HULLS OF LINEAR CODES AND THEIR APPLICATIONS

By

Ms. Satanan THIPWORAWIMON

A Thesis Submitted in Partial Fulfillment of the Requirements

for Doctor of Philosophy (MATHEMATICS)

Department of MATHEMATICS

Graduate School, Silpakorn University

Academic Year 2020

เปลือกหุ้มของรหัสเชิงเส้นและการประยุกต์

โดย

Ms.Satanan Thipworawimon

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปรัชญาดุษฎีบัณฑิต

สาขาวิชาคณิตศาสตร์ แบบ 2.1 ปรัชญาดุษฎีบัณฑิต นานาชาติ

ภาควิชาคณิตศาสตร์

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

ปีการศึกษา 2563

HULLS OF LINEAR CODES AND THEIR APPLICATIONS

By

Ms. Satanan THIPWORAWIMON

A Thesis Submitted in Partial Fulfillment of the Requirements

for Doctor of Philosophy (MATHEMATICS)

Department of MATHEMATICS

Graduate School, Silpakorn University

Academic Year 2020

Title	Hulls of linear codes and their applications
By	Satanan THIPWORAWIMON
Field of Study	(MATHEMATICS)
Advisor	Associate Professor SOMPHONG JITMAN , Ph.D.

Graduate School Silpakorn University in Partial Fulfillment of the Requirements for the Doctor of Philosophy

.... Dean of graduate school

(Associate Professor Jurairat Nunthanid, Ph.D.)

Approved by

.... Chair person

(Assistant Professor RATANA SRITHUS , Ph.D.)

.... Advisor

(Associate Professor SOMPHONG JITMAN , Ph.D.)

.... External Examiner

(Professor Patanee Udomkavanich , Ph.D.)

59305803 : MAJOR: MATHEMATICS

KEY WORDS : HULLS, LINEAR CODES, LINEAR ℓ-INTERSECTION PAIRS, SELF-ORTHOGONAL CODES, QUANTUM CODES

MISS SATANAN THIPWORAWIMON : HULLS OF LINEAR CODES AND THEIR APPLICATIONS. THESIS ADVISOR : ASSOC. PROF. SOMPONG JITMAN, Ph.D.

Hulls of linear codes have been of interest and extensively studied due to their rich algebraic structures and wide applications. In this thesis, properties and characterizations of hulls of linear codes are given in terms of the Gramians of their generator and parity-check matrices. The Gramian of a generator matrix of every linear code over a finite field of odd characteristic is shown to be diagonalizable. Consequently, it is shown that a linear code over a finite field of odd characteristic is complementary dual if and only if it has an orthogonal basis. Subsequently, a linear ℓ-intersection pair of linear codes is studied as a generalization of hulls. Characterizations and constructions of linear ℓ-intersection pairs of linear codes are given in terms of their corresponding generator and parity-check matrices. As applications, constructions of good entanglement-assisted quantum error-correcting codes are given using properties of hulls and linear ℓ-intersection pair of codes.

ACKNOWLEDGEMENTS

Firstly, I would like to express my sincere gratitude to my advisor, Assoc. Prof. Dr. Sompong Jitman, for the continuous support of my Ph.D. study and related researchs, for his patience, attention, suggestions, motivation, immense depth of knowledge, and giving me an opportunity to go abroad; fulfilled my childhood dreams. His guidance and willingness to give his time so generously have been very much appreciated. Without his steering in the right direction and precious support, it would not be possible to conduct this thesis succeed. I could not have imagined having a better advisor and mentor for my Ph.D. education.

Besides my advisor, I would like to thank the rest of my thesis committees: Prof. Dr. Patanee Udomkavanich and Asst. Prof. Dr. Ratana Srithus, for their insightful comments and suggestions incentivizing me to widen my research from various perspectives.

My sincere thanks also go to Prof. Dr. Aaron Gulliver, and Prof. Dr. Kenza Guenda, who dedicated to the role as my oversea supervisor and provided me an opportunity to join their team as a graduate visiting research student at the University of Victoria, Canada. Without kindness and precious support it would not be possible to gain a new experience in my life. I have very fond of valuable memories of my time there.

I would also like to extend my appreciation to all academic staffs who have instructed and taught me for valuable knowledge and the members of the Department of Mathematics in the Faculty of Science at Silpakorn University. Moreover, special thanks to the Development and Promotion of Science and Technology Talents Project (DPST) for financial support throughout my undergraduate, graduate, and research study in Canada.

