Intersection of Code Pairs

Nurgül Kangal nurgulkangal28@gmail.com
Mathematics / FSL / Mimar Sinan Fine Arts University , 2019

Engincan Varan evaran@sabanciuniv.edu
Computer Science / FENS / Sabancı University , 2019

Supervisor:
Cem Güneri Mathematics

Abstract

Linear complementary dual codes (LCD codes) are codes whose intersection with their dual codes are trivial. We study LCD codes (especially binary LCD codes) [n,k] with the largest minimum distance and their generator matrices. We created a table to show the largest minimum distance for each LCD code [n,k] where $1 \leq k \leq n \leq 24$, with the help of given boundaries. In addition, we researched the ways to construct the generator matrices for some fixed values of [n,k,d] using some techniques such as k-cover.

Keywords Binary LCD Codes, Generator Matrix, Minimum Distance, k-cover

1 Introduction

In Coding Theory *linear codes* mostly used in as an error-correcting codes for any codeword. Their applications are in the method of transmitting symbols (e.g. bits) through a communication channel so that, if any error occurs in the transmission, usually some of the errors can be detected or even corrected by the receiver. To define a linear code we introduce some parameters [n,k,d] length, dimension and largest minimum distance respectively. Using these parameters, it is possible to construct an optimal linear code to detect and fix the errors. In addition there are some tables[1] which presents the optimal linear codes with their parameters. In this paper, we studied *linear complementary dual codes* (LCD codes) a special type of linear codes. It was first introduced as a reversible code by Massey in 1964. LCD codes studied in literature and applied in data storage, communications systems and mostly in cryptography. Since it is mostly used in cryptography, LCD codes drew attention very recently and it is still an important topic to study. There exists some LCD codes with fixed length and dimension, which have the largest minimum distance, called “good” or “optimal” codes.

The aim of this paper is to study boundaries between the parameters of an LCD code, constructing LCD codes which are “good” in terms of the parameters and using the results to create a table for largest minimum distance for fixed n,k values where $1 \leq k \leq n \leq 24$. Also, we created a C++ program to calculate the largest minimum distance for the given n,k values to take our work further.

2 Preliminaries

An [n,k] linear code C over F_q is k-dimensional vector subspace of F_q^n , where F_q denotes the finite field of order q and q must be a prime power. A code over F_2 is called *binary*. Throughout this report, all codes mean binary. The parameters n and k are *length* and *dimension* of the linear code C respectively. A vector in C is called a *codeword* of C.

2.1. Minimum Distance:

The *minimum distance* of C is defined as,

$$d(C) = \min\{ d(x, y) : x, y \in C, x \neq y \},$$

where d(x,y) counts the number of coordinates where x and y differ (the so-called Hamming distance). For a code C to be optimal, the minimum distance should be as large as possible. This minimum distance is called the *largest minimum distance* for a linear code [n,k]. With the addition of the largest minimum distance, we denote each vector subspace as [n,k,d] code.

2.2. Dual code of a code C:

Let C be a linear code. The dual code of C is defined as the orthogonal complement of the subspace C of Fqn and it is denoted by $C\perp$.

$$C^{\perp} = \{ y \in F_q^n \mid < x,y > = 0, \text{ for all } x \in C \}, \text{ where } < x,y > \text{ is the standard inner product.}$$

[2]**Remark 1:** Let C be a linear code of length n over F_q. Then,

(i) $C^{\perp}$ is a linear code and $\dim(C^{\perp}) + \dim(C) = n$.

(ii) $(C^{\perp})^{\perp} = C$

1 ("CodeTables.de", 2019)

2 (Ling & Xing, 2004, p. 44-46)

2.3. Linear Complementary Dual Code:

Linear complementary dual codes (LCD Codes) are codes whose intersections with their dual codes are trivial.

$$C \cap C^{\perp} = \{0\}$$

Example:

Let C be a linear code and C = { 000 , 111 }. From the definition of dual code, $C^{\perp}$ = { 000 , 011 , 101 , 110 }. The intersection is $C \cap C^{\perp}$ = { 000 }. Since, the intersection has only 0 vector, this code is an LCD code.

2.4. Generator Matrix and Parity-Check Matrix:

Definition 1:

(i) A *generator matrix* for linear code C is matrix G whose rows form a basis for C.

(ii) A *parity-check matrix* H for a linear code C is a generator matrix for the $C^{\perp}$.

