Several constructions of optimal LCD codes over small finite fields*

Shitao Li[†], Minjia Shi[‡], Huizhou Liu[§]

Abstract

Linear complementary dual (LCD) codes are linear codes which intersect their dual codes trivially, which have been of interest and extensively studied due to their practical applications in computational complexity and information protection. In this paper, we give some methods for constructing LCD codes over small finite fields by modifying some typical methods for constructing linear codes. We show that all odd-like binary LCD codes, ternary LCD codes and quaternary Hermitian LCD codes can be constructed using the modified methods. Our results improve the known lower bounds on the largest minimum distances of LCD codes. Furthermore, we give two counterexamples to disprove the conjecture proposed by Bouyuklieva (Des. Codes Cryptogr. 89(11): 2445-2461, 2021).

Keywords: Binary LCD codes, ternary LCD codes, quaternary Hermitian LCD codes
Mathematics Subject Classification 94B05 15B05 12E10

1 Introduction

LCD codes were first introduced by Massey in 1992 to solve a problem in information theory [33]. In 2004, Sendrier [34] showed that LCD codes meet the asymptotic Gilbert-Varshamov bound by using the hull dimension spectra of linear codes. In 2016, Carlet and Guilley [10] investigated an application of binary LCD codes against Side-Channel Attacks (SCA) and Fault Injection Attack (FIA), and gave several constructions of LCD codes. They also have been employed to construct entanglement-assisted quantum error correction codes (see [30,31]). Recently, LCD codes were extensively studied [11–14,35,36]. In particular, an interesting result is that Carlet *et al.* [13] showed that any code over $\mathbb{F}_q$ is equivalent to some Euclidean LCD code for $q \geq 4$ and any code over $\mathbb{F}_{q^2}$ is equivalent

to some Hermitian LCD code for $q \geq 3$. This also motivates us to study LCD codes, especially LCD codes over small finite fields. Codes over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_4$ are called binary codes, ternary codes and quaternary codes, respectively.

It is also a fundamental topic to determine the largest minimum distance of LCD codes for various lengths and dimensions in coding theory. In recent years, much work has been done concerning this fundamental topic. The largest minimum distance among all binary LCD $[n, k]$ codes was partially determined in [3, 8, 15, 16, 22, 25] for $n \leq 40$. It is worth noting that there are many unknowns in [8] and [25]. The largest minimum distance among all ternary LCD $[n, k]$ codes was determined in [1, 5] for $n \leq 20$. The largest minimum diatance among all quaternary Hermitian LCD $[n, k]$ codes was partially determined in [30–32] for $n \leq 25$. More constructions of LCD codes can be seen [2, 4, 6, 19, 21, 29, 37, 38]. One of the interesting constructions is that Harada [19] gave two methods for constructing many LCD codes from a given LCD code by modifying some known methods for constructing self-dual codes [20, 26–28]. Using these methods, many new binary LCD codes and quaternary Hermitian LCD were constructed. Therefore, an open problem is to extend the above results and construct new LCD codes.

There are many typical methods for constructing new linear codes from old ones. For example, the puncturing and shortening techniques, subcodes construction. In this paper, we give some methods for constructing LCD codes by modifying the above typical methods. We show that all odd-like binary LCD codes, ternary LCD codes and quaternary Hermitian LCD codes can be constructed by our construction methods. That is to say, our methods are efficient for constructing LCD codes. Using theses methods, we obtain that some binary LCD codes with better parameters comparing with [8] and [25]. In addition, we also obtain some binary LCD codes, which are not equivalent to the codes in [25]. We extend the tables on ternary LCD codes to lengths up to 25. Some ternary LCD codes with better parameters are constructed comparing with [19]. Finally, we also construct some quaternary Hermitian LCD codes with new parameters comparing with [32]. These codes improve the previously known lower bounds on the largest minimum weights. It is worth mentioning that we give two counterexamples to disprove the conjecture proposed by Bouyuklieva [8].

The paper is organized as follows. In Section 2, we give some notations and definitions, which can be found in [24]. In Section 3, we give a method for constructing LCD $[n - \ell, k - \ell, \geq d]$ and $[n - \ell, k, d - \ell]$ codes from a given $[n, k, d]$ code with ℓ-dimensional hull. We also give a general method for constructing LCD $[n + 1, k]$ and $[n, k + 1]$ codes from a given LCD $[n, k]$ code. In Sections 4-6, we construct binary LCD codes, ternary LCD codes, quaternary Hermitian LCD codes and the related entanglement-assisted quantum error correction codes. In Section 7, we conclude the paper. All computations in this paper have been done with the computer algebra system MAGMA [7].

2 Preliminaries

Let $\mathbb{F}_q$ denote the finite field with q elements, where q is a prime power. For any $\mathbf{x} \in \mathbb{F}_q^N$, the *Hamming weight* wt($\mathbf{x}$) of $\mathbf{x}$ is the number of nonzero components of $\mathbf{x}$. An $[N, K, D]$

linear code C over $\mathbb{F}_q$ is a K-dimensional subspace of $\mathbb{F}_q^N$, where D is the minimum nonzero Hamming weight of C. Let $A_i(C)$ denote the number of codewords with Hamming weight i in C, where $0 \le i \le N$. Then the sequence $(A_0(C), A_1(C), \dots, A_N(C))$ is called the *weight distribution* of C. A *generator matrix* for an $[N, K]$ code C is any $K \times N$ matrix G whose rows form a basis for C. For any set of k independent columns of a generator matrix G, the corresponding set of coordinates forms an *information set* for C. A matrix is *monomial* if it contains exactly one nonzero element per row and per column. Two codes C and D are *equivalent* if there is a monomial matrix M such that $MC = D$. The *Euclidean dual* code $C^{\perp_E}$ of a linear code C over $\mathbb{F}_q$ is defined as

$$C^{\perp_E} = \{\mathbf{y} \in \mathbb{F}_q^N \mid \langle \mathbf{x}, \mathbf{y} \rangle_E = 0, \text{for all } \mathbf{x} \in C\},$$

where $\langle \mathbf{x}, \mathbf{y} \rangle_E = \sum_{i=1}^N x_i y_i$ for $\mathbf{x} = (x_1, x_2, \dots, x_N)$ and $\mathbf{y} = (y_1, y_2, \dots, y_N) \in \mathbb{F}_q^N$. The *Hermitian dual* code $C^{\perp_H}$ of a linear code C over $\mathbb{F}_{q^2}$ is defined as

$$C^{\perp_H} = \{\mathbf{y} \in \mathbb{F}_{q^2}^N \mid \langle \mathbf{x}, \mathbf{y} \rangle_H = 0, \text{for all } \mathbf{x} \in C\},$$

where $\langle \mathbf{x}, \mathbf{y} \rangle_H = \sum_{i=1}^N x_i \overline{y_i}$ for $\mathbf{x} = (x_1, x_2, \dots, x_N)$ and $\mathbf{y} = (y_1, y_2, \dots, y_N) \in \mathbb{F}_{q^2}^N$. Note that $\overline{x} = x^q$ for any $x \in \mathbb{F}_{q^2}$. The *Euclidean hull* (resp. *Hermitian hull*) of the linear code C is defined as

$$\text{Hull}_E(C) = C \cap C^{\perp_E} \ (\text{resp. } \text{Hull}_H(C) = C \cap C^{\perp_H}).$$

A linear code C over $\mathbb{F}_q$ is called (Euclidean) LCD if $C \cap C^{\perp_E} = \{\mathbf{0}\}$. A linear code C over $\mathbb{F}_{q^2}$ is called Hermitian LCD if $C \cap C^{\perp_H} = \{\mathbf{0}\}$. The following lemma is from [18,33].

Lemma 2.1. (1) *Let C be a code with the generator matrix G over $\mathbb{F}_q$. Then C is LCD if and only if GG^T is nonsingular, where G^T denotes the transpose of G.*
(2) *Let C be a code with the generator matrix G over $\mathbb{F}_{q^2}$. Then C is Hermitian LCD if and only if $G\overline{G}^T$ is nonsingular, where $\overline{G}^T$ denotes the conjugate transpose of G.*

Throughout this paper, let $d_q^E(N, K)$ denote the largest minimum weight among all LCD $[N, K]$ codes over $\mathbb{F}_q$ ($q = 2, 3$), and let $d_4^H(N, K)$ denote the largest minimum weight among all quaternary Hermitian LCD $[N, K]$ codes. An LCD $[N, K]$ code over $\mathbb{F}_q$ is *optimal LCD* if it has the minimum weight $d_q^E(N, K)$. An LCD $[N, K]$ code over $\mathbb{F}_q$ is called *almost optimal LCD* if it has the minimum weight $d_q^E(N, K) - 1$.

A vector $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$ is *even-like* if $\sum_{i=1}^n x_i = 0$ and is *odd-like* otherwise. A binary code is said to be *even-like* if it has only even-like codewords, and is said to be *odd-like* if it is not even-like.

Let C be an $[n, k, d]$ code over $\mathbb{F}_q$, and let T be a set of t coordinate positions in C. We puncture C by deleting all the coordinates in T in each codeword of C. The resulting code is still linear and has length $n - t$. We denote the *punctured code* by C^T. Consider the set $C(T)$ of codewords which are 0 on T; this set is a subcode of C. Puncturing $C(T)$ on T gives a code over $\mathbb{F}_q$ of length $n - t$ called the *shortened code* on T and denoted C_T. The following lemma is also valid with respect to the Hermitian inner product.

3

Lemma 2.2. [24] *Let C be an $[n, k, d]$ code over $\mathbb{F}_q$. Let T be a set of t coordinates. Then:*

(i) $(C^\perp)_T = (C^T)^\perp$ and $(C^\perp)^T = (C_T)^\perp$, and

(ii) if $t < d$, then C^T and $(C^\perp)_T$ have dimensions k and $n - t - k$, respectively.

