Cryptogr. Commun. (2018) 10:719–728
https://doi.org/10.1007/s12095-017-0258-1

Some bounds on binary LCD codes

Lucky Galvez[1] · Jon-Lark Kim[1] · Nari Lee[1] · Young Gun Roe[1] · Byung-Sun Won[1]

Received: 14 January 2017 / Accepted: 14 September 2017 / Published online: 26 September 201 7

Abstract A linear code with a complementary dual (or An LCD code) is defined to be a linear code C whose dual code $C^{\perp}$ satisfies $C \cap C^{\perp} = \{\mathbf{0}\}$. Let $LD(n, k)$ denote the maximum of possible values of d among $[n, k, d]$ binary LCD codes. We give the exact values of $LD(n, k)$ for $k = 2$ for all n and some bounds on $LD(n, k)$ for other cases. From our results and some direct search we obtain a complete table for the exact values of $LD(n, k)$ for $1 \leq k \leq n \leq 12$. As a consequence, we also derive bounds on the dimensions of LCD codes with fixed lengths and minimum distances.

Keywords Binary LCD codes · Bounds · Linear codes

Mathematics Subject Classification (2010) 94B05 · 94B65

1 Introduction

A linear code with complementary dual (or An LCD code) was first introduced by Massey [14] as a reversible code in 1964. Afterwards, LCD codes were extensively

✉ Jon-Lark Kim
jlkim@sogang.ac.kr

Lucky Galvez
legalvez97@gmail.com

Nari Lee
narilee3@gmail.com

Young Gun Roe
ygroe@naver.com

Byung-Sun Won
byungsun08@gmail.com

1 Department of Mathematics, Sogang University, Seoul 04107, South Korea

studied in literature and widely applied in data storage, communications systems, consumer electronics, and cryptography.

In [15] Massey showed that there exist asymptotically good LCD codes. Yang and Massey [23] gave a necessary and sufficient condition for a cyclic code to have a complementary dual. In [7] Esmaeili and Yari identified a few classes of LCD quasi-cyclic codes. It is shown by Kandasamy et al. [21] that maximum rank distance codes generated by the trace-orthogonal-generator matrices are LCD codes. Recently, Boonniyoma et al. [2] determined necessary and sufficient conditions for a linear code to be Hermitian complementary dual. Quasi-cyclic codes that are complementary dual are characterized and studied by using their concatenated structure by Güneri et al. [8]. In [18] Sari et al. obtained two classes of MDS negacyclic LCD codes. Zhu et al. [24] deduced the structure of the reversible negacyclic code over some finite fields. Li et al. studied a family of BCH codes over finite fields in [11] and extended the results to parameters of LCD BCH codes in [12].

For bounds of LCD codes, Tzeng and Hartmann [20] proved that the minimum distance of a class of reversible codes is greater than that given by the BCH bound. Sendrier [19] showed that LCD codes meet the asymptotic Gilbert-Varshamov bound using the hull dimension spectra of linear codes. Recently, Dougherty et al. [6] gave a linear programming bound on the largest size of an LCD code of a given length and minimum distance.

Constructions of LCD codes were studied by Mutto and Lal [17]. In 2014, Carlet and Guilley [4] introduced several constructions of LCD codes and investigated an application of LCD codes against side-channel attacks (SCA). Shortly after, Mesnager et al. [16] provided a construction of algebraic geometry LCD codes which could be good candidates to be resistant against SCA. Ding et al. [5] constructed several families of reversible cyclic codes over finite fields. Recently, Liu et al. [13] constructed LCD codes using quasi-orthogonal matrices. Jin [9] used generalized Reed-Solomon codes to contruct several classes of LCD MDS codes. In 2017, Li [10] showed construction of some cyclic Hermitian LCD codes over finite fields and employed Hermitian LCD codes to propose a Hermitian orthogonal direct sum masking scheme that achieves protection against fault injection attacks.