[3]**Remark 3:** If C is an [n,k,d] linear code, the generator matrix for C must be k x n matrix and parity-check matrix for C must be an (n-k) x n matrix.

Definition 2: A generator matrix of the form $(I_k|X)$ is said to be in *standard form*, where X is a k x (n-k) matrix.

[4]**Proposition 1:** Let C be a code. 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 i.e. $\det(GG^T) \neq 0$.

(iv) HH^T is nonsingular i.e. $\det(HH^T) \neq 0$.

3 (Ling & Xing, 2004, p. 52)

4 (Harada & Saito, 2019, p. 3)

Example for an LCD code:

Let G be a generator matrix for linear code C [5,3,2] .

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$GG^T = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$\det(GG^T) = 1 \neq 0$. From proposition 1, C is an LCD code.

Therefore from the generator matrix,

C = { 00000 , 00101 , 01001 , 01100 , 10011 , 10110 , 11010 , 11111 }

Using the given minimum distance definition above, we get 2 as our minimum distance for C.

Finally, we can say that G generates a [5,3,2] LCD code.

3 Some Bounds on the Parameters

There are some bounds we use to create a table that gives the largest minimum distance values of linear codes such as Singleton bound.

[5]**Singleton Bound:**The parameters [n,k,d] of any linear code over F_q (q is a prime power) satisfy,

$$k+d \leq n+1.$$

Example: Let C be a binary [4,2,2] linear code. Let G be a generator matrix for C.

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Therefore from the generator matrix,

C= { 0000, 1110, 0111, 1001 }

d(0000,1110) = 3	d(1110,0111) = 2
d(0000,0111) = 3	d(1110,1001) = 3
d(0000,1001) = 2	d(0111,1001) = 3

5 (Ling & Xing, 2004, p. 92-93)

So, the minimum distance is 2.
Finally, $2+2 \leq 4+1$ (n=4,k=2,d=2) provided.

Definition 3: $d(n,k) := \max\{\, d \mid \text{there exists a binary } [n,k,d] \text{ LCD code}\}$

3.1. Some Bounds for Minimum Distance on 2-Dimensional LCD Codes

[6]**Proposition 2:** Let $n \geq 2$. Then,

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

3.2. Some Bounds for Minimum Distance on 3-Dimensional LCD Codes

[7]**Proposition 3:** Let $n \geq 3$. Then,

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

3.3. Some Bounds for Minimum Distance on 4-Dimensional LCD Codes

[8]**Proposition 4:** Let $n \geq 4$. Then,

$$d(n,4) = \begin{cases} \left\lfloor \frac{8n}{15} \right\rfloor & , if\ n \equiv 5,9,13 \ (mod\ 15) \\ \left\lfloor \frac{8n}{15} \right\rfloor - 1 & \text{, if n} \equiv 2,3,4,6,10 \ (mod\ 15) \\ \left\lfloor \frac{8n}{15} \right\rfloor \ or\ \left\lfloor \frac{8n}{15} \right\rfloor - 1 & \text{, if n} \equiv 1,7,8,11,12,14 \ (mod 15) \\ \left\lfloor \frac{8n}{15} \right\rfloor \ or\ \left\lfloor \frac{8n}{15} \right\rfloor - 1 \text{ or } \left\lfloor \frac{8n}{15} \right\rfloor - 2 & \text{, if n} \equiv 0 \ (mod\ 15) \end{cases}$$

[8]**Remark 4:** There is no LCD[n,4,d] code for

(n,d) = (7,3) , (8,4) , (11,5) , (12,6) , (14,7) , (15,7) , (15,8) , (16,8) , (22,11) , (23,12)

6 (Galvez , Kim , Lee , Roe & Won, 2017, p. 3-4)
7 (Harada & Saito, 2019, p. 12)
8 (Araya & Harada, 2018, p. 2-8)