3 Several methods for constructing LCD codes

3.1 LCD codes from shortened codes and punctured codes of linear codes

The puncturing and shortening techniques are two very important tools for constructing new codes from old ones. In this subsection, we will use these two techniques to construct new LCD codes with interesting and new parameters from some old LCD codes. Firstly, we prove that Lemma 22 in [13] is valid with respect to the Hermitian inner product.

Theorem 3.1. *Any linear code C over $\mathbb{F}_q$ (resp. $\mathbb{F}_{q^2}$) is the direct sum of a self-orthogonal code and an LCD code with respect to the Euclidean (resp. Hermitian) inner product.*

Proof. We only consider the Hermitian inner product. Let $\{\alpha_1, \ldots, \alpha_\ell, \alpha_{\ell+1}, \ldots, \alpha_k\}$ be a basis of C such that $\{\alpha_1, \ldots, \alpha_\ell\}$ is a basis of $C_1 = \mathrm{Hull}_{\mathrm{H}}(C) = C \cap C^{\perp_H}$. Let C_2 be a linear code generated by $\alpha_{\ell+1}, \alpha_{l+2}, \ldots, \alpha_k$. Then $C = C_1 \oplus C_2$. For any $\mathbf{c} \in C_2 \cap C_2^{\perp_H}$, we have $\langle \mathbf{c}, \alpha_i \rangle_H = 0$. This implies that $\mathbf{c} \in C \cap C^{\perp_H}$. Since C is LCD, $\mathbf{c} = \mathbf{0}$. Therefore, C_2 is LCD with respect to the Hermitian inner product. This completes the proof. $\square$

The following two theorems are very important and interesting.

Theorem 3.2. *If there exists an $[n, k, d]$ linear code C with ℓ-dimensional hull. Then there exists a set of ℓ coordinates position T such that the shortened C_T of C on T is an $[n - \ell, k - \ell, \geq d]$ LCD code with respect to the Euclidean and Hermitian inner product.*

Proof. Let G be a generator matrix of C. Without loss of generality, we may assume that

$$G = (I_k | A) = (\mathbf{e}_{k,i} | \mathbf{a}_i)_{1 \leq i \leq k},$$

where $\mathbf{e}_{k,i}$ and $\mathbf{a}_i$ are the i-row of I_k (the identity matrix) and A, respectively. Assume that $\{\mathbf{r}_j\}_{j=1}^{\ell}$ is a basis of $\mathrm{Hull}(C)$ such that the first non-zero position of $\mathbf{r}_j$ is the i_j-th position. Without loss of generality, we may assume that $1 \leq i_1 < i_2 < \cdots < i_\ell$. Then $i_\ell \leq k$; otherwise $\mathbf{r}_{i_\ell} = \mathbf{0}$, which is a contradiction.

Let $T = \{i_1, i_2, \ldots, i_\ell\}$ and $J = \{1, 2, \ldots, k\} \setminus T = \{j_1, j_2, \ldots, j_{k-\ell}\}$ such that $j_1 < j_2 < \cdots < j_{k-\ell}$. Then we know that $\{\mathbf{r}_j\}_{j=1}^{\ell} \cup \{(\mathbf{e}_{k,i} | \mathbf{a}_i)\}_{i \in J}$ is a basis of C. So the code $C(T)$ by generating $\{(\mathbf{e}_{k,i} | \mathbf{a}_i)\}_{i \in J}$ is an LCD code by Theorem 3.1. In fact, the generator matrix for the shortened code C_T on T is

$$G_T = (\mathbf{e}_{k-l,i} | \mathbf{a}_{j_i})_{1 \leq i \leq k-l},$$

where $\mathbf{e}_{k-\ell,i}$ is the i-row of $I_{k-\ell}$ and $\mathbf{a}_{j_i}$ is the j_i-row of A for $1 \leq i \leq k - \ell$. It follows from $C(T)$ is LCD that C_T is LCD. The parameters for C_T are obvious. $\square$

Theorem 3.3. *Let C be an $[n, k, d]$ linear code with ℓ-dimensional hull. If $t < d$, then there exists a set of t coordinate position T such that the punctured code C^T of C on T is an LCD $[n - \ell, k, d^* \geq d - \ell]$ code with respect to the Euclidean and Hermitian inner product.*

Proof. The parameters for the punctured code C^T of C on T are obvious from (ii) of Lemma 2.2. Since C is an $[n, k]$ linear code with ℓ-dimensional hull, $C^\perp$ is an $[n, n - k]$ linear code with ℓ-dimensional hull. By Theorem 3.2, there exists a set of ℓ coordinate positions T such that the shortened code $(C^\perp)_T$ of $C^\perp$ on T is an LCD $[n - \ell, n - k - \ell]$ code. It follows from (i) of Lemma 2.2 that $(C^T)^\perp = (C^\perp)_T$ is an LCD $[n - \ell, n - k - \ell]$ code. It turns out that $C^T = ((C^T)^\perp)^\perp$ is an LCD $[n - \ell, k]$ code. $\qquad\square$

Remark 3.4. By Theorem 3.2, C_T is LCD if T is an information set of Hull(C). Compared to the randomness of [25] and [32], we determine the shortened set T. In addition, the corollary 25 in [13] proved that there exists an $[n + \ell, k, \geq d]$ Euclidean LCD code if there exists an $[n, k, d]$ code with ℓ-dimensional Euclidean hull. Hence, it is easy to see that Theorem 3.2 is more effective than [13, Corollary 25].

3.2 Construction method I

Firstly, we recall a typical construction method of linear codes. Let C be a linear $[n, k]$ code with the generator matrix G. Then for any $\mathbf{x} \in \mathbb{F}_q^n$, the following matrix

$$G' = \begin{pmatrix} 1 & \mathbf{x} \\ \mathbf{0} & G \end{pmatrix}$$

generates a linear $[n + 1, k + 1]$ code. In addition, any linear $[n + 1, k + 1]$ code over $\mathbb{F}_q$ can be obtained from some linear $[n, k]$ code using the above construction.

In this subsection, we give a method for constructing many LCD $[n+1, k+1]$ codes with interesting parameters from a given LCD $[n, k]$ code by modifying the above construction method of linear codes.

Theorem 3.5. (1) *Let C be a binary LCD $[n, k]$ code with the generator matrix G. Let $\mathbf{x} \in C^\perp$ such that $\mathrm{wt}(\mathbf{x})$ is even. Then the following matrix*

$$G' = \begin{pmatrix} 1 & \mathbf{x} \\ \mathbf{0} & G \end{pmatrix}$$

generates a binary odd-like LCD $[n + 1, k + 1]$ code.

(2) *Let C be a ternary LCD $[n, k]$ code with the generator matrix G. Let $\mathbf{x} \in C^\perp$ such that $\mathrm{wt}(\mathbf{x}) \neq 2 \pmod 3$. Then the following matrix*

$$G' = \begin{pmatrix} 1 & \mathbf{x} \\ \mathbf{0} & G \end{pmatrix}$$

generates a ternary LCD $[n + 1, k + 1]$ code.

(3) *Let C be a quaternary Hermitian LCD $[n, k]$ code with the generator matrix G. Let $\mathbf{x} \in C^{\perp_H}$ such that $\mathrm{wt}(\mathbf{x})$ is even. Then the following matrix*

$$G' = \begin{pmatrix} 1 & \mathbf{x} \\ \mathbf{0} & G \end{pmatrix}.$$

generates a quaternary Hermitian LCD $[n + 1, k + 1]$ code.

Proof. We only give the proof of (1), the other cases are similar. Let $\mathbf{r}_i$ be the i-th row of G for $1 \le i \le k$. Let $\mathbf{r}'_j$ be j-th row of G' for $1 \le j \le k + 1$. Then we have

$$\begin{aligned}
\langle \mathbf{r}'_1, \mathbf{r}'_1 \rangle_E &= 1 + \langle \mathbf{x}, \mathbf{x} \rangle_E = 1, \\
\langle \mathbf{r}'_1, \mathbf{r}'_j \rangle_E &= \langle \mathbf{x}, \mathbf{r}_{j-1} \rangle_E = 0 \text{ for } 2 \le j \le k + 1, \\
\langle \mathbf{r}'_j, \mathbf{r}'_j \rangle_E &= \langle \mathbf{r}_{j-1}, \mathbf{r}_{j-1} \rangle_E \text{ for } 2 \le j \le k + 1, \\
\langle \mathbf{r}'_j, \mathbf{r}'_{j'} \rangle_E &= \langle \mathbf{r}_{j-1}, \mathbf{r}_{j'-1} \rangle_E \text{ for } 2 \le j < j' \le k + 1.
\end{aligned}$$

Hence we obtain that

$$G'G'^T = \begin{pmatrix} 1 & 0 \cdots 0 \\ 0 & \\ \vdots & GG^T \\ 0 & \end{pmatrix}.$$

If C is a binary LCD code, then it follows from Lemma 2.1 that GG^T is nonsingular. This implies that $G'G'^T$ is nonsingular. By Lemma 2.1, G' generates a binary LCD $[n+1, k+1]$ code. This completes the proof. $\square$

It is easy to see that all binary LCD codes constructed by Theorem 3.5 are odd-like. Next, we prove that all odd-like binary LCD codes can be obtained by the construction in Theorem 3.5.

