Some Bounds on Binary LCD Codes

Lucky Galvez∗ Jon-Lark Kim† Nari Lee‡ Young Gun Roe§
Byung-Sun Won¶

Abstract

A linear code with a complementary dual (or LCD code) is defined to be a linear code $C$ whose dual code $C^\perp$ satisfies $C \cap C^\perp = \{0\}$. Let $\text{LCD}[n,k]$ denote the maximum of possible values of $d$ among $[n,k,d]$ binary LCD codes. We give exact values of $\text{LCD}[n,k]$ for $1 \leq k \leq n \leq 12$. We also show that $\text{LCD}[n,n-i] = 2$ for any $i \geq 2$ and $n \geq 2^i$. Furthermore, we show that $\text{LCD}[n,k] \leq \text{LCD}[n,k-1]$ for $k$ odd and $\text{LCD}[n,k] \leq \text{LCD}[n,k-2]$ for $k$ even.

Keywords : binary LCD codes bounds linear code

1 Introduction

A linear code with complementary dual (or LCD code) was first introduced by Massey [7] as a reversible code in 1964. Afterwards, LCD codes were extensively studied in literature and widely applied in data storage, communications systems, consumer electronics, and cryptography.

In [8], Massey showed that there exist asymptotically good LCD codes. Esmaeili and Yari [6] identified a few classes of LCD quasi-cyclic codes. For bounds of LCD codes, Tzeng and Hartmann [12] proved that the minimum distance of a class of reversible codes is greater than that given by the BCH bound. Sendrier [11] showed that LCD codes meet the asymptotic Gilbert-Varshamov bound using the hull dimension spectra of linear codes. Recently, Dougherty et al. [5] gave a linear programming bound on the largest size of an LCD $[n,d]$. Constructions of LCD codes were studied by Mutto and Lal [10]. Yang and Massey [15] gave a necessary and sufficient condition for a cyclic code to have a complementary dual. It is also shown by Kandasamy et al. [13] that maximum rank distance codes generated by the trace-orthogonal-generator matrices are LCD codes. In 2014, Calet and Guilley [3] introduced several constructions of LCD codes and investigated an application of LCD codes against side-channel attacks (SCA). Shortly after, Mesnager et al. [9] provided a construction of algebraic geometry LCD codes which could be good candidates to be resistant against SCA. Recently Ding et al. [4] constructed several families of reversible cyclic codes over finite fields.

The purpose of this paper is to study exact values of $\text{LCD}[n,k]$ (see [2]) which is the maximum of possible values of $d$ among $[n,k,d]$ binary LCD codes. We give exact values of $\text{LCD}[n,2]$ in Section

∗Department of Mathematics, Sogang University, Seoul 04107, South Korea. Email: legalvez97@gmail.com
†Department of Mathematics, Sogang University, Seoul 04107, South Korea. Email: jlkim@sogang.ac.kr
‡Department of Mathematics, Sogang University, Seoul 04107, South Korea. Email: narilee3@gmail.com
§Department of Mathematics, Sogang University, Seoul 04107, South Korea. Email: ygroevnaver.com
¶Department of Mathematics, Sogang University, Seoul 04107, South Korea. Email: byungsun08@gmail.com
In Section 3, we investigate \(LCD[n, k]\) and show that \(LCD[n, n - i] = 2\) for any \(i \geq 2\) and \(n \geq 2\). We prove that \(LCD[n, k] \leq LCD[n, k - 1]\) for \(k\) odd and that \(LCD[n, k] \leq LCD[n, k - 2]\) for \(k\) even using the notion of principal submatrices. In Section 4, we give exact values for \(LCK[n, d]\).

We have included tables for \(LCD[n, k]\) for \(1 \leq k \leq n \leq 12\) and \(LCK[n, d]\) for \(1 \leq d \leq n \leq 12\).

\[2\] LCD\([n, 2]\]

Let \(GF(q)\) be the finite field with \(q\) elements. An \([n, k]\) code \(C\) over \(GF(q)\) is a \(k\)-dimensional subspace of \(GF(q)^n\). If \(C\) is a linear code, we let

\[C^\perp = \{u \in V \mid u \cdot w = 0 \text{ for all } w \in C\}\]

We call \(C^\perp\) the dual or orthogonal code of \(C\).

