ASPECTS OF CODING THEORY WITH TWO RECENT APPLICATIONS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

ŞEYMA BODUR

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

AUGUST 2019

Approval of the thesis:

ASPECTS OF CODING THEORY WITH TWO RECENT APPLICATIONS

submitted by **ŞEYMA BODUR** in partial fulfillment of the requirements for the degree of **Master of Science in Cryptography Department, Middle East Technical University** by,

Prof. Dr. Ömür Uğur
Director, Graduate School of **Applied Mathematics** _____

Prof. Dr. Ferruh Özbudak
Head of Department, **Cryptography** _____

Prof. Dr. Ferruh Özbudak
Supervisor, **Department of Mathematics and IAM, METU** _____

Examining Committee Members:

Assoc. Prof. Dr. Ali Doğanaksoy
Department of Mathematics and IAM, METU _____

Prof. Dr. Ferruh Özbudak
Department of Mathematics and IAM, METU _____

Assoc. Prof. Dr. Sedat Akleylek
Department of Computer Engineering, Ondokuz Mayıs University _____

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: ŞEYMA BODUR

Signature :

ABSTRACT

ASPECTS OF CODING THEORY WITH TWO RECENT APPLICATIONS

Bodur, Şeyma
M.S., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

August 2019, 34 pages

Coding Theory is a deep subject having a lot of applications in different areas. In this thesis we explain some background for two recent applications: Code base Cryptography, Entanglement Assisted Quantum Error-Correcting Codes (EAQECC).

Keywords: Code Equivalence, Entaglement-Assisted Quantum Error Correcting Codes, Linear l-intersection pairs, Hulls, etc.

ÖZ

SON GÜNLERDEKİ İKİ UYGULAMA İLE KODLAMA TEORİSİNİN YÖNLERİ

Bodur, Şeyma
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Ağustos 2019, 34 sayfa

Kodlama Teorisi, farklı alanlarda çok fazla uygulamaya sahip olan derin bir konudur. Bu tezde, son günlerdeki iki uygulama alanı olan Kod tabanlı Şifreleme, Dolaşma Destekli Kuantum Hata Düzeltme Kodları (EAQECC) için bazı arka planlar açıklanmaktadır .

Anahtar Kelimeler: Kodların denkliği, Dolaşma Destekli Kuantum Hata Düzeltme Kodları, Doğrusal l-kesişme kod çiftleri, Hulls vd.

To My Family

ACKNOWLEDGMENTS

First and foremost, I would like to thank my supervisor Ferruh Özbudak, for his support, enlightening explanation, patient guidance and encouraging advice .

I would also like to thank Ali Doğanaksoy and Sedat Akleylek for joining my thesis defense committee

I would like to thank my dear friends Barış, Gizem, Gonca, Şahika, Tahir for motivating, helping and cheering me. Also I would like to thank Damla, who started writing a thesis at the same time as me, for supporting me.

Finally, and most importantly, I want to thank my family, my mom, Fatma Gül , my father, Murat, my grandmother, Halide , my uncle, Hasan, and most preciously my brother, Mehmet, for always supporting me, standing behind me.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

$\mathcal{F}_q$	The finite field with q elements
$\mathcal{F}_q^N$	N dimensional vector space over $\mathcal{F}_q$
GRS	Generalized Reed Solomon Code
MDS	Maximum Distance Separable Code
EAQECCs	Entanglement-assisted Quantum Error-correcting Codes

CHAPTER 1

INTRODUCTION

The beginning of the studies in Coding Theory is accepted in 1948 when Claude Shannon wrote the article called "A Mathematical Theory of Communication".

The most important feature of the Coding Theory is that it ensures the data is transmitted to the other party correctly. That is achieved by checking whether the data is affected by external factors like environmental conditions, radio waves etc. In such a case, the data can be corrected and transmitted. To illustrate, Coding Theory is commonly used in CDs and Hard Disks. When a CD is scratched, the data in it can be unreadable. In this case, Coding Theory is used for recovering the data since it corrects the changes in the data and ensures that the data is read correctly.

For better understanding, usage of coding theory in search engines can be examined. Search engines are used for finding the specific information about a specific subject. However, most of the time, the information which is entered to the search engine is not written correctly and contains many typographical errors. Despite all these, search engines correct these mistakes and give the accurate results about the desired subject. For instance, someone wants to find an information about Linear Codes and writes “What is Linaer Code” to the Google’s search bar. However, as it can be seen in the previous sentence, the spelling of the Linear is wrong. Despite the spelling mistake, Google understands what should be written actually and gives the right search results to the user. As can be understood from all these examples, coding theory is used for detecting and correcting the errors in the data to be sent.

Application areas of coding theory:

- Data compression,transmission and storage
- Error-correcting
- Cryptography

There are various of code types which are used in many different application areas and one of the most common types is the linear code. Classification of linear codes is an important problem in Coding theory. Therefore, code equivalence problem holds an important place in Coding Theory.

Code equivalence problem can be expressed as, if the given generator matrices, i.e. G and G', belong to two equivalent codes, find invertible $k \times k$ matrix S and find permutation matrix P. When private code is known, the code equivalence problem is related to the McEliece cryptosystem. In McEliece cryptosystem, the private key is (S, G, P), where S is a $k \times k$ matrix whose determinant is different than zero, G is a $k \times n$ generator matrix of the code, and P is a $n \times n$ permutation matrix. G' is a public key such that $G' = SGP$. If G and G' are known, obtaining S and P is related to code equivalence problem .

Petrank and Roth showed that If an efficient algorithm is found to solve the problem of code equivalence, an efficient algorithm is found to solve the graph isomorphism problem. This means that there is a polynomial time algorithm that reduces the graph isomorphism problem to the code equivalence problem [10]. In 1999, Senderier presented an algorithm which is called Support Splitting Algorithm(SSA) to find permutation equivalence [12]. Leon found a technique to compute authomorphism groups and this technique can also be used for finding equivalent codes [7].

Another important application of coding theory is quantum code. The use of Quantum Error Correcting Codes (QECCs) has many purposes, but the most important goal is to protect quantum information from decoherence and noise. Calderbank and Shor [2] and Steane [13] showed the construction of quantum codes from classical linear codes.

If linear code is dual-containing, quantum codes could be constructed. Dual condition has been relieved with EAQECC and it became easier to obtain EAQECC from linear codes. If the code uses pre-shared entanglement it is called as Entanglement Assisted Quantum Error Correcting Codes (EAQECC) [5] Thus, this problem was eliminated and the quantum code was generated from the classical linear code without dual condition. However, it was still difficult to find the number of pre-shared pairs. Guenda, Jitman and Gulliver showed that this number can be calculated by dimension of hull [6]. In this part of the thesis, a literature review is conducted.

This thesis organized as follows:

- Chapter 2 gives some definitions about Coding theory.
- Chapter 3 is about code equivalence problem. We focus on permutation version of code equivalence problem and in order to facilitate this problem studies have been made for codes of a certain length and size.
- Chapter 4 relates to some extra definitions of quantum codes. We mention important theorem on which this thesis is based. Then by using this theorem, some results obtained from literature review are given.
- In Chapter 5, we make a conclusion.

