Let \( Z_N = \{0, 1, \ldots, N - 1\} \). As shown in [11, Page 1206], for an integer \( a \in Z_N \), define

\[
S_a := \{u \in F^* : \text{Tr}_{F/E}(u^{1+2^s}) = 0, \text{Tr}_{F/E}(\omega^s u) = 0\}.
\]
Then all possible sizes of $S_a$’s are 0, $2^s - 1$, $2(2^s - 1)$. Based on this fact, we further define three subsets of $\mathbb{Z}_N$ as

\[
H_1 := \{a \in \mathbb{Z}_N : |S_a| = 2^s - 1\},
\]

\[
H_2 := \{a \in \mathbb{Z}_N : |S_a| = 2(2^s - 1)\},
\]

\[
H_3 := \{a \in \mathbb{Z}_N : |S_a| = 0\}.
\]

Thus, the sets $H_1$, $H_2$ and $H_3$ form a partition of $\mathbb{Z}_N$. The following lemma provides a symmetric three-class association scheme on the finite field $F$.

**Lemma 3.7.** [11, Theorem 5] With above notations, taking the following partition of $F$:

\[
R_0 = \{0\}, R_1 = \bigcup_{i \in H_1} C_i, R_2 = \bigcup_{i \in H_2} C_i, R_3 = \bigcup_{i \in H_3} C_i.
\]

Then $(F, \{R_i\}_{i=0}^3)$ is a three-class association scheme, whose first eigenmatrix is

\[
P = \begin{pmatrix}
1 & 2^{2s} - 1 & 2^{s-1}(2^{2s} - 1) & 2^{s-1}(2^s - 1)^2 \\
1 & 2^{2s} - 1 & -2^{s-1}(2^s + 1) & -2^{s-1}(2^s - 1) \\
1 & -1 & 2^{s-1}(2^s - 1) & -2^{s-1}(2^s - 1) \\
1 & -1 & -2^{s-1} & 2^{s-1}
\end{pmatrix}.
\]

Let $\mathcal{X} = (F, \{R_i\}_{i=0}^3)$ be the three-class association scheme constructed in Lemma 3.7 and $A_i$ be the the adjacency matrix of the relation $R_i$ for $i = 0, 1, 2, 3$. We set $Q = \sum_{i=0}^3 c_i A_i$ with $c_i \in \mathbb{Z}$ for $i = 0, 1, 2, 3$. Since the above three-class association scheme is symmetric, then $T_0, T_1, T_2$ and $T_3$ in Theorem 3.4 are given by

\[
\begin{align*}
T_0 &= [c_0 + (2^{2s} - 1)c_1 + 2^{s-1}(2^{2s} - 1)c_2 + 2^{s-1}(2^s - 1)^2 c_3]^2 + 1, \\
T_1 &= [c_0 + (2^{2s} - 1)c_1 - 2^{s-1}(2^s + 1)c_2 - 2^{s-1}(2^s - 1)c_3]^2 + 1, \\
T_2 &= [c_0 - c_1 + 2^{s-1}(2^s - 1)c_2 - 2^{s-1}(2^s - 1)c_3]^2 + 1, \\
T_3 &= [c_0 - c_1 - 2^{s-1}c_2 + 2^{s-1}c_3]^2 + 1.
\end{align*}
\]

(12)

Observe that all $T_i$’s are integers. By Theorem 3.4, we get the following theorem.