**Definition 2.1.** A linear code with complementary dual (LCD code) is a linear code \(C\) satisfying \(C \cap C^\perp = \{0\}\).

We note that if \(C\) is an LCD code, then so is \(C^\perp\) because \((C^\perp)^\perp = C\). The following proposition will be frequently used in the later sections.

**Proposition 2.2.** (8)

Let \(G\) be a generator matrix for a code over \(GF(q)\). Then \(\det(GG^T) \neq 0\) if and only if \(G\) generates an LCD code.

Throughout the rest of the paper, we consider only binary codes. Dougherty et al. [5] introduced \(LCD[n, k]\) which denotes the maximum of possible values of \(d\) among \([n, k, d]\) binary LCD codes. Formally we can define it as follows.

**Definition 2.3.** \(LCD[n, k] := \max\{d \mid \text{there exists a binary } [n, k, d] \text{ LCD code}\}\).

Dougherty et al. [5] gave a few bounds on \(LCD[n, k]\) and exact values of \(LCD[n, k]\) for \(k = 1\) only.

Now we obtain exact values of \(LCD[n, k]\) for \(k = 2\) for any \(n\).

**Lemma 2.4.** \(LCD[n, 2] \leq \left\lfloor \frac{2n}{3} \right\rfloor\) for \(n \geq 2\).

**Proof.** By the Griesmer Bound [14], any binary linear \([n, k, d]\) code satisfies

\[n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil\]

Letting \(k = 2\), we have \(n \geq d + \frac{d}{2}\). Hence

\[d \leq \left\lfloor \frac{2n}{3} \right\rfloor\]

Therefore any LCD \([n, k, d]\) code must satisfy this inequality. \(\square\)

**Proposition 2.5.** Let \(n \geq 2\). Then \(LCD[n, 2] = \left\lceil \frac{2n}{3} \right\rceil\) for \(n \equiv 1, \pm 2, \text{ or } 3 \pmod{6}\).
Proof. We only need to show the existence of LCD codes with minimum distance achieving the bound \( d = \lfloor \frac{2n}{3} \rfloor \).

(i) Let \( n \equiv 1 \pmod{6} \), i.e. \( n = 6m + 1 \) for some positive integer \( m \). Consider the code with generator matrix
\[
G = \begin{bmatrix}
1 & \ldots & 1 \\
0 & \ldots & 1 \\
2m + 1 & 2m - 1 & 2m + 1
\end{bmatrix}.
\]

This code has minimum weight \( 4m = \lfloor \frac{2(6m+1)}{3} \rfloor \) and \( GG^T = \begin{bmatrix} 0 & 1 \end{bmatrix} \), i.e., \( \det(GG^T) = 1 \neq 0 \). Therefore this code is an LCD code.

(ii) Let \( n \equiv \pm 2 \pmod{6} \), i.e., \( n = 6m + 2 \) for some non negative integer \( m \), or \( n = 6m - 2 \) for some positive integer \( m \). Consider the code with generator matrix
\[
G = \begin{bmatrix}
1 & \ldots & 1 \\
0 & \ldots & 1 \\
2m + k & 2m & 2m + k
\end{bmatrix}
\]
for \( k = 1, -1 \).

If \( k = 1 \), this code has minimum weight \( 4m + 1 = \lfloor \frac{2(6m+2)}{3} \rfloor \) and \( GG^T = \begin{bmatrix} 1 & 0 \end{bmatrix} \), i.e., \( \det(GG^T) = 1 \neq 0 \). Therefore this code is an LCD code.

If \( k = -1 \), this code has minimum weight \( 4m - 2 = \lfloor \frac{2(6m-2)}{3} \rfloor \) and \( GG^T = \begin{bmatrix} 1 & 0 \end{bmatrix} \), i.e., \( \det(GG^T) = 1 \neq 0 \). Therefore this code is an LCD code.