CHAPTER 2

PRELIMINARY TO THE SUBJECT

In this section, some important definitions which are the basis of coding theory are given.

Definition 1. *(Code) Let C has a dimension k, length n and minimum distance d over a finite field $\mathcal{F}_q$, then C is called code and it is denoted by $C : [n, k, d]$.*

Definition 2. *(Generator Matrix) Let G be a generator matrix of linear code $C : [n, k]$, then rows of G is a basis of C and G is a $k \times n$ matrix.*

Definition 3. *(Parity Check Matrix) Let H be a parity check matrix of linear code $C : [n, k]$, then H be a generator matrix of dual code $C^{\perp}$ and H is a $(n - k) \times n$ matrix.*

Definition 4. *(Hamming Distance) Let $x = (x_1, ..., x_2)$, $y = (y_1, ..., y_n) \in \mathcal{F}_q^n$. Hamming distance is the number of places where x,y take different values.*

Definition 5. *(Hamming Weight) Let $x = (x_1, ..., x_n) \in \mathcal{F}_q^n$. Hamming weight is the number of nonzero entries in x.*

Definition 6. *(Minimum Distance) If Hamming distance of two code words are minimum then it is called as minimum distance*

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

Definition 7. *(Dual Code) Let C be a code with parameters $[n, k]$. If*

$$C^{\perp} = \{a \in \mathcal{F}_q^n | a.c = 0, \forall c \in C\}$$

then $C^{\perp}$ is called as dual code with parameters $[n, n - k]$.

Definition 8. *(Singleton Bound) Let C be a code with parameters $[n, k]$. Parameters of C satisfies*

$$d(C) \leq n - k + 1.$$

Definition 9. *Let $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ and $\beta = (\beta_1, \beta_2, ..., \beta_n)$ be two vector over $\mathcal{F}_q^n$. The Euclidean inner product is defined as*

$$< \alpha, \beta >:= \sum \alpha_i \beta_i, \text{ where } i \in \{1, 2, ..., n\}.$$

Definition 10. *(Reed Solomon Code) Let $\mathcal{F}_q$ be a finite field. $x = (x_1, ..., x_n)$ be a code word in $\mathcal{F}_q$ and every element in x is different from each other. k-dimensional Reed Solomon Code RS(x) is defined as*

$$RS(x) = \{f(x_1), ..., f(x_n) | f \in F_q[x], deg(f(x)) < k\}$$

Generator matrix for $RS_{[n,k]}$ is

$$G = \begin{bmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & & & \\ x_1^{k-1} & x_2^{k-1} & \dots & x_n^{k-1} \end{bmatrix} \tag{2.1}$$

Definition 11. *(Generalized Reed Solomon Code) Let $\mathcal{F}_q$ be a finite field. $x = (x_1, x_2, ..., x_n)$ is a code word in $\mathcal{F}_q$ where every element in x is different from each other and every element in $v = (v_1, ..., v_n) \in \mathcal{F}_q$ is different than zero. k-dimensional Generalized Reed Solomon Code $GRS(x, v)$ is defined as*

$$GRS(x, v) = \{v_1 f(x_1), ..., v_n f(x_n) | f \in F_q[x], deg(f(x)) < k\}$$

Generator matrix of $GRS(x, v)$ is

$$G = \begin{bmatrix} v_1 & v_2 & \dots & v_n \\ v_1 x_1 & v_2 x_2 & \dots & v_n x_n \\ v_1 x_1^2 & v_2 x_2^2 & \dots & v_n x_n^2 \\ \vdots & & & \\ v_1 x_1^{k-1} & v_2 x_2^{k-1} & \dots & v_n x_n^{k-1} \end{bmatrix} \tag{2.2}$$

Definition 12. *(Maximum Distance Separable Codes) Let C be a GRS code with parameters $[n, k, d]$. If the minimum distance d is equal to $n - k + 1$,d=n-k+1, the C is called as Maximum Distance Separable Codes(MDS).*

Definition 13. *(Cauchy Matrices) Let $A = [a_{ij}]_{k,l}$ be Cauchy matrix, entry of A is defined as*

$$a_{ij} = \frac{c_i d_j}{x_i + y_j}, 0 \leq i \leq k, 0 \leq i \leq l \tag{2.3}$$

where $x_0, ..., x_k$ are distinct elements, $y_0, ..., y_l$ are distinct elements and $x_i + y_j$, c_i, d_j cannot be zero.

.

CHAPTER 3

CODE EQUIVALENCE PROBLEM

Coding equivalence problem holds an important place in Coding Theory. If codes have same dimension, length, Hamming weight and minimum distance, they are called as equivalent codes. We study the code equivalence problem by using Generalized Reed Solomon(GRS) code. When the generator matrix of GRS code in the linear code family is turned into standard form, it is known that the matrix remaining from the unit matrix is the Cauchy matrix. However, even if the Cauchy matrix is known, it is difficult to find that which code this matrix belongs to and at which point this code is evaluated.

In this chapter, we work on the code equivalence problem to facilitate it and make progress for codes of a certain length and dimension.

Definition 14. *[11] Matrix A is as called super-regular matrix over $\mathcal{F}_q$ if determinant of every square submatrix in A is non-zero.*

Proposition 1. *[11] Let C be a code with parameters $[n, k, d]_q$ and G is a generator matrix of C with standard form $G = [I|A]$. Code C is MDS if and only if A is super regular. In addition to that, C is MDS code if and only if one of the following conditions are satisfied :*

- *Every k columns of a generator matrix G is linearly independent.*
- *Every $n - k$ columns of a parity-check matrix is linearly independent.*

Remark: Cauchy matrix is super-regular since the determinant of each sub-matrix of the Cauchy matrix is nonzero. Therefore, if A ,i.e $G = [I|A]$, is a Cauchy Matrix, code C is an MDS code.

Definition 15. *[1] Let C_1 and C_2 be two code with parameters $[n,k]_q$ over $\mathcal{F}_q$. C_1 and C_2 are called as equivalent code if one of codeword which is element of code C_1 is acquired by the other.*

There are three types of the method of equivalent code :

(1) Permutation of the coordinate of the codeword digits.
(2) Scaler multiplication with non-zero elements in $\mathcal{F}_q$.
(3) Applying field automorphism to all coordinates of the codeword digits.

Example 1: Let codeword of C_1 is $\{0000, 1000, 0110, 1110\}$. If codeword of code C_2 is $\{0000, 0010, 1100, 1110\}$, then C_1 and C_2 are equivalent code since we changed the position of coordinate 1 and 3 in C_1 so that we obtained C_2 .

Also, if codeword of code C_3 is $\{000, 120, 210\}$ and codeword of code C_4 is $\{000, 220, 110\}$, C_3 and C_4 are equivalent code since we multiplied the first coordinates of C_3 by 2 and obtained C_4.

Remark : Let C_1 and C_2 be two code with parameter $[n,k,d]$. Generator matrix of C_1 and C_2 are G_1, G_2 respectively. Standard form of G_1 and G_2 are

$$G_1 = [I_{k\times k}|A]$$

$$G_2 = [I_{k\times k}|B]$$

where A and B are $k \times (n-k)$ matrix. G_1 and G_2 are equivalent if and only if Cauchy matrix A and B are equivalent.