Theorem 3.6. *Any binary odd-like LCD $[n, k]$ code is obtained from some binary LCD $[n - 1, k - 1]$ code (up to equivalence) using the construction of Theorem 3.5.*

Proof. Let C be a binary odd-like LCD $[n, k]$ code. According to [8, Propsition 3], there is at least one coordinate position i such that the shortened code $C_{\{i\}}$ of C on the i-th coordinate is a binary LCD $[n - 1, k - 1]$ code. Without loss of generality, we consider that $i = 1$. Assume that $C_{\{1\}}$ has the generator matrix G_1. Then there exists a binary vector $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{n-1})$ of length $n - 1$ such that the following matrix

$$G = \begin{pmatrix} 1 & \mathbf{x}' \\ \mathbf{0} & G_1 \end{pmatrix}$$

is a generator matrix of C. Since $C_{\{1\}}$ is a binary LCD code, $\mathbb{F}_2^{n-1} = C_{\{1\}} \oplus C_{\{1\}}^{\perp}$. So there are $\mathbf{x} = (x_1, x_2, \dots, x_{n-1}) \in C_{\{1\}}^{\perp}$ and $\mathbf{y} = (y_1, y_2, \dots, y_{n-1}) \in C_{\{1\}}$ such that $\mathbf{x}' = \mathbf{x} + \mathbf{y}$.

Using the binary vector $\mathbf{x} = (x_1, x_2, \ldots, x_{n-1}) \in C_{\{1\}}^{\perp}$ of length $n - 1$ and G_1 we get a generator matrix G' of a linear $[n, k]$ code C' by Theorem 3.5. And

$$G' = \begin{pmatrix} 1 & \mathbf{x} \\ \mathbf{0} & G_1 \end{pmatrix} \sim \begin{pmatrix} 1 & \mathbf{x} + \mathbf{y} \\ \mathbf{0} & G_1 \end{pmatrix} = G.$$

Thus the given code C is equivalent to C', as desired. We assert that $wt(x)$ is even; otherwise $(1|\mathbf{x}) \in C \cap C^{\perp}$, which is a contradiction. This completes the proof. $\square$

Finally, we give two counterexamples to show that Conjecture 1 in [8] is invalid.

Conjecture 3.7. [8, Conjecture 1] Let k be an even position integer and $n > k$ be another integer. If $d_2^E(n, k)$ is even and $d_2^E(n - 1, k) = d_2^E(n, k) - 1$, then all binary LCD $[n, k, d_2^E(n, k)]$ are even-like codes.

Proposition 3.8. *There exist optimal binary odd-like LCD $[14, 8, 4]$ and $[16, 10, 4]$ codes.*

Proof. According to [22, Table 3], there exist optimal binary odd-like LCD $[13, 7, 4]$ and $[15, 9, 4]$ codes, which have the following generator matrices respectively

$$\begin{pmatrix} 1000000110101 \\ 0100000011110 \\ 0010000001101 \\ 0001000100110 \\ 0000100001011 \\ 0000010111011 \\ 0000001111100 \end{pmatrix}, \quad \begin{pmatrix} 100000000110001 \\ 010000000011110 \\ 001000000011101 \\ 000100000110010 \\ 000010000011011 \\ 000001000010111 \\ 000000100111111 \\ 000000010110100 \\ 000000001111000 \end{pmatrix}.$$

By applying Theorem 3.5 to the LCD $[13, 7, 4]$ code, a binary LCD $[14, 8, 4]$ code C' is constructed, where $\mathbf{x} = (1001110001100)$. The code C' has weight distribution as:

$$[\langle 0, 1 \rangle, \langle 4, 24 \rangle, \langle 5, 36 \rangle, \langle 6, 36 \rangle, \langle 7, 60 \rangle, \langle 8, 45 \rangle, \langle 9, 28 \rangle, \langle 10, 20 \rangle, \langle 11, 4 \rangle, \langle 12, 2 \rangle].$$

Similarly, a binary LCD $[16, 10, 4]$ code is constructed, where $\mathbf{x} = (111111011001111)$, which has weight distribution as:

$$[\langle 0, 1 \rangle, \langle 4, 43 \rangle, \langle 5, 81 \rangle, \langle 6, 96 \rangle, \langle 7, 189 \rangle, \langle 8, 207 \rangle, \langle 9, 162 \rangle,$$
$$\langle 10, 144 \rangle, \langle 11, 66 \rangle, \langle 12, 21 \rangle, \langle 13, 13 \rangle, \langle 15, 1 \rangle].$$

In the sense of equivalence, these two LCD code are also constructed by [22]. Here we just show that we can also get such codes by our method. $\square$

Remark 3.9. Let $n = 14$ and $k = 8$. By [22, Table 3], $d_2^E(14, 8) = 4$ and $d_2^E(13, 8) = 3$. The condition of Conjecture 3.7 is satisfied. However, the binary LCD $[14, 8, 4]$ code in Proposition 3.8 is odd-like. Therefore, Conjecture 3.7 is invalid. Similarly, the odd-like binary LCD $[16, 10, 4]$ is also a counterexample of Conjecture 3.7.

3.3 Construction method II

In this subsection, we recall another typical construction methods of linear codes. Let C be a linear $[n, k]$ code with the generator matrix G over $\mathbb{F}_q$. For any $\mathbf{x} \in \mathbb{F}_q^n \setminus C$, the following matrix

$$G' = \begin{pmatrix} \mathbf{x} \\ G \end{pmatrix}$$

generates a linear $[n, k + 1]$ code. In addition, any linear $[n, k + 1]$ code over $\mathbb{F}_q$ can be obtained from some linear $[n, k]$ code using the above construction.

Next, we give a method for constructing many LCD $[n, k + 1]$ codes with interesting parameters from a given LCD $[n, k]$ code by modifying the above construction method of linear codes.

Theorem 3.10. (1) *Let C be a binary LCD $[n, k]$ code with the generator matrix G. Let $\mathbf{y} \in C^\perp$ such that $\mathrm{wt}(\mathbf{y})$ is odd. Then the following matrix*

$$G' = \begin{pmatrix} \mathbf{y} \\ G \end{pmatrix}.$$

generates a binary LCD $[n, k + 1]$ code.

(2) *Let C be a ternary LCD $[n, k]$ code with the generator matrix G. Let $\mathbf{y} \in C^\perp$ such that $\mathrm{wt}(\mathbf{y}) \neq 0 \pmod 3$. Then the following matrix*

$$G' = \begin{pmatrix} \mathbf{y} \\ G \end{pmatrix}.$$

generates a ternary LCD $[n, k + 1]$ code.

(3) *Let C be a quaternary Hermitian LCD $[n, k]$ code with the generator matrix G. Let $\mathbf{y} \in C^{\perp_H}$ such that $\mathrm{wt}(\mathbf{y})$ is odd. Then the following matrix*

$$G' = \begin{pmatrix} \mathbf{y} \\ G \end{pmatrix}.$$

generates a quaternary Hermitian LCD $[n, k + 1]$ code.

Proof. The proof is similar to that of Theorem 3.5, so we omit it here. $\qquad\square$

Next, we consider the converse of Theorem 3.10.

Theorem 3.11. *Any binary odd-like LCD $[n, k, d]$ code is obtained from some binary LCD $[n, k - 1, \geq d]$ code (up to equivalence) by the construction of Theorem 3.10.*

Proof. Let C be a binary odd-like LCD $[n, k, d]$ code with the generator matrix G. From [11, Theorem 3], there exists a basis $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k$ of C such that $\mathbf{c}_i \cdot \mathbf{c}_j = 1$ if $i = j$ and $\mathbf{c}_i \cdot \mathbf{c}_j = 0$ otherwise. Let C_0 be a binary code with the generator matrix $G_0 = (\mathbf{c}_i)_{1 \leq i \leq k-1}$, where c_i is the i-th row of G_0. From [11, Theorem 3], C_0 is LCD. This implies that $\mathbb{F}_2^n = C_0 \oplus C_0^\perp$. So there are $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in C_0$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in C_0^\perp$ such that $\mathbf{c}_k = \mathbf{x} + \mathbf{y}$. Since $\mathbf{c}_k \notin C_0$, $\mathbf{y} = \mathbf{c}_k - \mathbf{x} \notin C_0$.

8

Using the binary vector $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in C_0^{\perp}$ of length n and G_0 we get a generator matrix G' of a linear $[n, k+1]$ code C' by Theorem 3.10. And

$$G' = \begin{pmatrix} \mathbf{y} \\ G_0 \end{pmatrix} \sim \begin{pmatrix} \mathbf{x} + \mathbf{y} \\ G_0 \end{pmatrix} = \begin{pmatrix} \mathbf{c}_k \\ G_0 \end{pmatrix} \sim G.$$

Thus the given code C is equivalent to C', as desired. It turns out that $wt(\mathbf{y})$ is odd; otherwise $\mathbf{y} \in C_0 \cap C_0^{\perp}$, which is a contradiction. This completes the proof. □

Theorem 3.12. *Any ternary Euclidean (resp. quaternary Hermitian) LCD $[n, k]$ code is obtained from some ternary Euclidean (resp. quaternary Hermitian) LCD $[n, k-1]$ code by the construction of Theorem 3.10.*

Proof. According to [23, Propsition 4], we know that any ternary LCD $[n, k]$ code contains a ternary LCD $[n, k-1]$ subcode and any quaternary Hermitian LCD $[n, k]$ code contains a quaternary Hermitian LCD $[n, k-1]$ subcode. The rest of the proof is similar to that of Theorem 3.11, so we omit it here. □

4 New binary LCD codes

The constructions of optimal binary LCD $[n, k]$ codes were studies in [3,8,15,16,19,22,25]. It is worth noting that there are many unknowns in [8] and [25]. Hence, we will construct these unknown binary LCD codes by Constructions I and II in Section 3.

4.1 Some important inequalities

Let $d_2^E(n, k)$ denote the largest minimum weight among all binary Euclidean LCD $[n, k]$ codes. By adding zero column, the following inequality is obvious.

