Construction of quaternary Hermitian LCD codes

Keita Ishizuka

Received: 8 July 2022 / Accepted: 14 October 2022 / Published online: 22 October 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
We introduce a general construction of many Hermitian LCD $[n, k]$ codes from a given Hermitian LCD $[n, k]$ code. Furthermore, we present some results on punctured codes and shortened codes of quaternary Hermitian LCD codes. As an application, we improve some of the previously known lower bounds on the largest minimum weights of quaternary Hermitian LCD codes of length $26 \leq n \leq 30$.

Keywords Hermitian LCD code · Hermitian hull · Optimal Hermitian LCD code · Hermitian self-dual code

Mathematics Subject Classification (2010) 94B05

1 Introduction

Linear complementary dual codes, LCD codes for short, are codes that intersect their dual codes trivially. Massey [20] introduced Euclidean LCD codes and showed that Euclidean LCD codes provide an optimum linear coding solution for the two-user binary adder channel. Since then, much work has been done concerning both Euclidean LCD codes and Hermitian LCD codes. Carlet and Guilley [4] applied binary Euclidean LCD codes in side-channel attacks and fault non-invasive attacks. Lu, Li, Guo and Fu [17] proved that a quaternary Hermitian LCD code leads to a construction of a maximal-entanglement-assisted quantum error correcting code. In particular, Carlet, Mesnager, Tang, Qi and Pellikaan [6] 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 motivates us to study the largest minimum weights of quaternary Hermitian LCD codes. We say that a quaternary Hermitian LCD $[n, k]$ code is optimal if it has the largest minimum weight among all quaternary Hermitian LCD $[n, k]$ codes.

We discuss the recent research progress on the largest minimum weights of quaternary Hermitian LCD codes as follows. Let $d(n, k)$ denote the largest minimum weight of quaternary Hermitian LCD $[n, k]$ codes. For $n \in \{1, 2, \ldots, 11\}$ and an arbitrary value of $k,
Lu, Zhan, Yang and Cao [18] determined \( d(n, k) \). For an arbitrary value of \( n \) and \( k = 2, 3 \), Lu, Li, Guo and Fu [17] determined \( d(n, k) \). Ishizuka [14] classified optimal quaternary Hermitian LCD codes with dimension 2. For an arbitrary value of \( n \) and \( k = 3 \), the value of \( d(n, k) \) were determined by Lu, Li, Guo and Fu [17] and Araya, Harada and Saito [2]. Furthermore, Araya and Harada [1] classified optimal quaternary Hermitian LCD codes with dimension 3. Zhan, Li, Lu and Li [22] constructed quaternary Hermitian LCD codes with minimum weight \( d = 3, 4, 5, 6 \) of length \( n < 52 \). Sok [21] used unitary matrices to construct many quaternary Hermitian LCD codes. In [2], they also give the nonexistence of Hermitian LCD codes with dual distance greater than 2. Ishizuka and Saito [16] improved this result by proving that there exist no quaternary Hermitian LCD codes with dual distance greater than 2. Ishizuka and Saito [15] used unitary matrices to construct many quaternary Hermitian LCD codes. In this paper, we introduce a method for constructing many \([n, k] \) codes from a given \([n, k] \) code which preserves the dimension of the Hermitian hull, extending the result by Ishizuka and Saito [15]. Although we apply the method only to quaternary Hermitian LCD codes, it can be applied to both Hermitian self-dual codes and Hermitian LCD codes over \( \mathbb{F}_{q^2} \) with any prime power \( q \). Furthermore, we provide some theorems concerning punctured codes and shortened codes of quaternary Hermitian LCD codes, motivated by the result of Bouyuklieva [3] on binary Euclidean LCD codes. As an application, we study quaternary Hermitian LCD codes of length \( 26 \leq n \leq 30 \) and construct many Hermitian LCD \([n, k] \) codes, including the following optimal codes:

\[
(n, k, d) = (26, 5, 16), (26, 18, 6), (26, 21, 4), (27, 5, 17), (27, 22, 4), (28, 6, 17), (28, 23, 4), (29, 24, 4), (30, 24, 4), (30, 25, 4).
\]

Furthermore, we improve the previously known lower bounds on \( d(n, k) \) for \((n, k) = (28, 14), (30, 15)\).

This paper is organized as follows: In Section 2, we give some definitions, notations and basic results. In Section 3, we introduce the construction method. In Section 4, we give some theorems on punctured codes and shortened codes of quaternary Hermitian LCD codes. In Section 5, applying the results, we construct quaternary Hermitian LCD codes to improve some of the previously known lower bounds.

