Binary linear complementary dual codes

Masaaki Harada*and Ken Saito†

Dedicated to Professor Masahiko Miyamoto on His 65th Birthday

Abstract

Linear complementary dual codes (or codes with complementary duals) are codes whose intersections with their dual codes are trivial. We study binary linear complementary dual $[n, k]$ codes with the largest minimum weight among all binary linear complementary dual $[n, k]$ codes. We characterize binary linear complementary dual codes with the largest minimum weight for small dimensions. A complete classification of binary linear complementary dual $[n, k]$ codes with the largest minimum weight is also given for $1 \le k \le n \le 16$.

1 Introduction

An $[n, k]$ *code* C over $\mathbb{F}_q$ is a k-dimensional vector subspace of $\mathbb{F}_q^n$, where $\mathbb{F}_q$ denotes the finite field of order q and q is a prime power. A code over $\mathbb{F}_2$ is called *binary*. The parameters n and k are called the *length* and *dimension* of C, respectively. The *weight* $\mathrm{wt}(x)$ of a vector $x \in \mathbb{F}_q^n$ is the number of non-zero components of x. A vector of C is called a *codeword* of C. The minimum non-zero weight of all codewords in C is called the *minimum weight* $d(C)$ of C and an $[n, k]$ code with minimum weight d is called an $[n, k, d]$ code. Two $[n, k]$ codes C and C' over $\mathbb{F}_q$ are *equivalent*, denoted $C \cong C'$, if there is an $n \times n$ monomial matrix P over $\mathbb{F}_q$ with $C' = C \cdot P = \{xP \mid x \in C\}$.

*Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan. email: `mharada@m.tohoku.ac.jp`.

†Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan. email: `kensaito@ims.is.tohoku.ac.jp`.

The *dual* code $C^\perp$ of a code C of length n is defined as $C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot y = 0 \text{ for all } y \in C\}$, where $x \cdot y$ is the standard inner product. A code C is called *linear complementary dual* (or a linear code with complementary dual) if $C \cap C^\perp = \{\mathbf{0}_n\}$, where $\mathbf{0}_n$ denotes the zero vector of length n. We say that such a code is LCD for short.

LCD codes were introduced by Massey [12] and gave an optimum linear coding solution for the two user binary adder channel. LCD codes are an important class of codes for both theoretical and practical reasons (see [2], [3], [4], [7], [8], [10], [11], [12], [13], [14]). It is a fundamental problem to classify LCD $[n, k]$ codes and determine the largest minimum weight among all LCD $[n, k]$ codes. Recently, much work has been done concerning this fundamental problem (see [3], [4], [7], [8], [11], [13]). In particular, we emphasize the recent work by Carlet, Mesnager, Tang and Qi [4]. It has been shown in [4] that any code over $\mathbb{F}_q$ is equivalent to some LCD code for $q \geq 4$. This motivates us to study binary LCD codes.

Throughout this paper, let $d(n, k)$ denote the largest minimum weight among all binary LCD $[n, k]$ codes. Recently, some bounds on the minimum weights of binary LCD $[n, k]$ codes have been established in [8]. More precisely, $d(n, 2)$ has been determined and the values $d(n, k)$ have been calculated for $1 \leq k \leq n \leq 12$. In this paper, we characterize binary LCD $[n, k, d(n, k)]$ codes for small k. The concept of k-covers of m-sets plays an important role in the study of such codes. Using the characterization, we give a classification of binary LCD $[n, 2, d(n, 2)]$ codes and we determine $d(n, 3)$. In this paper, a complete classification of binary LCD $[n, k]$ codes having the minimum weight $d(n, k)$ is also given for $1 \leq k \leq n \leq 16$.

The paper is organized as follows. In Section 2, definitions, notations and basic results are given. We also give a classification of binary LCD $[n, k, d(n, k)]$ codes for $k = 1, n - 1$. In Section 3, we give some characterization of binary LCD codes using k-covers of m-sets. This characterization is used in Sections 4, 5 and 6. In Section 4, we study binary LCD codes of dimension 2. We give a classification of binary LCD $[n, 2, d(n, 2)]$ codes for $n = 6t$ $(t \geq 1)$, $6t + 1$ $(t \geq 1)$, $6t + 2$ $(t \geq 0)$, $6t + 3$ $(t \geq 1)$, $6t + 4$ $(t \geq 0)$ and $6t + 5$ $(t \geq 1)$ (Theorems 4.5 and 4.8). In Sections 5 and 6, we study binary LCD codes of dimension 3. In Section 5, we show that $d(n, 3) = \left\lfloor \frac{4n}{7} \right\rfloor$ if $n \equiv 3, 5, 10, 12 \pmod{14}$ and $\left\lfloor \frac{4n}{7} \right\rfloor - 1$ otherwise, for $n \geq 3$ (Theorem 5.1). In Section 6, we establish the uniqueness of binary LCD $[n, 3, d(n, 3)]$ codes for $n \equiv 0, 2, 3, 5, 7, 9, 10, 12 \pmod{14}$. In Section 7, we give a complete classification of binary LCD $[n, k]$ codes having the minimum weight $d(n, k)$ for

$2 \leq k \leq n-1 \leq 15$. Finally, in Section 8, we give constructions of LCD codes over $\mathbb{F}_q$ from self-orthogonal codes. As a consequence, the values $d(n,4)$ are determined for $n = 17, 18, 21, 25$.

All computer calculations in this paper were done with the help of MAGMA [1].

2 Preliminaries

2.1 Definitions, notations and basic results

Throughout this paper, $\mathbf{0}_s$ and $\mathbf{1}_s$ denote the zero vector and the all-one vector of length s, respectively. Let I_k denote the identity matrix of order k and let A^T denote the transpose of a matrix A.

Let C be an $[n,k]$ code over $\mathbb{F}_q$. The *weight enumerator* of C is given by $\sum_{i=0}^{n} A_i y^i$, where A_i is the number of codewords of weight i in C. It is trivial that two codes with distinct weight enumerators are inequivalent. The *dual* code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot y = 0 \text{ for all } y \in C\}$, where $x \cdot y$ is the standard inner product. A code C is called *linear complementary dual* (or a linear code with complementary dual) if $C \cap C^\perp = \{\mathbf{0}_n\}$. We say that such a code is LCD for short. A generator matrix of C is a $k \times n$ matrix whose rows are a set of basis vectors of C. A parity-check matrix of C is a generator matrix of $C^\perp$. The following characterization is due to Massey [12].

Proposition 2.1. *Let C be a code over $\mathbb{F}_q$. Let G and H be a generator matrix and a parity-check matrix of C, respectively. Then the following properties are equivalent:*

(i) *C is LCD,*

(ii) *$C^\perp$ is LCD,*

(iii) *GG^T is nonsingular,*

(iv) *HH^T is nonsingular.*

From now on, all codes mean binary unless otherwise specified. Throughout this paper, let $d(n,k)$ denote the largest minimum weight among all LCD $[n,k]$ codes.

Lemma 2.2. *Let G (resp. H) be a generator matrix (resp. a parity-check matrix) of an LCD code.*

(i) *Suppose that some two columns of G are identical. Let G' be the matrix obtained from G by deleting the two columns. Then the code with generator matrix G' is LCD.*

(ii) *Suppose that some two columns of H are identical. Let H' be the matrix obtained from H by deleting the two columns. Then the code with parity-check matrix H' is LCD.*

Proof. Since $GG^T = G'G'^T$ and $HH^T = H'H'^T$, the new codes are also LCD. □

Lemma 2.3. *Suppose that there is an LCD $[n, k, d]$ code C. If $d(n-1, k) \leq d-1$, then $d(C^\perp) \geq 2$.*

Proof. Suppose that $d(C^\perp) = 1$. Then some column of a generator matrix of C is $\mathbf{0}_k$. By deleting the column, an LCD $[n-1, k, d]$ code is constructed. □

Lemma 2.4. *Suppose that there is an LCD $[n, k, d]$ code C with $d(C^\perp) \geq 2$. If $n - k \geq 2^k$, then there is an LCD $[n-2, k]$ code D with $d(D^\perp) \geq 2$.*

Proof. We may assume without loss of generality that C has generator matrix of the form $G = \begin{pmatrix} I_k & M \end{pmatrix}$, where M is a $k \times (n-k)$ matrix. Since $d(C^\perp) \geq 2$, no column of M is $\mathbf{0}_k$. Since $n - k \geq 2^k$, some two columns of M are identical. By Lemma 2.2, D is LCD. □

Let C be an $[n+1, k, d]$ code with $d(C^\perp) = 1$. Then we may assume without loss of generality that

$$C = \{(x_1, x_2, \ldots, x_n, 0) \mid (x_1, x_2, \ldots, x_n) \in C^*\},$$

where C^* is a punctured $[n, k, d]$ code of C.

Lemma 2.5. *C is LCD if and only if C^* is LCD.*

In this way, every LCD $[n+1, k, d]$ code C with $d(C^\perp) = 1$ is constructed from some LCD $[n, k, d]$ code C^*. In addition, two LCD $[n+1, k, d]$ codes C with $d(C^\perp) = 1$ are equivalent if and only if two LCD $[n, k, d]$ codes C^* are equivalent. Hence, all LCD $[n+1, k, d]$ codes C with $d(C^\perp) = 1$, which must be checked to achieve a complete classification, can be obtained from all inequivalent LCD $[n, k, d]$ codes C^*.