Finally, but by no means least, I must express my very profound gratitude to my beloved family and to my lovely friends for providing me with unfailing support and unbelievable continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Satanan THIPWPORAWIMON

TABLE OF CONTENTS

Chapter 1

Introduction

Coding theory introduced in 1948 by Claude Shannon [40] is a branch of Mathematics concerned about the properties of codes with the design of error-correcting codes for the reliable transmission of information across noisy channels.

Self-orthogonal codes form an important class of linear codes due to their nice algebraic structures. Precisely, self-orthogonal codes can be constructed from combinatorial designs, polynomials, and invariant subspaces. Further, self-orthogonal codes are practically useful in communications systems, various applications, and link with other objects as shown in [30], [34] and references therein. Recently, these codes have become more interesting due to their applications in constructions of quantum error-correcting codes [17], [28] and [29].

Self-dual codes is a special case of self-orthogonal codes. The study of self-dual codes is also an interesting problem since these codes play an important role in applications. A number of best known codes are from the family of self-dual codes and they have rich mathematical properties. These codes link to other objects in mathematics such as geometries [24], designs [14], [15], graphs [22] and group rings [16], [20]. Such codes have extensively been studied by many coding theorists.

Many error correcting codes are known to be linear complementary dual (LCD) codes. A great deal of works on the constructions and studies of LCD codes has been done by several tasks. It has been introduced and applied in two-user binary adder channel in [33]. Later in [38], LCD codes have been shown to be asymptotically good and meet the Gilbert-Varshamov bound. LCD codes have applications in information protection such as the security of the information processed in [8]. This brings more attention to the study of a class of good LCD codes in [9], [19] and [27]. Recently, entanglement-assisted quantum error correcting codes (EAQECCs) can be constructed using LCD codes in [23] and [36].

The hull of a linear code has been introduced to classify finite projective planes in [1]. Later, it turned out that the hulls of linear codes play a vital role in determining the complexity of some algorithms in coding theory. Moreover, most of the algorithms do not work if the size of the hull is large. Recently, the hulls of linear codes have been applied in constructing good entanglement-assisted quantum error correcting codes in [23]. Due to these wide applications, the hulls of linear codes and their properties have been extensively studied. The number of linear codes of length n over $\mathbb{F}_q$ whose hulls have a common dimension and the average dimension of the hull of linear codes were studied in [39]. Moreover, it can be shown that the average dimension of the hull of linear codes is a positive constant dependent of n. It has been shown that either the average dimension of the hull of such codes is zero or it grows at the same rate with n. From above, the hull of a linear code over finite fields is interesting continuously studied.

Linear complementary pairs (LCP) of codes have been introduced in [4] and extensively studied recently due to their applications in cryptography. For example, in [2], [4], [7] and [12], it has been shown that a LCP of codes can be applied in counter passive and active side-channel analysis attacks on embedded cryptosystems. Several constructions of LCPs of codes have been given in [13].

In this thesis, we aim to give constructions of codes over finite fields with prescribed hull or hull dimension as well as their applications. Subsequently, we determine the parameters of the constructed codes. Linear ℓ-intersection pairs of linear codes are studied as a generalization of a LCP of codes. Finally, constructions of EAQECCs from these linear codes are given. The thesis is organized as follows. After this introduction, the definitions and preliminary results on linear codes are recalled in Chapter 2. In Chapter 3, alternative characterizations of hulls of linear codes and their properties are given in terms of the Gramians of their generator and parity-check matrices. A linear ℓ-intersection pair of codes as a generalization of LCPs of codes are given in Chapter 4. Applications of hulls and ℓ-intersection pairs in construction of entanglement-assisted quantum error-correcting codes are discussed in Chapter 5.

Chapter 2

Preliminaries

In this chapter, some terminologies, foundation, and basic concepts in coding theory are recalled. Definitions and basic concepts of linear codes are given in Section 2.1 and the notions of dual codes and hulls are provided in Section 2.2. The reader is referred to [37] for more details.

2.1 Linear Codes

For a prime power q and a positive integer n, let $\mathbb{F}_q$ denote the finite field of order q and let $\mathbb{F}_q^n$ be the vector space of all vectors of length n over $\mathbb{F}_q$, where

$$\mathbb{F}_q^n = \{(a_1, a_2, \dots, a_n) | a_i \in \mathbb{F}_q \text{ for all } i\}.$$

Definition 2.1. A subset C of $\mathbb{F}_q^n$ is called a ***linear code*** of length n over $\mathbb{F}_q$ if it is a subspace of the vector space $\mathbb{F}_q^n$. An element in a linear code C is called a ***codeword*** in C.