(iii) Let \( n \equiv 3 \pmod{6} \), i.e., \( n = 3i \) for some positive odd integer \( i \). Consider the code with generator matrix
\[
G = \begin{bmatrix}
1 & \ldots & 1 \\
0 & \ldots & 1 \\
i & \ldots & i
\end{bmatrix}.
\]

This code has minimum weight \( 2i = \lfloor \frac{2(3i)}{3} \rfloor \) and \( GG^T = \begin{bmatrix} 0 & 1 \end{bmatrix} \), i.e., \( \det(GG^T) = 1 \neq 0 \). Therefore this code is an LCD code.

Proposition 2.6. Let \( n \geq 2 \). Then \( \text{LCD}[n, 2] = \lfloor \frac{2n}{3} \rfloor - 1 \) for \( n \equiv 0, -1 \pmod{6} \).

Proof. (i) Let \( n \equiv 0 \pmod{6} \). Consider the generator matrix \( G \) in (iii) of the proof of Proposition 2.5 this time taking \( i \) to be an even integer. If the weight of any row of \( G \) is increased by one, the weight of the sum of the two rows is decreased by one. Hence, \( G \) is the only generator matrix for a binary code that achieves the upper bound, up to equivalence. Clearly, \( \det(GG^T) = 0 \) and so the code is not LCD. It follows that there are no LCD code with minimum distance \( \lfloor \frac{2n}{3} \rfloor \) for \( n \equiv 0 \pmod{6} \).

Next, consider the code with generator matrix
\[
G = \begin{bmatrix}
1 & \ldots & 1 \\
0 & \ldots & 1 \\
i + 1 & i - 1 & i
\end{bmatrix}.
\]
This code has minimum weight \(2i - 1 = \left\lfloor \frac{2(3i-1)}{3} \right\rfloor - 1\). We note that \(GG^T = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\), i.e., \(\det(GG^T) = 1 \neq 0\). Therefore this code is an LCD code.

(ii) Let \(C\) be a binary code of length \(n \equiv -1 \ (\text{mod } 6)\), i.e., \(n = 3i - 1\) for some positive even \(i\). Without loss of generality, the generator matrix for \(C\) can be expressed in the following form such that the first row is the codeword whose weight is the minimum weight \(d\).

\[
G = \begin{bmatrix}
1 & \cdots & 1 \\
0 & \ldots & 0 \\
i_1 & \ldots & i_2 \\
i_2 & \ldots & i_3
\end{bmatrix}
\]

Suppose \(d = \left\lfloor \frac{2(3i-1)}{3} \right\rfloor = 2i - 1\), i.e., \(i_1 + i_2 = 2i - 1\). This implies that \(i_3 = i\). Note that \(i_2 + i_3 \geq 2i - 1\) which implies \(i_2 \geq i - 1\) and \(i_1 + i_3 \geq 2i - 1\) which implies \(i_2 \geq i - 1\). This leaves only two possible cases: \((i_1, i_2, i_3) = (i - 1, i, i)\), \((i, i - 1, i)\), each of which gives \(GG^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\), \(\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\), respectively. In both cases, \(\det(GG^T) = 0\) and therefore they are not LCD. So there is no LCD code with minimum distance \(\left\lfloor \frac{24}{3} \right\rfloor\) for \(n \equiv -1 \ (\text{mod } 6)\).

Consider the case where \((i_1, i_2, i_3) = (i - 1, i - 1, i + 1)\). Then \(G\) generates a code of minimum distance \(2i - 2 = \left\lfloor \frac{2(3i-1)}{3} \right\rfloor - 1\). For this case, \(\det(GG^T) = 1\) and hence the code is LCD.

\[\square\]

3 \(\text{LCD} \ [n, k]\)

We begin with a rather straightforward lemma in order to prove Proposition 4.