**Theorem 3.8.** Let $C$ be a linear code over $\mathbb{F}_{p_0}$ with generator matrix $[I_{2^s}, Q]$ and $T_j$ be defined in Eq. (12) for $j = 0, 1, 2, 3$. Then $C$ is a $[2^{3s+1}, 2^{3s}]$ LCD code if and only if $\prod_{j=0}^3 T_j \neq 0$ (mod $p_0$), and $C$ is a $[2^{3s+1}, 2^{3s}]$ linear code with one-dimensional hull if

\[
T_0 \equiv 0 \text{ (mod } p_0\text{), } T_j \neq 0 \text{ (mod } p_0\text{) for } j = 1, 2, 3.
\]

**Example 3.** As the notations in Lemma 3.7 and Theorem 3.8, we set $s = 2$, then the first eigenmatrix is

\[
P = \begin{pmatrix}
1 & 15 & 30 & 18 \\
1 & 15 & -10 & -6 \\
1 & -1 & 6 & -6 \\
1 & -1 & -2 & 2
\end{pmatrix}.
\]

Let $C$ be a linear code over $\mathbb{F}_{p_0}$ with generator matrix $[I_{64}, Q]$, where $Q = A_0 + 2A_1 + 2A_2 + A_3$. By Eq. (12), we have $T_0 = 11882 = 2 \cdot 13 \cdot 457$, $T_1 = 26$, $T_2 = 26$, $T_3 = 10$ and $\prod_{j=0}^3 T_j = 2^4 \cdot 5 \cdot 13^3 \cdot 457$. If $p_0 \neq 2, 5, 13, 457$, then $C$ is a $[128, 64]$ LCD code. If $p_0 = 457$, then $C$ is a $[128, 64]$ linear code with one-dimensional hull.
3.3. Linear codes associated with four-class association schemes. In this subsection, we will introduce a four-class association scheme that doesn’t come from cyclotomic class. The following lemma taken from [14] provides such an association scheme.

**Lemma 3.9.** Let $p = 3, q = 3^s$ and $X = \mathbb{F}_q \times \mathbb{F}_q$ be a finite set. Define

$R_0 = \{(x, x) | x \in X\},$

$R_i = \{(x, y) | x = (x_1, x_2), y = (y_1, y_2) \in X, x_1 \neq y_1, Tr((-x_1 + y_1)(-x_2 + y_2)) = i\},$

$R_4 = \{(x, y) | x = (x_1, x_2), y = (y_1, y_2) \in X, x_1 = y_1, x_2 \neq y_2\},$

where $i = 1, 2, 3$ and $Tr$ is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. Then the association scheme $(X, \{R_i\}_{i=0}^4)$ is a symmetric association scheme with first eigenmatrix

$$P = \begin{pmatrix}
1 & 3^{s-1}(3^s - 1) & 3^{s-1}(3^s - 1) & 3^{s-1}(3^s - 1) & 3^s - 1 \\
1 & 2 \cdot 3^{s-1} & -3^{s-1} & -3^{s-1} & 1 \\
1 & -3^{s-1} & 2 \cdot 3^{s-1} & -3^{s-1} & -1 \\
1 & -3^{s-1} & -3^{s-1} & 2 \cdot 3^{s-1} & 1 \\
1 & -3^{s-1} & -3^{s-1} & -3^{s-1} & 3^s - 1
\end{pmatrix}.$$

Let $\mathcal{X} = (X, \{R_i\}_{i=0}^4)$ be the four-class association scheme constructed in Lemma 3.9 with $|X| = q^2$ and $A_i$ be the adjacency matrix of the relation $R_i$ for $i = 0, 1, 2, 3, 4$. We set $Q = \sum_{i=0}^4 c_i A_i$ with $c_i \in \mathbb{Z}$ for $i = 0, 1, 2, 3, 4$. Since the above four-class association scheme is symmetric, then $T_0, T_1, T_2, T_3, T_4$ in Theorem 3.4 is given by

$$T_0 = [c_0 + 3^{s-1}(3^s - 1)c_1 + 3^{s-1}(3^s - 1)c_2 + 3^{s-1}(3^s - 1)c_3 + (3^s - 1)c_4] + 1,$$

$$T_1 = [c_0 + 2 \cdot 3^{s-1}c_1 - 3^{s-1}c_2 - 3^{s-1}c_3 - c_4] + 1,$$

$$T_2 = [c_0 - 3^{s-1}c_1 + 2 \cdot 3^{s-1}c_2 - 3^{s-1}c_3 - c_4] + 1,$$

$$T_3 = [c_0 - 3^{s-1}c_1 - 3^{s-1}c_2 + 2 \cdot 3^{s-1}c_3 - c_4] + 1,$$

$$T_4 = [c_0 - 3^{s-1}c_1 - 3^{s-1}c_2 - 3^{s-1}c_3 + (3^s - 1)c_4] + 1.$$

Observe that all $T_i$’s are integers. By Theorem 3.4, we get the following theorem.