Lemma 4.1. *Suppose that $k \leq n$. Then $d_2^E(n+1, k) \geq d_2^E(n, k)$.*

The following lemmas are nontrivial and they were proved in [11] and [8].

Lemma 4.2. [11, Theorem 8] *Suppose that $2 \leq k \leq n$. Then $d_2^E(n, k) \leq d_2^E(n, k-1)$.*

Lemma 4.3. [8] *Let k and n be two integers such that $1 \leq k \leq n$. Then we have*

(1) *If k is odd, then $d_2^E(n, k) \leq d_2^E(n-1, k-1)$.*

(2) *If k is even and $d_2^E(n, k)$ is odd, then $d_2^E(n+1, k) \geq d_2^E(n, k) + 1$.*

(3) *If $d_2^E(n, k)$ is odd, then $d_2^E(n+2, k) \geq d_2^E(n, k) + 1$.*

Combining Theorem 3.2 and [8, Proposition 5], we give an improved upper bound.

Corollary 4.4. *Let k and n be two integers such that $2 \leq k \leq n$. Then we have*

$$d_2^E(n, k) \leq \max\{d_2^E(n-1, k-1), d_2^E(n-2, k-2)\}.$$

Proof. Assume that C is a binary $[n, k, d]$ LCD code. Let C_i be the shortened code of C on i-th coordinate for some $i \in \{1, 2, \ldots, n\}$. By [8, Proposition 5], we know that $\dim(\mathrm{Hull}(C_i)) \leq 1$. If $\dim(\mathrm{Hull}(C_i)) = 0$, then there exists a binary $[n-1, k-1, d]$ LCD code. If $\dim(\mathrm{Hull}(C_i)) = 1$, then there exists a binary $[n-1, k-1, d]$ code with one-dimension hull. By Theorem 3.2, there exists a binary $[n-2, k-2, d]$ LCD code. This completes the proof. $\qquad\square$

Let $C_{[n,k,d]_2}^{\ell}$ denote a binary $[n, k, d]$ linear code with the generator matrix $G_{[n,k,d]_2}^{\ell}$, where ℓ is the dimension of hull for such code. When $\ell = 0$, let $C_{[n,k,d]_2} = C_{[n,k,d]_2}^0$ denote a binary LCD $[n, k, d]$ code.

4.2 New binary LCD codes

From [8], only the exact value of $d_2^E(29, 11)$ remains unknown for $n = 29$.

Proposition 4.5. *There is a binary LCD $[29, 11, 9]$ code.*

Proof. By the MAGMA function BKLC, there is a binary linear $[30, 11, 10]$ code $C_{[30,11,10]_2}^1$ with one-dimensional hull. By Theorem 3.2, the shortened code $(C_{[30,11,10]_2}^1)_{\{1\}}$ on the first coordinate position is a binary LCD $[29, 10, 10]$ code $C_{[29,10,10]_2}$. We apply Construction II to the code $C_{[29,10,10]_2}$. Let us take $\mathbf{y} = (00010101101110101001100010001)$, one can construct a binary LCD $[29, 11, 9]$ code $C_{[29,11,9]_2}$. $\qquad\square$

Although the binary LCD code $C_{[29,11,9]_2}$ in Proposition 4.5 has the same parameters with the binary LCD $[29, 11, 9]$ code in [25, Proposition 3], their construction methods are different. In addition, the parameters in bold in Tables 1-3 denote that the corresponding code has new parameters according to [8] and [25].

Proposition 4.6. *There are binary LCD $[30, 11, 9]$ and $[30, 15, 7]$ codes.*

Proof. It follows from Lemma 4.1 and Proposition 4.5 that there is a binary LCD $[30, 11, 9]$ code. By the MAGMA function BKLC, there is a binary linear $[36, 21, 7]$ code $C_{[36,21,7]_2}^6$ with 6-dimensional hull. By Theorem 3.2, the shortened code $(C_{[36,21,7]_2}^6)_T$ of $C_{[36,21,7]_2}^6$ is a binary LCD $[30, 15, 7]$ code $C_{[30,15,7]_2}$, where $T = \{1, 2, 3, 5, 17, 19\}$. $\qquad\square$

Remark 4.7. We list in Tables 1-2 some binary LCD codes obtained by Theorems 3.2, 3.5 and 3.10. To save the space, the codes in Tables 1 and 2 can be obtained from `https://ahu-coding.github.io/code1/`.

Table 1: The binary LCD codes from Theorem 3.2

The code $C^{\ell}_{[n,k,d]_2}$	The set T	C_T	References
$C^1_{[30,11,10]_2}$	$\{1\}$	$[29,10,10]$	Theorem 3.2
$C^6_{[36,21,7]_2}$	$\{1,2,3,5,17,19\}$	$[\mathbf{30},\mathbf{15},\mathbf{7}]$	Theorem 3.2
$C^1_{[32,21,6]_2}$	$\{1\}$	$[31,20,6]$	Theorem 3.2
$C^1_{[34,15,9]_2}$	$\{1\}$	$[33,14,9]$	Theorem 3.2
$C^0_{[33,22,6]_2}$	$\setminus$	$[33,22,6]$	Theorem 3.2
$C^0_{[34,22,6]_2}$	$\setminus$	$[34,22,6]$	Theorem 3.2
$C^0_{[36,16,10]_2}$	$\setminus$	$[36,16,10]$	Theorem 3.2
$C^7_{[43,27,7]_2}$	$\{1,2,3,5,9,17,25\}$	$[\mathbf{36},\mathbf{20},\mathbf{7}]$	Theorem 3.2
$C^3_{[40,13,13]_2}$	$\{2,3,5\}$	$[\mathbf{37},\mathbf{10},\mathbf{13}]$	Theorem 3.2
$C^8_{[45,29,7]_2}$	$\{1,2,3,5,9,17,21,25\}$	$[\mathbf{37},\mathbf{21},\mathbf{7}]$	Theorem 3.2

Note that the code $C^{\ell}_{[n,k,d]_2}$ is the best-known binary $[n,k,d]$ code from MAGMA [7].

Table 2: The binary LCD codes from Theorem 3.5 and Theorem 3.10

The given $C_{[n,k,d]_2}$	The vector $\mathbf{x}$ or $\mathbf{y}$	C'	References
$[30,15,7]$	$(110001101111110101111111001001)$	$[\mathbf{31},\mathbf{16},\mathbf{7}]$	Theorem 3.5
$[31,16,7]$	$(1110101000111010001110111011001)$	$[\mathbf{32},\mathbf{17},\mathbf{7}]$	Theorem 3.5
$[32,17,7]$	$(11010011101011101011011000110111)$	$[\mathbf{33},\mathbf{18},\mathbf{7}]$	Theorem 3.5
$[33,14,9]$	$(111000000011111011010110010000110)$	$[34,15,9]$	Theorem 3.5
$[34,18,8]$	$(1100000000000110001000101101010110)$	$[\mathbf{35},\mathbf{19},\mathbf{7}]$	Theorem 3.5
$[34,22,6]$	$(1111111111111111111111111111111111)$	$[\mathbf{35},\mathbf{23},\mathbf{6}]$	Theorem 3.5
$[36,16,10]$	$(110100000100001000011010100001101110)$	$[37,17,9]$	Theorem 3.5
$[37,21,7]$	$(0011101010001001101010110111111001111)$	$[\mathbf{38},\mathbf{22},\mathbf{7}]$	Theorem 3.5
$[38,10,14]$	$(11110000110000000000000000111111110)$	$[39,11,13]$	Theorem 3.5
$[38,22,7]$	$(10011010101101001101010111000000101111)$	$[\mathbf{39},\mathbf{23},\mathbf{7}]$	Theorem 3.5
$[29,10,10]$	$(00010101101110101001100010001)$	$[29,11,9]$	Theorem 3.10
$[31,20,6]$	$(0000111101010000100101010011100)$	$[31,21,5]$	Theorem 3.10

Note that the given code $C_{[n,k,d]_2}$ in Table 2 is from Tables 1-2. In addition, the codes $C_{[34,18,8]_2}$ and $C_{[38,10,14]_2}$ are the extendcodes of the codes $C_{[33,18,7]_2}$ and $C_{[37,10,13]_2}$, respectively (see Table 3).

We list in Table 3 some binary LCD codes by using some inequalities, where the given code C in Table 3 is from Tables 1-3.