**Lemma 3.1.** If \(n \geq 8\), any \([n, n - 3, d]\) binary code \(C\) satisfies \(d \leq 2\).

**Proof.** Let \(G\) be a standard generator matrix of \(C\), i.e., \(G = [I_{n-3} \mid A]\) where \(A\) is an \((n - 3) \times 3\) matrix. By the Singleton bound, \(d \leq 4\). But it is well known there is no non-trivial binary code achieving the bound. Thus, we may say that \(d \leq 3\). Suppose \(d = 3\). Then each row of \(A\) must have weight at least 2. However there are only \(\binom{3}{2} + \binom{3}{3} = 4\) possible choices for the rows of \(A\). Note that \(A\) has at least 5 rows and this contradict our assumption that \(d = 3\). Hence \(d \leq 2\).

\[\square\]

Motivated by the above lemma, we can consider more general dimension \(n - i\) rather than \(n - 3\) as follows.

**Proposition 3.2.** Given \(i \geq 2\), \(\text{LCD} \ [n, n - i] = 2\) for all \(n \geq 2^i\).

**Proof.** Let \(G\) be a standard generator matrix of an \([n, n - i, d]\) binary code \(C\), i.e., \(G = [I_{n-i} \mid A]\) where \(A\) is an \((n - i) \times i\) matrix. By the Singleton bound, \(d \leq i + 1\). But there is no non-trivial binary code achieving the bound. Thus, we may say that \(d \leq i\). If the minimum distance of \(C\) is at least 3, each row of \(A\) must have weight at least 2. And there are \(\binom{i}{2} + \binom{i}{3} + \cdots + \binom{i}{i} = 2^i - i - 1\) possible choices for the rows of \(A\). Thus, if \(n - i\) (number of rows in \(A\)) \(> 2^i - i - 1\), then there exists a row of weight 1 in \(A\). This forces the minimum distance of \(C\) to be 2, which is a contradiction. Therefore, \(d \leq 2\) for all \(n \geq 2^i\). Since this statement holds true for any linear code, it holds true for LCD codes as well, i.e., \(\text{LCD} \ [n, n - i] \leq 2\) for all \(n \geq 2^i\).
Next, we show that there exists an $[n, n-i, 2]$ LCD code for $n \geq 2^i$. For $i$ even, let $G = [I_{n-i} | 1 \cdots 1]$, and for $i$ odd, let $G = [I_{n-i} | 1 \cdots 10]$ where 1 denotes the all one vector and 0 the all zero vector, both of which are of size $(n-i) \times 1$. In both cases, $GG^T = I_{n-i}$. Thus, $G$ is a generator matrix for the $[n, n-i]$ LCD code with minimum distance 2.

Hence $LCD[n, n-i] = 2$ for all $n \geq 2^i$.

So far we have shown the exact value of $LCD[n, 2]$. The relation between $LCD[n, k]$ and $LCD[n, k-1]$ (or $LCD[n, k-2]$) was unknown before. Using the idea of principal submatrices, we have Proposition 3.5 below.

**Definition 3.3.** Let $A$ be a $k \times k$ matrix over a field. An $m \times m$ submatrix $P$ of $A$ is called a principal submatrix of $A$ if $P$ is obtained from $A$ by removing all rows and columns of $A$ indexed by the same set $\{i_1, i_2, \ldots, i_{n-m}\} \subset \{1, 2, \ldots, k\}$.

**Definition 3.4.** Let $A$ be a $k \times k$ symmetric matrix over a field. The principal rank characteristic sequence of $A$ (simply, pr-sequence of $A$ or $pr(A)$) is defined as $pr(A) = r_0 \mid r_1 r_2 \ldots r_k$ where for $1 \leq m \leq k$

$$r_m = \begin{cases} 
1 & \text{if } A \text{ has an } m \times m \text{ principal submatrix of rank } m \\
0 & \text{otherwise}
\end{cases}$$

For convenience, define $r_0 = 1$ if and only if $A$ has a 0 in the diagonal.

**Proposition 3.5.** Let $A$ be a $k \times k$ symmetric matrix over a field with characteristic 2, a principal rank characteristic sequence of a $k \times k$ symmetric matrix $A$ is attainable if and only if it has one of the following forms:

(i) $0 \mid 1 \overline{10}$

(ii) $1 \mid 0 \overline{10}$

(iii) $1 \mid 1 \overline{10}$

where $\overline{1} = 11\ldots1$ (or empty), $\overline{0} = 00\ldots0$ (or empty), $\overline{10} = 0101\ldots01$ (or empty).