**Theorem 3.10.** Let $C$ be a linear code over $\mathbb{F}_{p_0}^5$ with generator matrix $[I_{3^2s}, Q]$ and $T_j$ be defined in Eq. (13) for $j = 0, 1, \ldots, 4$. Then $C$ is a $[2 \cdot 3^{2s}, 3^{2s}]$ LCD code if and only if $\prod_{j=0}^4 T_j \equiv 0 (\text{mod } p_0)$, and $C$ is a $[2 \cdot 3^{2s}, 3^{2s}]$ linear code with one-dimensional hull if $T_0 \equiv 0 (\text{mod } p_0), T_j \equiv 0 (\text{mod } p_0)$ for $j = 1, 2, 3, 4$.

**Example 4.** As the notations in Lemma 3.9 and Theorem 3.10, we set $s = 2$. Then the first eigenmatrix is

$$P = \begin{pmatrix}
1 & 24 & 24 & 24 & 8 \\
1 & 6 & -3 & -3 & -1 \\
1 & -3 & 6 & -3 & -1 \\
1 & -3 & -3 & 6 & -1 \\
1 & -3 & -3 & -3 & 8
\end{pmatrix}.$$

Let $C$ be a linear code over $\mathbb{F}_{p_0}^{10}$ with generator matrix $[I_{3^{2}}, Q]$, where $Q = A_0 + 2A_1 + A_2$. By Eq. (13), we have $T_0 = 5330 = 2 \cdot 5 \cdot 13 \cdot 41, T_1 = 101, T_2 = 2, T_3 = 65, T_4 = 65$ and $\prod_{j=0}^4 T_j = 2^2 \cdot 5^3 \cdot 13^3 \cdot 41 \cdot 101$. If $p_0 \neq 2, 5, 13, 41, 101,$
then $C$ is a [162, 81] LCD code. If $p_0 = 41$, then $C$ is a [162, 81] linear code with one-dimensional hull.

3.4. Linear codes from association schemes with irrational first eigenmatrix. Observe that the first eigenmatrix $P$ of all association schemes constructed in above three subsections belongs to $M_1(X)(Z)$. A natural question is whether there exists an association scheme whose first eigenmatrix $P \notin M_1(X)(Z)$. The answer is yes. In this subsection, we will show an example of an association scheme with first eigenmatrix $P$ such that there exists $(j, i)$-entry of $P$, namely $p_i(j)$ is irrational number.

Let $\Gamma$ be a connected undirected graph on $X$ with $|X| = n$. For $x, y \in X$, a path from $x$ to $y$ of length $r$ is a sequence of vertices $x_0 = x, x_1, \ldots, x_r = y$ such that for each $i \in \{0, 1, \ldots, r - 1\}$, $(x_i, x_{i+1})$ is an edge of $\Gamma$. The distance of $x$ and $y$ is the minimum length of paths from $x$ to $y$, which is denoted by $\partial(x, y)$. Here $\partial(x, x)$ is defined to be 0. The maximum distance $d$ between vertices in the graph $\Gamma$ is called the diameter of $\Gamma$.