Table 3: The binary LCD codes from some inequalities

The given C	C'	References	The given C	C'	References
[29,11,9]	[30,11,9]	Lemma 4.1	[35,21,6]	[36,21,6]	Lemma 4.1
[29,11,9]	[31,11,10]	(3) of Lemma 4.3	[35,23,6]	[36,23,6]	Lemma 4.1
[31,16,7]	[31,15,7]	Lemma 4.2	[36,18,8]	[37,18,8]	Lemma 4.1
[31,16,7]	**[32,16,8]**	(2) of Lemma 4.3	[35,19,7]	**[37,19,8]**	(3) of Lemma 4.3
[32,16,8]	**[32,15,8]**	Lemma 4.2	[36,20,7]	**[37,20,8]**	(2) of Lemma 4.3
[31,21,5]	[32,21,5]	Lemma 4.1	[36,23,6]	[37,23,6]	Lemma 4.1
[32,15,8]	[33,15,8]	Lemma 4.1	[37,10,13]	**[38,10,14]**	(2) of Lemma 4.3
[32,16,8]	**[33,16,8]**	Lemma 4.1	[37,17,9]	[38,17,9]	Lemma 4.1
[32,17,7]	**[33,17,7]**	Lemma 4.1	[37,19,8]	[38,19,8]	Lemma 4.1
[33,22,6]	**[33,21,6]**	Lemma 4.2	[37,20,8]	**[38,20,8]**	Lemma 4.1
[33,18,7]	**[34,18,8]**	(2) of Lemma 4.3	[37,21,7]	[38,21,7]	Lemma 4.1
[34,18,8]	**[34,17,8]**	Lemma 4.2	[37,23,6]	[38,23,6]	Lemma 4.1
[34,17,8]	[34,16,8]	Lemma 4.2	[38,10,14]	[39,10,14]	Lemma 4.1
[33,21,6]	[34,21,6]	Lemma 4.1	[38,20,8]	[39,20,8]	Lemma 4.1
[34,17,8]	**[35,17,8]**	Lemma 4.1	[38,22,7]	**[39,22,8]**	(2) of Lemma 4.3
[34,18,8]	**[35,18,8]**	Lemma 4.1	[39,22,8]	**[39,21,8]**	Lemma 4.2
[34,21,6]	**[35,21,6]**	Lemma 4.1	[39,10,14]	[40,10,14]	Lemma 4.1
[34,15,9]	[36,15,10]	(3) of Lemma 4.3	[39,11,13]	[40,11,13]	Lemma 4.1
[35,17,8]	[36,17,8]	Lemma 4.1	[39,21,8]	**[40,21,8]**	Lemma 4.1
[35,18,8]	**[36,18,8]**	Lemma 4.1	[39,22,8]	**[40,22,8]**	Lemma 4.1
[35,19,7]	[36,19,7]	Lemma 4.1	[39,23,7]	[40,23,7]	Lemma 4.1

Remark 4.8. We give Tables 4 and 5 by combining Tables 1-3, [25, Tables 1-3] and [8, Tables 1-2]. Furthermore, the diamond "⋄" indicates that the construction method of the corresponding binary LCD code is different from that of [25]. The asterisk "∗" indicates that the corresponding binary LCD code has new parameters comparing with [8] and [25].

Table 4: Bounds on the minimum diatance of binary LCD codes

$n \backslash k$	9	10	11	12	13	14	15	16	17
29	10	10	**9**⋄	8	8	8	6	6	6
30	11	10	**9**⋄-10	9	8	8	**7**∗	6	6
31	11	10	**10**⋄	10	9	8	**7**⋄-8	**7**∗	6
32	12	11	10	10	9-10	8-9	**8**∗	**8**∗	**7**∗
33	12	12	10-11	10	10	9-10	**8**⋄-9	**8**⋄	**7**∗-8
34	13	12	11-12	11	10	10	**9**⋄-10	**8**⋄-9	**8**∗
35	13-14	12-13	12	12	10-11	10	9-10	9-10	**8**∗
36	14	12-14	12-13	12	10-12	10-11	**10**⋄	10	**8**⋄-9
37	14	**13**∗-14	12-14	12-13	10-12	10-12	10-11	10	**9**⋄-10
38	14-15	**14**∗	12-14	12-14	11-12	10-12	10-12	10-11	**9**⋄-10
39	14-16	**14**⋄-15	**13**⋄-14	12-14	11-13	11-12	10-12	10-12	10-11
40	15-16	**14**⋄-16	**13**⋄-15	13-14	12-14	11-13	10-12	10-12	10-12

12

Table 5: Bounds on the minimum diatance of binary LCD codes

$n\backslash k$	18	19	20	21	22	23	24	25	26	27	28	29	30
29	6	5	4	4	4	3	2	2	2	2	2	1	
30	6	5-6	5	4	4	4	3	2	2	2	2	1	1
31	6	6	6	$5^\diamond$	4	4	4	3	2	2	2	2	2
32	6	6	6	$5^\diamond$-6	5	4	4	3-4	3	2	2	2	2
33	7^*	6	6	$6^\diamond$	6	5	4	4	4	3	2	2	2
34	8^*	6-7	6	$6^\diamond$	6	5-6	4	4	4	3-4	3	2	2
35	8^*	7^*-8	6-7	6^*	6	$6^\diamond$	5	4	4	4	4	3	2
36	8^*	$7^\diamond$-8	7^*-8	$6^\diamond$-7	6	$6^\diamond$	6	5	4	4	4	3-4	3
37	$8^\diamond$-9	8^*	8^*	7^*-8	6-7	$6^\diamond$	6	5-6	5	4	4	4	4
38	9-10	$8^\diamond$-9	$8^\diamond$	$7^\diamond$-8	7^*-8	$6^\diamond$-7	6	6	6	5	4	4	4
39	10	9-10	$8^\diamond$-9	8^*	8^*	7^*-8	6-7	6	6	5-6	5	4	4
40	10-11	9-10	9-10	8^*-9	$8^\diamond$	$7^\diamond$-8	6-8	6-7	6	6	6	5	4

5 New ternary LCD codes

The constructions of optimal ternary LCD $[n, k]$ codes were studies in [1,5,19]. Hence, we will construct some unknown ternary LCD codes and extend a result of Araya, Harada and Saito to length 25 by Constructions I and II in Section 3.

5.1 Some important inequalities

Let $d_3^E(n, k)$ denote the largest minimum weight among all ternary Euclidean LCD $[n, k]$ codes. By adding zero column, we have $d_3^E(n + 1, k) \geq d_3^E(n, k)$.

Lemma 5.1. [23] *Suppose that $2 \leq k \leq n$. Then $d_3^E(n, k) \leq d_3^E(n, k - 1)$.*

Lemma 5.2. [5] *If $20 \leq n \leq 25$, then we have*

$$d_3^E(n, n - 2) = 2, \ d_3^E(n, n - 3) = 2, \ d_3^E(n, n - 4) = 3.$$

According to [1], we know that $d_3^E(n, n-1) = 1$ if $n \equiv 0 \pmod 3$ and $d_3^E(n, n-1) = 2$ if $n \equiv 1, 2 \pmod 3$. The following proposition is a generalization of [8, Proposition 5].

Proposition 5.3. *Let C be a ternary linear $[n, k, d]$ code and $\dim(C \cap C^\perp) = s$. If C_i is the shortened code of C in i-th coordinate for some $1 \in \{1, \ldots, n\}$, then $dim(C_i \cap C_i^\perp) \leq s + 1$.*

Proof. Without loss of generality, we can consider the shortened code C_1 of C on the first coordinate. If all codewords have 0 as a first coordinate, then $\dim(C_1 \cap C_1) = \dim(C \cap C^\perp) = s$. Otherwise $C = (0|C_1) \cup (1|u + C_1) \cup (2|2u + C)$ for a codeword $(1, u) \in C$. Let $\mathcal{H} = C \cap C^\perp$ and $\mathcal{H}_1 = C_1 \cap C_1^\perp$. There are two possibilities for $\mathcal{H}$, namely $\mathcal{H} = (0|\mathcal{H}')$ or $\mathcal{H} = (0|\mathcal{H}') \cup (1|v + \mathcal{H}') \cup (2|2v + \mathcal{H}')$. In both cases, $\mathcal{H}' \subseteq \mathcal{H}_1$.

(i) If $\mathcal{H}' = \mathcal{H}_1$, then $\dim(\mathcal{H}_1) = \dim(\mathcal{H})$ or $\dim(\mathcal{H}) - 1$.

(ii) If $\mathcal{H}' \subsetneq \mathcal{H}_1$. Take $y_1, y_2 \in \mathcal{H}_1 \backslash \mathcal{H}' \subseteq C_1 \cap C_1^\perp$. It follows from $y_i \in C_1$ that $(0, y_i) \in C$. If follows from $y_i \in C_1^\perp = (C^\perp)^1$ that $(\lambda_i, y_i) \in C^\perp$ for some $\lambda_i \in \mathbb{F}_3$. If $\lambda_i = 0$, then $(0, y_i) \in C \cap C^\perp = \mathcal{H}$. Implying that $y_i \in \mathcal{H}'$, which is a contradiction. Hence

13

$\lambda_i \neq 0$. So $(0, \lambda_2 y_1 - \lambda_1 y_2) \in \mathcal{H}$, which implies that $\lambda_2 y_1 - \lambda_1 y_2 \in \mathcal{H}'$. It turns out that $\mathcal{H}_1 = \mathcal{H}' \cup (y_1 + \mathcal{H}') \cup (2y_1 + \mathcal{H}')$ and $\dim(\mathcal{H}_1) = \dim(\mathcal{H}') + 1$. Since $\dim(\mathcal{H}') = \dim(\mathcal{H})$ or $\dim(\mathcal{H}) - 1$, we have $\dim(\mathcal{H}_1) = \dim(\mathcal{H})$ or $\dim(\mathcal{H}) + 1$. This completes the proof. $\square$

Corollary 5.4. *Let k and n be two integers such that $2 \leq k \leq n$. Then we have*

$$d_3^E(n, k) \leq \max\{d_3^E(n-1, k-1), d_3^E(n-2, k-2)\}.$$

Proof. The proof is similar to that of Corollary 4.4. The main difference is that we use Proposition 5.3 instead of [8, Proposition 5]. $\square$

5.2 New ternary LCD codes

Firstly, we give some known ternary LCD codes from [5].

$$13 \leq d_3(23, 4) \leq 14, \ d_3(24, 4) = 15, \ 15 \leq d_3(25, 4) \leq 16.$$

According to [5], there are ternary LCD codes $C_{[19,6,9]_3}$, $C_{[20,5,11]_3}$, $C_{[20,6,10]_3}$ and $C_{[20,8,8]_3}$, they have the following generator matrices respectively.