Remark : Let G be a generator matrix of code $C : [n,k]$ and row permutation of G is G' which is belongs to code $C' : [n,k]$ such that permutation $\sigma \in S_n$, and $c = (c_1, c_2, ..., c_n)$ is a codeword in C, so $(c_{\sigma(1)}, c_{\sigma(2)}, ..., c_{\sigma(n)}) \in C'$. Hence $G \neq G'$ but C and C' are equivalent code.

Example 2: Let consider the code $C : GRS_{[5,3]}(\alpha, v)$ over the field $\mathcal{F}_5$, where evaluation point $\alpha = (0, 1, 2, 3, 4)$ and $v = (1, 1, 1, 1, 1)$.

Generator matrix of C is

$$G=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 4 & 1 \end{bmatrix}$$

If we do some elementary row operation to G, we obtain standard form of G such that

$$G=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 4 & 1 \end{bmatrix} = \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 1 & 3 & 1 \end{array}\right] = [I|A] \text{ , and}$$

$A = \begin{bmatrix} 1 & 3 \\ 2 & 2 \\ 3 & 1 \end{bmatrix}$ is Cauchy matrix.

This example shows that how we can find the Cauchy matrix from the GRS code and its evaluation point. However, it is not an easy task to find the points at which the GRS code is calculated by using the Cauchy matrix.

Let's try to find the evaluation point of $C : GRS_{[5,3]}(\alpha, v)$. Assume that the Cauchy matrix A of code C is known, but the evaluation point α is unknown. When we look at Cauchy matrix A which has length 5 and dimension 3, we understand that evaluation point has 5 element and each element in α must be different from each other.

Assumption 1: Let assume that evaluation point $\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ is:

$$\begin{aligned} &\alpha_1 = x_1 = 0, \quad \alpha_3 = x_3 = 2, \quad \alpha_5 = y_2 = 4, \\ &\alpha_2 = x_2 = 1, \quad \alpha_4 = y_1 = 3, \end{aligned}$$

Using definition of Cauchy matrix, we can find matrix M which is generated from evaluation point α . If the evaluation point of Cauchy matrix A is $\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$, then M must be equal to A.

Let's try to see whether matrix M is equal to matrix A or not

$$M = \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array} \begin{array}{c} \begin{array}{cc} y_1 & y_2 \end{array} \\ \begin{pmatrix} \frac{c_1 d_1}{0-3} & \frac{c_1 d_2}{0-4} \\ \frac{c_2 d_1}{1-3} & \frac{c_2 d_2}{1-4} \\ \frac{c_3 d_1}{2-3} & \frac{c_3 d_2}{2-4} \end{pmatrix} \end{array} \stackrel{?}{=} \begin{bmatrix} 1 & 3 \\ 2 & 2 \\ 3 & 1 \end{bmatrix}$$

Let's define $\frac{1}{d_1} = d_1^*$ and $\frac{1}{d_2} = d_2^*$. If there are proper values of c_i and d_j, where $i \in \{1, 2, 3\}$ and $j \in \{1, 2\}$, Assumption 1 is correct.

For each entry of M, we have following six equations;

1. $\frac{c_1 d_1}{0-3} \stackrel{?}{=} 1 \Rightarrow c_1 d_1 - 3 \times 1 \equiv 2 \mod (5) \Longrightarrow c_1 = 2d_1^*$
2. $\frac{c_1 d_2}{0-4} \stackrel{?}{=} 3 \Rightarrow c_1 d_2 = -4 \times 3 \equiv 3 \mod (5) \Longrightarrow c_1 = 3d_2^*$
3. $\frac{c_2 d_1}{1-3} \stackrel{?}{=} 2 \Rightarrow c_2 d_1 = -2 \times 2 \equiv 1 \mod (5) \Longrightarrow c_2 = d_1^*$
4. $\frac{c_2 d_2}{1-4} \stackrel{?}{=} 2 \Rightarrow c_2 d_2 = -3 \times 2 \equiv 4 \mod (5) \Longrightarrow c_2 = 4d_2^*$
5. $\frac{c_3 d_1}{2-3} \stackrel{?}{=} 3 \Rightarrow c_3 d_1 = -1 \times 3 \equiv 2 \mod (5) \Longrightarrow c_3 = 2d_1^*$
6. $\frac{c_3 d_2}{2-4} \stackrel{?}{=} 1 \Rightarrow c_3 d_2 = -2 \times 1 \equiv 3 \mod (5) \Longrightarrow c_3 = 3d_2^*$

Equation 1 and 2 implies $c_1 = 2d_1^* = 3d_2^*$.

Equation 3 and 4 implies $c_2 = d_1^* = 4d_2^*$.

Equation 5 and 6 implies $c_3 = 2d_1^* = 3d_2^*$.

Therefore, pair of d_1^*, d_2^* can take one of these values $(1, 4)$, $(2, 3)$, $(3, 2)$ or $(4, 1)$.

Let's try to find if there are suitable c_1, c_2, c_3 values for d_1^*, d_2^*

For $(d_1^*, d_2^*) = (1, 4) \Rightarrow c_1 = 2$, $c_2 = 1$, $c_3 = 2$

For $(d_1^*, d_2^*) = (2, 3) \Rightarrow c_1 = 4$, $c_2 = 2$, $c_3 = 4$

For $(d_1^*, d_2^*) = (3, 2) \Rightarrow c_1 = 1$, $c_2 = 3$, $c_3 = 1$

For $(d_1^*, d_2^*) = (4, 1) \Rightarrow c_1 = 3$, $c_2 = 4$, $c_3 = 3$

Hence evaluation point can be $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3 = 2$, $\alpha_4 = 3$, $\alpha_5 = 4$.

Assumption 2: Assume that elements of evaluating points are $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3 = 2$, $\alpha_4 = 4$, $\alpha_5 = 3$.

$$N = \begin{bmatrix} \frac{c_1 d_1}{0-4} & \frac{c_1 d_2}{0-3} \\ \frac{c_2 d_1}{1-4} & \frac{c_2 d_2}{1-3} \\ \frac{c_3 d_1}{2-4} & \frac{c_3 d_2}{2-3} \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 2 & 2 \\ 3 & 1 \end{bmatrix},$$

Let's define $\frac{1}{d_1} = d_1^*$ and $\frac{1}{d_2} = d_2^*$.

In the Assumption 1, we found the equations for each entry of M. Similarly, we have following these equations for N;

1. $\frac{c_1 d_1}{0-3} \stackrel{?}{=} 1 \Rightarrow c_1 d_1 - 3 \times 1 \equiv 2 \mod (5) \Longrightarrow c_1 = 2d_1^*$
2. $\frac{c_1 d_2}{0-4} \stackrel{?}{=} 3 \Rightarrow c_1 d_2 = -4 \times 3 \equiv 3 \mod (5) \Longrightarrow c_1 = 3d_2^*$
3. $\frac{c_2 d_1}{1-3} \stackrel{?}{=} 2 \Rightarrow c_2 d_1 = -2 \times 2 \equiv 1 \mod (5) \Longrightarrow c_2 = d_1^*$
4. $\frac{c_2 d_2}{1-4} \stackrel{?}{=} 2 \Rightarrow c_2 d_2 = -3 \times 2 \equiv 4 \mod (5) \Longrightarrow c_2 = 4d_2^*$
5. $\frac{c_3 d_1}{2-4} \stackrel{?}{=} 3 \Rightarrow c_3 d_1 = -2 \times 3 \equiv 4 \mod (5) \Longrightarrow c_3 = 4d_1^*$
6. $\frac{c_3 d_1}{2-3} \stackrel{?}{=} 1 \Rightarrow c_3 d_2 = -1 \times 1 \equiv 4 \mod (5) \Longrightarrow c_3 = 4d_2^*$

Since first four points are equal, we can obtain same results as in the first assumption.