Based on the definition of distance as above, one can define the relation $R_i$ on $X$ by $(x, y) \in R_i$ if and only if $\partial(x, y) = i$ for each $i \in \{0, 1, \ldots, d\}$. If $X = (X, \{R_i\}_{0 \leq i \leq d})$ forms a $d$-class association scheme, $\Gamma$ is called a distance-regular graph. It is clear that $X$ is always symmetric. For further information about distance-regular graphs and association schemes, the reader is referred to [1] and [3]. From these references, there exists a generalized 6-gon, denoted by $H(6)$, whose points and lines are defined through the complement of a hermitian space of dimension 3 over $F_{32}$. We omit the specific construction details here. This generalized 6-gon $H(6)$ is a distance-regular graph of diameter 6 with 126 vertices. In the remaining part of this subsection, we set $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq 6})$ as the 6-class association scheme defined by $H(6)$. The following matrix is the first eigenmatrix $P$ of $H(6)$, which is taken from [1, Page 71].

\begin{equation}
P = \begin{pmatrix}
1 & 3 & 6 & 12 & 24 & 48 & 32 \\
1 & \sqrt{6} & 3 & \sqrt{6} & 0 & -2\sqrt{6} & -4 \\
1 & \sqrt{2} & -1 & -3\sqrt{2} & -4 & 2\sqrt{2} & 4 \\
1 & 0 & -3 & 0 & 6 & 0 & -4 \\
1 & -\sqrt{2} & -1 & 3\sqrt{2} & -4 & -2\sqrt{2} & 4 \\
1 & -\sqrt{6} & 3 & -\sqrt{6} & 0 & 2\sqrt{6} & -4 \\
1 & -3 & 6 & -12 & 24 & -48 & 32
\end{pmatrix}
\end{equation}

Let $\mathcal{X} = (X, \{R_i\}_{i=0}^{6})$ with $|X| = 126$ be the 6-class association scheme defined by distance-regular graph $H(6)$ and $A_i$ be the the adjacency matrix of the relation $R_i$ for $i = 0, 1, \ldots, 6$. We set $Q = \sum_{i=0}^{6} c_i A_i$ with $c_i \in Z$ for $i = 0, 1, \ldots, 6$. Since this 6-class association scheme is symmetric, then for each $t \in \{0 \leq t \leq 6\}$, the number $T_i$ in Theorem 3.4 is given by

\begin{equation}
T_i = \left(\sum_{i=0}^{6} c_i p_i(t)\right)^2 + 1,
\end{equation}

where $p_i(t)$ denotes the $(t, i)$-entry of $P$ given as Eq. (14). By employing the Theorem 3.4, we get the following theorem.

**Theorem 3.11.** Let $C$ be a linear code over $\mathbb{F}_{p_0}$ with generator matrix $[I_{126}, \overline{Q}]$ and $T_j$ be defined in Eq. (15) for $j = 0, 1, \ldots, 6$. If all $T_i$'s are rational numbers, then
we have $C$ is a $[252, 126]$ LCD code if and only if $\prod_{j=0}^6 T_j \not\equiv 0 (\text{mod } p_0)$, and $C$ is a $[252, 126]$ linear code with one-dimensional hull if $T_0 \equiv 0 (\text{mod } p_0), T_j \not\equiv 0 (\text{mod } p_0)$ for $j = 1, \ldots, 6$.

Example 5. With the notations as in Theorem 3.11, let $C$ be a linear code over $\mathbb{F}_{p_0^6}$ with generator matrix $[I_{126}, Q]$, where $Q = 2A_1$. By Eq. (15), we have $T_0 = (2 \cdot 3)^2 + 1 = 37, T_1 = (2\sqrt{6})^2 + 1 = 25, T_2 = (2\sqrt{2})^2 + 1 = 9, T_3 = (0)^2 + 1 = 1,$

$
T_4 = (-2\sqrt{2})^2 + 1 = 9, T_5 = (-2\sqrt{3})^2 + 1 = 25, T_6 = (-6)^2 + 1 = 37 \text{ and } \prod_{j=0}^6 T_j = 3^4 \cdot 5^4 \cdot 37^2. \text{ Observe that all } T_i \text{'s are integers. By Theorem 3.11, if } p_0 \not\equiv 3, 5, 37, \text{ then } C \text{ is a } [252, 126] \text{ LCD code.}$

Actually, based on Theorem 3.4 and the results on algebraic number theory given in Section 2, we can derive the following theorem.