$$\begin{pmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,1\,0\,0\,0\,0\,0\,0\,1\,1\,2\,2\,2\,1\,1\,1\,0\,0 \\ 0\,0\,1\,0\,0\,0\,1\,1\,1\,2\,1\,1\,1\,1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,1\,2\,2\,2\,1\,2\,0\,0\,1\,1\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,1\,2\,0\,1\,2\,1\,1\,0\,1\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,1\,1\,1\,2\,1\,0\,1\,0\,1\,0\,1\,2\,0\,1\,1\,0 \end{pmatrix}, \quad \begin{pmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,1\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,0\,1\,1\,1\,1\,2\,2\,2 \\ 0\,0\,1\,0\,0\,0\,1\,2\,2\,1\,2\,2\,1\,0\,2\,1\,1\,2\,2\,1 \\ 0\,0\,0\,1\,0\,1\,1\,2\,1\,1\,0\,2\,2\,2\,2\,1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,1\,2\,0\,1\,2\,2\,0\,2\,1\,2\,1\,2\,1\,0\,1 \end{pmatrix},$$

$$\begin{pmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,1\,0\,0\,0\,0\,0\,0\,1\,1\,1\,2\,2\,1\,1\,1\,1\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,1\,1\,2\,1\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,1\,0\,0\,1\,2\,0\,2\,1\,1\,1\,0\,1\,1\,0\,1\,1\,0\,0\,1\,0 \\ 0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,2\,1\,0\,0\,2\,0\,1\,1\,1\,0 \\ 0\,0\,0\,0\,0\,1\,1\,2\,2\,0\,0\,1\,2\,2\,1\,2\,0\,0\,0\,1 \end{pmatrix}, \quad \begin{pmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1 \\ 0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0\,0\,1\,1\,1\,2\,2\,1\,1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0\,0\,1\,2\,2\,1\,0\,1\,0\,2\,1\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0\,0\,1\,2\,2\,2\,1\,0\,0\,1\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,2\,0\,2\,2\,0\,2\,0\,0\,2\,0 \\ 0\,0\,0\,0\,0\,0\,1\,0\,1\,2\,0\,1\,2\,2\,0\,0\,0\,1\,1\,0 \\ 0\,0\,0\,0\,0\,0\,0\,1\,0\,2\,0\,2\,0\,2\,2\,2\,1\,1\,1\,0 \end{pmatrix}.$$

Proposition 5.5. *There are ternary LCD $[20, 7, 9]$ and $[20, 12, 6]$ codes.*

Proof. We start from the ternary LCD code $C_{[19,6,9]_3}$. By applying Theorem 3.5, we can construct a ternary LCD $[20, 7, 9]$ code $C_{[20,7,9]_3}$ with the generator matrix

$$G_{[20,7,9]_3} = \left(\begin{array}{c|cccccccccccccccccccc} 1 & 1 & 1 & 0 & 2 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 2 & 2 & 2 \\ \hline 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 1 & 0 & 1 & 0 & 1 & 2 & 0 & 1 & 1 & 0 \end{array} \right).$$

By the MAGMA function BKLC, one can construct a ternary LCD $[20, 12, 6]$ code. $\square$

14

Remark 5.6. We list in Tables 6-7 some ternary LCD codes obtained by Theorems 3.2, 3.3, 3.5 and 3.10. To save the space, the codes in Table 6 can be obtained from `https://ahu-coding.github.io/code1/`.

Table 6: The ternary LCD codes from Theorems 3.2 and 3.3

The code $C_{[n,k,d]_3}^\ell$	The set T	C_T	References
$C_{[20,12,6]_3}^0$	\	[20,12,6]	Theorem 3.2
$C_{[21,12,6]_3}^0$	\	[21,12,6]	Theorem 3.2
$C_{[21,15,4]_3}^0$	\	[21,15,4]	Theorem 3.2
$C_{[21,17,3]_3}^0$	\	[21,17,3]	Theorem 3.2
$C_{[25,9,11]_3}^3$	{1,2,3}	[22,6,11]	Theorem 3.2
$C_{[25,13,8]_3}^3$	{1,2,9}	[22,10,8]	Theorem 3.2
$C_{[23,17,4]_3}^0$	\	[23,17,4]	Theorem 3.2
$C_{[24,18,4]_3}^0$	\	[24,18,4]	Theorem 3.2
$C_{[44,29,8]_3}^9$	{2,3,4,5,6,7,8,9,10}	[35,20,8]	Theorem 3.2
$C_{[40,29,6]_3}^1$	{2}	[39,28,6]	Theorem 3.2
The code $C_{[n,k,d]_3}^\ell$	The set T	C^T	References
$C_{[27,5,16]_3}^3$	{1,2,5}	[24,5,13]	Theorem 3.3
$C_{[29,6,16]_3}^4$	{1,2,3,4}	[25,6,13]	Theorem 3.3

Note that the code $C_{[n,k,d]_3}^\ell$ is the best-known ternary $[n,k,d]$ code from MAGMA [7].

Proposition 5.7. *There are ternary LCD* $[22,11,7]$ *and* $[24,16,5]$ *codes.*

Proof. We start from the ternary LCD codes $C_{[22,10,8]_3}$ and $C_{[24,15,6]_3}$ (see Tables 6 and 7). By applying Theorem 3.10, we can construct ternary LCD codes $C_{[22,11,7]_3}$ and $C_{[24,16,5]_3}$ with the following generator matrices, respectively,

$$G_{[22,11,7]_3} = \begin{pmatrix} \underline{1101222110122211012200} \\ 1000010000002002210122 \\ 0100020000102002111010 \\ 0010010000101020000122 \\ 0001020000222012211022 \\ 0000110000110010202010 \\ 0000001000011020021021 \\ 0000000100221002122200 \\ 0000000010212022221211 \\ 0000000001101002102021 \\ 0000000000000111111110 \end{pmatrix}, \quad G_{[24,16,5]_3} = \begin{pmatrix} \underline{001121202101001122102021} \\ 100000000000000120201111 \\ 010000000000000112011000 \\ 001000000000000112110022 \\ 000100000000000020110211 \\ 000010000000000020021220 \\ 000001000000000002002122 \\ 000000100000000012220010 \\ 000000010000000001222001 \\ 000000001000000021102102 \\ 000000000100000011100011 \\ 000000000010000022120200 \\ 000000000001000002212020 \\ 000000000000100000221202 \\ 000000000000010012012221 \\ 000000000000001022211121 \end{pmatrix}.$$

□

15

Table 7: The ternary LCD codes from Theorem 3.5 and Theorem 3.10

The given $C_{[n,k,d]_3}$	The vector **x** or **y**	C'	References
[19,6,9]	(1102001100000110222)	[20,7,9]	Theorem 3.5
[20,5,11]	(21112201000000010021)	[21,6,10]	Theorem 3.5
[20,6,10]	(02112000000000121221)	[21,7,9]	Theorem 3.5
[20,8,8]	(12021210000020212222)	[21,9,8]	Theorem 3.5
[21,6,10]	(200002221000002020221)	[22,7,10]	Theorem 3.5
[21,7,9]	(222210000000002002222)	[22,8,9]	Theorem 3.5
[21,12,6]	(120000022222120122212)	[22,13,6]	Theorem 3.5
[21,15,4]	(010000111012101011211)	[22,16,4]	Theorem 3.5
[21,17,3]	(010021201100021201212)	[22,18,3]	Theorem 3.5
[22,6,11]	(1211021222210000112200)	[23,7,11]	Theorem 3.5
[22,7,10]	(1112202121010001202201)	[23,8,10]	Theorem 3.5
[22,8,9]	(2210022110000011120021)	[23,9,9]	Theorem 3.5
[22,11,7]	(0010002100121001211101)	[23,12,7]	Theorem 3.5
[22,13,6]	(2110210002112020111112)	[23,14,6]	Theorem 3.5
[23,7,11]	(10112100000000000102211)	[24,8,10]	Theorem 3.5
[23,12,7]	(00100211121000112121012)	[24,13,7]	Theorem 3.5
[23,14,6]	(22100010002211222202121)	[24,15,6]	Theorem 3.5
[24,8,10]	(020212110000000020010011)	[25,9,10]	Theorem 3.5
[24,15,6]	(102200010201120202000120)	[25,16,6]	Theorem 3.5
[24,16,5]	(010000010021012212210010)	[25,17,5]	Theorem 3.5
[24,18,4]	(121000002021110021222212)	[25,19,4]	Theorem 3.5
[35,20,8]	(12202110000000002101221001212020220)	[36,21,8]	Theorem 3.5
[36,21,8]	(100200212100000112200221222000012121)	[37,22,8]	Theorem 3.5
[39,28,6]	(021020210000200202112021120012101111112)	[40,29,6]	Theorem 3.5
[22,10,8]	(1101222110122211012200)	[22,11,7]	Theorem 3.10
[22,13,6]	(0020100000102202121012)	[22,14,5]	Theorem 3.10
[23,14,6]	(00020100000102202121012)	[23,15,5]	Theorem 3.10
[24,15,6]	(001121202101001122102021)	[24,16,5]	Theorem 3.10
[25,9,10]	(1112101001021000011020001)	[25,10,9]	Theorem 3.10
[25,10,9]	(1222121000002000212020021)	[25,11,8]	Theorem 3.10

Note that the given code $C_{[n,k,d]_3}$ in Table 7 is from Tables 6-7.

Corollary 5.8. $d_3^E(21,9) = 8, d_3^E(22,10) = 8, d_3^E(23,11) \in \{7,8\}, d_3^E(24,12) \in \{7,8\}$.

Proof. By Tables 6 and 7, there are ternary LCD $[21,9,8]$, $[22,10,8]$, $[23,11,7]$ and $[24,12,7]$ codes. From [5, Table 7], we know that $d_3^E(19,7) = d_3^E(20,8) = 8$. It follows from Corollary 5.4 that $d_3^E(21,9) \leq \max\{d_3^E(20,8), d_3^E(19,7)\} = 8$. Similarly, we have $d_3^E(22,10) \leq 8$, $d_3^E(23,11) \leq 8$ and $d_3^E(24,12) \leq 8$. □

Remark 5.9. Combining the Database [17] and the above results, we give lower and upper bounds on minimal distance of ternary LCD codes with length $20 \leq n \leq 25$, where the parameters for ternary LCD codes of the length 20 can be found in [5]. All results are listed in Tables 8-9.