From equation 5 and 6 ;

$$\frac{c_3 d_1}{2-4} \stackrel{?}{=} 3 \Rightarrow c_3 = 4d_1^*$$

$$\frac{c_3 d_2}{2-3} \stackrel{?}{=} 1 \Rightarrow c_3 = 4d_2^*$$

These equations show that $d_1^* = d_2^*$ but this cannot be achieved since there are no such d_1^* and d_2^*, i.e $4d_1^* \neq d_1^*$. Hence assumption is wrong and there is no such evaluation point.

Question: Which evaluation points provide the same Cauchy matrix?

In this thesis we find that in $GRS_{[5,3]}(\alpha, v)$ code over finite field $\mathcal{F}_5$, if one evaluation point which provides Cauchy matrix A is found, all possible evaluation points can be found easily.

In example 1, we find that (0,1,2,3,4) is an evaluation point. Other points are found as follows

1. When we shift the (0,1,2,3,4), we get another evaluation point of matrix A such that

   (1,2,3,4,0) (2,3,4,0,1)
   (3,4,0,1,2) (4,0,1,2,3).

2. When we multiply evaluation point (0,1,2,3,4) by scalar c, i.e $c \in F_5$, we get another evaluation point and also if this point is shifted then get another evaluation point such that

   If $c = 2$ then (0,2,4,1,3) is the evaluation point of A. From item 1, we can shift (0,2,4,1,3). Therefore,

   (2,4,1,3,0), (4,1,3,0,2),
   (1,3,0,2,4), (3,0,2,4,1),

   are also evaluation points of A.

In the following proof, if two elements of the evaluation point are fixed and the other points are displaced, it is examined whether the obtained point can have the same cauchy matrix.

Proof: Let $C : GRS_{[5,3]}(\alpha, v)$ be a code, α=(x_1,x_2, x_3, y_1, y_2) be an evaluation point and A be a Cauchy matrix of the code.
Assume that y_1, y_2 are fixed and x_i, where $i \in \{1, 2, 3\}$ can be replaced among themselves. If the new point satisfies the matrix A, then this point is also an evaluation point for the same Cauchy matrix.

$$A=\begin{bmatrix} \frac{c_1d_1}{x_1-y_1} & \frac{c_1d_2}{x_1-y_2} \\ \frac{c_2d_1}{x_2-y_1} & \frac{c_2d_2}{x_2-y_2} \\ \frac{c_3d_1}{x_3-y_1} & \frac{c_3d_2}{x_3-y_2} \end{bmatrix} \stackrel{?}{=} \begin{bmatrix} \frac{c_1^*d_1^*}{x_1^*-y_1} & \frac{c_1^*d_2^*}{x_1^*-y_2} \\ \frac{c_2^*d_1^*}{x_2^*-y_1} & \frac{c_2^*d_2^*}{x_2^*-y_2} \\ \frac{c_3^*d_1^*}{x_3^*-y_1} & \frac{c_3^*d_2^*}{x_3^*-y_2} \end{bmatrix}$$

From first row, we have

$$\left.\begin{array}{l} \frac{c_1d_1}{x_1-y_1} \stackrel{?}{=} \frac{c_1^*d_1^*}{x_1^*-y_1} \\ \frac{c_1d_2}{x_1-y_2} \stackrel{?}{=} \frac{c_1^*d_2^*}{x_1^*-y_2} \end{array}\right\} \frac{c_1d_1}{c_1^*d_1^*} = \frac{x_1-y_1}{x_1^*-y_1}, \frac{c_1d_2}{c_1^*d_2^*} = \frac{x_1-y_2}{x_1^*-y_2}. \tag{3.1}$$

So, we get

$$\frac{c_1d_1}{c_1^*d_1^*}\frac{c_1^*d_2^*}{c_1d_2} = \frac{x_1-y_1}{x_1^*-y_1}\frac{x_1^*-y_2}{x_1-y_2}. \tag{3.2}$$

Similarly, From second and third row

$$\frac{c_2d_1}{c_2^*d_1^*}\frac{c_2^*d_2^*}{c_2d_2} = \frac{x_2-y_1}{x_2^*-y_1}\frac{x_2^*-y_2}{x_2-y_2},$$

$$\frac{c_3d_1}{c_3^*d_1^*}\frac{c_3^*d_2^*}{c_3d_2} = \frac{x_3-y_1}{x_3^*-y_1}\frac{x_3^*-y_2}{x_3-y_2}. \tag{3.3}$$

If equation (3.2) and (3.3) are combined, we can get

$$k = \frac{d_1}{d_1^*}\frac{d_2^*}{d_2} = \frac{x_1-y_1}{x_1^*-y_1}\frac{x_1^*-y_2}{x_1-y_2} = \frac{x_2-y_1}{x_2^*-y_1}\frac{x_2^*-y_2}{x_2-y_2} = \frac{x_3-y_1}{x_3^*-y_1}\frac{x_3^*-y_2}{x_3-y_2}, \tag{3.4}$$

where $k \in \mathcal{F}_5$.

Let $y_1 = 0$, $y_2 = 1$ and substitute these values into the equation (3.4)

$$k = \frac{x_1(x_1^*-1)}{x_1^*(x_1-1)} \Rightarrow x_1x_1^* - x_1 = k(x_1^*x_1 - x_1^*).$$

Thus, we get

$$(1-k)(x_1x_1^*) + kx_1^* - x_1 = 0.$$

For $k \neq 1$, if we change variable, we get

$$\left.\begin{array}{l} x_1 = \beta \\ x_1^* = \gamma \end{array}\right\} (1-k)(\beta\gamma) + k\gamma - \beta = 0.$$

Since every element in the evaluation point different from each other, (β, γ) can be :

(2,3), (3,2), (2,4)
(4,2), (3,4), (4,3)
(2,2), (3,3), (4,4)

Let's examine the point (2,3):
$\beta = 2, \gamma = 3$

$$\left.\begin{array}{r} (1-k)(\beta\gamma) + k\gamma - \beta = 0 \\ (1-k)6 + k.3 - 2 = 0 \end{array}\right\} k = 3$$

So (x_1, x_1^*) can be (2,3).
Now let's try if there is an appropriate (x_2, x_2^*) value when $(x_1, x_1^*) = (2, 3)$

From equation (3.4),

$$\frac{x_2(x_2^* - 1)}{x_2^*(x_2 - 1)} = k = 3 \Longrightarrow 3x_2^* x_2 - 3x_2^* = x_2 x_2 * - x_2 \tag{3.5}$$

Since $y_1 = 0$, $y_2 = 1$, $x_1 = 2$ and $x_1^* = 3 \Rightarrow (x_2, x_2^*)$ can be (3,2), (3,4), (4,2), (4,4).