A linear code C of length n over $\mathbb{F}_q$ is referred as an $[n,k]_q$ code if the dimension $\dim(C)$ of C is k.

Example 2.2. Let $C = \{000000, 010101, 101010, 111111\}$. Then C is a linear code of length 6 over $\mathbb{F}_2$. Since $\dim(C) = 2$, C is a $[6,2]_2$ code.

Definition 2.3. For $\boldsymbol{u} = (u_1, u_2, \dots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \dots, v_n)$ in $\mathbb{F}_q^n$, the ***Ham-***

ming weight of $\boldsymbol{u}$ is defined by

$$\mathrm{wt}(\boldsymbol{u}) := |\{i \mid u_i \neq 0\}|$$

and the ***Hamming distance*** between $\boldsymbol{u}$ and $\boldsymbol{v}$ is defined by

$$\mathrm{d}(\boldsymbol{u}, \boldsymbol{v}) := |\{i \mid u_i \neq v_i\}|.$$

Definition 2.4. An $[n, k]_q$ linear code C over $\mathbb{F}_q$ is said to have parameters $[n, k, d]_q$ if the ***minimum Hamming distance*** of C is

$$d = \mathrm{d}(C) := \min\{\mathrm{d}(\boldsymbol{u}, \boldsymbol{v}) \mid \boldsymbol{u}, \boldsymbol{v} \in C, \boldsymbol{u} \neq \boldsymbol{v}\}.$$

It is well-known (see [37, Theorem 4.3.8]) that

$$\mathrm{d}(C) = \mathrm{wt}(C) := \min\{\mathrm{wt}(\boldsymbol{u}) \mid \boldsymbol{u} \in C \setminus \{\mathbf{0}\}\}$$

for every linear code C over $\mathbb{F}_q$.

Example 2.5. Let $C = \{000000, 010101, 101010, 111111\}$ be a linear code of length 6 over $\mathbb{F}_2$. Since

$$\mathrm{wt}(010101) = 3,\ \mathrm{wt}(101010) = 3 \text{ and } \mathrm{wt}(111111) = 6,$$

we have $\mathrm{d}(C) = \mathrm{wt}(C) = \min\{\mathrm{wt}(\boldsymbol{v}) \mid \boldsymbol{v} \in C \setminus \{000000\}\} = \min\{3, 6\} = 3$. Therefore, C is a $[6, 2, 3]_2$ code.

The minimum Hamming distance is used to determine the error-detecting and error-correcting capabilities of codes.

Definition 2.6. Let t be a positive integer. A code C is t***-error detecting*** if a codeword incurs at least one but at most t errors and the resulting word is not a codeword in C.

Theorem 2.7 ([37, Theorem 2.5.6]). *Let t be a positive integer. A code C is t-error detecting if and only if*

$$\mathrm{d}(C) \geq t + 1.$$

Definition 2.8. Let t be a positive integer. A code C is ***t-error correcting*** if the minimum distance decoding is able to correct t or fewer errors.

Theorem 2.9 ([37, Theorem 2.5.10]). *Let t be a positive integer. A code C is t-error correcting if and only if*

$$\mathrm{d}(C) \geq 2t + 1.$$

2.2 Dual Codes and Hulls

The notation of duals and hulls of linear codes are recalled together with their basic properties.

Definition 2.10. For $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ in $\mathbb{F}_q^n$, the ***Euclidean inner product*** of $\boldsymbol{u}$ and $\boldsymbol{v}$ is defined to be

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle := \sum_{i=1}^{n} u_i v_i.$$

In addition, if $q = r^2$ for some prime power r, the ***Hermitian inner product*** of $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ in $\mathbb{F}_q^n$ is defined to be

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle_H := \sum_{i=1}^{n} u_i v_i^r.$$

Definition 2.11. For a linear code C of length n over $\mathbb{F}_q$, denote by $C^{\perp}$ and $C^{\perp_H}$ the ***Euclidean dual*** and the ***Hermitian dual*** of C, respectively. Precisely,

$$C^{\perp} := \{\boldsymbol{v} \in \mathbb{F}_q^n \mid \langle \boldsymbol{c}, \boldsymbol{v} \rangle = 0 \text{ for all } \boldsymbol{c} \in C\}$$

and

$$C^{\perp_H} := \{\boldsymbol{v} \in \mathbb{F}_q^n \mid \langle \boldsymbol{c}, \boldsymbol{v} \rangle_H = 0 \text{ for all } \boldsymbol{c} \in C\}.$$