**Proposition 3.6.** We have the following:

(i) If $k \geq 3$ and $k$ is odd,

$$LCD[n, k] \leq LCD[n, k-1]$$

for any $n \geq k$.

(ii) If $k \geq 4$ and $k$ is even,

$$LCD[n, k] \leq LCD[n, k-2]$$

for any $n \geq k$.

**Proof.** (i) It suffices to show that any binary $[n, k]$ LCD code $C$ has an $[n, k-1]$ LCD subcode for any odd $k \geq 3$. Let $G$ be a $k \times n$ generator matrix of $C$. Let $A = GG^T$ which is symmetric. Then $rank(A) = k$. Since $k$ is odd, case (ii) of Proposition 3.5 is not possible. Thus the only possible cases are (i) and (iii) of Proposition 3.5 which are $0 \mid 11\ldots1$ and $1 \mid 11\ldots1$, respectively. Hence,
there exists a principal submatrix $P_1$ of rank $k - 1$ which is obtained from $A$ by deleting some $i^{th}$ row and column of $A$ ($1 \leq i \leq k$).

Define $G_1$ to be a $(k - 1) \times n$ matrix obtained from $G$ by deleting the $i^{th}$ row of $G$. Since $G_1G_1^T = P_1$ and $\text{rank}(P_1) = k - 1 \neq 0$, $P_1$ is invertible. Then the linear code $C_1$ with generator matrix $G_1$ is LCD as well.

(ii) It suffices to show that any binary $[n, k]$ LCD code $C$ has an $[n, k - 2]$ LCD subcode for any even $k \geq 4$. Let $G$ be a $k \times n$ generator matrix of $C$ and $A = GG^T$. Then $\text{rank}(A) = k$ since $C$ is LCD. By Proposition 3.5, we have the following three cases.

(i) $0|1\ldots 1$  
(ii) $1|01\ldots 01$  
(iii) $1|1\ldots 1$

So there exists a principal submatrix $P_2$ of rank $k - 2$ which is obtained from $A$ by deleting some $i^{th}$, $j^{th}$ rows and columns of $A$ ($1 \leq i \neq j \leq k$).

Define $G_2$ to be a $(k - 2) \times n$ matrix obtained from $G$ by deleting the $i^{th}$ and $j^{th}$ rows of $G$. Since $G_2G_2^T = P_2$ and $\text{rank}(P_2) = k - 2 \neq 0$, $P_2$ is invertible. Then the linear $[n, k - 2]$ code $C_2$ with generator matrix $G_2$ is LCD as well.

Since the minimum distance of a code is always less than or equal to the minimum distance of a subcode, this completes the proof of (a) and (b).

In Table 1 we give exact values of $LCD[n, k]$ for $1 \leq k \leq n \leq 12$. Based on Proposition 3.6 and Table 1, we conjecture the following.

**Conjecture** If $2 \leq k \leq n$, then $LCD[n, k] \leq LCD[n, k - 1]$.

(Note: It suffices to show that this is true when $k$ is even.)

---

### Table 1: $LCD[n, k]$ for $1 \leq k \leq n \leq 12$

| $n/k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|-------|---|---|---|---|---|---|---|---|---|----|----|----|
| 1     | 1 |   |   |   |   |   |   |   |   |    |    |    |
| 2     | 1 | 1 |   |   |   |   |   |   |   |    |    |    |
| 3     | 3 | 2 | 1 |   |   |   |   |   |   |    |    |    |
| 4     | 3 | 2 | 1 | 1 |   |   |   |   |   |    |    |    |
| 5     | 5 | 2 | 2 | 1 |   |   |   |   |   |    |    |    |
| 6     | 5 | 3 | 2 | 1 | 1 |   |   |   |   |    |    |    |
| 7     | 7 | 4 | 2 | 2 | 2 | 1 |   |   |   |    |    |    |
| 8     | 7 | 5 | 3 | 2 | 2 | 1 | 1 |   |   |    |    |    |
| 9     | 9 | 6 | 4 | 3 | 2 | 2 | 2 | 1 |   |    |    |    |
| 10    | 9 | 6 | 5 | 4 | 3 | 2 | 2 | 1 | 1 |    |    |    |
| 11    | 11| 6 | 5 | 4 | 3 | 3 | 2 | 1 | 2 | 1 |    |    |
| 12    | 11| 7 | 6 | 5 | 4 | 3 | 3 | 2 | 1 | 1 | 1 |    |