3.4. Some Bounds for Minimum Distance on 5-Dimensional LCD Codes

[9]**Proposition 5:** Let n $\geq$5. Then,

$$d(n,5)=\begin{cases} \left\lfloor \frac{16n}{31} \right\rfloor - 1, & if\ n \equiv 3,5,7,11,19,20,22,26\ (mod\ 31) \\ \left\lfloor \frac{16n}{31} \right\rfloor - 2 & ,\text{if n} \equiv 4\ (mod\ 31) \\ \left\lfloor \frac{16n}{31} \right\rfloor - 1\ or\ \left\lfloor \frac{16n}{31} \right\rfloor - 2 & ,\text{if n} \equiv 2,6,8,10,14,18\ (mod\ 31) \\ \left\lfloor \frac{16n}{31} \right\rfloor - 2\ or\ \left\lfloor \frac{16n}{31} \right\rfloor - 3 & ,\text{if n} \equiv 12\ (mod\ 31) \\ \left\lfloor \frac{16n}{31} \right\rfloor\ or\ \left\lfloor \frac{16n}{31} \right\rfloor - 1\ or\ \left\lfloor \frac{16n}{31} \right\rfloor - 2 & ,if\ n \equiv 0,16\ (mod\ 31) \\ \left\lfloor \frac{16n}{31} \right\rfloor\ or\ \left\lfloor \frac{16n}{31} \right\rfloor - 1 & ,otherwise \end{cases}$$

3.5. Some Bounds for Minimum Distance on k-Dimensional LCD Codes

[10]**(1)** Let n $\geq$ 3 and n is *odd*, then we have the following equalities,

(i) d(n,1) = n

(ii) d(n,n-1) = 2.

[10]**(2)** Let n $\geq$ 3 and n is *even*, then we have the following equalities,

(i) d(n,1) = n-1

(ii) d(n,n-1) = 1.

[11]**(3)** Let 2$\leq$ k $\leq$ n, then we have the following inequalities,

(i) d(n, k) $\leq$ d(n, k-1).

[11]**(4)** Given i $\geq$ 2, d(n, n-i) = 2 for all n $\geq$ 2^i.

4 Construction Methods for Generator Matrix

For the given LCD [n,k,d] code, there are different methods of creating the generator matrix. In this section, we will consider creating generator matrix with k-cover method and a theorem for d(n,2) where n $\geq$ 2. Also, there is an algorithm to construct the generator matrix for the given q,n,k parameters. It is described in section 6. However, this method requires more computational power, so using powerful computers would be more suitable for this job.

9 (Araya & Harada, 2018, p. 2, 9-15)

10 (Dougherty, Kim, Özkaya, Sok, & Sole 2015, p. 4)

11 (Galvez,Kim & Lee, 2018, p. 6-7)

4.1. Generating Matrix for LCD codes [n,2,d(n,2)] where n ≥ 2

From section 3.1 proposition 2, we know the largest minimum distances for LCD codes of dimension 2, where $n \geq 2$. To construct the generator matrices for we can use the following instructions.

(i) Let $n \equiv 1 \pmod 6$, i.e $n = 6m+1$ for some positive integer m. The generator matrix would be of the form:

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

(ii) Let $n \equiv 2,-2 \pmod 6$, i.e $n = 6m+2$ for some positive integer m or $6m-2$ for some positive integer m. The generator matrix would be of the form, where k is an integer:

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

(iii) Let $n \equiv 3 \pmod 6$, i.e $n = 3i$ for some positive odd integer i. The generator matrix would be of the form:

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

[12]4.2. Constructing Generator Matrix from k-covers

Let *k, m, l* (even) be positive integers.

Proposition 6: The code C is an LCD[$lm+k$, k, d] code with $d(C^{\perp})=2$. ($lm+k$ = n parameter)

For the given parameters [n, k, d], let us select the values *l* and *m* in coherent with the equation $n = lm + k$.

Let X be a set of m element in the form of {1,2,…,m} and $Y = (Y_1, Y_2, ..., Y_k)$ be a k-cover of X.

The Y_i (i=1,2,...k) here are the subsets of the set X, which are not necessarily distinct.

We consider all possibilities for $(Y_1, Y_2, ..., Y_k)$, choose the ones that give the LCD code.

Then, using the sets $(Y_1, Y_2, ..., Y_k)$, we create sets of $Z_1, Z_2, ..., Z_k$ in order to give the rows of the generator matrix. We create sets $Z_1, Z_2, ..., Z_k$ as follows:

12 (Harada & Saito, 2019, p. 4-7)

$$Z_1 = \{1\} \cup (k + Y_1) \cup (k + m + Y_1) \cup \ldots \cup (k + (l\text{-}1)\, m + Y_1),$$
$$Z_2 = \{2\} \cup (k + Y_2) \cup (k + m + Y_2) \cup \ldots \cup (k + (l\text{-}1)\, m + Y_2),$$
$$\vdots$$
$$Z_k = \{k\} \cup (k + Y_k) \cup (k + m + Y_k) \cup \ldots \cup (k + (l\text{-}1)\, m + Y_k).$$

Here, $a + Y_i = \{ a + y \mid y \in Y_i \}$ for a positive integer a.
Let G be a generator matrix in that form k x n and a_{ij} is the i-th row, j-th column element.

$$((i = 1,\ldots k) , (j = 1,\ldots n))$$

Then, i-th row is created in the form of $a_{ij} = 1$ if $j \in Z_i$ or $a_{ij} = 0$ if $j \notin Z_i$.