Let's examine possible evaluation points of (x_2, x_2^*) and (x_2, x_2^*):

Case 1.1 $(x_2, x_2^*) = (3, 2)$
Substitute (x_2, x_2^*) into equation (3.5),

$$3x_2^* x_2 - 3x_2^* = x_2 x_2 * - x_2$$
$$3.2 - 3.2 \neq 3.2 - 3,$$

so $(x_2, x_2^*) \neq (3, 2)$.

Case 1.2 $(x_2, x_2^*) = (3, 4)$,
Substitute (x_2, x_2^*) into equation (3.5)

$$3x_2^* x_2 - 3x_2^* = x_2 x_2 * - x_2$$
$$3.4.3 - 3.4 = 3.4 - 3,$$

so (x_2, x_2^*) can be (3,4).

Case 1.2.1 (x_3, x_3^*) can take only (4,2). But this point does not satisfy equation(3.5). Therefore, $(x_2, x_2^*) \neq (3, 4)$.

Case 1.3 $(x_2, x_2^*) = (4, 2)$
Substitute (x_2, x_2^*) into equation (3.5),

$$3x_2^* x_2 - 3x_2^* = x_2 x_2 * - x_2$$
$$3.4.2 - 3.2 \neq 4.2 - 4,$$

$(x_2, x_2^*) \neq (4, 2)$.

Case 1.4 $(x_2, x_2^*) = (4, 4)$
Substitute (x_2, x_2^*) into equation (3.5),

$$3x_2^* x_2 - 3x_2^* = x_2 x_2 * - x_2$$
$$3.4.4 - 3.4 \neq 4.4 - 4,$$

so, $(x_2, x_2^*) \neq (4, 4)$.

Hence Case 1.1 is wrong, $(x, y) = (x_1, x_1^*) \neq (2, 3)$.

Doing the same operation for

(3,2), (2,4), (4,2),
(3,4), (4,3), (2,2),
(3,3), (4,4)

We see that none of them satisfy Equation (3.5). Hence if y_1, y_2 are fixed, this point does not satisfy Cauchy matrix A.

Remark : In above example, we say that if one evaluation point is found, other evaluation points which satisfy Cauchy matrix can be found, such that it will be the shifted elements of known evaluation point or it will be multiplication of the elements of known evaluation point .

In code $C : [5, 3]$, evaluation point α has 5 elements , so there will be 4 shift operations:
$\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$

Shift 1: $(\alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_1)$ **Shift 2:** $(\alpha_3, \alpha_4, \alpha_5, \alpha_1, \alpha_2)$
Shift 3: $(\alpha_4, \alpha_5, \alpha_1, \alpha_2, \alpha_3)$ **Shift4:** $(\alpha_5, \alpha_1, \alpha_2, \alpha_3, \alpha_4)$

In $\mathcal{F}_5$, there are 3 constant multiplications since multiplying 0 and 1 would be meaningless. Therefore, In $GRS_{[5,3]}(\alpha, v)$ over $\mathcal{F}_5$, all the following evaluation points have the same Cauchy matrix.

- (0,1,2,3,4), (1,2,3,4,0), (2,3,4,0,1), (3,4,0,1,2), (4,0,1,2,3)
- (0,2,4,1,3), (2,4,1,3,0), (4,1,3,0,2), (1,3,0,2,4), (3,0,2,4,1)
- (0,3,1,4,2), (3,1,2,4,0), (1,2,4,0,3), (2,4,0,3,1), (4,0,3,1,2)
- (0,4,3,2,1), (4,3,2,1,0), (3,2,1,0,4), (2,1,0,4,3), (1,0,4,3,2)

Hence twenty evaluation points have the same Cauchy matrix. Five elements in evaluation point can take $5! = 120$ different positions. Therefore code $C : [5, 3]$ has six different Cauchy matrices. These Cauchy matrices are:

$$\begin{bmatrix} 1 & 3 \\ 2 & 2 \\ 3 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 1 & 3 \\ 3 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 1 \\ 2 & 2 \\ 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ 3 & 1 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 3 & 1 \\ 1 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 1 \\ 1 & 3 \\ 2 & 2 \end{bmatrix}.$$

Remark : There are 120 different evaluation points in the code $C : [5, 3]$ and it takes time to find the right one. At the beginning of the above example, we said that we could easily find other evaluation points when we find the evaluation point that is provided by the Cauchy matrix. So, trying six different evaluation points will increase the probability of finding the right point in the assumption.

Let's try same shift and constant multiplication operations for code $C : [7, 4]$ over finite field $\mathcal{F}_7$.

Example 3: Let consider the code $C : GRS_{[7,4]}(\alpha, v)$ over the field $\mathcal{F}_7$ where $\alpha = (0, 1, 2, 3, 4, 5, 6)$ and $v = (1, 1, 1, 1, 1, 1, 1)$.

Generator matrix of C is

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 2 & 2 & 4 & 1 \\ 0 & 1 & 1 & 6 & 1 & 6 & 6 \end{bmatrix}$$

Standard form of G is

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 2 & 2 & 4 & 1 \\ 0 & 1 & 1 & 6 & 1 & 6 & 6 \end{bmatrix} = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 6 & 3 & 4 \\ 0 & 1 & 0 & 0 & 4 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 4 \\ 0 & 0 & 0 & 1 & 4 & 3 & 6 \end{array}\right] = [I|A].$$

Cauchy matrix A is

$$A = \begin{bmatrix} 6 & 3 & 4 \\ 4 & 1 & 1 \\ 1 & 1 & 4 \\ 4 & 3 & 6 \end{bmatrix}$$

We want to find the evaluation points that satisfies the matrix A. By looking matrix A, we can say that length of the code is 7 and dimension of the code is 4. Therefore, evaluation point has seven elements.

If the point $(0,1,2,3,4,5,6)$ puts in the definition of the Cauchy matrix, it satisfies the matrix A.

Let's check if the shift and constant multiplication is valid in the code $C:[7,4]$. Firstly, try to find Cauchy matrix of $(1,2,3,4,5,6,0)$:

$$G=\begin{bmatrix}1&1&1&1&1&1&1\\1&2&3&4&5&6&0\\1&4&2&2&4&1&0\\1&1&6&1&6&6&0\end{bmatrix}=\left[\begin{array}{cccc|ccc}1&0&0&0&6&3&4\\0&1&0&0&4&1&1\\0&0&1&0&1&1&4\\0&0&0&1&4&3&6\end{array}\right]=[I|A]\ ,$$

So, evaluation point $(1,2,3,4,5,6,0)$ has the same Cauchy matrix. If other shifting points are tried, same Cauchy matrix is obtained. In addition to that multiplication of constant $c\in\mathcal{F}_7$, i.e $c\neq 0,1$ has the same Cauchy matrix. In addition, Since Cauchy matrix $A_{4\times 3}$ has 4 rows, there are $4!=24$ different Cauchy matrices.