---

4 **$LCK\ [n, d]$**

We define another combinatorial function $LCK\ [n, d]$. 

---
Definition 4.1. \( LCK[n, d] := \max\{k \mid \text{there exists a binary } [n, k, d] \text{ LCD code}\} \)

For convenience, define \( LCK[n, d] = 0 \) if and only if there is no LCD code with the given \( n \) and \( d \).

| \( n/d \) | 1   | 2   | 3   | 4   | 5   | 6   | 7   | 8   | 9   | 10  | 11  | 12  |
|-------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 1     | 1   |     |     |     |     |     |     |     |     |     |     |     |
| 2     | 2   | 0   |     |     |     |     |     |     |     |     |     |     |
| 3     | 3   | 2   | 1*  |     |     |     |     |     |     |     |     |     |
| 4     | 4   | 2   | 1*  | 0   |     |     |     |     |     |     |     |     |
| 5     | 5   | 4   | 1   | 0   | 1   |     |     |     |     |     |     |     |
| 6     | 6   | 4   | 2   | 2   | 1*  | 0   |     |     |     |     |     |     |
| 7     | 7   | 6   | 3   | 2   | 1*  | 0   | 1   |     |     |     |     |     |
| 8     | 8   | 6   | 4   | 2   | 2   | 0   | 1*  | 0   |     |     |     |     |
| 9     | 9   | 8   | 5   | 4   | 2*  | 2   | 0   | 0   | 0   |     |     |     |
| 10    | 10  | 8   | 6   | 4   | 3   | 3   | 2   | 1   | 0   | 1   | 0   | 0   |
| 11    | 11  | 10  | 7   | 6   | 3   | 2   | 1   | 0   | 0   | 1   | 0   |     |
| 12    | 12  | 10  | 7   | 6   | 4   | 3   | 2*  | 0   | 1   | 0   | 1*  | 0   |

Table 2: \( LCK[n, d] \) for \( 1 \leq d \leq n \leq 12 \)

It is noticeable in Table 2 that more zeros appear as \( n \) gets larger. Dougherty et al. [5] showed \( LCK[n, d] = 0 \) for \( n \) even and when \( d = n \). Now we show that this is a special case of the following general proposition.

Proposition 4.2.  
(i) Suppose that \( n \) is even, \( k \geq 1 \), and \( i \geq 0 \). If \( n \geq 6i \), then there is no \([n, k, n - 2i] \) LCD code, i.e., \( LCK[n, n - 2i] = 0 \).

(ii) Suppose that \( n \) is odd, \( k \geq 1 \), and \( i \geq 0 \). If \( n > 6i + 3 \), then there is no \([n, k, n - 2i - 1] \) LCD code, i.e., \( LCK[n, n - 2i - 1] = 0 \).

Proof.  
(i) Suppose \( C \) is an LCD \([n, k, n - 2i] \) code with parameters in the hypothesis. Let \( G \) be a generator matrix of \( C \).

If \( k = 1 \), then \( GG^T = 0 \) since the minimum distance \( n - 2i \) is even. Then by Proposition 2.2 there is no \([n, 1, n - 2i] \) LCD code with \( n \) even.

Now suppose \( k \geq 2 \). Then there should exist an LCD \([n, 2, n - 2i] \) subcode of \( C \). By the Griesmer Bound with \( k = 2 \), we obtain \( n \geq n - 2i + \frac{n - 2i}{2} \) which implies \( n \leq 6i \). Thus we can say that there is no \([n, 2, n - 2i] \) code if \( n > 6i \). When \( n \) meets the Griesmer Bound, i.e., \( n = 6i \), there is no \([6i, 2, 4i] \) LCD code because by Proposition 2.3 the maximum of the possible minimum distance among any \([6i, 2] \) LCD codes is \( 4i - 1 \).