2 Preliminaries

Let \( \mathbb{F}_q \) be the finite field of order \( q \), where \( q \) is a prime power and let \( \mathbb{F}_q^n \) be the vector space of all \( n \)-tuples over \( \mathbb{F}_q \). Especially, let \( \mathbb{F}_4 = \{0, 1, \omega, \omega^2\} \) be the finite field of order four, where \( \omega \) satisfies \( \omega^2 + \omega + 1 = 0 \). An \([n, k] \) code over \( \mathbb{F}_q \) is a \( k \)-dimensional subspace of \( \mathbb{F}_q^n \). Codes over \( \mathbb{F}_4 \) are said to be quaternary codes. For an \([n, k] \) code \( C \) over \( \mathbb{F}_q \), the parameters \( n \) and \( k \) are said to be the length and the dimension of \( C \), respectively. The elements of a code are known as codewords. The weight of \( x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n \) is defined as \( \text{wt}(x) = |\{i \mid x_i \neq 0\}| \). The minimum weight of a code \( C \) is defined as \( \text{wt}(C) = \min\{\text{wt}(x) \mid x \in C, x \neq \mathbf{0}_n\} \), where \( \mathbf{0}_n \) denotes the zero vector of length \( n \). An \([n, k, d] \) code over \( \mathbb{F}_q \) is an \([n, k] \) code with minimum weight \( d \). We say that a code is even if every codeword has even weight. If a code is not even, then it is said to be odd.

Let \( C \) be a code over \( \mathbb{F}_q \) with length \( n \) and let \( T \subseteq \{1, 2, \ldots, n\} \). Deleting every coordinate \( i \in T \) in every codeword of \( C \) gives a code called the punctured code on \( T \) and denoted by \( C^T \). Define a subcode \( C(T) = \{(c_1, c_2, \ldots, c_n) \in C \mid c_i = 0 \text{ for all } i \in T\} \). Puncturing
C(T) on T gives a code called the shortened code on T and denoted by C_T. If |T| = 1, say T = {i}, then we will write C^{[i]} and C_{-i} as C' and C', respectively.

For a ∈ F_q^n, the conjugate of a is defined as a = a^T. The Hermitian inner product of x = (x_1, x_2, …, x_n), y = (y_1, y_2, …, y_n) ∈ F_q^n is defined as (x, y)_h = ∑_{i=1}^n x_i y_i^q. For any [n, k] code over F_q^n, the Hermitian dual code of C is defined as C^{Lh} = {x ∈ F_q^n | (x, y)_h = 0 for all y ∈ C}. Given a code C, we denote by d^Lh the minimum weight of C^{Lh}. A code C over F_q^n is said to be a Hermitian LCD code if C ∩ C^{Lh} = {0_n}. We say that a Hermitian LCD [n, k] code over F_q^n is optimal if it has the largest minimum weight among all Hermitian LCD [n, k] codes over F_q^n. A code C over F_q^n is said to be a Hermitian self-orthogonal code if C ⊆ C^{Lh}. If C satisfies C = C^{Lh}, then we say that C is a Hermitian self-dual code. The Hermitian hull of a code C is defined as Hull_h(C) = C ∩ C^{Lh}. By definition, Hermitian self-dual codes and Hermitian LCD codes are maximum and minimum with respect to the dimensions of the Hermitian hulls, respectively. The construction method introduced in this paper preserves the dimension of the Hermitian hull. Thus, it can be applied to constructions of Hermitian self-dual codes and Hermitian LCD codes over F_q^2 for any prime power q. In this paper, however, we apply the method only to quaternary Hermitian LCD codes.

A generator matrix of a code C is any matrix whose rows form a basis of C. For a matrix A, we denote by A^T and A^adj the transpose and the conjugate of A, respectively. The following results will be important in Sections 3 and 4.

Lemma 2.1 ([7, Proposition 3.5]) Let C be an [n, k] code over F_q^n with generator matrix G. Then C is a Hermitian LCD code if and only if the k × k matrix GG^T is nonsingular.

Lemma 2.2 ([19, Theorem 1]) A quaternary code is Hermitian self-orthogonal if and only if the code is an even code.

Lemma 2.3 ([9, Proposition 3.3]) Let C be an [n, k] code over F_q^n with generator matrix G. Then

\[ \text{rank}(GG^T) = k - \dim(\text{Hull}_h(C)). \]

3 Construction method

Recently, Harada [11] introduced a method to construct many Euclidean LCD [n, k] codes from a given Euclidean LCD [n, k] code, modifying a known method for Euclidean self-dual codes [10]. Extending the result, Ishizuka and Saito [15] provided a method to construct many [n, k] code from a given [n, k] code, preserving the dimension of the Euclidean hull. In this section, we give a construction method similar to that of [15], which preserves the dimension of the Hermitian hull.

Let C be an [n, k] code over F_q^n with generator matrix \((I_k, A)\), where \(I_k\) denotes the identity matrix of order k and A is a k × (n − k) matrix. We denote by \(r_i\) the i-th row of A. For A and \(x, y \in F_q^{n-k}\), define a k × (n − k) matrix \(A(x, y)\), where the i-th row \(r'_i\) is defined as follows:

\[ r'_i = r_i + (r_i, y)_h x - (r_i, x)_h y. \]

We denote by \(C(A(x, y))\) the code with generator matrix \((I_k, A(x, y))\).
Remark 3.1  With the above notation, suppose that \( x = 0_{n-k} \) or \( y = 0_{n-k} \). Then it holds that \( A(x, y) = A \). Hereafter, we assume that \( x \neq 0_{n-k} \) and \( y \neq 0_{n-k} \).