2.2 LCD codes of dimensions $1, n-1$

It is trivial that $\mathbb{F}_2^n$ is an LCD $[n, n, 1]$ code. It is known [7] that

$$(d(n,1), d(n,n-1)) = \begin{cases} (n,2) & \text{if } n \text{ is odd,} \\ (n-1,1) & \text{if } n \text{ is even.} \end{cases}$$

Proposition 2.6. *There is a unique LCD $[n, 1, d(n, 1)]$ code, up to equivalence.*

Proof. Let C be an LCD $[n, 1, d(n, 1)]$ code. We may assume without loss of generality that C has generator matrix of the following form:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 & \cdots & 1 & 0 \end{pmatrix},$$

if n is odd and even, respectively. The result follows. ◻

Proposition 2.7. (i) *Suppose that n is odd. Then there is a unique LCD $[n, n-1, 2]$ code, up to equivalence.*

(ii) *Suppose that n is even. Then there are $n/2$ inequivalent LCD $[n, n-1, 1]$ codes.*

Proof. Let C be an LCD $[n, n-1, d(n, n-1)]$ code. We may assume without loss of generality that C has generator matrix of the following form:

$$G((a_1, \dots, a_{n-1})) = \left(\begin{array}{cc} & a_1 \\ I_{n-1} & \vdots \\ & a_{n-1} \end{array} \right),$$

where $a_i \in \mathbb{F}_2$ $(i = 1, 2, \dots, n-1)$. Then

$$H = \begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & 1 \end{pmatrix}$$

is a parity-check matrix of C.

(i) Suppose that n is odd. Since $d(C) = 2$, $a_i = 1$ $(i = 1, 2, \dots, n-1)$. Since n is odd, $HH^T = \begin{pmatrix} 1 \end{pmatrix}$. Hence, there is a unique LCD $[n, n-1, 2]$ code, up to equivalence.

(ii) Suppose that n is even. Since C is LCD, the weight of $(a_1, \dots, a_{n-1})$ is even. Let $C(x)$ denote the code with generator matrix of the form $G(x)$, where $x \in \mathbb{F}_2^{n-1}$ and $\mathrm{wt}(x)$ is even. It is easy to see that $C(x)$ and $C(y)$ are equivalent if and only if $\mathrm{wt}(x) = \mathrm{wt}(y)$. Hence, there are $n/2$ LCD $[n, n-1, 1]$ codes, up to equivalence.

This completes the proof. ◻

3 Constructions of LCD codes from k-covers

In this section, we study LCD codes constructed from k-covers of m-sets. We give a characterization of LCD codes of dimensions 2 and 3 using k-covers.

3.1 LCD codes from k-covers

Let m and k be positive integers. Let X be a set with m elements (for short m-set). A *k-cover* of X is a collection of k not necessarily distinct subsets of X whose union is X [5]. This concept plays an important role in the study of LCD codes for small dimensions.

We define a generator matrix from a k-cover $\{Y_1, Y_2, \ldots, Y_k\}$ of an m-set $X = \{1, 2, \ldots, m\}$ as follow. Since the matrix depends on the ordering chosen for $Y_1, Y_2, \ldots, Y_k$, in this paper, we fix the order. More precisely, we define a k-cover as a sequence $\mathcal{Y} = (Y_1, Y_2, \ldots, Y_k)$. Let $\mathcal{Y} = (Y_1, Y_2, \ldots, Y_k)$ be a k-cover of X. We define the following subsets of $\{1, 2, \ldots, k + \ell m\}$:

$$\begin{aligned}
Z_1 &= \{1\} \cup (k + Y_1) \cup (k + m + Y_1) \cup \cdots \cup (k + (\ell - 1)m + Y_1), \\
Z_2 &= \{2\} \cup (k + Y_2) \cup (k + m + Y_2) \cup \cdots \cup (k + (\ell - 1)m + Y_2), \\
&\vdots \\
Z_k &= \{k\} \cup (k + Y_k) \cup (k + m + Y_k) \cup \cdots \cup (k + (\ell - 1)m + Y_k),
\end{aligned}$$

where ℓ is an even positive integer and $a + Y_i = \{a + y \mid y \in Y_i\}$ for a positive integer a. Let z_i be the characteristic vector of Z_i ($i = 1, 2, \ldots, k$). Then define the $k \times (k + \ell m)$ matrix $G(\mathcal{Y})$ such that z_i is the i-th row. We denote the code with generator matrix of the form $G(\mathcal{Y})$ by $C(\mathcal{Y})$.

Proposition 3.1. *The code $C(\mathcal{Y})$ is an LCD $[\ell m + k, k]$ code with $d(C(\mathcal{Y})^\perp) = 2$.*

Proof. Since ℓ is even, $G(\mathcal{Y})G(\mathcal{Y})^T = I_k$. Thus, $C(\mathcal{Y})$ is LCD. Since $\mathcal{Y}$ is a k-cover of X, no column of $G(\mathcal{Y})$ is $\mathbf{0}_k$ and some two columns of $G(\mathcal{Y})$ are identical. This implies that $d(C(\mathcal{Y})^\perp) = 2$. $\square$

Now we consider the case $k = 2, 3$ and $\ell = 2$. Let $\mathcal{Y}$ be a 2-cover and a 3-cover of X, respectively. Let $C(\mathcal{Y})$ be a $[2m + 2, 2]$ code and a $[2m + 3, 3]$ code with generator matrix of the form $G(\mathcal{Y})$, respectively. Let $C'(\mathcal{Y})$ denote the $[2m + 3, 2]$ code and the $[2m + 4, 3]$ code with generator matrix of the following form:

$$G'(\mathcal{Y}) = \begin{pmatrix} & G(\mathcal{Y}) & & \begin{matrix} 1 \\ 1 \end{matrix} \end{pmatrix} \text{ and } \begin{pmatrix} & G(\mathcal{Y}) & & \begin{matrix} 0 \\ 1 \\ 1 \end{matrix} \end{pmatrix},$$

respectively.

Proposition 3.2. *The code $C'(\mathcal{Y})$ is LCD.*

Proof. For $k = 2$ and 3, the result follows from

$$G'(\mathcal{Y})G'(\mathcal{Y})^T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

respectively. □

3.2 LCD codes from 2-covers

Proposition 3.3. *Suppose that $m \geq 1$. Let C be an LCD $[2m+2, 2]$ code with $d(C^{\perp}) \geq 2$. Then there is a 2-cover (Y_1, Y_2) such that $C \cong C((Y_1, Y_2))$.*

Proof. We may assume without loss of generality that C has generator matrix of the following form:

$$\begin{pmatrix} \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} & & M & \end{pmatrix}, \tag{1}$$

where M is a $2 \times 2m$ matrix such that no column is $\mathbf{0}_2$. If $2m \geq 4$, then an LCD $[2m, 2]$ code is constructed by Lemma 2.4. By continuing this process, an LCD $[4, 2]$ code with generator matrix of the form (1) is constructed. Hence, we show that such a code is constructed from a 2-cover.

Since no column of M is $\mathbf{0}_2$, it is sufficient to consider the codes with generator matrices:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Only the first code and the last two codes are LCD. It can be seen by hand that the last two LCD codes are equivalent. This means that the first code and the last code are $C((Y_1, Y_2))$ and $C((Y'_1, Y'_2))$, respectively, where $Y_1 = \emptyset, Y_2 = Y'_1 = Y'_2 = \{1\}$. □

Proposition 3.4. *Suppose that $m \geq 1$. Let C be an LCD $[2m+3, 2]$ code with $d(C^{\perp}) \geq 2$. Then there is a 2-cover (Y_1, Y_2) such that $C \cong C'((Y_1, Y_2))$.*

Proof. We may assume without loss of generality that C has generator matrix of the following form:

$$\left(\begin{array}{ccc} 1 & 0 & \\ 0 & 1 & \end{array} M' \right), \tag{2}$$

where M' is a $2 \times (2m+1)$ matrix such that no column is $\mathbf{0}_2$. If $2m+1 \geq 4$, then an LCD $[2m+1, 2]$ code is constructed by Lemma 2.4. By continuing this process, an LCD $[5, 2]$ code with generator matrix of the form (2) is constructed.

Since no column of M' is $\mathbf{0}_2$, it is sufficient to consider the $[5, 2]$ codes with generator matrices (2), where

$$M' = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Only the third code and the last code are LCD. It can be seen by hand that the two LCD codes are equivalent. In addition, the last code is $C'((Y_1, Y_2))$, where $Y_1 = Y_2 = \{1\}$. This completes the proof. □

3.3 LCD codes from 3-covers

Proposition 3.5. *Suppose that $m \geq 1$. Let C be an LCD $[2m+3, 3]$ code with $d(C^{\perp}) \geq 2$. Then there is a 3-cover (Y_1, Y_2, Y_3) such that $C \cong C((Y_1, Y_2, Y_3))$.*

Proof. We may assume without loss of generality that C has generator matrix of the following form:

$$\left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \quad M \right), \tag{3}$$

where M is a $3 \times 2m$ matrix such that no column is $\mathbf{0}_3$. If $2m \geq 8$, then an LCD $[2m+1, 3]$ code is constructed by Lemma 2.4. By continuing this process, an LCD $[n, 3]$ code with generator matrix of the form (3) is constructed, where $n = 5, 7, 9$. Hence, we show that such a code is constructed from a 3-cover.