**Theorem 3.12.** Let $p_0$ be a prime and $K = \mathbb{Q}(\zeta_m)$ be the cyclotomic field with $m = p_0^6m'$ ($l \geq 0, p_0 \nmid m'$) and $O_K = \mathbb{Z}[\zeta_m]$. Let $P$ be a prime ideal in $O_K$ containing $p_0O_K$, $f$ be the degree of $P$ given by Lemma 2.1 and $u$ be a positive integer such that $f|u$. Let $C$ be a $[2n, n]$ linear code over $\mathbb{F}_{p_0^6}$ with generator matrix $G = [I_n, Q]$, where $Q$ is given by Eq. (1). Taking the same notation as in Theorem 3.4. If $T_i \not\in O_K$ for all $i \in \{0, 1, \ldots, d\}$, then we have the following.

1. The code $C$ is LCD if and only if $\prod_{i=0}^d T_i \not\equiv 0 (\text{mod } P)$;
2. The code $C$ has one-dimensional hull if $T_0 \equiv 0 (\text{mod } P)$ and $T_i \not\equiv 0 (\text{mod } P)$ for $t = 1, 2, \ldots, d$.

**Proof.** As we mentioned in Section 2, we have $[O_K/P : \mathbb{F}_{p_0}] = f$ and so $O_K/P = \mathbb{F}_{p_0^f}$, which is a subfield of $\mathbb{F}_{p_0^6}$. Since $T_i$’s are all eigenvalues of $QQ^T$ and $P$ is a prime ideal containing $p_0O_K$, the desired results follow by the same arguments as in Theorem 3.4.

Since the calculation on prime ideal is more complicated, we just give an example based on Theorem 3.12 and generalized 6-gon instead of presenting more constructions.

**Example 6.** Let $p_0$ be a prime, $K = \mathbb{Q}(\zeta_m)$ with $m = p_0^6m'$ ($l \geq 0, p_0 \nmid m'$) and $P$ be a prime ideal in $O_K$ over $p_0$. The degree $f$ of $P$ is given by Lemma 2.1. Set $u$ to be a positive integer such that $f|u$. Let $Q = A_1 + A_2$ and $C$ be a linear code over $\mathbb{F}_{p_0^6}$ with generator matrix $[I_{126}, Q]$. By Eq. (15), we have $T_0 = (3+6)^2 + 1 = 82 = 2 \cdot 41, T_1 = (\sqrt{6}+3)^2 + 1 = 16 + 6\sqrt{6}, T_2 = (\sqrt{6} - 1)^2 + 1 = 4 - 2\sqrt{2}, T_3 = (4)^2 + 1 = 10 = 2 \cdot 5, T_4 = (-\sqrt{2} - 1)^2 + 1 = 4 + 2\sqrt{2}, T_5 = (-\sqrt{6} + 3)^2 + 1 = 16 - 6\sqrt{6}, T_6 = (-3 + 6)^2 + 1 = 10 = 2 \cdot 5$ and $\prod_{j=0}^6 T_j = 2^9 \cdot 3^5 \cdot 41$. Note that if $\mu \in \mathbb{Z}$, then $\overline{\mu} = \mu (\text{mod } P) \in \mathbb{F}_{p_0}$. Thus, if $p_0 \not\equiv 2, 5, 41$, then $C$ is a $[252, 126]$ LCD code.

Taking $p_0 = 41$, for the prime ideal $P$ over $p_0 = 41$, we set $T_i = T_i \not\in P$ for $i \in \{0, 1, \ldots, 6\}$. Obviously, $T_0 = 0, T_5 \not\in 0$ and $T_6 \not\in 0$. Since gcd $(8, 41) = 1$, then $T_2T_4 = 8 \not\equiv 0$ and so $T_2 \not\equiv 0, T_4 \not\equiv 0$. By the same arguments, we have $T_1 \not\equiv 0$ and $T_5 \not\equiv 0$. It follows that $C$ is a $[252, 126]$ linear code with one-dimensional hull.