It is said in the Example 2 that $(0,1,2,3,4)$ and $(1,2,3,4,0)$ have the same Cauchy matrix in code $C:[5,3]$ over the field $\mathcal{F}_5$. The next example examines the same code over the finite field $\mathcal{F}_7$.

Example 4: Let consider the code $C:GRS_{[5,3]}(\alpha,v)$ over the field $\mathcal{F}_7$ where $\alpha=(0,1,2,3,4)$ and $v=(1,1,1,1,1)$. Generator matrix of $C_{[5,3]}$ is

$$G_1=\begin{bmatrix}1&1&1&1&1\\0&1&2&3&4\\0&1&4&2&2\end{bmatrix}=\left[\begin{array}{ccc|cc}1&0&0&1&3\\0&1&0&4&6\\0&0&1&3&6\end{array}\right]=[I|A_1].$$

If $C:GRS_{[5,3]}(\alpha,v)$ over finite field $\mathcal{F}_7$ where $\alpha=(1,2,3,4,0)$ and $v=(1,1,1,1,1)$. Generator matrix of $C_{[5,3]}$ is

$$G_2=\begin{bmatrix}1&1&1&1&1\\1&2&3&4&0\\1&4&2&2&0\end{bmatrix}=\left[\begin{array}{ccc|cc}1&0&0&1&3\\0&1&0&4&4\\0&0&1&3&1\end{array}\right]=[I|A_2].$$

These codes have different Cauchy matrices, $A_1 \neq A_2$. Therefore, if the length of code smaller than number of field element, above rules,i.e. shifting evaluation point and multiplication of constant number, are not satisfied.

CHAPTER 4

ENTANGLEMENT ASSISTED QUANTUM ERROR CORRECTING CODE (EAQECC)

Entanglement Assisted Quantum Error Correcting Code (EAQECC) is another important application area of coding theory. Before EAQECCs, in order to obtain a quantum code from a linear code, the linear code had to be dual containing.

Definition 16. *Let C be a linear code and $C^{\perp}$ be a dual code of C. If $C^{\perp} \subset C$ then it is called dual containing.*

If quantum code uses pre-shared entanglement then it is called Entanglement Assisted Quantum Error Correcting Code (EAQECC) and it is denoted by $[[n, k, d; c]]_q$ where k is a logical qudits, n is a physical qudits, c is a copies of maximal entanglement states. Generalized Reed Solomon (GRS) codes are good codes for constructing EAQECCs.

The definition of Singleton bound for quantum code is different than the linear code. Following theorem gave the bound for EAQECCs:

Theorem 1. *[5] Let C be an EAQECC with parameter $[[n, k, d; c]]_q$. Parameters of C satisfies*

$$n + c - k \geq 2(d - 1)$$

where $0 \leq c \leq n - 1$. This is the singleton bound for EAQECC.

Hull of code makes easy to calculate pre-shared entanglement. The definition of Hull is as follows:

Definition 17. *Let C be a code over $\mathcal{F}_q$. The Hull of C is*

$$Hull(C) := C^{\perp} \cap C$$

If $Hull(C) = 0$ then C is called Linear Complementary Dual (LCD).

Definition 18. *Let C_1 and C_2 be two linear codes over $\mathcal{F}_q$. The Hull is*

$$Hull(C_1, C_2) := C_1^{\perp} \cap C_2.$$

4.1 CONSTRUCTION Of ENTANGLEMENT ASSISTED QUANTUM ERROR CORRECTING CODES

The following theorem shows that how to obtain EAQECCs from linear codes.

Theorem 2. *[14] Let $C_1 : [n, k_1, d_1]_q$ and $C_2 : [n, k_2, d_2]_q$ are two linear codes with parity check matrices H_1 and H_2, respectively. Then there exists an Entanglement Assisted Quantum Error Correcting Codes(EAQECC) with parameters $[[n, k_1 + k_2 - n + c, min\{d_1, d_2\}; c]]_q$ where required number of maximally entanglement states is $c = rank(H_1 H_2^{\top})$.*

In this part, we did literature review about which article used this theorem and examined how they used it.

4.1.1 USING ℓ-INTERSECTION PAIRS

Definition 19. *[4] If two linear codes intersect and dimension of intersection equal to ℓ then we say that these codes are linear ℓ-intersection pair .*

Theorem 3. *[4] Let $C_1 = [n, k_1]_q$ and $C_2 = [n, k_2]_q$ are two linear codes, G_1 and G_2 are their generator matrices and H_1 and H_2 are their parity check matrices, respectively . If C_1 and C_2 dimension of intersection is ℓ then rank of $H_1 G_2^t$ and $G_1 H_2^t$ independent of H_1, H_2 , G_1, G_2 and equal to*

$$rank(G_1 H_2^t) = k_1 - \ell,$$
$$rank(H_1 G_2^t) = k_2 - \ell$$

where $0 \leq \ell \leq min\{k_1, k_2\}$.

Proof: If dimension of the intersection C_1 , C_2 is ℓ then

$$rank(G_1 H_2^t) = rank(H_2 G_1^t) = k_1 - \ell,$$
$$rank(G_2 H_1^t) = rank(H_1 G_2^t) = k_2 - \ell.$$

$C_1 = \{xG_1 | x \in F_q^k\} \subseteq F_q^n$
$C_2 = \{y \in F_q^n | yH_2^T = 0 \in F_q^{n-k_2}\}$

$$\left.\begin{array}{r} G_1 : k_1 \times n, G_2 : k_2 \times n \\ H_1 : (n-k_1) \times n, H_2 : (n-k_2) \times n \end{array}\right\} G_1 H_2^T : k_1 \times (n - k_2)$$

Let ψ is a map such that $\psi : x \to xG_1 H_2^T \in F_q^{n-k_2}$
Claim: $dim(Im\psi) = k_1 - l$
Proof of claim: $F_q^{k_1} \xrightarrow{\psi_1} F_q^n \xrightarrow{\psi_2} F_q^{n-k_2}$

$$\left.\begin{array}{r} \psi_1 : x \mapsto xG_1 \\ \psi_2 : y \mapsto yH_2^T \end{array}\right\} \psi = (\psi_1 \circ \psi_2)$$

$Ker(\psi_2) = C_2$, $Im(\psi_1) = C_1 = k_1$
$Im(\psi) \cong Im(\psi_1)/(Im(\psi_1) \cap Ker(\psi_2))$
$dim(\psi) = rank(G_1 H_2^T) = k_1 - dim(Im(\psi_1) \cap ker(\psi_2)) = k_1 - l$

Remark: In addition to Theorem 3 :
Let C_1 and C_2 are linear ℓ-intersection pair. Let C be a code which is equal to

$$C = C_1^{\perp} : [n, k_1', d_1^{\perp}], \text{ where } k_1' = n - k_1.$$

Generator matrix of C is G. Since parity check matrix is generator matrix of dual code, G is equal to parity check matrix of code C_1, i.e $G = H_1$.
From Theorem 2 we know that $rank(GH_2^T) = k_1' - l$ where H_2 is parity check matrix of C_2 . Hence there is an EAQECC with parameter $[[n, k_2 - l, min\{d_1^{\perp}, d_2\}; k_1' - l]]_q$.