Let C_9 be an LCD $[9,3]$ code with generator matrix of the form (3) satisfying that all columns of M are distinct. Our computer search shows that C_9 is equivalent to the code D_9 with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

In addition, our computer search shows that D_9 is equivalent to the code with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

This means that the code is $C((Y_1,Y_2,Y_3))$, where $Y_1=\{1,2,3\}$, $Y_2=\{1,3\}$ and $Y_3=\{1,2\}$.

Let C_7 be an LCD $[7,3]$ code with generator matrix of the form (3) satisfying that all columns of M are distinct. Our computer search shows that C_7 is equivalent to one of the codes $D_{7,1}$ and $D_{7,2}$ with generator matrices

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix},$$

respectively. In addition, our computer search shows that $D_{7,1}$ and $D_{7,2}$ are equivalent to the codes with generator matrices

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix},$$

respectively. This means that the codes are $C((Y_1,Y_2,Y_3))$ and $C((Y_1',Y_2',Y_3'))$, respectively, where $Y_1=Y_2=Y_1'=\{1,2\}$, $Y_3=Y_3'=\{1\}$ and $Y_2'=\{2\}$.

Our computer search shows that an LCD $[5,3]$ code is equivalent to one of the codes $C_{5,1}, C_{5,2}$ and $C_{5,3}$ with generator matrices

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix},$$

respectively. This means that the codes are $C((Y_1, Y_2, Y_3))$, $C((Y_1', Y_2', Y_3'))$ and $C((Y_1'', Y_2'', Y_3''))$, respectively, where $Y_1 = Y_1' = Y_2' = Y_1'' = Y_2'' = Y_3'' = \{1\}$ and $Y_2 = Y_3 = Y_3' = \emptyset$. $\square$

Proposition 3.6. *Suppose that $m \geq 1$. Let C be an LCD $[2m+4, 3]$ code with $d(C^\perp) \geq 2$. Then there is a 3-cover (Y_1, Y_2, Y_3) such that $C \cong C'((Y_1, Y_2, Y_3))$.*

Proof. We may assume without loss of generality that C has generator matrix of the following form:

$$\left(\begin{array}{cccc} 1 & 0 & 0 & \\ 0 & 1 & 0 & M' \\ 0 & 0 & 1 & \end{array} \right), \tag{4}$$

where M' is a $3 \times (2m+1)$ matrix such that no column is $\mathbf{0}_3$. If $2m+1 \geq 8$, then an LCD $[2m+2, 3]$ code is constructed by Lemma 2.4. By continuing this process, an LCD $[n, 3]$ code with generator matrix of the form (4) is constructed, where $n = 6, 8, 10$.

Let C_{10} be an LCD $[10, 3]$ code with generator matrix of the form (4) satisfying that all columns of M' are distinct. Then C_{10} is equivalent to the code D_{10} with generator matrix

$$\left(\begin{array}{cccccccccc} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right).$$

Our computer search shows that D_{10} is equivalent to the code with generator matrix

$$\left(\begin{array}{cccccccccc} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{array} \right).$$

This means that the code is $C'((Y_1, Y_2, Y_3))$, where $Y_1 = \{1, 2, 3\}$, $Y_2 = \{1, 3\}$ and $Y_3 = \{1, 2\}$.

Let C_8 be an LCD $[8, 3]$ code with generator matrix of the form (4) satisfying that all columns of M' are distinct. Our computer search shows that C_8 is equivalent to the code D_8 with generator matrix

$$\left(\begin{array}{cccccccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{array} \right).$$

In addition, our computer search shows that D_8 is equivalent to the code with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

This means that the code is $C'((Y_1, Y_2, Y_3))$, where $Y_1 = Y_2 = \{1, 2\}$ and $Y_3 = \{1\}$.

Our computer search shows that an LCD $[6, 3]$ code with generator is equivalent to one of the codes $C_{6,1}, C_{6,2}$ and $C_{6,3}$ with generator matrices $\begin{pmatrix} I_3 & A \end{pmatrix}$, where

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

respectively, In addition, these codes are

$$C'((Y_1, Y_2, Y_3)), C'((Y_1', Y_2', Y_3')) \text{ and } C'((Y_1'', Y_2'', Y_3'')),$$

respectively, where $Y_1 = Y_2' = Y_3' = \emptyset$ and $Y_2 = Y_3 = Y_1' = Y_1'' = Y_2'' = Y_3'' = \{1\}$. $\square$

3.4 Remarks

The elements of an m-set X may be taken to be identical. In this case, X is called *unlabelled*. Let $\mathcal{Y} = (Y_1, Y_2, \ldots, Y_k)$ be a k-cover of X. The order of the sets $Y_1, Y_2, \ldots, Y_k$ may not be material. In this case, $\mathcal{Y}$ is called *disordered* [5].

Proposition 3.7. *Let $\mathcal{Y}$ be a k-cover of an m-set X. Let $\mathcal{Y}'$ be the k-cover obtained from $\mathcal{Y}$ by a permutation of $Y_1, Y_2, \ldots, Y_k$ and a permutation of the elements of X. Then $C(\mathcal{Y}) \cong C(\mathcal{Y}')$.*

Proof. Consider a generator matrix G of the LCD code $C(\mathcal{Y})$ constructed from a k-cover $\mathcal{Y} = (Y_1, Y_2, \ldots, Y_k)$. A permutation of $Y_1, Y_2, \ldots, Y_k$ implies a permutation of rows of G. A permutation of the elements of X implies a permutation of columns of G. The result follows. $\square$

By the above proposition, when we consider codes $C(\mathcal{Y})$ constructed from all k-covers $\mathcal{Y}$, which must be checked to achieve a complete classification, it is sufficient to consider only disordered k-covers of unlabelled m-sets.

Now let us consider LCD codes constructed from 4-covers. Our computer search shows that there are six inequivalent LCD $[6,4]$ codes $D_{6,i}$ $(i=1,2,\ldots,6)$ with $d(D_{6,i}^{\perp}) \geq 2$. These codes $D_{6,i}$ have generator matrices $\begin{pmatrix} I_4 & A \end{pmatrix}$, where

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

respectively. The weight enumerators $W_{6,i}$ of the codes $D_{6,i}$ are listed in Table 1. It is easy to see that the number of disordered 4-covers of an unlabelled 1-set is 4 [5, Table 1]. Only the codes $D_{6,i}$ $(i=1,2,3,4)$ are constructed from 4-covers.

Table 1: $W_{6,i}$ $(i=1,2,\ldots,6)$

i	$W_{6,i}$	i	$W_{6,i}$
1	$1+3y+3y^2+2y^3+3y^4+3y^5+y^6$	4	$1+6y^2+4y^3+y^4+4y^5$
2	$1+2y+2y^2+4y^3+5y^4+2y^5$	5	$1+6y^2+9y^4$
3	$1+y+3y^2+6y^3+3y^4+y^5+y^6$	6	$1+4y^2+6y^3+3y^4+2y^5$

4 LCD codes of dimension 2

It was shown in [8] that

$$d(n,2) = \begin{cases} \lfloor \frac{2n}{3} \rfloor & \text{if } n \equiv 1,2,3,4 \pmod 6, \\ \lfloor \frac{2n}{3} \rfloor - 1 & \text{otherwise,} \end{cases}$$

for $n \geq 2$. Throughout this section, we denote $d(n,2)$ by d_n. In this section, we give a classification of LCD $[n,2,d_n]$ codes for $n=6t$ $(t \geq 1)$, $6t+1$ $(t \geq 1)$, $6t+2$ $(t \geq 0)$, $6t+3$ $(t \geq 1)$, $6t+4$ $(t \geq 0)$ and $6t+5$ $(t \geq 1)$. In Section 3, we gave some observation of LCD codes of dimension 2, which is established from the concept of 2-covers of m-sets. The observation is useful to complete the classification.

Lemma 4.1. *Suppose that $n \geq 2$ and $n \equiv 0, 1, 2, 3 \pmod 6$. If there is an LCD $[n, 2, d_n]$ code C then $d(C^{\perp}) \geq 2$.*

Proof. Write $n = 6t + s$, where $0 \leq s \leq 5$. For s and d_n, we have the following:

s	d_n	s	d_n	s	d_n
0	$4t-1$	2	$4t+1$	4	$4t+2$
1	$4t$	3	$4t+2$	5	$4t+2$

The result follows by Lemma 2.3. □

Now suppose that C and C' are an LCD $[2m+2, 2]$ code and an LCD $[2m+3, 2]$ code with $d(C^{\perp}) \geq 2$ and $d(C'^{\perp}) \geq 2$, respectively, for $m \geq 1$. By Propositions 3.3 and 3.4, we may assume without loss of generality that C and C' have generator matrices of the following form:

$$G^0(a,b,c) = \begin{pmatrix} 1 & 0 & M(a,b,c) & M(a,b,c) \\ 0 & 1 & & \end{pmatrix} \text{ and}$$
$$G^1(a,b,c) = \begin{pmatrix} 1 & 0 & M(a,b,c) & M(a,b,c) & 1 \\ 0 & 1 & & & 1 \end{pmatrix},$$

respectively, where

$$M(a,b,c) = \begin{pmatrix} \mathbf{1}_a & \mathbf{1}_b & \mathbf{0}_c \\ \mathbf{1}_a & \mathbf{0}_b & \mathbf{1}_c \end{pmatrix}. \tag{5}$$