The purpose of this paper is to study exact values of $LD(n, k)$ (see [6]) which is the maximum of possible values of d among $[n, k, d]$ binary LCD codes. We give exact values of $LD(n, 2)$ in Section 2. In Section 3, we investigate $LD(n, k)$ and show that $LD(n, n - i) = 2$ for any $i \geq 2$ and $n \geq 2^i$. We prove that $LD(n, k) \leq LD(n, k-1)$ for k odd and that $LD(n, k) \leq LD(n, k-2)$ for k even using the notion of principal submatrices. In Section 4, we give exact values for $LK(n, d)$, the maximum dimension k such that an $[n, k, d]$ LCD code exists for a given n and d. We have included tables for $LD(n, k)$ for $1 \leq k \leq n \leq 12$ and $LK(n, d)$ for $1 \leq d \leq n \leq 12$.

2 Bounds on minimum distances of $[n, 2]$ LCD codes

We begin by giving some definitions related to LCD codes.

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

$$C^{\perp} = \left\{ \mathbf{u} \in GF(q)^n \mid \mathbf{u} \cdot \mathbf{w} = 0 \text{ for all } \mathbf{w} \in C \right\}.$$

We call $C^{\perp}$ the *dual* or *orthogonal* code of C.

Definition 1 A *linear code with complementary dual* (An LCD code) is a linear code C satisfying $C \cap C^{\perp} = \{\mathbf{0}\}$.

Note that if C is an LCD code, then so is $C^{\perp}$ because $(C^{\perp})^{\perp} = C$. The following proposition, found in [15], will be frequently used in the later sections.

Proposition 1 *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 this paper, we consider only binary codes. Dougherty et al. [6] introduced the combinatorial function $LCD[n, k]$, for integers n and k such that $n \geq k$, which denotes the maximum of possible values of d among $[n, k, d]$ binary LCD codes. We use $LD(n, k)$ instead of $LCD[n, k]$ in order to avoid any confusion. Formally, it is defined as follows.

Definition 2 $LD(n, k) := \max\{d \mid \text{there exists a binary } [n, k, d] \text{ LCD code}\}$.

Dougherty et al. [6] gave a few bounds on $LD(n, k)$ and exact values for $k = 1$.

Now we obtain exact values of $LD(n, k)$ for $k = 2$ and arbitrary n. First, we give a simple upper bound for the minimum distance of binary $[n, k]$ LCD codes.

Lemma 1 $LD(n, 2) \leq \left\lfloor \frac{2n}{3} \right\rfloor$ *for $n \geq 2$.*

Proof By the Griesmer Bound [22], 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 $[n, 2, d]$ LCD code must satisfy this inequality. □

Based on the bound given above, we can obtain the exact values of $LD(n, 2)$.

Theorem 1 *Let $n \geq 2$. Then $LD(n, 2) = \left\lfloor \frac{2n}{3} \right\rfloor$ for $n \equiv 1, \pm 2,$ or $3 \pmod 6$.*

Proof We only need to show the existence of LCD codes with minimum distance achieving the bound $d = \left\lfloor \frac{2n}{3} \right\rfloor$.

(i) Let $n \equiv 1 \pmod 6$, i.e. $n = 6m + 1$ for some positive integer m. Consider the code with generator matrix

$$G = \left[\underbrace{\begin{matrix} 1 \dots 1 \\ 0 \dots 0 \end{matrix}}_{2m+1} \middle| \underbrace{\begin{matrix} 1 \dots 1 \\ 1 \dots 1 \end{matrix}}_{2m-1} \middle| \underbrace{\begin{matrix} 0 \dots 0 \\ 1 \dots 1 \end{matrix}}_{2m+1} \right].$$