The following theorem shows that when $n \leq q-1$, there exists an ℓ-intersection pair of code for all probable parameters.

Theorem 4. *[4] Let $q \geq 3$ be a prime power and C_1, C_2 are two code n, k_1, k_2, l be non-negative integers such that $k_1 \leq n \leq q+1$. If $l \leq \{k_1, k_2\}$ and $k_1 + k_2 \leq n + l$ then there is a linear ℓ-intersection pair of MDS codes with parameters $[n, k_1, n - k_1 + 1]$ and $[n, k_2, n - k_2 + 1]$.*

Remark : Let combine Theorem 4 and previous remark, when $q \geq 3$ there exists an MDS EAQECC $[[n, k_2 - l, min\{k_1 + 1, n - k_2 + 1\}; k_1 - l]]$.

If $n = k_1 + k_2$, we get following theorem:

Theorem 5. *[4]. Let q be a prime power which is greater than 2 and $0 \leq k \leq n \leq q+1$ and $0 \leq l \leq min\{k, n-k\}$. Then there is an $[[n, n-k-l, k+1; k-l]]_q$ MDS EAQECC .*

4.1.2 USING HULL OF CODE

Theorem 2 is about constructing EAQECC from linear code but it can be difficult to calculate the required entanglement $c = rank(H_1 H_2^t)$. With Lemma 1 thanks to the hull we can find entanglement without calculating rank,

Lemma 1: [9] Let C_1 and C_2 be linear codes with parameters $[n, k_1, d_1]_q$,$[n, k_2, d_2]_q$, respectively. H_1 and H_2 are parity check matrices of C_1 and C_2. Assume that $dim(Hull(C_1, C_2)) = l_1$ and $dim(Hull(C_2, C_1)) = l_2$, then $rank(H_1 H_2^T) = n - max\{k_1 + l_1, k_2 + l_2\}$.

Proof: Let $C_1 = \{x \in F_q^n | H_1 x^T = O_{(n-k_1)\times 1}\}$, $C_2 = \{y \in F_q^n | H_2 y^T = O_{(n-k_2)\times 1}\}$ be two linear codes. $H_1 : (n-k_1) \times n$ and $H_2 : (n-k_2) \times n$ are two parity check matrices of these linear codes.

$$dim(Hull(C_1, C_2)) = l_1 \Rightarrow dim(C_1^{\perp} \cap C_2) = l_1,$$
$$dim(Hull(C_2, C_1)) = l_2 \Rightarrow dim(C_2^{\perp} \cap C_1) = l_2.$$

Let assume that $k_1+l_1 \leq k_2+l_2$. We want to show that $rank(H_1H_2^T) = n-(k_2+l_2) = n-k_2-l_2$. Since H_2 is generator matrix of dual of C_2, $\alpha \in C_2^{\perp}$ if and only if α in row space of H_2. We know that $rank(H_1) = n-k_1$. Let ψ_1 and $\psi_2^{(-1)}$ are two maps.

$$\psi_1 : F_q^n \longrightarrow F_q^{n-k_1}$$
$$x \longmapsto H_1x^T$$

$$\psi_2^{(-1)} : F_q^{n-k_2} \longrightarrow F_q^n$$
$$y \longmapsto yH_2$$

$Ker(\psi_1) = C_1$

$rank(C_2^t) = n-k_2$

$Im(\psi_2^{(-1)}) = C_2^{\perp}$, since
$< yH_2, c_2 >= yH_2c_2^T = 0$

Consider, $\psi : F_q^{n-k_2} \xrightarrow{\psi_2^{(-1)}} F_q^n \xrightarrow{\psi_1} F_q^{n-k_1}$
$$y \longmapsto H_1H_2^{\top}y^{\top}$$

So, $Im(\psi) \cong Im(\psi_2^{(-1)})/(Im(\psi_2^{(-1)}) \cap Ker(\psi_1))$.
Hence $dim(\psi) = rank(H_1H_2^T) = n-k_2-dim(Im(\psi_2^{(-1)}) \cap Ker(\psi_1)) = n-k_2-l_2$.

Remark: In addition to Lemma 1:
If $k_1+l_1 \geq k_2+l_2$ then there exist an EAQECC with parameter $[[n, k_2-l_1, min\{d_1, d_2\}; n-k_1-l_1]]_q$. Since $c = rank(H_1H_2^{\top}) = n-max\{k_1+l_1, k_2+l_2\}$, $k_1+l_1 \geq k_2+l_2$ then we get $c = rank(H_1H_2^{\top}) = n-(k_1+l_1)$.

Corrollary 1: [9] $C_1 : [n, k_1, d_1]_q$, $C_2 : [n, k_2, d_2]_q$ are two linear codes and $Hull(C_1, C_2) = l_1 = 0$ and $Hull(C_1, C_2) = l_2$ with $k_1 \geq k_2 + l_2$. Using Theorem 3 we can easily show that ,

$$k = k_1 + k_2 - n + c = k_1 + k_2 - n + (n-(k_1-l_1)) = k_2 - l_1 = k_2$$

then there exits an EAQACC with parameters $[[n, k_2, min\{d_1, d_2\}; n-k_1]]$.

Corrollary 2: [9] Assume that $C : [n, k, d]_q$ MDS LCD code then there exists and MDS maximal entanglement EAQECC code with parameter $[[n, k, d, n-k]]_q$.

From Corollary 2, If we have MDS LCD code, then MDS maximal entanglement EAQECC can be constructed .

Lemma 2: [3] Let $c = (v_1 f(x_1), v_2 f(x_2), ..., v_n f(x_n))$ be a codeword of k-dimensional $GRS(x, v)$ and c also codeword of dual of $GRS(x, v)$, i.e $GRS^{\perp}(x, v)$, if and only if there exists a polynomial $g(x) \in \mathcal{F}_q[x]$ with degree of $g(x)$ is less than or equal to $n - k + 1$ then

$$(v_1^2 f(x_1), v_2^2 f(x_2), ..., v_n^2 f(x_n)) = (u_1 g(x_1), u_2 g(x_2), ..., u_n g(x_n))$$

where $u_i = \prod_{1 \leq j \leq n j \neq i} (x_i - x_j)^{-1}$ for $i \leq i \leq n$.

Proposition 2. *[6] Let C be a linear code with parameters $[n, k, d]_q$, G be a generator matrix of C and H be a parity check matrix of C. Rank of (HH^T) and rank of (GG^T) are independent of H and G and equal to*

$$rank(HH^T) = n - k - dim(Hull(C)) = n - k - dim(Hull(C^{\perp}))$$
$$rank(GG^T) = k - dim(Hull(C)) = k - dim(Hull(C^{\perp})).$$

Proposition 3. *[6] Let C be a linear code with parameters $[n, k, d]_q$ and dual of C is $C^{\perp} : [n, n - k, d^{\perp}]_q$. There are*

$$[[n, k - dim(Hull(C)), d; n - k - dim(Hull(C))]] \text{ and}$$
$$[[n, n - k - dim(Hull(C)), d^{\perp}; k - dim(Hull(C))]] \text{ EAQECC.}$$

In addition, if C is MDS code then these two EAQECCare also MDS.