Theorem 3.2  Let \( C \) be an \([n, k]\) code over \( \mathbb{F}_{q^2} \) with generator matrix \( G = (I_k \ A) \) and let \( x, y \in \mathbb{F}_{q^{n-k}}^{*} \). Suppose that \((x, x)_h = (y, y)_h = (x, y)_h = 0\). Then \( \dim(\text{Hull}_h(C(A(x, y)))) = \dim(\text{Hull}_h(C)) \).

Proof  We denote by \( r_i \) and \( r'_i \) the \( i \)-th rows of \( A \) and \( A(x, y) \), respectively. It holds that
\[
(r'_i, r'_j)_h = (r_i + (r_i, y)_h x - (r_i, x)_h y, r_j + (r_j, y)_h x - (r_j, x)_h y)_h
\]
\[
= (r_i, r_j)_h + (r_i, y)_h (r_j, x)_h - (r_i, x)_h (r_j, y)_h
\]
\[
+ (r_i, y)_h (x, r_j)_h - (r_i, x)_h (y, r_j)_h
\]
\[
= (r_i, r_j)_h.
\]

Therefore, it follows that
\[
\left( I_k \ A(x, y) \right) \left( I_k \ A(x, y) \right)^T = I_k + A(x, y)A(x, y)^T
\]
\[
= I_k + AA^T
\]
\[
= \left( I_k \ A \right) \left( I_k \ A \right)^T.
\]

By Theorem 2.3, the result follows.

Theorem 3.2 states that the construction method preserves the dimension of the Hermitian hull. Recall that Hermitian self-dual codes and Hermitian LCD codes are maximum and minimum with respect to the dimensions of the Hermitian hulls, respectively. Therefore, we obtain Corollaries 3.3 and 3.4.

Corollary 3.3  Let \( C \) be an \([n, k]\) code over \( \mathbb{F}_{q^2} \) with generator matrix \( G = (I_k \ A) \) and let \( x, y \in \mathbb{F}_{q^{n-k}}^{*} \). Suppose that \((x, x)_h = (y, y)_h = (x, y)_h = 0\). Then \( C(A(x, y)) \) is a Hermitian LCD code if and only if \( C \) is a Hermitian LCD code.

Corollary 3.4  Let \( C \) be an \([n, k]\) code over \( \mathbb{F}_{q^2} \) with generator matrix \( G = (I_k \ A) \) and let \( x, y \in \mathbb{F}_{q^{n-k}}^{*} \). Suppose that \((x, x)_h = (y, y)_h = (x, y)_h = 0\). Then \( C(A(x, y)) \) is a Hermitian self-dual code if and only if \( C \) is a Hermitian self-dual code.

Remark 3.5  It was shown in [15] that analogous results to Theorem 3.2, Corollaries 3.3 and 3.4 hold for the Euclidean hull dimension.

4 Punctured codes and shortened codes of quaternary Hermitian LCD codes

Recently, Bouyuklieva [3] gave a characterization of both punctured codes and shortened codes of binary LCD codes. In this section, we show that similar results hold for quaternary Hermitian LCD codes.
For a code $C$ of length $n$ and a set $T \subseteq \{1, 2, \ldots, n\}$, define a subcode $C(T) = \{(c_1, c_2, \ldots, c_n) \in C | c_i = 0 \text{ for all } i \in T\}$. For Euclidean dual codes, a result similar to Lemma 4.1 is given in [13, Theorem 1.5.7]. By an argument similar to that in the proof of [13, Theorem 1.5.7], we obtain Lemma 4.1.

**Lemma 4.1** Let $C$ be a code of length $n$ over $\mathbb{F}_q$ and $T \subseteq \{1, 2, \ldots, n\}$. Then $(C^\perp)_T = (C^T)^\perp$ and $(C^\perp)_T^n = (C^T)^\perp^n$.

**Proof** Let $c \in C^\perp(T)$ and let $c^{\ast}$ be the codeword obtained from $c$ by removing the coordinates in $T$. If $x \in C$, then $0 = (x, c)_h = (x^\ast, c^\ast)_h$, where $x^\ast$ is the codeword $x$ punctured on $T$. Hence $(C^\perp(T))_h \subset (C^T)^\perp_h$. Any vector $c \in (C^T)^\perp$ can be extended to a vector $\hat{c}$ by inserting 0s in the positions of $T$. If $x \in C$, then puncture $x$ on $T$ to obtain $x^\ast$. Since $(\hat{c}, x)_h = (c, x^\ast)_h = 0$, it follows that $c \in (C^\perp)_T$. Hence $(C^\perp)_T = (C^T)^\perp$. Replacing $C$ by $C^\perp$ gives $(C^\perp)_T^n = (C^T)^\perp^n$.

