INTERSECTION OF CODE PAIRS

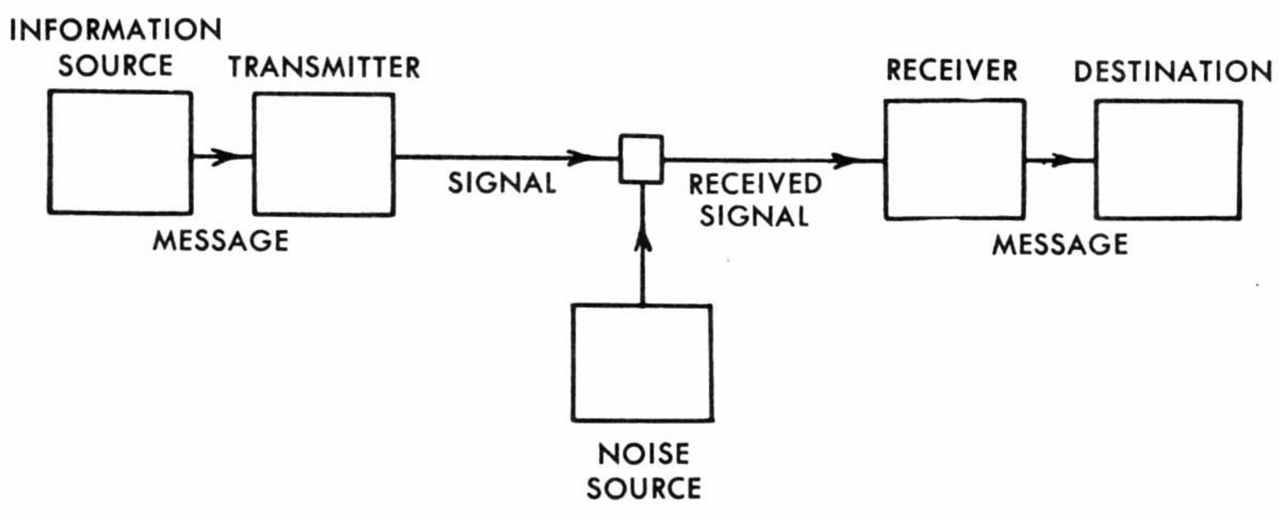
STUDENTS / UNIVERSITIES
ENGİNCAN VARAN / SABANCI UNIVERSITY
NURGÜL KANGAL / MİMAR SİNAN UNIVERSITY

SUPERVISOR(S)
CEM GÜNERİ

Sabancı Üniversitesi

pure PROGRAM FOR UNDERGRADUATE RESEARCH

Introduction



Linear Codes

- An [n,k,d] code C over F_q is a k-dimensional vector subspace of $F_q^{\,n}$ with minimum distance d, where F_q denotes the finite field of order q. Here, 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).

Linear Complementary Dual Codes (LCD)

- Let C be a linear code. The ***dual*** code of C is defined as the orthogonal complement of the subspace C of $F_q^{\,n}$ and it is denoted by $C^{\perp}$.

  $$C^{\perp} = \{ y \in F_q^{\,n} \mid \langle x,y \rangle = 0, \text{ for all } x \in C \}$$

  where $\langle x,y \rangle$ is the standard inner product.
- Linear complementary dual codes (LCD Codes) are codes whose intersections with their dual codes are ***trivial***.

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

- LCD codes drew attention in recent years especially due to their applications in cryptography.

Generator Matrix and Parity-Check Matrix

- A ***generator matrix*** for a linear code C is a matrix G whose rows forms a basis for C.
- A ***parity-check matrix*** H for a linear code C is a generator matrix for the dual code $C^{\perp}$.

  Remark: 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.

  [2]Proposition: 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. $\det(HH^T) \neq 0$

Aim of the Study

- Constructing LCD Codes and their generator matrices with the k-cover technique.
- Studying and establishing the boundaries between the parameters n,k and d for LCD Codes.
- There are many tables[4] for linear codes over F_q, but no table for LCD codes over F_q. So, we want to create an up to date table for largest minimum distance among all binary LCD [n,k,d]-codes.
- For every LCD [n,k,d]-codes, we want to give the generator matrices and observing the d parameter boundaries with the given fixed n and k parameters.

Largest Minimum Distance of Binary LCD [n,k,d]-Codes

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

Here you can see the color coded table for binary LCD [n,k,d]-Codes. For any n and k (less than 24) values, the table provides us the best d parameter possible. Colors here references to the articles that we used to create the table.

Example: Let C be a binary [8,2,5] LCD code. Let G be a generator matrix for C.

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

Since $\det(GG^T) = 1$, this linear code is indeed a binary LCD code with parameters [8,2,5].

Then, from G, C has the following elements.

C = { 00000000 , 00011111 , 11111000 , 11100111 }

d(00000000 , 00011111) = 5

d(00000000 , 11111000) = 5

d(00000000 , 11100111) = 6

d(11111000 , 00011111) = 6

d(11111000 , 11100111) = 5

d(00011111 , 11100111) = 5

So, the minimum distance is 5.

References

- [1]Galvez, L., Kim, JL., Lee, N. et al. Cryptogr. Commun. (2018) 10: 719. https://doi.org/10.1007/s12095-017-0258-1 (orange cells)
- [2]Harada, M. & Saito, K. Cryptogr. Commun. (2019) 11: 677. https://doi.org/10.1007/s12095-018-0319-0 (green cells)
- [3]Ling, S., & Xing, C. (2004). Coding Theory: A First Course. Cambridge, UK: Cambridge University Press. (red cells)
- [4]http://www.codetables.de/
- [5]Araya, M., & Harada, M. (2018). On the minimum weights of binary linear complementary dual codes. (blue cells)
- [6]Dougherty, S. T., Ozkaya, B., Sok, L., Sole, P., & Kim, J. (2014). The combinatorics of LCD codes: Linear Programming bound and orthogonal matrices. (purple cells)