Article [8] gives the construction of some MDS codes using the hull of the code. Theorem 6, Theorem 7, Theorem 8, Theorem 9, Theorem 10 are some of these constructions.

Theorem 6. *[8] Let q be power of 2 which is greater than 2. Assume that $3 < n \leq q$ then there is an $[n, k]$ MDS code which has ℓ-dimensional hull for any $1 \leq \ell \leq k$.*

Theorem 7. *[8] Let q be an odd prime power which is greater than 3. Assume that $n > 3$ and n divides $(q - 1)$ then exists an $[n, k]$ MDS code which has ℓ-dimensional hull for any $1 \leq \ell \leq k - 1$.*

Theorem 8. *[8] Let q be an odd prime power which is sutisfy $q \equiv 1 \mod 4$ and let m be an integer number greater than 1 such that m divides $(q - 1)$. Assume that $n = 2m < q - 1$, there is an $[n, k]$ MDS code which has ℓ-dimensional hull for any $1 \leq \ell \leq k - 1$.*

Theorem 9. *[8] Let q be an odd prime power which is greater than 3. Assume that $n > 3$ and n divides (q) then is an $[n, k]$ MDS code which has ℓ-dimensional hull for any $1 \leq \ell \leq k$.*

Theorem 10. *[8] Let q be an odd prime power which is sutisfied $q \equiv 1 \mod 4$ and let m be an integer number greater than 1 such that m divides (q). Assume that $n = 2m < q$, there is an $[n, k]$ MDS code which has ℓ-dimensional hull for any $1 \leq \ell \leq k$.*

If Theorem 6, Theorem 9, Theorem 10 are combined with Proposition 3 , following MDS EAQECCs are obtained [8]:

For $1 \leq s \leq k$ and $3 < q$

1. Combination of Theorem 6 and the Main theorem:
   If q be a power of 2 which is greater than 2 and $1 \leq n \leq q$ then there are $[[n, k-s, n-k+1; n-k-s]]_q$ and $[[n, n-k-s, k+1; k-s]]_q$ MDS EAQECCs.

2. Combination of Theorem 9 and the Main theorem
   If n is greater than 3 and n divides q then there are $[[n, k-s, n-k+1; n-k-s]]_q$ and $[[n, n-k-s, k+1; k-s]]_q$ MDS EAQECCs.

3. Combination of Theorem 10 and the Main theorem
   Let m be an integer number which is greater than 1, and $n = 2m$. If $q \equiv 1 \mod 4$ and $n < q$ then there are $[[n, k-s, n-k+1; n-k-s]]_q$ and $[[n, n-k-s, k+1; k-s]]_q$ MDS EAQECCs.

If Theorem 7, Theorem 8 are combined with Proposition 3 , following MDS EAQECCs are obtained [8]:

For $1 \leq s \leq k-1$ and $3 < q$

1. Combination of Theorem 7 and the Main theorem
   If $n \mid q$ where $n > 3$ then there are $[[n, k-s, n-k+1; n-k-s]]_q$ and $[[n, n-k-s, k+1; k-s]]_q$ MDS EAQECCs.

2. Combination of Theorem 8 and the Main theorem

   Let m be an integer number which is greater than 1, and $n = 2m$. If $q \equiv 1 \mod 4$ and $n < q - 1$ then there are $[[n, k - s, n - k + 1; n - k - s]]_q$ and $[[n, n - k - s, k + 1; k - s]]_q$ MDS EAQECCs.

CHAPTER 5

CONCLUSION

In this thesis, we explain Code Equivalence Problem and Entanglement Assisted Quantum Error Correcting Codes (EAQECCs) which are taken an important place in Coding Theory.

In the first chapter, in order to understand what is coding theory , example from daily life are given, its historical process and its application areas are mentioned. We give some information about EAQECC and code equivalence problem which are application areas of coding theory.

In Chapter 2, we give some definitions and their mathematical notation that are the basis of coding theory, which will be used in all other chapters.

In Chapter 3, we study code equivalence problem using Generalized Reed Solomon (GRS) Codes and we dwell upon permutation equivalence. We have shown an easy way to find equivalent linear codes which have same Cauchy matrices in $[5, 3]$ over $\mathcal{F}_5$ and $[7, 4]$ over $\mathcal{F}_7$ codes. We've seen that this easy way works for $[5, 4]$ over $\mathcal{F}_5$ and $[7, 3]$,$[7, 5]$,$[7, 6]$ over $\mathcal{F}_7$ codes using *SageMath*. As future work, we plan to generalize and prove this technique.

In Chapter 4, we do some literature review about quantum codes. At the beginning of the chapter some definitions are given which are about quantum codes. EAQECC allows us to obtain quantum code from linear code without dual containing condition. We based on Theorem 3 and examined how some articles use this theorem. We give the EAQECC parameters which construct using this theorem.

REFERENCES

[1] I. G. Bouyukliev, About the code equivalence, Advances in Coding Theory and Cryptology, Shaska, T., Huffman, W.C., Joyner, D., and Ustimenko, V., Eds., Series on Coding Theory and Cryptology, 3, p. 126–151, 2007.

[2] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exists, Phys. Rev. A, Gen. Phys., 54(2), pp. 1098–1105, 1996.

[3] B. Chen and H. Liu, New constructions of mds codes with complementary duals, IEEE Transactions on Information Theory, 64(8), pp. 5776–5782, Aug 2018, ISSN 0018-9448.

[4] K. Guenda, T. Gulliver, S. Jitman, and S. Thipworawimon, Linear l- intersection pairs of codes and their applications, 2018.

[5] M. H. Hsieh, I. Devetak, and T. Brun, Correcting quantum errors wtih entanglement, Science, 314, pp. 436–439, 2006.

[6] K.Guenda, S. Jitman, and T. Gulliver, Constructions of good entanglement-assisted quantum error correcting codes, Des. Codes Cryptogr., 86, pp. 121–136, 2018.

[7] J. Leon, Computing automorphism groups of error-correcting codes, IEEE Trans. Inform. Theory, 28, pp. 496–511, 1982.

[8] G. Luo, X. Cao, and X. Chen, Mds codes with hulls of arbitrary dimensions and their quantum error correction, IEEE Transactions on Information Theory, 65(5), pp. 2944–2952, May 2019, ISSN 0018-9448.

[9] F. R. F. Pereira, R. Pellikaan, G. G. L. Guardia, and F. M. de Assis, Entanglement-assisted quantum codes from algebraic geometry codes, ArXiv, abs/1907.06357, 2019.

[10] E. Petrank and R. Roth, Is code equivalence easy to decide?, IEEE Trans. Inform. Theory, 43, pp. 1602–1604, 1997.

[11] R. Roth, *Introduction to Coding Theory*, Cambridge, U.K.: Cambridge Univ. Press, 2006.

[12] N. Sendrier, The support splitting algorithm, IEEE Trans. Inform. Theory, 46, pp. 1193–1203, 2000.

[13] A. M. Steane, Error correcting codes in quantum theory, Phys. Rev. A, Gen. Phys., 77(5), pp. 793–797, 1996.

[14] M. M. Wilde and T. A. Brun, Optimal entanglement formulas for entanglement-assisted quantum coding, Phys. Rev. A, 77, 064302, 2008.