We denote the codes by $C^0(a,b,c)$ and $C^1(a,b,c)$, respectively. Then the codes $C^{\delta}(a,b,c)$ have the following weight enumerators for $\delta \in \{0,1\}$:

$$1 + y^{1+2(a+b)+\delta} + y^{1+2(a+c)+\delta} + y^{2+2(b+c)} \tag{6}$$

For nonnegative integers a, b, c, n and $\delta \in \{0,1\}$, we consider the following conditions:

$$d_n \leq 1 + 2(a+b) + \delta, \tag{7}$$
$$d_n \leq 1 + 2(a+c) + \delta, \tag{8}$$
$$d_n \leq 2 + 2(b+c), \tag{9}$$
$$2(a+b+c) + 2 + \delta = n, \tag{10}$$
$$b \leq c. \tag{11}$$

Lemma 4.2. (i) *Let S be the set of (a,b,c) satisfying the conditions* (7)–(11)*, where $\delta = 1$.*

(1) *If $n = 6t+1$ $(t \geq 1)$, then $S = \{(t-1,t,t),(t,t-1,t)\}$.*
(2) *If $n = 6t+3$ $(t \geq 1)$, then $S = \{(t,t,t)\}$.*
(3) *If $n = 6t+5$ $(t \geq 1)$, then*

$$S = \left\{ \begin{array}{l} (t-1,t+1,t+1),(t,t,t+1), \\ (t+1,t-1,t+1),(t+1,t,t) \end{array} \right\}.$$

(ii) *Let S be the set of (a,b,c) satisfying the conditions* (7)–(11)*, where $\delta = 0$.*

(1) *If $n = 6t$ $(t \geq 1)$, then $S = \{(t-1,t,t),(t,t-1,t)\}$.*
(2) *If $n = 6t+2$ $(t \geq 1)$, then $S = \{(t,t,t)\}$.*
(3) *If $n = 6t+4$ $(t \geq 0)$, then $S = \{(t+1,t,t)\}$.*

Proof. All cases are similar, and we only give the details for $n = 6t+1$.

From (9) and (10), we have $a \leq t$. From (7), (8) and (10), we have $t-1 \leq a$. Thus, we have

$$a \in \{t-1,t\}.$$

Suppose that $a = t-1$. From (7), we have $t \leq b$. From (8), we have $t \leq c$. From (10), we have $b+c = 2t$. Hence, we have $b = c = t$.

Suppose that $a = t$. From (7), we have $t-1 \leq b$. From (8), we have $t-1 \leq c$. From (10), we have $b+c = 2t-1$. From (11), we have $(b,c) = (t-1,t)$. ☐

Lemma 4.3. *$C^\delta(a,b,c) \cong C^\delta(a,c,b)$ for $\delta \in \{0,1\}$.*

Proof. The matrix $G^\delta(a,c,b)$ is obtained from $G^\delta(a,c,b)$ by permutations of rows and columns. ☐

Lemma 4.4. *$C^1(a,b,c) \cong C^1(b,a,c) \cong C^1(c,b,a)$.*

Proof. We denote the code with generator matrix of the form $M(a,b,c)$ in (5) by $D(a,b,c)$. Let r_i be the i-th row of $M(a,b,c)$. By considering the matrices $\begin{pmatrix} r_1 \\ r_1+r_2 \end{pmatrix}$ and $\begin{pmatrix} r_1+r_2 \\ r_2 \end{pmatrix}$, we have $D(a,b,c) = D(b,a,c) = D(c,b,a)$. Since $C^1(a,b,c) \cong D(2a+1,2b+1,2c+1)$, the result follows. ☐

Theorem 4.5. (i) *For $t \geq 1$, there are two inequivalent LCD $[6t, 2, 4t-1]$ codes.*

(ii) *For $t \geq 1$, there is a unique LCD $[6t+1, 2, 4t]$ code, up to equivalence.*

(iii) *For $t \geq 1$, there is a unique LCD $[6t+2, 2, 4t+1]$ code, up to equivalence.*

(iv) *For $t \geq 1$, there is a unique LCD $[6t+3, 2, 4t+2]$ code, up to equivalence.*

Proof. Let C be an LCD $[n, 2]$ code with $n \geq 4$. For the parameters $[6t, 2, 4t-1]$, $[6t+1, 2, 4t]$, $[6t+2, 2, 4t+1]$ and $[6t+3, 2, 4t+2]$ $(t \geq 1)$, by Lemma 4.1, we may assume without loss of generality that C has generator matrix of the form $G^{\delta}(a, b, c)$ for $\delta = 0, 1, 0, 1$, respectively. In addition, C satisfies (7)–(10). By Lemma 4.3, we may assume without loss of generality that C satisfies (11).

(i) Assume that $n = 6t$ $(t \geq 1)$. By Lemma 4.2 (ii), (a, b, c) is $(t-1, t, t)$ or $(t, t-1, t)$. Let C_1 and C_2 be the LCD codes with generator matrices $G^0(a, b, c)$ for these (a, b, c), respectively. By (6), the codes C_1 and C_2 have the following weight enumerators:

$$1 + 2y^{4t-1} + y^{4t+2} \text{ and } 1 + y^{4t-1} + y^{4t} + y^{4t+1},$$

respectively. Hence, the two codes are inequivalent.

(ii) Assume that $n = 6t+1$ $(t \geq 1)$. By Lemma 4.2 (i), (a, b, c) is $(t-1, t, t)$ or $(t, t-1, t)$. Let C_1 and C_2 be the LCD codes with generator matrices $G^1(a, b, c)$ for these (a, b, c), respectively. By Lemma 4.4, C_1 and C_2 are equivalent.

(iii) For $n = 6t + 2$ $(t \geq 1)$, the uniqueness follows from Lemma 4.2 (ii).

(iv) For $n = 6t + 3$ $(t \geq 1)$, the uniqueness follows from Lemma 4.2 (i).

This completes the proof. $\square$

We remark that there is a unique LCD $[3, 2, 2]$ code, up to equivalence, by Proposition 2.7.

Lemma 4.6. (i) *For $t \geq 0$, there is a unique LCD $[6t+4, 2, 4t+2]$ code C with $d(C^{\perp}) \geq 2$, up to equivalence.*

(ii) *For $t \geq 1$, there are two inequivalent LCD $[6t+5, 2, 4t+2]$ codes C with $d(C^{\perp}) \geq 2$.*

Proof. Let C be an LCD $[n, 2]$ code with $d(C^{\perp}) \geq 2$ and $n \geq 4$. For the parameters $[6t+4, 2, 4t+2]$ $(t \geq 0)$ and $[6t+5, 2, 4t+2]$ $(t \geq 1)$, since $d(C^{\perp}) \geq 2$, we may assume without loss of generality that C has generator matrix of the form $G^{\delta}(a, b, c)$ for $\delta = 0, 1$, respectively. In addition, C satisfies (7)–(10). By Lemma 4.3, we may assume without loss of generality that C satisfies (11).

(i) For $n = 6t + 4$ $(t \geq 0)$, the uniqueness follows from Lemma 4.2 (ii).

(ii) Assume that $n = 6t + 5$ $(t \geq 1)$. By Lemma 4.2 (i), (a, b, c) is $(t-1, t+1, t+1)$, $(t, t, t+1)$, $(t+1, t-1, t+1)$ or $(t+1, t, t)$. Let C_i $(i = 1, 2, 3, 4)$ be the LCD code with generator matrix $G^1(a, b, c)$ for these (a, b, c), respectively. By Lemma 4.4, $C_1 \cong C_3$ and $C_2 \cong C_4$. By (6), the codes C_1 and C_2 have the following weight enumerators:

$$1 + 2y^{4t+2} + y^{4t+4} \text{ and } 1 + y^{4t+2} + 2y^{4t+4},$$

respectively. Hence, the two codes are inequivalent.

This completes the proof. □

Remark 4.7. By [8, Theorem 3], the dual codes of the codes given in the above lemma have minimum weight 2.

Theorem 4.8. (i) *For $t \geq 0$, there are two inequivalent LCD $[6t+4, 2, 4t+2]$ codes.*

(ii) *For $t \geq 1$, there are four inequivalent LCD $[6t+5, 2, 4t+2]$ codes.*

Proof. By Lemma 2.5, all LCD $[n+1, k, d]$ codes C with $d(C^{\perp}) = 1$, which must be checked to achieve a complete classification, can be obtained from all inequivalent LCD $[n, k, d]$ codes.

(i) By Theorem 4.5, there is a unique LCD $[6t+3, 2, 4t+2]$ code, up to equivalence, for $t \geq 1$. The result follows from Lemma 4.6.

(ii) The result follows from Lemma 4.6 and the part (i).

This completes the proof. □

We remark that there are three inequivalent LCD $[5, 2, 2]$ codes (see Table 3).

5 LCD codes of dimension 3: $d(n,3)$

The aim of this section is to show the following theorem. In Section 3, we gave some observation of LCD codes of dimension 3, which is established from the concept of 3-covers of m-sets. The observation is useful to do this.

Theorem 5.1. *For $n \geq 3$,*

$$d(n,3) = \begin{cases} \left\lfloor \frac{4n}{7} \right\rfloor & \text{if } n \equiv 3,5,10,12 \pmod{14}, \\ \left\lfloor \frac{4n}{7} \right\rfloor - 1 & \text{otherwise.} \end{cases}$$

Throughout this section, we denote $\left\lfloor \frac{4n}{7} \right\rfloor$ by α_n.