Example: Let's take the example we used above. Let C be a binary [5,3,2] linear code. Let's find the generator matrix from 3-cover.

Let $l = 2$. İf $n = 2m + 3$ and $n = 5$, being ‘$m = 1$’.
X being a set of in the form of {1}. Let's choose $Y_1 = Y_2 = Y_3 = \{1\}$. From here,

$$Z_1 = \{1\} \cup (3 + Y_1) \cup (3+1 + Y_1) = \{1,4,5\}$$
$$Z_2 = \{2\} \cup (3 + Y_2) \cup (3+1 + Y_2) = \{2,4,5\}$$
$$Z_3 = \{3\} \cup (3 + Y_3) \cup (3+1 + Y_3) = \{3,4,5\}$$

Finally,

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

4.3. Generating Matrix for LCD Codes [n,n-1,d(n,n-1)]

If we want to generate matrix for LCD codes with the parameters [n,n-1,d(n,n-1)], then we can use the following function:

$$G = \begin{cases} \left[\begin{array}{c|c} \mathrm{I} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \end{array}\right] & , if\ n\ is\ even \\ \left[\begin{array}{c|c} \mathrm{I} & \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \end{array}\right] & , if\ n\ is\ odd \end{cases}$$

Where I denotes the identity matrix of size (n-1) x (n-1).

5 Table for Largest Minimum Distance for Binary LCD Codes

The exact values of d(n,k) for 1 ≤ k ≤ n ≤ 24 are given in Table 1. These values are obtained from the articles and the main theorems and boundaries presented in the previous sections. From the table, we can find the largest minimum distance with the given parameters [n,k]. The table is color coded and each color represents an article that is used to find the values.

Table 1 d(n,k) for 1 ≤ k ≤ n ≤ 24

n/k:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
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												
13	13	8	6	6	5	4	4	3	2	2	2	2	1											
14	13	9	7	6	5	5	4	4	3	2	2	2	1	1										
15	15	10	7	6	6	6	5	4	4	3	2	2	2	2	1									
16	15	10	8	7	6	6	5	5	4	4	3	2	2	2	1	1								
17	17	10	9	8	7	6	6	6	5	4	3	3	2	2	2	2	1							
18	17	11	9	8	7	7	6	6	5	4	4	4	3	2	2	2	1	1						
19	19	12	10	9	8	8	7	6	6	5	4	4	3	3	2	2	2	2	1					
20	19	13	10	10	9	8	7	6	6	6	5	4	4	4	3	2	2	2	1	1				
21	21	14	11	10	9	8	8	7	6	6	5	5	4	4	3	3	2	2	2	2	1			
22	21	14	11	10	10	9	8	8	7	6	6	6	5	4	4	4	3	2	2	2	1	1		
23	23	14	12	11	10	9	9	8	7	7	6	6	5	4	4	4	3	3	2	2	2	2	1	
24	23	15	13	12	11	10	9	8	8	8	7	6	6	5	4	4	4	4	3	2	2	2	1	1

Orange-coded cells are from Galvez,Kim & Lee, 2018

Green-coded cells are from Harada & Saito, 2019

Red-coded cells are from Singleton Bound in Section 3

Blue-coded cells are from Araya & Harada, 2018

Purple-coded cells are from Dougherty, Kim, Özkaya, Sok, & Sole 2015

6 An Algorithm to Find the Generator Matrix

There are some techniques to find the generator matrix of an LCD code, as we discussed k-cover in section 4. An alternative but exhausting way is to check every possible linear code and check if this code satisfies some conditions. For instance, let's assume C [n,k] is a linear code generated by matrix G. First, we need to check if C is an LCD code or not. Then if C is indeed an LCD code, we need to calculate the minimum distance for C and checks the possible largest minimum distance for the given [n,k] values. That's another way to find a generator matrix, yet it is still based on our inputs. What this algorithm does is that it creates all possible codeword combinations of C for the given inputs q,n and k where q determines the finite field we are working on, n is the length of the code and k is the dimension. After creating all combinations, we need to check if these codewords are linearly independent or not. If they are linearly independent it means these codewords are the basis of some subspace C* of C. After