This code has minimum weight $4m = \left\lfloor \frac{2(6m+1)}{3} \right\rfloor$ and $GG^T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, 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

$$G = \left[\begin{array}{c|c|c} \underbrace{\begin{matrix} 1\dots1 \\ 0\dots0 \end{matrix}}_{2m+k} & \underbrace{\begin{matrix} 1\dots1 \\ 1\dots1 \end{matrix}}_{2m} & \underbrace{\begin{matrix} 0\dots0 \\ 1\dots1 \end{matrix}}_{2m+k} \end{array}\right]$$

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

If $k = -1$, this code has minimum weight $4m - 2 = \left\lfloor \frac{2(6m-2)}{3} \right\rfloor$ and $GG^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, 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

$$G = \left[\begin{array}{c|c|c} \underbrace{\begin{matrix} 1\dots1 \\ 0\dots0 \end{matrix}}_{i} & \underbrace{\begin{matrix} 1\dots1 \\ 1\dots1 \end{matrix}}_{i} & \underbrace{\begin{matrix} 0\dots0 \\ 1\dots1 \end{matrix}}_{i} \end{array}\right].$$

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

$\square$

Theorem 2 *Let $n \geq 2$. Then $LD(n, 2) = \left\lfloor \frac{2n}{3} \right\rfloor - 1$ 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 Theorem 1, 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 is no LCD code with minimum distance $\left\lfloor \frac{2n}{3} \right\rfloor$ for $n \equiv 0 \pmod 6$.

Next, consider the code with generator matrix

$$G = \left[\begin{array}{c|c|c} \underbrace{\begin{matrix} 1\dots1 \\ 0\dots0 \end{matrix}}_{i+1} & \underbrace{\begin{matrix} 1\dots1 \\ 1\dots1 \end{matrix}}_{i-1} & \underbrace{\begin{matrix} 0\dots0 \\ 1\dots1 \end{matrix}}_{i} \end{array}\right]$$

This code has minimum weight $2i - 1 = \left\lfloor \frac{2(3i)}{3} \right\rfloor - 1$. 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 $n \equiv -1 \pmod 6$, 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.

$$G = \left[\begin{array}{c|c|c} 1\dots1 & 1\dots1 & 0\dots0 \\ 0\dots0 & 1\dots1 & 1\dots1 \end{array} \right]$$
$$\qquad\;\; \underbrace{}_{i_1} \; \underbrace{}_{i_2} \; \underbrace{}_{i_3}$$

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

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.

□

So far we have obtained exact values for $LD(n, 2)$. As in Lemma 1, we can have an upper bound for $LD(n, k)$ for $k \geq 3$ as follows.

Lemma 2 *$LD(n, k) \leq \left\lfloor \frac{n \cdot 2^{k-1}}{2^k - 1} \right\rfloor$ for $3 \leq k \leq n$.*

Proof By the Griesmer bound [22], any binary linear $[n, k, d]$ code satisfies

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

Solving it in terms of d and simplifying the expression, we have

$$d \leq \left\lfloor \frac{n \cdot 2^{k-1}}{2^k - 1} \right\rfloor.$$

Therefore any $[n, k, d]$ LCD code must satisfy this inequality. □

Remark 1 One can generalize the upper bound in Lemma 2 for a q-ary $[n, k, d]$ code. Using the Griesmer bound for q-ary $[n, k, d]$ codes we have that a q-ary $[n, k, d]$ code must have an upper bound for d as follows.

$$d \leq \left\lfloor \frac{n \cdot q^{k-1}}{q^k - 1} \right\rfloor \text{ for } k \geq 1.$$

Remark 2 It is interesting to note that optimal binary $[n, 2]$ LCD codes (nearly) attain the Greismer bound. Whether this observation also holds for binary codes of higher dimension is yet to be confirmed. The constructions done in the proof of Theorems 1 and 2 may become more complicated for higher dimensional binary LCD codes and/or for q-ary LCD codes.

3 Bounds on minimum distances of $[n, k]$ LCD codes

In this section we compute the exact value of $LD(n, n-i) = 2$ and give a relation between $LD(n, k)$ and $LD(n, k-1)$ or $LD(n, k-2)$.