Lemma 5.2. *There is no LCD $[n,3,\alpha_n]$ code for $n \equiv 2 \pmod 7$.*

Proof. Suppose that there is an (unrestricted) $[n,3,d]$ code. By the Griesmer bound, we have

$$n \geq d + \left\lceil \frac{d}{2} \right\rceil + \left\lceil \frac{d}{4} \right\rceil.$$

Hence, we have

$$d(n,3) \leq \begin{cases} \alpha_n - 1 & \text{if } n \equiv 2 \pmod 7, \\ \alpha_n & \text{otherwise.} \end{cases}$$

The result follows. □

Lemma 5.3. *Suppose that $n \geq 3$ and $n \equiv 0,4,6,7,11,13 \pmod{14}$. If there is an LCD $[n,3,\alpha_n]$ code C, then $d(C^{\perp}) \geq 2$.*

Proof. Write $n = 14t + s$, where $0 \leq s \leq 13$. For s and α_n, we have the following:

s	α_n	s	α_n	s	α_n	s	α_n	s	α_n
0	$8t$	3	$8t+1$	6	$8t+3$	9	$8t+5$	12	$8t+6$
1	$8t$	4	$8t+2$	7	$8t+4$	10	$8t+5$	13	$8t+7$
2	$8t+1$	5	$8t+2$	8	$8t+4$	11	$8t+6$		

The result follows by Lemma 2.3. □

For nonnegative integers $a, b, c, d, e, f, g, m, \alpha$ and $\delta \in \{0, 1\}$, we consider the following conditions:

$$\alpha \leq 1 + 2(a + b + f + g), \tag{12}$$
$$\alpha \leq 1 + 2(a + c + e + g) + \delta, \tag{13}$$
$$\alpha \leq 1 + 2(a + d + e + f) + \delta, \tag{14}$$
$$\alpha \leq 2 + 2(b + c + e + f) + \delta, \tag{15}$$
$$\alpha \leq 2 + 2(b + d + e + g) + \delta, \tag{16}$$
$$\alpha \leq 2 + 2(c + d + f + g), \tag{17}$$
$$\alpha \leq 3 + 2(a + b + c + d), \tag{18}$$
$$a + b + c + d + e + f + g = m. \tag{19}$$

Define the following sets:

$$R_1 = \left\{ r \in \mathbb{Z} \mid \alpha - m - \frac{3 + \delta}{2} \leq r \leq m - \frac{3}{4}\alpha + \frac{3 + \delta}{2} \right\},$$
$$R_2 = \left\{ r \in \mathbb{Z} \mid \alpha - m - \frac{4 + \delta}{2} \leq r \leq m - \frac{3}{4}\alpha + \frac{2 + \delta}{2} \right\}.$$

Lemma 5.4. *Let a, b, c, d, e, f, g be nonnegative integers satisfying the conditions* (12)–(19)*.*

(i) *If $\delta = 0$, then $a, e, f, g \in R_1$ and $b, c, d \in R_2$.*

(ii) *If $\delta = 1$, then $a, f, g \in R_1$ and $b, c, d, e \in R_2$.*

Proof. All cases are similar, and we only give the details for $a \in R_1$ and $b \in R_2$.

From (15), (16), (17) and (19), we have $a \leq m - \frac{3}{4}\alpha + \frac{3+\delta}{2}$. From (12), (13), (14), (18) and (19), we have $\alpha - m - \frac{3+\delta}{2} \leq a$. Similarly, from (13), (14), (17) and (19), we have $b \leq m - \frac{3}{4}\alpha + \frac{4+\delta}{2}$. From (12), (15), (16), (18) and (19), we have $\alpha - m - \frac{4+\delta}{2} \leq b$. The result follows. □

Now suppose that C and C' are an LCD $[2m + 3, 3]$ code and an LCD $[2m + 4, 3]$ code with $d(C^{\perp}) \geq 2$ and $d(C'^{\perp}) \geq 2$, respectively for $m \geq 1$. By Propositions 3.5 and 3.6, we may assume without loss of generality that C

and C' have generator matrices of the following form:

$$\left(\begin{array}{ccccc} 1 & 0 & 0 & & \\ 0 & 1 & 0 & M(a,b,c,d,e,f,g) & M(a,b,c,d,e,f,g) \\ 0 & 0 & 1 & & \end{array}\right) \text{ and}$$
$$\left(\begin{array}{cccccc} 1 & 0 & 0 & & & 0 \\ 0 & 1 & 0 & M(a,b,c,d,e,f,g) & M(a,b,c,d,e,f,g) & 1 \\ 0 & 0 & 1 & & & 1 \end{array}\right),$$

respectively, where

$$M(a,b,c,d,e,f,g) = \left(\begin{array}{ccccccc} \mathbf{1}_a & \mathbf{1}_b & \mathbf{0}_c & \mathbf{0}_d & \mathbf{0}_e & \mathbf{1}_f & \mathbf{1}_g \\ \mathbf{1}_a & \mathbf{0}_b & \mathbf{1}_c & \mathbf{0}_d & \mathbf{1}_e & \mathbf{0}_f & \mathbf{1}_g \\ \mathbf{1}_a & \mathbf{0}_b & \mathbf{0}_c & \mathbf{1}_d & \mathbf{1}_e & \mathbf{1}_f & \mathbf{0}_g \end{array}\right). \tag{20}$$

We denote the codes by $C^0(a,b,c,d,e,f,g)$ and $C^1(a,b,c,d,e,f,g)$, respectively. Then the codes $C^\delta(a,b,c,d,e,f,g)$ have the following weight enumerators for $\delta \in \{0,1\}$:

$$\begin{aligned} &1 + y^{1+2(a+b+f+g)} + y^{1+2(a+c+e+g)+\delta} + y^{1+2(a+d+e+f)+\delta} \\ &\quad + y^{2+2(b+c+e+f)+\delta} + y^{2+2(b+d+e+g)+\delta} + y^{2+2(c+d+f+g)} + y^{3+2(a+b+c+d)}. \end{aligned} \tag{21}$$

Lemma 5.5. *There is an LCD* $[n,3,\alpha_n]$ *code for* $n \equiv 3,5,10,12 \pmod{14}$.

Proof. $\mathbb{F}_2^3$ is the LCD $[3,3,1]$ code. Suppose that $n \geq 5$. Consider the following codes:

$$\begin{aligned} &C^0(t+1,t,t,t,t,t,t), C^1(t+1,t,t,t,t,t+1,t+1), \\ &C^1(t+1,t+1,t,t,t,t+1,t+1) \text{ and} \\ &C^0(t+1,t+1,t+1,t+1,t+1,t+1,t+1), \end{aligned}$$

for $t \geq 0$. These codes have lengths $14t+5$, $14t+10$, $14t+12$ and $14t+17$, respectively. By (21), these codes have the following weight enumerators:

$$\begin{aligned} &1 + 3y^{8t+2} + 3y^{8t+3} + y^{8t+5}, 1 + 3y^{8t+5} + 3y^{8t+6} + y^{8t+7}, \\ &\qquad 1 + y^{8t+5} + y^{8t+6} + 3y^{8t+7} + 2y^{8t+8} \text{ and } 1 + 3y^{8t+9} + 3y^{8t+10} + y^{8t+11}, \end{aligned}$$

respectively. The result follows. ∎

For the above parameters, the uniqueness of LCD codes is established in Section 6.

Lemma 5.6. *There is no LCD $[n,3,\alpha_n]$ code for $n \equiv 0,4,6,7,11,13 \pmod{14}$.*

Proof. There is no LCD $[4,3,2]$ code (see [8, Table 1]). Assume that $n \equiv 0,4,6,7,11,13 \pmod{14}$ and $n \geq 6$. Suppose that there is an LCD $[n,3,\alpha_n]$ code C. By Lemma 5.3, $d(C^{\perp}) \geq 2$. Hence, $C \cong C^0(a,b,c,d,e,f,g)$ if $n \equiv 7,11,13 \pmod{14}$ and $C \cong C^1(a,b,c,d,e,f,g)$ if $n \equiv 0,4,6 \pmod{14}$ for some (a,b,c,d,e,f,g).

Since C has minimum weight α_n, (a,b,c,d,e,f,g) satisfies (12)–(19) with $n = 3+2m+\delta$ and $\alpha = \alpha_n$.

- $(n,\alpha_n) = (14t, 8t)$ $(t \geq 1)$: We have $R_2 = \emptyset$, which is a contradiction.
- $(n,\alpha_n) = (14t+4, 8t+2)$ $(t \geq 1)$, $(14t+6, 8t+3)$ $(t \geq 0)$: We have

  $$(a,b,c,d,e,f,g) = (t,t,t,t,t,t,t)$$

  by Lemma 5.4. These contradict (12) and (19), respectively.
- $(n,\alpha_n) = (14t+7, 8t+4)$ $(t \geq 0)$: We have $R_1 = \emptyset$, which is a contradiction.
- $(n,\alpha_n) = (14t+11, 8t+6)$, $(14t+13, 8t+7)$ $(t \geq 0)$: We have

  $$(a,b,c,d,e,f,g) = (t+1,t,t,t,t+1,t+1,t+1)$$

  by Lemma 5.4. These contradict (18) and (19), respectively.