Table 8: Bound on the minimum distance of ternary LCD codes

$n\backslash k$	4	5	6	7	8	9	10	11	12	13	14
20	12	11	10	**9**	8	7-8	7	6	**6**	5	4
21	12	11-12	10-11	9-10	8-9	8	7-8	6-7	6	5-6	4-5
22	12-13	11-12	11-12	10-11	9-10	8-9	8	7-8	6-7	6	5-6
23	13-14	11-13	11-12	11-12	10-11	9-10	8-9	7-8	7-8	6-7	6
24	15	13-14	11-13	11-12	10-11	9-11	8-10	7-9	7-8	7-8	6-7
25	15-16	13-15	13-14	11-13	10-12	10-11	9-11	8-10	7-9	7-8	6-8

The parameters in bold denote the corresponding code has new parameters according to [5].

Table 9: Bound on the minimum distance of ternary LCD codes

$n\backslash k$	15	16	17	18	19	20	21	22	23	24	25
20	3-4	3	2	2	2	1					
21	4	3	3	2	2	1	1				
22	4-5	4	3	3	2	2	2	1			
23	5-6	4-5	4	3	3	2	2	2	1		
24	6	5-6	4-5	4	3	3	2	2	1	1	
25	6-7	6	5-6	4-5	4	3	3	2	2	2	1

Proposition 5.10. *There are ternary LCD* $[37, 22, 8]$ *and* $[40, 29, 6]$ *codes.*

Proof. We start from the ternary LCD code $C_{[35,20,8]_3}$ (see Table 6). By applying Theorem 3.5, we can construct a ternary LCD $[36, 21, 8]$ code $C_{[36,21,8]_3}$, where $\mathbf{x} = (122021100000000$ $02101221001212020220)$. We start from the ternary LCD code $C_{[36,21,8]_3}$. By applying Theorem 3.5, we can construct a ternary LCD $[37, 22, 8]$ code $C_{[37,22,8]_3}$ with the generator matrix

$$G_{[37,22,8]_3} = \begin{pmatrix} 1 & 1 & 0020021210000011220022122000012121 \\ 0 & 1 & 1220211000000002101221001212020220 \\ 0 & 0 & 1000000000000000020222210101011110 \\ 0 & 0 & 0100000000000000001000102121110222 \\ 0 & 0 & 0010000000000000001012011212012220 \\ 0 & 0 & 0001000000000000001020101211002220 \\ 0 & 0 & 0000100000000000001011202212110220 \\ 0 & 0 & 0000010000000000000011011011221211 \\ 0 & 0 & 0000001000000000001000222021120121 \\ 0 & 0 & 0000000100000000002010122110001211 \\ 0 & 0 & 0000000010000000001001002211120122 \\ 0 & 0 & 0000000001000000001000000220120202 \\ 0 & 0 & 0000000000100000001022110121221020 \\ 0 & 0 & 0000000000010000002002210101110220 \\ 0 & 0 & 0000000000001000000012210020002210 \\ 0 & 0 & 0000000000000100000101010210000010121 \\ 0 & 0 & 0000000000000010000201111012120220211 \\ 0 & 0 & 0000000000000001000200121101010111101 \\ 0 & 0 & 0000000000000000100101120100120000001 \\ 0 & 0 & 0000000000000000010202002111112002020 \\ 0 & 0 & 0000000000000000001000121212121002010 \\ 0 & 0 & 0000000000000000000010120211010122001 \end{pmatrix}.$$

17

We start from the ternary LCD code $C_{[39,28,6]_3}$ (see Table 6). By applying Theorem 3.5, we can construct a ternary LCD $[40, 29, 6]$ code $C_{[40,29,6]_3}$, where $\mathbf{x} = (02102021000020020211$ $2021120012101111112)$. $\square$

Remark 5.11. We can construct some ternary LCD codes with better parameters compared with [19]. For example, the ternary LCD code of the length 37 with the dimension 22 has the minimum distance 8, while the ternary LCD code of the length 37 with the dimension 22 in [19, Corollary 6.3] has the minimum distance 7. That is to say, the ternary LCD code $C_{[37,22,8]_3}$ we obtained is also considered new. The code $C_{[40,29,6]}$ also has better parameters compared with [19, Corollary 6.3].

6 New quaternary Hermitian LCD codes

Let $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$. Let $d_4^H(n,k)$ denote the largest minimum distance among all quaternary Hermitian LCD $[n, k]$ codes.

Proposition 6.1. *There are quaternary Hermitian LCD* $[22, 12, 7]$, $[23, 13, 7]$, $[24, 14, 7]$ *and* $[25, 15, 7]$ *codes.*

Proof. By the MAGMA function BKLC, one can construct a quaternary $[25, 15, 7]$ code $C_{[25,15,7]_4}^4$ with 4-dimensional Hermitian hull. According to Theorem 3.2, the shortened code $(C_{[25,15,7]_4}^4)_T$ on $T = \{1, 2, 3, 4\}$ is a quaternary Hermitian LCD $[21, 11, 7]$ code $C_{[21,11,7]_4}$, which has the following generator matrix

$$
G_{[21,11,7]_4} = \begin{pmatrix}
1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & \omega & \omega^2 & 0 & \omega^2 & \omega^2 & \omega & 1 & \omega & 1 & \omega^2 \\
0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 1 & 0 & 1 & 1 & 1 & \omega^2 & 0 & \omega & \omega & \omega \\
0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0 & \omega^2 & 1 & \omega^2 & \omega^2 & 0 & 0 & \omega^2 & 1 & 1 & \omega^2 \\
0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0 & \omega^2 & 1 & \omega & \omega^2 & \omega^2 & \omega & 0 & \omega & \omega^2 & 0 \\
0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0 & \omega^2 & \omega^2 & \omega & 0 & \omega & 1 & 0 & \omega & \omega^2 & \omega \\
0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0 & 0 & \omega^2 & 1 & 0 & \omega & \omega & \omega^2 & 0 & \omega & 1 \\
0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0 & \omega & \omega^2 & 1 & 1 & 0 & \omega & 0 & 0 & 0 & \omega \\
0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0 & \omega & \omega^2 & \omega & 0 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 \\
0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0 & 0 & \omega & 0 & 1 & 0 & \omega^2 & \omega & \omega & 0 & \omega^2 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0 & 1 & 0 & \omega^2 & \omega^2 & \omega & 0 & \omega & 1 & \omega^2 & \omega \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1 & 1 & 1 & \omega & \omega & 1 & 0 & 0 & \omega & 1 & \omega
\end{pmatrix}.
$$

By applying Theorem 3.5, one can construct a quaternary Hermitian LCD $[22, 12, 7]$ code, where $\mathbf{x} = (1\omega1100000\omega0\omega\omega^2\omega\omega00\omega^2\omega^2\omega^20)$.

By the MAGMA function BKLC, one can construct a quaternary $[26, 16, 7]$ code $C_{[26,16,7]_4}^3$ with 3-dimensional Hermitian hull. According to Theorem 3.2, the shortened code $(C_{[26,16,7]_4}^3)_T$ on $T = \{1, 2, 3\}$ is a quaternary Hermitian LCD $[23, 13, 7]$ code $C_{[23,13,7]_4}$,

which has the following generator matrix

$$G_{[23,13,7]_4} = \begin{pmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\ 0\ \omega^2\ \omega^2\ 0\ \omega^2\ \omega^2\ 0\ 1\ 0\ 1 \\ 0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\ \omega\ 0\ 1\ \omega^2\ 0\ \omega^2\ 0\ 0\ 1\ 1 \\ 0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\ \omega^2\ 1\ 0\ 1\ \omega\ 1\ \omega^2\ 1\ \omega^2\ \omega^2 \\ 0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\ \omega^2\ \omega^2\ 0\ 0\ \omega^2\ 0\ \omega\ \omega^2\ 0\ \omega \\ 0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\ \omega^2\ \omega\ 0\ \omega^2\ 1\ \omega^2\ 1\ 1\ \omega^2\ \omega \\ 0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,1\ \omega\ \omega^2\ \omega\ \omega\ \omega^2\ 1\ 1\ 1\ \omega \\ 0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\ \omega^2\ 1\ 0\ \omega\ \omega\ \omega^2\ 0\ \omega\ 1\ 0 \\ 0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\ \omega\ 1\ \omega^2\ 0\ 0\ \omega\ \omega\ 1\ 0\ 1 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\ \omega\ \omega\ \omega\ \omega^2\ 1\ 1\ 1\ \omega\ 1\ 1 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\ \omega\ 0\ 1\ 0\ \omega^2\ \omega\ \omega\ 0\ \omega^2\ 0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\ \omega^2\ \omega^2\ \omega\ \omega\ 1\ \omega^2\ 0\ 0\ \omega^2\ \omega^2 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\ \omega\ \omega\ \omega^2\ 1\ 1\ 1\ \omega^2\ \omega\ \omega^2\ \omega^2 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\ \omega^2\ 0\ 1\ 0\ 1\ 1\ 1\ \omega^2\ 1\ \omega^2 \end{pmatrix}.$$

By applying Theorem 3.5 to the code $C_{[23,13,7]_4}$, one can construct a quaternary Hermitian LCD $[24, 14, 7]$ code $C_{[24,14,7]_4}$, where $\mathbf{x} = (0\omega\omega^2 0\omega 001\omega 01\omega\omega\omega^2\omega^2\omega^2 00\omega 11\omega\omega)$.