Theorem 3 *Given $i \geq 2$, $LD(n, n-i) = 2$ for all $n \geq 2^i$.*

Proof Consider an $[n, n-i, d]$ binary code. By the sphere packing bound, we have $2^{n-i} \sum_{j=o}^{t} \binom{n}{j} \leq 2^n$ for $t = \lfloor \frac{d-1}{2} \rfloor$. This implies that $\sum_{j=o}^{t} \binom{n}{j} \leq 2^i$. For all $n \geq 2^i$, it must be that $t = 0$ and so $d \leq 2$. It then directly follows that $LD(n, n-i) \leq 2$.

Next, we show that there exists an $[n, n-i, 2]$ LCD code for $n \geq 2^i$. For i even, let $G = [I_{n-i} \mid \underbrace{\mathbf{11}\cdots\mathbf{1}}_{i}]$, and for i odd, let $G = [I_{n-i} \mid \underbrace{\mathbf{11}\cdots\mathbf{10}}_{i}]$ where $\mathbf{1}$ denotes the all one vector and $\mathbf{0}$ 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 $LD(n, n-i) = 2$ for all $n \geq 2^i$. □

Note that Theorem 3 suggests that some binary LCD codes with very large size ($n \geq 2^i$) and $k = n - i$ are optimal codes with largest possible minimum distance.

So far we have shown the exact value of $LD(n, 2)$. In order to obtain bounds for a more general case for any k, we introduce the idea of principal submatrix and pr-sequence which will be used in the next result.

Definition 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 $\{i_1, i_2, \ldots, i_{k-m}\} \subset \{i_1, i_2, \ldots, i_k\}$.

Definition 4 ([1]) 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 $pr(A) = r_0]r_1r_2 \ldots r_k$ 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.

We say that a pr-sequence is *attainable* if there exists some symmetric matrix satisfying the pr-sequence. For fields of characteristic 2, the only attainable pr-sequences are given in [1].

Proposition 2 *Over a field with characteristic 2, a principal rank characteristic sequence is attainable if and only if it has one of the following forms:*

$$(i)0]1\,\overline{1}\,\overline{0} \quad (ii)1]\overline{01}\,\overline{0} \quad (iii)1]1\,\overline{1}\,\overline{0}$$

where $\overline{1} = 11\ldots1$ *(or empty),* $\overline{0} = 00\ldots0$ *(or empty),* $\overline{01} = 0101\ldots01$ *(or empty).*

Theorem 4 *We have the following:*

(i) *If $k \geq 3$ and k is odd, then any $[n, k]$ LCD code C has a $(k - 1)$ dimensional subcode which is also LCD. Hence*

$$LD(n, k) \leq LD(n, k - 1)$$

for any $k \leq n$.

(ii) *If $k \geq 4$ and k is even, then any $[n, k]$ LCD code C has a $(k - 2)$-dimensional LCD subcode. Hence*

$$LD(n, k) \leq LD(n, k - 2)$$

for any $k \leq n$.

Proof (i) Suppose $k \geq 3$ and k is odd. We claim that any $[n, k]$ LCD code C has a $(k - 1)$ dimensional subcode which is also LCD. Since the minimum distance of a code is always less than or equal to the minimum distance of a subcode, it then immediately follows that $LD(n, k) \leq LD(n, k - 1)$.

Indeed, let G be a $k \times n$ generator matrix of C and $A = GG^T$. Then A is symmetric and of full rank k. Hence, $r_k \neq 0$ in the pr-sequence of A. Also, since k is odd, case (ii) of Proposition 2 is not attained by A. So the only possible pr-sequences for A are of the form $0]11\ldots1$ and $1]11\ldots1$. Therefore, 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 $rank(P_1) = k-1 \neq 0$, P_1 is invertible. Then the subcode C_1 with generator matrix G_1 is LCD as well. This proves the claim.