This completes the proof. □

Lemma 5.7. *There is no LCD $[n,3,\alpha_n]$ code for $n \equiv 1,8 \pmod{14}$.*

Proof. Assume that $n \equiv 1,8 \pmod{14}$ and $n \geq 8$. Suppose that there is an LCD $[n,3,\alpha_n]$ code C. Since $n-1 \equiv 0,7 \pmod{14}$ and $\alpha_n = \alpha_{n-1}$, we have

$$d(n-1,3) \leq \alpha_{n-1} - 1 = \alpha_n - 1$$

by Lemma 5.6. By Lemma 2.3, $d(C^{\perp}) \geq 2$. Hence, $C \cong C^0(a,b,c,d,e,f,g)$ if $n \equiv 1 \pmod{14}$ and $C \cong C^1(a,b,c,d,e,f,g)$ if $n \equiv 8 \pmod{14}$ for some (a,b,c,d,e,f,g).

Since C has minimum weight α_n, (a,b,c,d,e,f,g) satisfies (12)–(19) with $n = 3+2m+\delta$ and $\alpha = \alpha_n$.

- $(n, \alpha_n) = (14t+1, 8t)$ $(t \geq 1)$: We have
$$(a, e, f, g) = (t, t, t, t) \text{ and } b, c, d \in \{t-1, t\}$$
by Lemma 5.4. From (19), $b + c + d = 3t - 1$. Hence,
$$(b, c, d) = (t-1, t, t), (t, t-1, t) \text{ and } (t, t, t-1).$$
These contradict (12), (13) and (14), respectively.

- $(n, \alpha_n) = (14t+8, 8t+4)$ $(t \geq 0)$: We have
$$a, f, g \in \{t, t+1\} \text{ and } (b, c, d, e) = (t, t, t, t)$$
by Lemma 5.4. From (19), $a + f + g = 3t + 2$. Hence,
$$(a, f, g) = (t, t+1, t+1), (t+1, t, t+1) \text{ and } (t+1, t+1, t).$$
These contradict (18), (15) and (16), respectively.

This completes the proof. □

Lemma 5.8. *There is an LCD* $[n, 3, \alpha_n - 1]$ *code for* $n \equiv 0, 1, 2, 4, 6, 7, 8, 9, 11, 13 \pmod{14}$ *and* $n \geq 4$.

Proof. There is an LCD $[4, 3, 2]$ code (see [8, Table 1]). Suppose that $n \geq 6$. Consider the following codes:
$$\begin{aligned}
&C^1(t+1, t, t, t, t, t, t), C^0(t, t, t, t, t, t+1, t+1),\\
&C^1(t, t, t, t, t, t+1, t+1), C^0(t+1, t, t, t, t, t+1, t+1),\\
&C^0(t+1, t, t, t, t+1, t+1, t+1),\\
&C^0(t+1, t+1, t, t, t+1, t+1, t+1),\\
&C^1(t+1, t, t, t+1, t+1, t+1, t+1),\\
&C^0(t+1, t+1, t, t+1, t+1, t+1, t+1),\\
&C^1(t+1, t+1, t, t+1, t+1, t+1, t+1) \text{ and}\\
&C^1(t+1, t+1, t+1, t+1, t+1, t+1, t+1),
\end{aligned}$$
for $t \geq 0$. We denote these codes by C_i $(i = 1, 2, \ldots, 10)$, respectively. The codes C_i have lengths $14t+6$, $14t+7$, $14t+8$, $14t+9$, $14t+11$, $14t+13$, $14t+14$, $14t+15$, $14t+16$ and $14t+18$, respectively. The weight enumerators W_i of C_i $(i = 1, 2, \ldots, 10)$ are obtained by (21), where W_i are listed in Table 2. The result follows. □

Lemmas 5.2, 5.5, 5.6, 5.7 and 5.8 complete the proof of Theorem 5.1.

Table 2: W_i ($i = 1, 2, \ldots, 10$)

i	W_i	i	W_i
1	$1 + y^{8t+2} + 3y^{8t+3} + 2y^{8t+4} + y^{8t+5}$	6	$1 + y^{8t+6} + 3y^{8t+7} + 2y^{8t+8} + y^{8t+9}$
2	$1 + 3y^{8t+3} + 2y^{8t+4} + y^{8t+5} + y^{8t+6}$	7	$1 + 3y^{8t+7} + 2y^{8t+8} + y^{8t+9} + y^{8t+10}$
3	$1 + y^{8t+3} + 2y^{8t+4} + 3y^{8t+5} + y^{8t+6}$	8	$1 + y^{8t+7} + 2y^{8t+8} + 3y^{8t+9} + y^{8t+10}$
4	$1 + 2y^{8t+4} + 3y^{8t+5} + y^{8t+6} + y^{8t+7}$	9	$1 + 2y^{8t+8} + 3y^{8t+9} + y^{8t+10} + y^{8t+11}$
5	$1 + y^{8t+5} + 3y^{8t+6} + 3y^{8t+7}$	10	$1 + y^{8t+9} + 3y^{8t+10} + 3y^{8t+11}$

6 LCD codes of dimension 3: uniqueness

In this section, we establish the uniqueness of LCD $[n, 3, d(n, 3)]$ codes C for $n \equiv 0, 2, 3, 5, 7, 9, 10, 12 \pmod{14}$ and $n \geq 5$. By Lemma 2.3 and Theorem 5.1, $d(C^\perp) \geq 2$. By Propositions 3.5 and 3.6, $C \cong C^0(a, b, c, d, e, f, g)$ if $n \equiv 3, 5, 7, 9 \pmod{14}$ and $C \cong C^1(a, b, c, d, e, f, g)$ if $n \equiv 0, 2, 10, 14 \pmod{14}$ for some (a, b, c, d, e, f, g)

Lemma 6.1. (i) $C^0(a, b, c, d, e, f, g) \cong C^0(a, b, d, c, e, g, f)$
$\cong C^0(a, c, b, d, f, e, g) \cong C^0(a, c, d, b, f, g, e) \cong C^0(a, d, b, c, g, e, f)$
$\cong C^0(a, d, c, b, g, f, e)$.

(ii) $C^1(a, b, c, d, e, f, g) \cong C^1(a, b, d, c, e, g, f)$.

Proof. The result follows by considering permutations of rows and columns of the generator matrices of $C^0(a, b, c, d, e, f, g)$ and $C^1(a, b, c, d, e, f, g)$. □

By the above lemma, we may assume without loss of generality that

$$\begin{aligned} b \leq c \leq d \quad &\text{if} \quad \delta = 0, \\ c \leq d \quad &\text{if} \quad \delta = 1. \end{aligned} \tag{22}$$

Lemma 6.2. *Let S be the set of (a, b, c, d, e, f, g) satisfying* (12)–(19) *and* (22)*.*

(i) *If $(n, \alpha) = (14t + 3, 8t + 1)$ $(t \geq 1)$, then $S = \{(t, t, t, t, t, t, t)\}$.*

(ii) *If $(n, \alpha) = (14t + 5, 8t + 2)$ $(t \geq 0)$, then $S = \{(t + 1, t, t, t, t, t, t)\}$.*

(iii) *If $(n, \alpha) = (14t+10, 8t+5)$ $(t \geq 0)$, then $S = \{(t+1, t, t, t, t, t+1, t+1)\}$.*

(iv) *If* $(n, \alpha) = (14t + 12, 8t + 6)$ $(t \geq 0)$, *then*

$$S = \{(t + 1, t + 1, t, t, t, t + 1, t + 1)\}.$$

Proof. All cases are similar, and we only give the details for (iv), which is the complicated case.

Suppose that $n = 14t + 12$ and $\alpha = 8t + 6$ $(t \geq 0)$. By Lemma 5.4, $R_1 = R_2 = \{t, t + 1\}$. From (12), $4t + \frac{5}{2} \leq a + b + f + g$. Hence, we have

$$|\{s \in \{a, b, f, g\} \mid s = t + 1\}| \geq 3.$$

From (19), $a + b + c + d + e + f + g = 7t + 4$. Hence, we have

$$|\{s \in \{a, b, c, d, e, f, g\} \mid s = t + 1\}| = 4.$$

Therefore, we have

$$(a, b, f, g) \in \left\{ \begin{array}{l} (t+1, t+1, t+1, t), (t+1, t+1, t, t+1), \\ (t+1, t, t+1, t+1), (t, t+1, t+1, t+1), \\ (t+1, t+1, t+1, t+1) \end{array} \right\}.$$

Here, we remark that

$$|\{s \in \{c, d, e\} \mid s = t + 1\}| \leq 1. \tag{23}$$

- $(a, b, f, g) = (t + 1, t + 1, t + 1, t)$: From (13), (16) and (17),

  $$2t + 1 \leq c + e, 2t + \frac{1}{2} \leq d + e \text{ and } 2t + 1 \leq c + d,$$

  respectively. This contradicts (23).

- $(a, b, f, g) = (t + 1, t + 1, t, t + 1)$: From (14), (15) and (17),

  $$2t + 1 \leq d + e, 2t + \frac{1}{2} \leq c + e \text{ and } 2t + 1 \leq c + d,$$

  respectively. This contradicts (23).