**Theorem 4.2** Let $C$ be a quaternary Hermitian LCD $[n, k, d]$ code with $d, d^\perp \geq 2$. For all $1 \leq i \leq n$, exactly one of $C_i$ and $C_1$ is a Hermitian LCD code.

**Proof** Without loss of generality, we may assume that $i = 1$. Since $C$ is a Hermitian LCD code, any vector in $\mathbb{F}_4^n$ can be written uniquely as the sum of a vector in $C$ and a vector in $C^\perp$. Especially, one of the following holds:

(i) $(1, 0, \ldots, 0) = (\omega, v) + (\omega^2, v)$, where $(\omega, v) \in C$ or $(\omega, v) \in C^\perp$.

(ii) $(1, 0, \ldots, 0) = (0, v) + (1, v)$, where $(0, v) \in C$ or $(0, v) \in C^\perp$.

Suppose that $(1, 0, \ldots, 0) = (\omega, v) + (\omega^2, v)$. If $(\omega, v) \in C$, then $(\omega^2, v) \in C^\perp$. Hence $((\omega, v), (\omega^2, v))_h = 0$. However, this is impossible because $((\omega, v), (\omega^2, v))_h = \omega^2 + (v, v)_h \neq 0$. By the same argument, it is verified that $(\omega, v) \in C^\perp$ is not possible. Therefore, we only consider (ii).

First, consider the case where $(0, v) \in C$. It follows that $v \in C_1$ and $v \in (C^\perp)_1$. By Lemma 4.1, $v \in C_1 \cap (C^\perp)_1$. Therefore, $C_1$ is not a Hermitian LCD code. Note that $v$ is a nonzero vector since $d, d^\perp \geq 2$. Suppose that $C^\perp$ is not a Hermitian LCD code either. Then there exists a nonzero vector $u \in C_1 \cap (C^\perp)_1$. From $u \in (C^\perp)_1 = (C^\perp)_1$, it follows that $(0, u) \in C^\perp$. From $u \in C_1$, one of the following holds: $(0, u), (1, u), (\omega, u), (\omega^2, u) \in C$.

(i) Let $(0, u) \in C$. Then it holds that $(0, u) \in C \cap C^\perp$. This is a contradiction as $C$ is a Hermitian LCD code.

(ii) Let $(1, u) \in C$. It holds that $(1, 0) = (0, v) + (1, v) = (0, u) + (1, u)$. Note that $v \neq u$ since $(0, v), (1, u) \in C$ and $d \geq 2$. This is a contradiction as $C$ is a Hermitian LCD code.

(iii) Let $(\omega, u) \in C$. Then it follows that $(1, \omega^2 u) \in C$. Therefore, $(1, 0) = (0, v) + (1, v) = (0, \omega^2 u) + (1, \omega^2 u)$. Note that $v \neq \omega^2 u$ since $(0, v), (\omega, u) \in C$ and $d \geq 2$. This is a contradiction as $C$ is a Hermitian LCD code.

(iv) Then it follows that $(1, \omega u) \in C$. Therefore, $(1, 0) = (0, v) + (1, v) = (0, \omega u) + (1, \omega u)$. Note that $v \neq \omega u$ since $(0, v), (\omega^2, u) \in C$ and $d \geq 2$. This is a contradiction as $C$ is a Hermitian LCD code.
Therefore, it holds that $C^1$ is a Hermitian LCD code.

Consider the case where $(1, v) \in C$. It follows that $v \in C^1$ and $v \in (C^1_h)_1$. By the same argument as above, it holds that $C^1$ is not a Hermitian LCD code and $C_1$ is a Hermitian LCD code.

**Remark 4.3** Theorem 4.2 generalizes [3, Lemma 2].

Lemma 4.4 is obtained by Ken Saito (private communication, Dec. 31, 2021). In [5], a similar result was given for binary Euclidean LCD codes.

**Lemma 4.4** (Ken Saito) Let $C$ be a quaternary Hermitian LCD $[n, k]$ code. Then there exists a generator matrix $G$ of $C$ such that $GG^T = I_k$.

**Proof** Suppose that $C$ is an even code. Then, by Lemma 2.2, $C$ is a Hermitian self-dual code. This is a contradiction as $C$ is a Hermitian LCD code. Thus, we assume that $C$ is an odd code. Then there exists a codeword which has an odd weight. From the proof of [12, Proposition 4], $C$ has a generator matrix of the form $G_0 = \begin{pmatrix} x_1 \\ G_1 \end{pmatrix}$, satisfying that $(x_1, x_1)_h \neq 0$ and $x_1G_1^T = 0_{k-1}$. The code $C_1$ with generator matrix $G_1$ is a Hermitian LCD $[n, k-1]$ code. After finitely many steps, we obtain a generator matrix $G$ of $C$:

$$G = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix},$$

where $(x_i, x_j)_h = \delta_{ij}$ for all $1 \leq i, j \leq n$. Here $\delta_{ij}$ is the Kronecker delta function. Hence $GG^T = I_k$. This completes the proof.