4. A generalized construction of linear codes

All linear codes $C$ with generator matrix $[I_n, Q]$ in Section 3 we construct are $[2n, n]$ linear codes. It means that the matrix $Q$ in the generator matrix is a square matrix of order $n$. In this section, we will generalize the constructions in Section
so that $Q$ is not necessarily a square matrix to construct LCD codes and linear codes with one-dimensional hull.

As the notations in Section 3, let $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ be a commutative $d$-class association scheme with $|X| = n$ and $\mathcal{M} = \langle A_0, A_1, \ldots, A_d \rangle$ be the corresponding commutative algebra. We set $\ell$ to be an integer with $\ell \geq 1$. For each $j$ such that $1 \leq j \leq \ell$, define

$$Q_j = \sum_{i=0}^{d} c_{ij} A_i \in \mathcal{M} \text{ with } c_{ij}(0 \leq i \leq d) \in \mathbb{Z}. \tag{16}$$

For each matrix $Q_j$ ($1 \leq j \leq \ell$), we define $Q_j$ by Eq. (2). Let

$$\mathcal{Q} = [\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_\ell]. \tag{17}$$

Then we have $QQ^T = \sum_{j=1}^{\ell} Q_j Q_j^T$. For each $t \in \{0, 1, \ldots, d\}$, we get the eigenvalue of $QQ^T$ on $V_t$ is

$$T_t' = \sum_{j=1}^{\ell} \left( \sum_{i=0}^{d} c_{ij} p_i(t) \right) \left( \sum_{i=0}^{d} c_{ij} p_i'(t) \right), \tag{18}$$

where $A_i^T = A_{i'}$ for some $i' \in \{0, 1, \ldots, d\}$ by Lemma 3.3 and Eq. (3). In particular, if the association scheme is symmetric, then we have

$$T_t' = \sum_{j=1}^{\ell} \left( \sum_{i=0}^{d} c_{ij} p_i(t) \right)^2 \tag{19}$$

for each $t \in \{0, 1, \ldots, d\}$.

Notice that the matrix $Q$ mentioned in Lemma 3.1 and Lemma 3.2 is not necessarily a square matrix. With above notations, it’s easy to deduce the following theorem by the same arguments as in Theorem 3.4.

**Theorem 4.1.** Let $C$ be an $[(\ell + 1)n, n]$ linear code over $\mathbb{F}_{p_0}$ with generator matrix $G = [I_n, \mathcal{Q}]$, where $\mathcal{Q}$ is given by Eq. (17). For each $t \in \{0, 1, \ldots, d\}$, let $T_t'$ be defined by Eq. (18) as the eigenvalue of $QQ^T$ on $V_t$ and $T_t = T_t' + 1$. If all $T_t'$’s are rational numbers, then the code $C$ is LCD if and only if $\Pi_{t=0}^{d} T_t \not\equiv 0$(mod $p_0$) and the code $C$ has one-dimensional hull if $T_0 \equiv 0$(mod $p_0$) and $T_t \not\equiv 0$(mod $p_0$) for $t = 1, 2, \ldots, d$.

**Remark 2.** The construction in Theorem 4.1 can be regarded as the generalization of Theorem 3.4. It’s obvious that the minimum distance of the linear code $C$ with generator matrix $[I_n, \mathcal{Q}]$ in Theorem 4.1 is larger than or equal to that of the linear code $C'$ with generator matrix $[I_n, \mathcal{Q}_1]$. By the same arguments, the results of Theorem 3.6, Theorem 3.8, Theorem 3.10 and Theorem 3.11 in Section 3 can be generalized by taking the matrix $\mathcal{Q}$ as the form of Eq. (17). Therefore, we can construct $[(\ell + 1)n, n]$ LCD codes and linear codes with one-dimensional hull by employing the association schemes given in Section 3 and Theorem 4.1.