- $(a, b, f, g) = (t + 1, t, t + 1, t + 1)$: From (15), (16) and (18),

  $$2t + \frac{1}{2} \leq c + e, 2t + \frac{1}{2} \leq d + e \text{ and } 2t + \frac{1}{2} \leq c + d,$$

  respectively. This contradicts (23).

- $(a, b, f, g) = (t, t+1, t+1, t+1)$: From (13), (14) and (18),

  $$2t+1 \leq c+e, 2t+1 \leq d+e \text{ and } 2t+\frac{1}{2} \leq c+d,$$

  respectively. This contradicts (23).

The result follows. $\square$

Therefore, we have the following theorem.

Theorem 6.3. (i) *For $t \geq 1$, there is a unique LCD $[14t+3, 3, 8t+1]$ code, up to equivalence.*

(ii) *For $t \geq 0$, there is a unique LCD $[14t+5, 3, 8t+2]$ code, up to equivalence.*

(iii) *For $t \geq 0$, there is a unique LCD $[14t+10, 3, 8t+5]$ code, up to equivalence.*

(iv) *For $t \geq 0$, there is a unique LCD $[14t+12, 3, 8t+6]$ code, up to equivalence.*

Now we consider LCD $[n, 3, d(n, 3)]$ codes for $n \equiv 0, 2, 7, 9 \pmod{14}$ and $n \geq 7$.

Lemma 6.4. *Let S be the set of (a, b, c, d, e, f, g) satisfying (12)–(19) and (22).*

(i) *If $(n, \alpha) = (14t, 8t-1)$ $(t \geq 1)$, then*

$$S = \{(t, t-1, t, t, t-1, t, t), (t, t-1, t-1, t, t, t, t)\}.$$

(ii) *If $(n, \alpha) = (14t+2, 8t)$ $(t \geq 1)$, then*

$$S = \{(t, t, t, t, t-1, t, t), (t, t, t-1, t, t, t, t)\}.$$

(iii) *If $(n, \alpha) = (14t+7, 8t+3)$ $(t \geq 0)$, then*

$$S = \left\{ \begin{array}{l} (t, t, t, t, t+1, t, t+1), (t, t, t, t, t+1, t+1, t), \\ (t, t, t, t, t, t+1, t+1) \end{array} \right\}.$$

(iv) *If* $(n, \alpha) = (14t+9, 8t+4)$ $(t \ge 0)$, *then*

$$S = \left\{ \begin{array}{l} (t+1, t, t, t, t+1, t, t+1), (t+1, t, t, t, t+1, t+1, t), \\ (t+1, t, t, t, t, t+1, t+1) \end{array} \right\}.$$

Proof. All cases are similar, and we only give the details for (i).

Suppose that $n = 14t$ and $\alpha = 8t-1$ $(t \ge 1)$. By Lemma 5.4, $R_1 = R_2 = \{t-1, t\}$. From (19), $a+b+c+d+e+f+g = 7t-2$. Hence, we have

$$|\{s \in \{a, b, c, d, e, f, g\} \mid s = t-1\}| = 2. \tag{24}$$

From (12), (13) and (14),

$$\begin{array}{l} 4t-1 \le a+b+f+g, \\ 4t-\frac{3}{2} \le a+c+e+g \text{ and} \\ 4t-1 \le a+d+e+f, \end{array} \tag{25}$$

respectively.

Now suppose that $a = t-1$. From (25), we have $b = c = d = e = f = g = t$. Since this contradicts (24), we have $a = t$. Suppose that $g = t-1$. From (25), we have $b = c = d = e = f = t$. Since this contradicts (24), we have $g = t$. From (17),

$$4t - \frac{3}{2} \le c+d+f+g. \tag{26}$$

Suppose that $f = t-1$. From (25) and (26), we have $b = c = d = e = t$. Since this contradicts (24), we have $f = t$. Suppose that $d = t-1$. From (26), we have $c = t$, which contradicts (22). Therefore, we have

$$(b, c, e) \in \{(t-1, t-1, t), (t-1, t, t-1)\}.$$

The result follows. ☐

We denote the code with generator matrix of the form $M(a, b, c, d, e, f, g)$ in (20) by $D(a, b, c, d, e, f, g)$. It is trivial that $C^0(a, b, c, d, e, f, g) \cong D(2a, 2b+1, 2c+1, 2d+1, 2e, 2f, 2g)$ and $C^1(a, b, c, d, e, f, g) \cong D(2a, 2b+1, 2c+1, 2d+1, 2e+1, 2f, 2g)$.

Lemma 6.5. (i) *For* $t \ge 1$, $D(2t, 2t-1, 2t+1, 2t+1, 2t-1, 2t, 2t) \cong D(2t, 2t-1, 2t-1, 2t+1, 2t+1, 2t, 2t)$.

(ii) *For* $t \geq 1$, $D(2t, 2t+1, 2t-1, 2t+1, 2t+1, 2t, 2t) \cong D(2t, 2t+1, 2t+1, 2t+1, 2t-1, 2t, 2t)$.

Proof. Let r_i be the i-th row of $M(a, b, c, d, e, f, g)$. Consider the following matrices:

$$\begin{pmatrix} r_1 \\ r_3 \\ r_2 + r_3 \end{pmatrix} \text{ and } \begin{pmatrix} r_1 \\ r_2 \\ r_2 + r_3 \end{pmatrix}$$

for (i) and (ii), respectively. The result follows. $\square$

Theorem 6.6. (i) *For* $t \geq 1$, *there is a unique LCD* $[14t, 3, 8t-1]$ *code, up to equivalence.*

(ii) *For* $t \geq 1$, *there is a unique LCD* $[14t+2, 3, 8t]$ *code, up to equivalence.*

(iii) *For* $t \geq 0$, *there is a unique LCD* $[14t+7, 3, 8t+3]$ *code, up to equivalence.*

(iv) *For* $t \geq 0$, *there is a unique LCD* $[14t+9, 3, 8t+4]$ *code, up to equivalence.*

Proof. For (i) and (ii), the result follows from Lemmas 6.4 and 6.5. For (iii) and (iv), the result follows from Lemmas 6.1 and 6.4. $\square$

For the parameters $[4, 3, 1]$, $[6, 3, 2]$, $[8, 3, 3]$, $[11, 3, 5]$, $[13, 3, 6]$ and $[15, 3, 7]$, a number of inequivalent LCD codes are known (see Table 3).

7 Classification of LCD codes for small parameters

In this section, we give a complete classification of LCD $[n, k]$ codes having minimum weight $d(n, k)$ for $2 \leq k \leq n-1 \leq 15$.

We describe how LCD $[n, k]$ codes having minimum weight $d(n, k)$ were classified. Let $d_{\text{all}}(n, k)$ denote the largest minimum weight among all (unrestricted) $[n, k]$ codes. The values $d_{\text{all}}(n, k)$ can be found in [9]. For a fixed pair (n, k), we found all inequivalent $[n, k]$ codes by one of the following methods. If there is no LCD $[n, k, d_{\text{all}}(n, k)]$ code, then we consider the case $d_{\text{all}}(n, k) - 1$.

Let C be an $[n,k,d]$ code with parity-check matrix H. Let D be a code with parity-check matrix obtained from H by deleting a column. The code D is an $[n-1,k-1,d']$ code with $d' \geq d$. By considering the inverse operation, all $[n,k,d]$ codes are obtained from $[n-1,k-1,d']$ codes with $d' \geq d$. Starting from $[n,1,d']$ codes with $d' \geq d$, all $[n+t,1+t,d]$ codes are found for a given $t \geq 1$. This was done one column at a time, and complete equivalence tests are carried out for each new column added. It is obvious that all codes, which must be checked to achieve a complete classification, can be obtained.

For some parameters, we employ the following method, due to the computational complexity. Every $[n,k,d]$ code is equivalent to a code with generator matrix of the form $\begin{pmatrix} I_k & A \end{pmatrix}$, where A is a $k \times (n-k)$ matrix. The set of matrices A was constructed, row by row. Permuting the rows and columns of A gives rise to different generator matrices which generate equivalent codes. Here, we consider a natural (lexicographical) order $<$ on the set of the vectors of length $n-k$. Let r_i be the i-th row of A. We consider only matrices A, satisfying the condition $r_1 < r_2 < \cdots < r_k$ and $\mathrm{wt}(r_i) \geq d-1$. It is obvious that all codes, which must be checked to achieve a complete classification, can be obtained.

For $2 \leq k \leq n-1 \leq 15$, the numbers $N(n,k,d(n,k))$ of inequivalent LCD $[n,k,d(n,k)]$ codes are listed in Table 3, along with the values $d(n,k)$. All generator matrices of the codes in the table can be obtained electronically from `http://www.math.is.tohoku.ac.jp/~mharada/LCD/`.