**Theorem 4.5** Let $C$ be a quaternary Hermitian LCD $[n, k]$ code and let $G$ be a generator matrix of $C$ such that $GG^T = I_k$. Let $l_i$ denote the $i$-th column of $G$. Then $C^i$ is a Hermitian LCD code if and only if $\text{wt}(l_i)$ is even.

**Proof** Without loss of generality, we may assume that

$$l_i = (0, \ldots, 0, 1, \ldots, 1, \omega, \ldots, \omega, \omega^2, \ldots, \omega^2)^T.$$

Let $p$, $q$ and $r$ be the numbers of coordinates whose entries equal to $1, \omega$ and $\omega^2$, respectively. Let $G'$ be a generator matrix of $C^i$ obtained by deleting $i$-th column of $G$. Since $GG^T = I_k$, it holds that

$$G'G^T = \begin{pmatrix} I_{n-p-q-r} & O & O & O \\ O & J-I_p & \omega^2J & \omega J \\ O & \omega J & J-I_q & \omega^2 J \\ O & \omega^2 J & \omega J & J-I_r \end{pmatrix},$$

where $J$ and $O$ denote the all-ones matrices and the zero matrix of suitable sizes, respectively. Let $M$ be
Then $M$ is a submatrix of $G^\top G$ and $\det G^\top G = \det M$.

(i) Suppose $p \equiv q \equiv r \equiv 0 \pmod{2}$. The value of $\det M$ is calculated as follows: Let $M_1$ denote the matrix whose rows consist of the $i$-th rows of $M$ for $1 \leq i \leq p$. First, add the $i$-th rows of $M_1$ to the first row for $i = 2, \ldots, p$. Adding the first row to $i$-th rows for $i = 2, \ldots, p$, we obtain

$$
A = \begin{pmatrix}
1 & 1 & \ldots & 1 \\
0 & 1 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & 1
\end{pmatrix},
$$

$$
B = \begin{pmatrix}
0 & \ldots & 0 \\
\omega^2 & \ldots & \omega^2 \\
\vdots & \vdots & \vdots \\
\omega^2 & \ldots & \omega^2
\end{pmatrix},
$$

$$
C = \begin{pmatrix}
0 & \ldots & 0 \\
\omega & \ldots & \omega \\
\vdots & \vdots & \vdots \\
\omega & \ldots & \omega
\end{pmatrix}.
$$

By the same row operations, we obtain

$$
\det M = \det \begin{pmatrix}
A & B & C \\
C & A & B \\
B & C & A
\end{pmatrix}.
$$

Add the first row of $\det M$ multiplied by $\omega$ and $\omega^2$ to $i$-th rows for $i = p + 2, \ldots, p + q$ and $p + q + 2, \ldots, p + q + r$, respectively. Then add the $(p + 1)$-st row multiplied by $\omega^2$ and $\omega$ to $i$-th rows for $i = 2, \ldots, p$ and $p + q + 2, \ldots, p + q + r$. Finally, adding the $(p + q + 1)$-st row multiplied by $\omega$ and $\omega^2$ to $i$-th rows for $i = 2, \ldots, p$ and $p + 2, \ldots, p + q$, respectively, we obtain

$$
\det M = \det \begin{pmatrix}
A & O & O \\
O & A & O \\
O & O & A
\end{pmatrix}.
$$

Therefore, it follows that $\det M = 1$.

(ii) Suppose that $p \equiv q \equiv r \equiv 1 \pmod{2}$. The value of $\det M$ is calculated as follows: By the same row operations as in (i), we obtain

$$
\det M = \det \begin{pmatrix}
J - A & \omega^2 J - B & \omega J - C \\
\omega J - C & J - A & \omega^2 J - B \\
\omega^2 J - B & \omega J - C & J - A
\end{pmatrix}.
$$
Add the first row of $\det M$ to the $(p + q + 1)$-st row. Then add the $(p + 1)$-st row of $\det M$ to the first row. Multiplying the first row by $\omega$, we verify that the first row and $(p + q + 1)$-st row is identical. Therefore, it follows that $\det M = 0$.

(iii) Suppose that $p \equiv 0 \pmod{2}$, $q \equiv r \equiv 1 \pmod{2}$. The value of $\det M$ is calculated as follows: By the same row operations as in (i), we obtain

$$\det M = \det \begin{pmatrix} A & B & C \\ \omega J - C & J - A & \omega^2 J - B \\ \omega^2 J - B & \omega J - C & J - A \end{pmatrix}.$$  

Add the first row of $\det M$ multiplied by $\omega$ to the $(p + 1)$-st row. Furthermore, add the first row multiplied by $\omega^2$ to the $(p + q + 1)$-st row. Transposing the $(p + 1)$-st row with the $(p + q + 1)$-st row, we obtain

$$\det M = \det \begin{pmatrix} A & B & C \\ O & D & O \\ O & O & E \end{pmatrix},$$

where

$$D = \begin{pmatrix} \omega & \omega & \cdots & \omega \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

$$E = \begin{pmatrix} \omega^2 & \omega^2 & \cdots & \omega^2 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Therefore, it follows that $\det M = 1$. By the same argument, it holds that if only one of $p$, $q$, $r$ is even, then $\det M = 1$.