(ii) Likewise, we claim that any $[n, k]$ LCD code C has a $(k - 2)$-dimensional LCD subcode for any even $k \geq 4$ and so the inequality $LD(n, k) \leq LD(n, k-2)$ follows.

Indeed, let G be a $k \times n$ generator matrix of C and $A = GG^T$. Since A is of full rank k, we have the following pr-sequences for A by Proposition 2:

$$0]11\ldots1 \qquad 1]01\ldots0101 \qquad 1]11\ldots1$$

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 $rank(P_2) = k-2 \neq 0$, P_2 is invertible. The code generated by G_2 is the desired LCD subcode.

□

In the above proof, we have presented a construction of LCD subcode using the pr-sequence. This can be extended to other fields based on some results in [1] but a complete classification of attainable pr-sequences is only presented for fields of characteristic 2.

The exact values of $LD(n, k)$ for $1 \leq k \leq n \leq 12$ are given in Table 1. These values were obtained from the main theorems presented in the last two sections and, in some cases, by exhaustive search using MAGMA [3]. From this table and Theorem 4, we infer the following inequality.

Conjecture If $2 \leq k \leq n$, then $LD(n, k) \leq LD(n, k - 1)$.
(Note: It suffices to show that this is true when k is even.)

Table 1 $LD(n,k)\ for\ 1 \le k \le n \le 12$

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	2	1							
6	5	3	2	2	1	1						
7	7	4	3	2	2	2	1					
8	7	5	3	3	2	2	1	1				
9	9	6	4	4	3	2	2	2	1			
10	9	6	5	4	3	3	2	2	1	1		
11	11	6	5	4	4	4	3	2	2	2	1	
12	11	7	6	5	4	4	3	2	2	2	1	1

4 The maximum dimensions of LCD codes with fixed *n* and *d*

In this section, we consider the maximum dimension k for an LCD code with given length n and minimum distance d. To this end, we define another combinatorial function, denoted by $LK(n,d)$.

Definition 5 $LK(n,d) := \max\{k \mid \text{there exists a binary } [n,k,d] \text{ LCD code}\}$

For convenience, define $LK(n,d) = 0$ if and only if there is no LCD code with the given n and d.

It can be infered from Table 2 that more zeros appear as n gets larger. Dougherty et al. [6] showed that $LK(n,d) = 0$ for n even and when $d = n$. This is, in fact, a special case of the following general result.

Table 2 $LK(n,d)\ for\ 1 \le d \le n \le 12$

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	1	0	1			
10	10	8	6	4	3	2	1	0	1*	0		
11	11	10	7	6	3	2	1	0	1	0	1	
12	12	10	7	6	4	3	2*	0	1	0	1*	0

Theorem 5 *The following hold.*

(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., $LK(n, n-2i) = 0$.*

(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., $LK(n, n-2i-1) = 0$.*

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 1, there is no $[n, 1, n-2i]$ LCD code with n even.

Now suppose $k \geq 2$. By succesively applying the subcode construction in the proof of Theorem 4, we can find an $[n, 2, n-2i]$ LCD subcode of C. By the Griesmer Bound with $k = 2$, we obtain $n \geq n - 2i + \frac{n-2i}{2}$ which implies $n \leq 6i$. So 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 Theorem 2 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 $k \geq 2$. Again, by application of the subcode construction in the proof of Theorem 4, we can find $[n, 2, n-2i-1]$ LCD 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. □

In Table 2, the values of $LK(n, d)$ are given for $1 \leq d \leq n \leq 12$. These values are obtained using Table 1, Theorem 1, and two tables from [6]. The values with * are the ones that are corrected here as they are incorrectly reported in Table 1 of [6].

5 Conclusion

This paper devoted to bounds on the minimum distance of LCD codes. In particular, the maximum possible values of d among all $[n, k, d]$ LCD codes, denoted $LD(n, k)$, are presented for $1 \leq k \leq n \leq 12$. Some relations between the values of $LD(n, k)$ for varying parameters are also presented. Then we define another combinatorial function $LK(n, d)$ which is the maximum dimension over all LCD codes of length n and minimun distance d. Using the results from $LD(n, k)$, the values of $LK(n, d)$ are obtained for $1 \leq d \leq n \leq 12$.