We continue a classification of LCD codes with parameters $[2m+3,2m,2]$ and $[2m+4,2m+1,2]$. In Proposition 3.5, for an LCD $[2m+3,2m,2]$ code C, there is a 3-cover (Y_1,Y_2,Y_3) such that $C^\perp \cong C((Y_1,Y_2,Y_3))$. In addition, by Proposition 3.7, when we consider codes $C(\mathcal{Y})$ constructed from all k-covers $\mathcal{Y}$, which must be checked to achieve a complete classification, it is sufficient to consider only disordered k-covers of unlabelled m-sets. According to [5], let $\mathrm{Tdu}(m,k)$ denote the number of disordered k-covers of an unlabelled m-set. The formula $\mathrm{Tdu}(m,k)$ is given in [5, Theorem 2]. For $m \leq 7$ and $k \leq 8$, $\mathrm{Tdu}(m,k)$ is numerically determined in [5, Table 1] (see also A005783 in [15]). Our computer search shows the following:

Proposition 7.1. *If* $1 \leq m \leq 11$*, then*

$$N(2m+3,2m,2) = N(2m+4,2m+1,2) = \mathrm{Tdu}(m,3).$$

Table 3: $(d(n,k), N(n,k,d(n,k)))$

$n\backslash k$	2	3	4	5	6	7	8
3	$(2,1)$						
4	$(2,2)$	$(1,2)$					
5	$(2,3)$	$(2,1)$	$(2,1)$				
6	$(3,2)$	$(2,3)$	$(2,4)$	$(1,3)$			
7	$(4,1)$	$(3,1)$	$(2,9)$	$(2,2)$	$(2,1)$		
8	$(5,1)$	$(3,3)$	$(3,1)$	$(2,9)$	$(2,6)$	$(1,4)$	
9	$(6,1)$	$(4,1)$	$(4,1)$	$(3,2)$	$(2,23)$	$(2,3)$	$(2,1)$
10	$(6,2)$	$(5,1)$	$(4,5)$	$(3,11)$	$(3,2)$	$(2,23)$	$(2,9)$
11	$(6,4)$	$(5,6)$	$(4,20)$	$(4,4)$	$(4,1)$	$(3,1)$	$(2,51)$
12	$(7,2)$	$(6,1)$	$(5,6)$	$(4,37)$	$(4,11)$	$(3,22)$	$(2,396)$
13	$(8,1)$	$(6,6)$	$(6,2)$	$(5,5)$	$(4,146)$	$(4,4)$	$(3,27)$
14	$(9,1)$	$(7,1)$	$(6,16)$	$(5,101)$	$(5,4)$	$(4,301)$	$(4,8)$
15	$(10,1)$	$(7,8)$	$(6,89)$	$(6,10)$	$(6,2)$	$(5,1)$	$(4,985)$
16	$(10,2)$	$(8,1)$	$(7,7)$	$(6,283)$	$(6,60)$	$(5,1596)$	$(5,1)$
$n\backslash k$	9	10	11	12	13	14	15
10	$(1,5)$						
11	$(2,4)$	$(2,1)$					
12	$(2,51)$	$(2,12)$	$(1,6)$				
13	$(2,619)$	$(2,103)$	$(2,5)$	$(2,1)$			
14	$(3,31)$	$(2,1370)$	$(2,103)$	$(2,16)$	$(1,7)$		
15	$(4,2)$	$(3,34)$	$(2,2143)$	$(2,196)$	$(2,7)$	$(2,1)$	
16	$(4,1772)$	$(4,7)$	$(3,34)$	$(2,4389)$	$(2,196)$	$(2,20)$	$(1,8)$

8 A construction of LCD codes over $\mathbb{F}_q$ using self-orthogonal codes

A code C over $\mathbb{F}_q$ is called *self-orthogonal* and *self-dual* if $C \subset C^\perp$ and $C = C^\perp$, respectively. In this section, we give a construction of LCD codes over $\mathbb{F}_q$ using self-orthogonal codes.

Proposition 8.1. *Suppose that there is a self-orthogonal $[n_1, k, d_1]$ code over $\mathbb{F}_q$ and there is an LCD $[n_2, k, d_2]$ code over $\mathbb{F}_q$. Then there is an LCD $[n_1 + n_2, k, d']$ code over $\mathbb{F}_q$ with $d' \geq d_1 + d_2$.*

Proof. Let G_1 and G_2 be generator matrices of a self-orthogonal $[n_1, k, d_1]$ code C_1 over $\mathbb{F}_q$ and an LCD $[n_2, k, d_2]$ code C_2 over $\mathbb{F}_q$, respectively. Consider an $[n_1+n_2, k, d']$ code C with generator matrix of the form $G = \begin{pmatrix} G_1 & G_2 \end{pmatrix}$.

Since $GG^T = G_2G_2^T$, C is LCD. The minimum weight of C follows from the minimum weights of C_1 and C_2. $\square$

Remark 8.2. Theorem 18 in [13] corresponds to the case $G_2 = I_k$.

By considering the case $q = 2$, the above proposition yields lower bounds on $d(n,k)$ as follow. There is a self-dual $[2k,k,2]$ code and there is self-orthogonal $[2k+1,k,2]$ code for $k \geq 1$. Hence, Proposition 8.1 gives

$$\begin{aligned} d(n+2k,k) &\geq d(n,k)+2 \text{ for } k \geq 1, \\ d(n+2k+1,k) &\geq d(n,k)+2 \text{ for } k \geq 1. \end{aligned}$$

In addition, it is known that there is a self-orthogonal code for the parameters $[7,3,4]$, $[8,4,4]$, $[11,5,4]$. Hence, Proposition 8.1 gives

$$\begin{aligned} d(n+7,3) &\geq d(n,3)+4, \\ d(n+8,4) &\geq d(n,4)+4, \\ d(n+11,5) &\geq d(n,5)+4. \end{aligned} \tag{27}$$

It is known that there is a self-dual $[n,n/2,d]$ code:

$$\begin{aligned} d &= 4 \text{ if and only if } n = 8, n \geq 12, \\ d &= 6 \text{ if and only if } n \geq 22, \\ d &= 8 \text{ if and only if } n = 24, 32, n \geq 36, \\ d &= 10 \text{ if and only if } n \geq 46, \end{aligned}$$

(see [6]). Hence, Proposition 8.1 gives

$$\begin{aligned} d(n+2k,k) &\geq d(n,k)+4 \text{ for } k \geq 6, \\ d(n+2k,k) &\geq d(n,k)+6 \text{ for } k \geq 11, \\ d(n+2k,k) &\geq d(n,k)+8 \text{ for } k = 12, 16, k \geq 18, \\ d(n+2k,k) &\geq d(n,k)+10 \text{ for } k \geq 23. \end{aligned}$$

As a consequence, we determine $d(n,4)$ for $n = 17, 18, 21, 25$.

Proposition 8.3.

$$d(17,4) = 8, d(18,4) = 8, d(21,4) = 10, d(25,4) = 12.$$

Proof. From Table 3, $d(n,4) = d$ for $(n,d) = (9,4), (10,4), (13,6)$. From (27), we have $d(17,4) \geq 8$, $d(18,4) \geq 8$ and $d(21,4) \geq 10$. Again, applying (27) to $d(17,4) \geq 8$, we have $d(25,4) \geq 12$. It is known that $d_{\text{all}}(17,4) = 8$, $d_{\text{all}}(18,4) = 8$, $d_{\text{all}}(21,4) = 10$ and $d_{\text{all}}(25,4) = 12$ (see [9]). The result follows. $\square$

Similarly, we have the following:

$$
\begin{array}{lll}
d(19,4) = 8 \text{ or } 9, & d(20,4) = 9 \text{ or } 10, & d(22,4) = 10 \text{ or } 11, \\
d(23,4) = 11 \text{ or } 12, & d(24,4) = 11 \text{ or } 12, & d(26,4) = 12 \text{ or } 13, \\
d(27,4) = 12, 13 \text{ or } 14, & d(28,4) = 13 \text{ or } 14, & d(29,4) = 14 \text{ or } 15.
\end{array}
$$

We remark that an LCD $[19,4,9]$ code is constructed in [13, Table 1]. Hence, $d(19,4) = 9$.

Acknowledgment. This work was supported by JSPS KAKENHI Grant Number 15H03633. The authors would like to thank Makoto Araya for his useful discussions.

References

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[2] C. Carlet and S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, In: E.R. Pinto et al. (eds.), Coding Theory and Applications, CIM Series in Mathematical Sciences, vol. 3, pp. 97–105, Springer, 2014.

[3] C. Carlet, S. Mesnager, C. Tang and Y. Qi, Euclidean and Hermitian LCD MDS codes, *Des. Codes Cryptogr.*, (to appear), arXiv:1702.08033.

[4] C. Carlet, S. Mesnager, C. Tang and Y. Qi, Linear codes over $\mathbb{F}_q$ which are equivalent to LCD codes, *IEEE Trans. Inform. Theory*, (to appear), arXiv:1703.04346.

[5] R.J. Clarke, Covering a set by subsets, *Discrete Math.* **81** (1990), 147–152.

[6] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1990), 1319–1333.

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

[8] L. Galvez, J.-L. Kim, N. Lee, Y.G. Roe and B.-S. Won, Some bounds on binary LCD codes, *Cryptogr. Commun.*, (to appear), arXiv:1701.04165.

[9] M. Grassl, Code tables: Bounds on the parameters of various types of codes, Available online at `http://www.codetables.de/`, Accessed on 2018-01-22.

[10] C. G̈uneri, B. Özkaya and P. Solé, Quasi-cyclic complementary dual codes, *Finite Fields Appl.* **42** (2016), 67–80.

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

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

[13] E.R. Lina, Jr. and E.G. Nocon, On the construction of some LCD codes over finite fields, *Manila J. Science* **9** (2016), 67–82.

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

[15] N. Sloane and S. Plouffe, The Encyclopedia of Integer Sequences, Academic Press, San Diego, CA, 1995 (Available online at `https://oeis.org`).