(iv) Suppose that $p \equiv 1 \pmod{2}$, $q \equiv r \equiv 0 \pmod{2}$. The value of $\det M$ is calculated as follows: By the same row operations as in (i), we obtain

$$\det M = \det \begin{pmatrix} J - A & \omega^2 J - B & \omega J - C \\ C & A & B \\ B & C & A \end{pmatrix}.$$  

Add the $(p + 1)$-st row of $\det M$ multiplied by $\omega^2$ to the first row. Furthermore, add the $(p + q + 1)$-st row multiplied by $\omega$ to the first row. Consequently, the first row equals to the zero vector. Therefore, it follows that $\det M = 0$. By the same argument, it holds that if only one of $p$, $q$, $r$ is odd, then $\det M = 0$.

Therefore, it holds that $\det M = 1$ if and only if $\text{wt}(c_i) = p + q + r \equiv 0 \pmod{2}$. This completes the proof.

**Corollary 4.6** Let $C$ be a quaternary Hermitian LCD $[n, k]$ code and let $G$ be a generator matrix of $C$ such that $GG^\top = I_k$. Let $l_i$ denote the $i$-st column of $G$. Then $C_i$ is a Hermitian LCD code if and only if $\text{wt}(l_i)$ is odd.

**Proof** By Theorems 4.2 and 4.5, the result follows.
5 Optimal quaternary Hermitian LCD codes

Let \(d(n, k)\) denote the largest minimum weight of quaternary Hermitian LCD \([n, k]\) codes. As stated in Section 1, we consider \(d(n, k)\) for \(26 \leq n \leq 30\) and \(4 \leq k \leq n - 4\). In this section, we improve some of the previously known lower bounds on \(d(n, k)\) for \(26 \leq n \leq 30\) and \(4 \leq k \leq n - 4\), using the results of Sections 3 and 4. The punctured codes and shortened codes in this section were constructed by the Magma functions ShortenCode and PunctureCode, respectively.

In order to improve lower bounds, we use the following method: Let \(d_k(n, k)\) denote the largest minimum weight among currently known \([n, k]\) codes. By the Magma function BestKnownLinearCode, one can construct an \([n, k, d_k(n, k)]\) code for all \(26 \leq n \leq 30\) and \(4 \leq k \leq n - 4\). In addition, considering shortened codes and punctured codes of \([n, k, d_k(n, k)]\) codes, we found quaternary Hermitian LCD \([n, k, d_k(n, k)]\) codes for

\[(n, k, d_k(n, k)) = (26, 5, 16), (26, 18, 6), (26, 21, 4), (27, 5, 17), (27, 22, 4),
(28, 6, 17), (28, 23, 4), (29, 24, 4), (30, 24, 4), (30, 25, 4). \tag{1} \]

In order to reduce the above computation, we used the following method: Suppose that the punctured (resp. shortened) code of a quaternary Hermitian LCD code \(C\) with respect to a coordinate, say \(i\), is not a quaternary Hermitian LCD code. Then, by Theorem 4.2, the shortened (resp. punctured) code of \(C\) with respect to the coordinate \(i\) is a quaternary Hermitian LCD code. Thus, if an \([n, k, d_k(n, k)]\) code is a quaternary Hermitian LCD code, then we only need to check, for each coordinate, whether the punctured code of \(C\) is a quaternary Hermitian LCD code or not. Consequently, we obtain Proposition 5.1.

**Proposition 5.1** There exists an optimal quaternary Hermitian LCD \([n, k, d]\) code for \((n, k, d)\) listed in (1).

By a method similar to that given in the above, we found quaternary Hermitian LCD \([n, k, d_k(n, k) - 1]\) codes and quaternary Hermitian LCD \([n, k, d_k(n, k) - 2]\) codes for

\[(n, k, d_k(n, k) - 1) = (26, 4, 17), (26, 17, 6), (26, 19, 5), (26, 20, 4), (27, 18, 6),
(27, 19, 5), (27, 20, 5), (27, 21, 4), (28, 5, 17), (28, 17, 7),
(28, 19, 6), (28, 20, 5), (28, 21, 5), (28, 22, 4), (29, 5, 18),
(29, 6, 17), (29, 18, 7), (29, 20, 6), (29, 21, 5), (29, 22, 5),
(29, 23, 4), (30, 5, 19), (30, 16, 9), (30, 19, 7), (30, 21, 6),
(30, 22, 5), (30, 23, 5).
\tag{2} \]
\[(n, k, d_k(n, k) - 2) = (26, 6, 14), (26, 7, 13), (26, 8, 12), (26, 12, 9),
(26, 14, 7), (26, 15, 7), (26, 16, 6), (27, 4, 17), (27, 7, 14),
(27, 10, 11), (27, 13, 9), (27, 14, 8), (27, 15, 7), (27, 16, 7),
(27, 17, 6), (28, 7, 14), (28, 8, 14), (28, 10, 12), (28, 14, 9),
(28, 15, 8), (28, 16, 7), (28, 18, 6), (29, 4, 18), (29. 7, 15),
(29, 8, 14), (29, 9, 14), (29, 10, 13), (29, 15, 9), (29, 16, 8),
(29, 17, 7), (29, 19, 6), (30, 4, 19), (30, 6, 17), (30, 8, 15),
(30, 9, 14), (30, 10, 14), (30, 17, 8), (30, 18, 7), (30, 20, 6).
\]

Consequently, we obtain Proposition 5.2.