Let $\mathcal{X} = (\mathbb{F}_q^\ast, \{R_i\}_{0 \leq i \leq N})$ be the cyclotomic association scheme of class $N$ and $A_0, A_1, \ldots, A_N$ be the corresponding adjacency matrices. We now employ Theorem 4.1 to present two examples as the generalization of the constructions given in Theorem 3.6.
Example 7. Let \( p = 3, \gamma = 1, N = 4 \). Then we have \( j_0 = 1 \) and \( q = 9 \) by the assumption of Lemma 3.5. The first eigenmatrix of this case is given by Eq. (10). Let \( \mathcal{C} \) be a linear code over \( \mathbb{F}_{p_0} \) with generator matrix \( [I_q, Q_1, Q_2] \), where \( Q_1 = A_1 + 2A_2 + A_3 + 4A_4, Q_2 = 2A_0 + 2A_1 + 3A_2 + 4A_3 \). Since this association scheme is symmetric, then we employ Eq. (19) and compute that \( T_0 = 801, T_1 = 30, T_2 = 21, T_3 = 51, T_4 = 51 \) and \( \Pi_{t=0}^{4} T_t = 2 \cdot 3^5 \cdot 5 \cdot 7 \cdot 17^2 \cdot 89 \). If \( p_0 \neq 2, 3, 5, 7, 17, 89 \), then \( \mathcal{C} \) is a \([27,9]\) LCD code. In particular, if \( p_0 = 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79 \), then \( \mathcal{C} \) is a \([27,9,16]\) LCD code. If \( p_0 = 89 \), then \( \mathcal{C} \) is a \([27,9,16]\) linear code with one-dimensional hull.

Example 8. Let \( p = 2, \gamma = 1, N = 3 \). Then we have \( j_0 = 1 \) and \( q = 4 \) by the assumption of Lemma 3.5. The first eigenmatrix of this case is given by Eq. (11). Let \( \mathcal{C} \) be a linear code over \( \mathbb{F}_{p_0} \) with generator matrix \( [I_q, Q_1, Q_2] \), where \( Q_1 = 2A_0 + A_1 + 6A_2 + A_3, Q_2 = A_0 + 2A_1 + 5A_2 + 4A_3 \). Since this association scheme is symmetric, then we employ Eq. (19) and compute that \( T_0 = 339, T_1 = 75, T_2 = 11, T_3 = 11 \) and \( \Pi_{t=0}^{3} T_t = 3 \cdot 5^2 \cdot 11^2 \cdot 113 \). If \( p_0 \neq 3, 5, 11, 13, 113 \), then \( \mathcal{C} \) is a \([12,4]\) LCD code. In particular, if \( p_0 = 37, 61, 67, 73, 83, 89, 97, 101, 103, 107, 109, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173 \), then \( \mathcal{C} \) is a \([12,4,9]\) LCD MDS code. If \( p_0 = 113 \), then \( \mathcal{C} \) is a \([12,4,9]\) MDS linear code with one-dimensional hull.

5. Concluding Remarks

In this paper, we give a method for constructing LCD codes and linear codes with one-dimensional hull with association schemes. Based on association schemes, some sufficient and necessary conditions for LCD codes and sufficient conditions for linear codes with one-dimensional hull have been presented in this paper. With these conditions, we can construct plenty of LCD codes and linear codes with one-dimensional hull by known association schemes. Based on our constructions, we give some examples of LCD (almost) MDS codes and (almost) MDS codes with one-dimensional hull by Magma in Section 3 and 4.

Acknowledgments

This work was supported by National Natural Science Foundation of China under Grant No. 11771392. The authors would like to thank Prof. Tao Feng for his helpful ideas and advice in preparing this paper, and also thank the referees for their detailed comments and suggestions.