By applying Theorem 3.5 to the code $C_{[24,14,7]_4}$, one can construct a quaternary Hermitian LCD $[25, 15, 7]$ code $C_{[25,15,7]_4}$, where $\mathbf{x} = (11001\omega^2 1\omega\omega^2 0\omega^2\omega^2 100\omega^2\omega^2\omega\omega\omega^2 01\omega^2\omega)$. ☐

Remark 6.2. Compared with Table 3 in [32], the quaternary Hermitian LCD codes in Lemma 6.1 have better parameters than their parameters. For example, the quaternary Hermitian LCD code of the length 24 with the dimension 14 has the minimum distance 7, while the quaternary Hermitian LCD code of the length 24 with the dimension 14 in [32, Table 3] has the minimum distance 6. That is to say, the quaternary Hermitian LCD code $C_{[24,14,7]_4}$ we obtained is also considered new.

As an application, we can construct some EAQECCs with different parameters from quaternary Hermitian LCD codes. We use $[[n, k, d; c]]_2$ to denote a binary entanglement-assisted quantum error correcting code (EAQECC) that encodes k information qubits into n channel qubits with the help of c pre-shared entanglement pairs, and d is called the minimum distance of the EAQECC. EAQECCs were introduced by Brun et al. in [9], which include the standard quantum stabilizer codes as a special case. It has shown that if there is a quaternary Hermitian LCD $[n, k, d]$ code, then there is a binary EAQECC with parameters $[[n, k, d; n - k]]_2$ (see [31, Lemma 2.1']). Hence, as a consequence of Proposition 6.1 and [2, Lemma 3.3], we have that

Corollary 6.3. *For* $(n, k, d) \in \{(22, 12, 7), (23, 13, 7), (24, 14, 7), (25, 15, 7)\}$ *and a non-negative integer* s, *there is a binary EAQECC with parameters* $[[n + \frac{4^k-1}{3}s, k, d + 4^{k-1}s; n + \frac{4^k-1}{3}s - k]]_2$.

Proof. Combining with Proposition 6.1 and [2, Lemma 3.3], we know that there is a quaternary Hermitian LCD $[n + \frac{4^k-1}{3}s, k, d + 4^{k-1}s]$ code for $(n, k, d) \in \{(22, 12, 7), (23, 13, 7), (24, 14, 7), (25, 15, 7)\}$ and a nonnegative integer s. According to [31, Lemma 2.1'], there is a binary EAQECC with parameters $[[n + \frac{4^k-1}{3}s, k, d + 4^{k-1}s; n + \frac{4^k-1}{3}s - k]]_2$. ☐

19

Example 6.4. According to Corollary 6.3, there are binary EAQECCs with parameters $[[22, 12, 7; 10]]_2$, $[[23, 13, 7; 10]]_2$, $[[24, 14, 7; 10]]_2$ and $[[25, 15, 7; 10]]_2$. However, the best known binary EAQECCs in [17] have parameters $[[22, 12, 6; 6]]_2$, $[[23, 13, 6; 7]]_2$, $[[24, 14, 6; 7]]_2$ and $[[25, 15, 6; 8]]_2$. The EAQECCs we construct have larger minimum distances.

7 Conclusion

In this paper, we have introduced some methods for constructing LCD codes over small finite fields by modifying some typical methods. We have constructed many new binary LCD codes, ternary LCD codes and quaternary Hermitian LCD codes, which improve the known lower bounds on the largest minimum weights. As a consequence, we used two counterexamples to disprove the conjecture proposed by Bouyuklieva. Finally, as an application of quaternary Hermitian LCD codes, we found some binary EAQECCs with new parameters. We believe that our methods can produce more results for LCD codes.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Data Deposition Information

Our data can be obtained from the authors upon reasonable request.

Acknowledgement

References

[1] M. Araya, M. Harada, On the classification of linear complementary dual codes, Discrete Math., 2019, **342**(1): 270-278.

[2] M. Araya, M. Harada, On the classification of quaternary optimal Hermitian LCD codes, Cryptogr. Commun., 2022, **14**(4): 833-847.

[3] M. Araya, M. Harada, On the minimum weights of binary linear complementary dual codes, Cryptogr. Commun., 2020, **12**(2): 285-300.

[4] M. Araya, M. Harada, K. Saito, Characterization and classification of optimal LCD codes, Des. Codes Cryptogr., 2021, **89**: 617-640.

[5] M. Araya, M. Harada, K. Saito, On the minimum weights of binary LCD codes and ternary LCD codes, Finite Fields Appl., 2021, **76**: 101925.

[6] M. Araya, M. Harada, K. Saito, Quaternary Hermitian linear complementary dual codes, IEEE Trans. Inf. Theory, 2020, **66**: 2751-2759.

[7] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput., 1997, **24**: 235-265.

[8] S. Bouyuklieva, Optimal binary LCD codes, Des. Codes Cryptogr., 2021, **89**(11): 2445-2461.

[9] T. Brun, I. Devetak, M. H. Hsieh, Correcting quantum errors with entanglement, Science, 2006, **314**(5789): 436-439.

[10] C. Carlet, S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, Adv. Math. Commun., 2016, **10**(1): 131-150.

[11] C. Carlet, S. Mesnager, C. Tang, Y. Qi, New characterization and parametrization of LCD codes, IEEE Trans. Inf. Theory, 2019, **65**(1): 39-49.

[12] C. Carlet, S. Mesnager, C. Tang, Y. Qi, On σ-LCD codes, IEEE Trans. Inf. Theory, 2019, **65**(3): 1694-1704.

[13] C. Carlet, S. Mesnager, C. Tang, Y. Qi, R. Pellikaan, Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$, IEEE Trans. Inf. Theory, 2018, **64**(4): 3010-3017.

[14] S. T. Dougherty, J. Kim, B. Özkaya, L. Sok, P. Solé, The combinatorics of LCD codes: linear programming bound and orthogonal matrices, Int. J. Inf. Coding Theory, 2017, **4**(2-3): 116-128.

[15] Q. Fu, R. Li, F. Fu, Y. Rao, On the construction of binary optimal LCD codes with short length, Int. J. Found. Comput. Sci., 2019, **30**: 1237-1245.

[16] L. Galvez, J. L. Kim, N. Lee, Y. G. Roe, B. S. Won, Some bounds on binary LCD codes, Cryptogr. Commun., 2018, **10**(4): 719-728.

[17] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, http://www.codetables.de. Accessed 4 March 2022.

[18] C. Güneri, B. Özkaya, P. Solé, Quasi-cyclic complementary dual codes, Finite Fields Appl., 2016, **42**: 67-80.

[19] M. Harada, Construction of binary LCD codes, ternary LCD codes and quaternary Hermitian LCD codes. Des. Codes Cryptogr., 2021, **89**(10): 2295-2312.

[20] M. Harada, Existence of new extremal doubly-even codes and extremal singly–even codes. Des. Codes Cryptogr., 1996, **8**(3): 273-283.

[21] M. Harada, Some optimal entanglement-assisted quantum codes constructed from quaternary Hermitian linear complementary dual codes. Int. J. Quantum Inf., 2019, **17**: 1950053.

[22] M. Harada, K. Saito, Binary linear complementary dual codes, Cryptogr. Commun., 2019, **11**(4): 677-696.

[23] M. Harada, K. Saito, Remark on subcodes of linear complementary dual codes, Inform. Process. Lett., 2020, **159**(160): 105963.

[24] W. C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, 2003.

[25] K. Ishizuka, K. Saito, Construction for both self-dual codes and LCD codes, Adv. Math. Commun., 2023, **17**(1): 139-151.

[26] J. L. Kim, New extremal self-dual codes of lengths 36, 38 and 58, IEEE Trans. Inf. Theory, 2001, **47**(1): 386-393.

[27] J. L. Kim, New self-dual codes over $GF(4)$ with the highest known minimum weights, IEEE Trans. Inf. Theory, 2001, **47**(4): 1575-1580.

[28] J. L. Kim, Y. Lee, Euclidean and Hermitian self-dual MDS codes over large finite fields, J. Comb. Theory, Ser. A, 2004, **105**(1): 79-95.

[29] M. E. Koroglu, M. Sari, On MDS negacyclic LCD codes, Filomat, 2019, **33**(1): 1-12.

[30] C. Lai, A. Ashikhmin, Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators, IEEE Trans. Inf. Theory, 2018, **64**(1): 622-639.

[31] L. Lu, R. Li, L. Guo, Q. Fu, Maximal entanglement entanglement-assisted quantum codes constructed from linear codes. Quantum Inf. Process., 2015, **14**(1): 165-182.

[32] L. Lu, X. Zhan, S. Yang, H. Cao, Optimal quaternary Hermitian LCD codes, 2020, https://arxiv.org/pdf/2010.10166.pdf.

[33] J. Massey, Linear codes with complementary duals, Discrete Math., 1992, **106-107**: 337-342.

[34] N. Sendrier, Linear codes with complementary duals meet the Gilbert-Varshamov bound, Discrete Math., 2004, **285**(1): 345-347.

[35] M. Shi, S. Li, J. Kim, P. Solé, LCD and ACD codes over a noncommutative non-unital ring with four elements, Cryptogr. Commun., 2022, **14**(3): 627-640.

[36] M. Shi, F. Özbudak, L. Xu, P. Solé. LCD codes from tridiagonal Toeplitz matrices, Finite Fields Appl., 2021, **75**: 101892.

[37] L. Sok, On Hermitian LCD codes and their Gray image, Finite Fields Appl., 2020, **62**(2), 101623.

[38] L. Sok, M. Shi, P. Solé, Construction of optimal LCD codes over large finite fields, Finite Fields Appl., 2018, **50**: 138-153.