**Proposition 5.2** There exists a quaternary Hermitian LCD \([n, k, d]\) code for \((n, k, d)\) listed in (2) and (3).

Furthermore, applying Corollary 3.3 to quaternary Hermitian LCD \([n, k, d]\) codes for \((n, k, d)\) listed in Table 1, we found quaternary Hermitian LCD \([n, k, d]\) codes for
\[(n, k, d) = (27, 6, 15), (27, 8, 13), (27, 9, 12), (27, 11, 10), (28, 11, 11),
(29, 11, 11), (30, 7, 16), (30, 12, 11).
\]

Therefore, we obtain Proposition 5.3.

**Proposition 5.3** There exists a quaternary LCD \([n, k, d]\) code for \((n, k, d)\) listed in (4).

The vectors \(x, y\) in Corollary 3.3 are listed in Table 1. For each of the parameters given in (1) through (4), a quaternary Hermitian LCD code can be obtained electronically from [https://www.math.is.tohoku.ac.jp/~mharada/Ishizuka/F4_HLCD_genmat.txt](https://www.math.is.tohoku.ac.jp/~mharada/Ishizuka/F4_HLCD_genmat.txt). Note that, the generator matrix used to construct a quaternary Hermitian LCD code in Proposition 5.3 can be obtained from \(x, y\) in Table 1 and the generator matrix given in [https://www.math.is.tohoku.ac.jp/~mharada/Ishizuka/F4_HLCD_genmat.txt](https://www.math.is.tohoku.ac.jp/~mharada/Ishizuka/F4_HLCD_genmat.txt).

For a quaternary Hermitian LCD \([n, k]\) codes with \(26 \leq n \leq 30\) and \(4 \leq k \leq n - 4\), we used the following to obtain upper bounds:

| \((n, k, d)\) | \(x\) | \(y\) |
|---------------|--------|--------|
| (27, 6, 14)   | \(a_0a_1^2a_211a_001a_20000a_20a_00a_0a_2^2a_2\) | \(a_0a_10a_20a_0000000a_20a_00a_0a_20a_2\) |
| (27, 8, 12)   | \(a_20a_011a_20a_20a_0a_2a_0a_2a_0a_20a_0a_20a_0a_210\) | \(a_20a_21a_0a_2a_0a_2a_011a_01001a_000a_20\) |
| (27, 9, 11)   | \(110a_01000a_20a_00a_20a_01a_2a_0\) | \(00a_00a_20a_00a_20a_011a_01001a_000\) |
| (27, 11, 9)   | \(a_20a_2110a_000a_20a_000a_0a_011a_0^2a_2\) | \(000011a_01010a_01010a_20\) |
| (28, 11, 10)  | \(a_00a_10a_20a_00a_01a_0100011a_2a_0\) | \(00a_00a_21001a_0a_010000a_20\) |
| (29, 11, 10)  | \(00a_0010a_0a_00a_20a_01000a_20a_2a_00a_00a_00\) | \(a_00a_20a_20a_00a_20a_01000a_000a_20\) |
| (30, 7, 15)   | \(a_02a_110a_02a_20a_01000a_20a_0a_000a_0a_00\) | \(1a_01001a_0110100a_00a_20a_2a_00\) |
| (30, 12, 10)  | \(1001a_00a_20a_20a_2a_01a_0001\) | \(1a_00a_20a_0a_00a_20a_0a_20a_001a_2a_00\) |
where $D(n, k)$ denotes the largest minimum weight among all $[n, k]$ codes. The values of $D(n, k)$ are given in [8].

In Tables 2 and 3, we give $d(n, k)$ for $4 \leq k \leq 12$. For the parameters listed in Proposition 5.3, we mark $d(n, k)$ by * in Tables 2 and 3. Furthermore, for the parameters listed in Propositions 5.1 through 5.3, we give $d(n, k)$ in boldface. We improve the previously known lower bounds on $d(n, k)$ for $(n, k) = (28, 14), (30, 15)$. In Tables 2 and 3, we give the previously known lower bounds in parentheses.

### 6 Conclusion

In this paper, we proposed a method to construct many $[n, k]$ codes from a given $[n, k]$ code, preserving the Hermitian hull dimension. Furthermore, we studied punctured codes and shortened codes of quaternary Hermitian LCD codes. As an application, we constructed $[n, k]$ quaternary Hermitian LCD codes.