References

[1] E. Bannai and T. Ito, Algebraic Combinatorics I: Association Schemes, The Benjamin/Cummings, London, 1984.
[2] L. D. Baumert, W. H. Mills and R. L. Ward, Uniform cyclotomy, J. Number Theory, 14 (1982), 67–82.
[3] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-regular Graphs, Springer-Verlag, Berlin, 1989.
[4] C. Carlet and S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, Adv. Math. Commun., 10 (2016), 131–150.
[5] C. Carlet, C. Li and S. Mesnager, Linear codes with small hulls in semi-primitive case, Des. Codes Cryptogr., 87 (2019), 3063–3075.
[6] C. Carlet, S. Mesnager, C. Tang and Y. Qi, Euclidean and Hermitian LCD MDS codes, Des. Codes Cryptogr., 86 (2018), 2605–2618.
[7] C. Carlet, S. Mesnager, C. Tang and Y. Qi, New characterization and parametrization of LCD codes, IEEE Trans. Inform. Theory, 65 (2019), 39–49.
[8] 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.
[9] C. Ding and J. Yang, Hamming weights in irreducible cyclic codes, Discrete Math., 313 (2013), 434–446.
[10] K. Feng, An Introduction to Algebraic Number Theory, Science Press, Beijing, 2000.
[11] T. Feng and K. Momihara, Three-class association schemes from cyclotomy, J. Combin. Theory Ser. A, 120 (2013), 1202–1215.
[12] K. Ireland and M. Rosen, A classical introduction to modern number theory, 2nd edition, Graduate Texts in Mathematics, 84, Springer-Verlag, New York, 1990.
[13] L. Jin and C. Xing, Algebraic geometry codes with complementary duals exceed the asymptotic Gilbert-Varshamov bound, IEEE Trans. Inform. Theory, 64 (2018), 6277–6282.
[14] H. Kharaghani and S. Suda, Symmetric Bush-type generalized Hadamard matrices and association schemes, Finite Fields Appl., 37 (2016), 72–84.
[15] C. Li, C. Ding and S. Li, LCD cyclic codes over finite fields, IEEE Trans. Inform. Theory, 63 (2017), 4344–4356.
[16] C. Li and P. Zeng, Constructions of linear codes with one-dimensional hull, IEEE Trans. Inform. Theory, 65 (2019), 1668–1676.
[17] S. Li, C. Li, C. Ding and H. Liu, Two families of LCD BCH codes, IEEE Trans. Inform. Theory, 63 (2017), 5699–5717.
[18] X. Liu and H. Liu, Matrix-product complementary dual codes, preprint, arXiv:1604.03774.
[19] J. L. Massey, Linear codes with complementary duals, Discret. Math., 106 (1992), 337–342.
[20] S. Mesnager, C. Tang and Y. Qi, Complementary dual algebraic geometry codes, IEEE Trans. Inform. Theory, 64 (2018), 2390–2397.
[21] B. Pang, S. Zhu and Z. Sun, On LCD negacyclic codes over finite fields, J. Syst. Sci. Complex., 31 (2018), 1065–1077.
[22] N. Sendrier, Finding the permutation between equivalent linear codes: The support splitting algorithm, IEEE Trans. Inform. Theory, 46 (2000), 1193–1203.
[23] N. Sendrier and G. Skersys, On the computation of the automorphism group of a linear code, in :Proceedings of IEEE ISIT2001, Washington, DC, 2001.
[24] X. Shi, Q. Yue and S. Yang, New LCD MDS codes constructed from generalized Reed-Solomon codes, J. Algebra Appl., 18 (2019), 1950150.
[25] E. R. van Dam and M. Muzychuk, Some implications on amorphic association schemes, J. Combin. Theory Ser. A, 117 (2010), 111–127.

Received April 2020; revised August 2020.

E-mail address: ye_wang@zju.edu.cn
E-mail address: rant@zju.edu.cn