constructing our subspace C*, we need to check if C* is LCD code or not. If C* is LCD code, we can start calculating the minimum distance. After all this exhausting search, for given [n,k], we are going to end up with the possible LCD codes with calculated minimum distances. Finally, we can select the largest minimum distance among all of them and look for the basis combination that we already created. In the end, as an output, we will have the largest minimum distance and generator matrices to construct this LCD code.
Here is the pseudocode for the algorithm:

```
LCD Code Generator ( q , n , k)
        combinations[] = findAllCombinations ( q , n , k )          // returns all the combinations of  C(q^n , k)
        possibleBases[] = checkForBasis( combinations[] , q , n )     // returns the possible basis, linearly independence check
        LCDBases[] = checkForLCD ( possibleBases[] , q , n , k )      // returns the LCD bases among all possible bases
        minDistances[] = calculateMinDistance ( LCDBases[] , n )      // calculates the minimum distance for all LCD codes
        largestMinDistance = findLargest ( mindDistance[] )           // finds the largest number
        for each element i in LCDBases:                               // for every code in LCDBases
                if ( largestMinDistance == minDistance[i] )           // compare the minDistance of the C in LCDBases
                        print LCDBases[i]                             // if they are equal print the bases of C
```

To analyze the pseudocode;
1- We get the inputs from the user for the parameters q,n,k
2- We create all possible combinations of vectors / codewords. There will be $C(q^n , k)$ many combinations and store it in combinations array.
3- From all these combinations, we check if the vectors are linearly independent, which is essential to form a basis. If the vectors indeed form a basis, we store it in the possibleBases array.
4- We check if the created bases are forming an LCD code using proposition 1. If they are, we store it in the LCDBases array.
5- For every basis in LCDBases, we calculate the minimum distance and store it in minDistance array. The index i in minDistance array corresponds to the minimum distance of the i^{th} index of the LCDBases array.
6- Among all minimum distance values we find the largest one.
7- For every element in minDistance array we check for equality and if the condition is satisfied, we print the basis from the corresponding index from the LCDBases.

The algorithm has $O(kq^n)$ time and space complexity. Therefore as q,n and k parameters gets bigger, the algorithm takes too much time and space. We can decrease the space complexity by deleting the combinations as we surpass them, but decreasing time complexity is much harder. Of course, we can speed up our algorithm or we can use much more advanced computational power to construct out generator matrices. From exhausting searches, the algorithm generated a table which is exactly the same with given table in the previous section. (Table 1) In the end, this algorithm gives the generator matrices for a “good” LCD code [n,k] for us.

7 Conclusion

This paper committed to find and generate “optimal” binary LCD codes. In particular, the largest minimum distance for given [n,k] LCD codes and how to construct this code’s generator matrices. Some boundaries for certain parameters and construction methods to construct these generator matrices also presented. A largest minimum distance for binary LCD codes table is provided for the values $1 \leq k \leq n \leq 24$ for the simplicity. For future work it would be nice to have the table extended and adapted to general q-ary case. Aim is to prepare a database for “optimal” LCD codes just like the database prepared for the linear codes[13].

13 ("CodeTables.de", 2019)

8 References

- Ling, S., & Xing, C. (2004). Coding theory: A first course. Cambridge, UK: Cambridge University Press.
- Galvez, L., Kim, JL., Lee, N. et al. Cryptogr. Commun. (2018) 10: 719. https://doi.org/10.1007/s12095-017-0258-1
- Grassl, Markus. "Bounds on the minimum distance of linear codes and quantum codes." Online available at http://www.codetables.de. Accessed on 2019-08-06.
- Harada, M. & Saito, K. Cryptogr. Commun. (2019) 11: 677. https://doi.org/10.1007/s12095-018-0319-0
- Araya, M., & Harada, M. (2018). On the minimum weights of binary linear complementary dual codes. Retrieved July 18, 2019, from https://arxiv.org/abs/1807.03525v1.
- Galindo, C., Geil, O., Hernando, F., & Ruano, D. (2019). New Binary and Ternary LCD Codes.
- Dougherty, Steven T., et al. “The Combinatorics of LCD Codes: Linear Programming Bound and Orthogonal Matrices.” 2015, https://arxiv.org/abs/1506.01955v1. Accessed 23 July 2019.