It is natural to extend definitions of these combinatorial functions to general q-ary LCD codes. Whether the techniques presented in this paper hold for a general q-ary case is a good topic for future work.

Acknowledgments J.-L. Kim was supported by Basic Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2016R1D1A1B03933259).

References

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

2. Boonniyom, K., Jitman, S.: Complementary dual subfield linear codes over finite fields. arXiv:1605.06827 (2016)
3. Bosma, W., Cannon, J.: Handbook of Magma Functions. School of Mathematics and Statistics, University of Sydney (1996)
4. Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. In: In Coding Theory and Applications, pp. 97–105. Springer, Cham (2015)
5. Ding, C., Li, C., Li, S.: LCD cyclic codes over finite fields. IEEE Trans. Inf. Theory **63**(7), 4356–4344 (2017)
6. Dougherty, S.T., Kim, J.-L., Ozkaya, B., Sok, L., Solé, P.: The combinatorics of LCD codes : Linear Programming bound and orthogonal matrices. Int. J. Info. Coding Theory **4**(2-3), 116–128 (2015)
7. Esmaeili, M., Yari, S.: On complementary-dual quasi-cyclic codes. Finite Fields Appl **15**(3), 375–386 (2009)
8. Güneri, C., Özkaya, B., Solé, P.: Quasi-cyclic complementary dual codes. Finite Fields Appl. **42**, 67–80 (2016)
9. Jin, L.: Construction of MDS codes with complementary duals. IEEE Trans. Info. Theory, **63**(5), 2843–2847 (2017)
10. Li, C.: On Hermitian LCD codes from cyclic codes and their applications to orthogonal direct sum masking. arXiv preprint arXiv:1701.03986v1 (2017)
11. Li, S., Ding, C., Liu, H.: A family of reversible BCH codes. arXiv:1608.02169 (2016)
12. Li, S., Ding, C., Liu, H.: Parameters of two classes of LCD BCH codes. arXiv preprint arXiv:1608.02670v2 (2017)
13. Liu, X., Liu, H.: Matrix-product complementary dual codes. arXiv:1604.03774 (2016)
14. Massey, J.L.: Reversible codes. Inf. Control. **7**(3), 369–380 (1964)
15. Massey, J.L.: Linear codes with complementary duals. Discrete Math. **106-107**, 337–342 (1992)
16. Mesnager, S., Tang, C., Qi, Y.: Complementary dual algebraic geometry codes. arXiv:1609.05649 (2016)
17. Muttoo, S.K., Lal, S.: A reversible code over $GF(q)$. Kybernetika **22**(1), 85–91 (1986)
18. Sari, M.: On MDS Negacyclic LCD Codes. arXiv:1611.06371 (2016)
19. Sendrier, N.: Linear codes with complementary duals meet the Gilbert-Varshamov bound. Discrete Math. **285**(1), 345–347 (2004)
20. Tzeng, K., Hartmann, C.: On the minimum distance of certain reversible cyclic codes (Corresp.) IEEE Trans. Inf. Theory. **16**(5), 644–646 (1970)
21. Kandasamy, W.V., Smarandache, F., Sujatha, R., Duray, R.R.: Erasure Techniques in MRD Codes. Zip Publishing, Ohio (2012)
22. Huffman, W.C., Pless, V.: Fundamentals of Error-correcting Codes. Cambridge University Press, Cambridge (2010)
23. Yang, X., Massey, J.L.: The condition for a cyclic code to have a complementary dual. Discrete Math. **126**(1–3), 391–393 (1994)
24. Zhu, S., Pang, B., Sun, Z.: The reversible negacyclic codes over finite fields. arXiv:1610.08206 (2016)