(ii) A similar argument to (i) shows that there is no \([n, 1, n - 2i - 1] \) LCD code with \( n \) odd because the minimum distance \( n - 2i - 1 \) is even.

Suppose \( k \geq 2 \). Then there should exist an LCD \([n, 2, n - 2i - 1] \) subcode of \( C \). By the Griesmer Bound with \( k = 2 \), we have \( n \geq n - 2i - 1 + \frac{n - 2i - 1}{2} \) which implies \( n \leq 6i + 3 \). Thus we can say that there is no \([n, 2, n - 2i - 1] \) code if \( n > 6i + 3 \). That is, there is no such an LCD code. \( \square \)
In Table 2, the values of $LCK[n,d]$ are given for $1 \leq d \leq n \leq 12$. These values are obtained using Table 1, Proposition 4.2, and two tables from [5]. The values with * are the ones that are corrected here as they are incorrectly reported in Table 1 of [5].

5 Appendix

Below is an exhaustive search program written by MAGMA [2] in order to compute $LCD[n,k]$ which run slowly for large $n$ and $k$.

```plaintext
LCD:=function(n,k)
    I:=IdentityMatrix(GF(2),k);
    Max:=0;
    for g in RMatrixSpace(GF(2),k,n-k) do
        if Determinant(I+(g*Transpose(g))) eq 1
            then if Max lt MinimumDistance
                (LinearCode(HorizontalJoin(I,g)))
                then Max:=MinimumDistance
                    (LinearCode(HorizontalJoin(I,g)));
            end if;
        end if;
    end for;
    return Max;
end function;
```

References

[1] Barret, W., Butler, S., Catral, M., Fallat, S.M., Hall, H.T., Hogben, L., Driessche, P.van den, Young, M.: The principal rank characteristic sequence over various fields. Linear Algebra and its Applications. 459, 222-236 (2014)

[2] Bosma, W., Cannon, J.: Handbook of Magma functions, Sydney (1995)

[3] Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. In Coding Theory and Applications. Springer International Publishing, 97-105 (2015)

[4] Ding, C., Li, C., Li, S.: LCD cyclic codes over finite fields. arXiv preprint arXiv:1608.02170 (2016)

[5] Dougherty, S.T. Kim, J.-L., Ozkaya, B., Sok, L., Sole, P.: The combinatorics of LCD codes : Linear Programming bound and orthogonal matrices. Submitted to Linear Algebra and Applications on June, 1 (2015)

[6] Esmaeili, M., S. Yari.: On complementary-dual quasi-cyclic codes. Finite Fields and Their Applications 15, no. 3, 375-386 (2009)

[7] Massey, J. L.: Reversible codes. Information and Control, 7(3), 369-380 (1964)
[8] Massey, J. L.: Linear Codes with Complementary Duals. Discrete Mathematics. 106-107, 337-342 (1992)

[9] Mesnager, S., Tang, C., Qi, Y.: Complementary Dual Algebraic Geometry Codes. arXiv preprint arXiv:1609.05649 (2016)

[10] Muttoo, S.K., Lal, S.: A reversible code over $GF(q)$. Kybernetika, 22(1), 85-91 (1986)

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

[12] Tzeng, K., Hartmann, C.: On the minimum distance of certain reversible cyclic codes (Corresp.). IEEE Transactions on Information Theory. 16(5), 644-646 (1970)

[13] Kandasamy, W.V., Smarandache, F., Sujatha, R., Duray, R.R.: Erasure Techniques in MRD codes. Infinite Study (2012)

[14] Huffman, W.C., Pless, V.: Fundamentals of error-correcting codes. Cambridge university press (2010)

[15] Yang, X., Massey, J.L.: The condition for a cyclic code to have a complementary dual. Discrete Mathematics. 126(1-3), 391-393 (1994)