Although we applied the method to construct a quaternary Hermitian LCD codes, the construction method can be applied to Hermitian self-dual codes over any finite field, as stated in Theorem 3.4. For the Euclidean hull dimension, an analogous result was given in [15] and used to construct self-dual codes. On the other hand, we have proved Theorem 4.2 only for quaternary Hermitian LCD codes. It is an interesting question whether Theorem 4.2 holds for Hermitian LCD codes over any finite field.

**Acknowledgements** The author would like to thank supervisor Professor Masaaki Harada for his helpful advice and encouragement. The author also would like to thank Ken Saito for his kind permission to publish his result in Lemma 4.4. The author would also like to thank the anonymous referees for their helpful comments and suggestions.
Author contributions The author confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation.

Funding There has been no significant financial support for this work.

Data availability The data that support the findings of this study are openly available at https://www.math.is.tohoku.ac.jp/~mharada/Ishizuka/F4_HLCD_genmat.txt.

Declarations

Ethical approval and Consent to participate We confirm that the manuscript has been read and approved by all named authors and that there are no other persons who satisfied the criteria for authorship but are not listed.

Consent for publication All authors reviewed the manuscript draft and revised it critically on intellectual content. All authors approved the final version of the manuscript to be published.

Conflicts of interest There are no known conflicts of interest associated with this publication.

References

1. Araya, M., Harada, M.: On the classification of quaternary optimal Hermitian LCD codes. Cryptogr. Commun. 14(4), 833–847 (2022) MR 4366621
2. Araya, M., Harada, M., Saito, K.: Quaternary Hermitian linear complementary dual codes. IEEE Trans. Inform. Theory 66(5), 2751–2759 (2020) MR 4089750
3. Bouyuklieva, S.: Optimal binary LCD codes. Des. Codes Cryptogr. 89(11), 2445–2461 (2021) MR 4321779
4. Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. Adv. Math. Commun. 10(1), 131–150 (2016) MR 3471065
5. Carlet, C., Mesnager, S., Tang, C., Qi, Y.: New characterization and parametrization of LCD codes. IEEE Trans. Inform. Theory 65(1), 39–49 (2019) MR 3900976
6. Carlet, C., Mesnager, S., Tang, C., Qi, Y., Pellikaan, R.: Linear codes over \( F_q^2 \) are equivalent to LCD codes for \( q > 3 \). IEEE Trans. Inform. Theory 64(4, part 2), 3010–3017 (2018) MR 3784604
7. Güneri, C., Özkaya, B., Solé, P.: Quasi-cyclic complementary dual codes. Finite Fields Appl. 42, 67–80 (2016) MR 3550383
8. Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. Available online at http://codetables.de/, Accessed on 2022-05-14
9. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. 86(1), 121–136 (2018) MR 3742836
10. Harada, M.: Existence of new extremal doubly-even codes and extremal singly-even codes. Des. Codes Cryptogr. 8(3), 273–283 (1996) MR 1403866
11. Harada, M.: Construction of binary LCD codes, ternary LCD codes and quaternary Hermitian LCD codes. Des. Codes Cryptogr. 89(10), 2295–2312 (2021) MR 4314168
12. Harada, M., Saito, K.: Remark on subcodes of linear complementary dual codes. Inform. Process. Lett. 159(160), 105963, 3 (2020) MR 4088439
13. Huffman, W.C., Pless, V.: Fundamentals of error-correcting codes. Cambridge University Press, Cambridge (2003) MR 1996953
14. Ishizuka, K.: Classification of optimal quaternary Hermitian LCD codes of dimension 2. J. Algebra Comb. Discrete Struct. Appl. 7(3), 229–236 (2020) MR 4221779
15. Ishizuka, K., Saito, K.: Construction for both self-dual codes and LCD codes. Adv. Math. Commun. (2022) (to appear)
16. Ishizuka, K., Saito, K.: On the existence of quaternary Hermitian LCD codes with Hermitian dual distance 1. Discrete Math. 345(2), Paper No. 112702, 3 (2022) MR 4338405
17. Lu, L., Li, R., Guo, L., Fu, Q.: Maximal entanglement entanglement-assisted quantum codes constructed from linear codes. Quantum Inf. Process. 14(1), 165–182 (2015) MR 3296312
18. Lu, L., Zhan, X., Yang, S., Cao, H.: Optimal quaternary Hermitian LCD codes. (2020) arXiv:2010.10166
19. MacWilliams, F.J. Odlyzko, A.M. Sloane, N.J.A. Ward, H.N. Self-dual codes over GF(4). J. Combin. Theory Ser. A 25(3), 288–318 (1978) MR 514624

20. Massey, J.L.: Linear codes with complementary duals. Discrete Math. 106/107, 337–342 (1992) MR 1181930

21. Sok, L.: On Hermitian LCD codes and their Gray image. 62, 101623, 20 (2020) MR 4038250

22. Zhan, X., Li, R., Lu, L., Li, H.: Quaternary Hermitian linear complementary dual codes with small distance. In: 2020 International Conference on Information Science and Education (ICISE-IE). pp. 38–41 (2020)

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.