Theorem 2.12 ([37, Theorem 2.5.10])**.** *Let C be a linear code of length n over $\mathbb{F}_q$. Then $C^\perp$ is a linear code,* $\dim(C) + \dim(C^\perp) = n$*, and* $(C^\perp)^\perp = C$*.*

Example 2.13. Let $C = \{000, 011, 110, 101\}$ be a linear code of length 3 over $\mathbb{F}_2$. Then $\dim(C) = 2$ and

$$\begin{aligned} C^\perp &= \{\boldsymbol{u} \in \mathbb{F}_2^3 \mid \langle \boldsymbol{u}, \boldsymbol{c} \rangle = 0 \text{ for all } \boldsymbol{c} \in C\} \\ &= \{000, 111\}. \end{aligned}$$

It is easily seen that

$$\begin{aligned} (C^\perp)^\perp &= \{\boldsymbol{u} \in \mathbb{F}_2^3 \mid \langle \boldsymbol{u}, \boldsymbol{c} \rangle = 0 \text{ for all } \boldsymbol{c} \in C^\perp\} \\ &= \{000, 011, 110, 101\} \\ &= C. \end{aligned}$$

Therefore, $\dim(C) + \dim(C^\perp) = 2 + 1 = 3 = n$ and $(C^\perp)^\perp = C$.

Definition 2.14. Let C be a linear code over $\mathbb{F}_q$.

- C is said to be ***Euclidean self-orthogonal code*** if

$$C \subseteq C^\perp.$$

- C is said to be ***Euclidean self-dual*** if

$$C = C^\perp.$$

- C is called ***maximal Euclidean self-orthogonal*** if it is Euclidean self-orthogonal and it is not contained in any Euclidean self-orthogonal codes.

- C is said to be ***linear Euclidean complementary dual (LECD)*** if

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

Example 2.15. Let

$$C_1 = \{0000, 1010, 0101, 1111\} \text{ and } C_2 = \{0000, 1011, 0111, 1100\}$$

be linear codes of length 4 over $\mathbb{F}_2$. Then

$$C_1^{\perp} = \{0000, 1010, 0101, 1111\} \text{ and } C_2^{\perp} = \{0000, 1110, 1101, 0011\}.$$

It follows that $C_1 = C_1^{\perp}$ and $C_2 \cap C_2^{\perp} = \{0000\}$. Therefore, C_1 is Euclidean self-orthogonal and Euclidean self-dual, and C_2 is LECD. Moreover, C_1 is maximal Euclidean self-orthogonal because $\dim(C_1) = 2 \geq 2 = n/2$.

Definition 2.16. The ***Euclidean Hull*** of a linear code C is defined by

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

From above definition, the Euclidean hull can be viewed as a general notion of self-orthogonal and complementary dual codes in the following senses.

Remark 2.17. *It is not difficult to see that a linear code C is Euclidean self-orthogonal if*

$$\mathrm{Hull}(C) = C,$$

and a linear code C is LECD if

$$\mathrm{Hull}(C) = \{\mathbf{0}\}.$$

Definition 2.18. For a positive integer n, an $n \times n$ matrix $D = [d_{ij}]$ over $\mathbb{F}_q$ is called a ***diagonal matrix*** if its entries outside the main diagonal are all zero, i.e., $d_{ij} = 0$ for all $1 \leq i, j \leq n$ and $i \neq j$. Denote by

$$D = \mathrm{diag}(d_{11}, d_{22}, d_{33}, \ldots, d_{nn})$$

the diagonal matrix D.

Definition 2.19. Two linear codes of length n over $\mathbb{F}_q$ are ***equivalent*** if one can be obtained from the other by a combination of operations of the following types:

(i) permutation of the n digits of the codewords;

(ii) multiplication of the symbols appearing in a fixed position by a nonzero element in $\mathbb{F}_q$.

Definition 2.20. A square matrix over $\mathbb{F}_q$ is called a ***weighted permutation matrix*** if it has exactly one nonzero entry in each row and each column and 0s elsewhere.

Remark 2.21. *Linear codes C_1 and C_2 of length n over $\mathbb{F}_q$ are equivalent if and only if there exists an $n \times n$ weighted permutation matrix P such that*

$$C_2 = \{Pc \mid c \in C_1\}.$$

Definition 2.22. A $k \times n$ matrix G over $\mathbb{F}_q$ is called a ***generator matrix*** for an $[n, k, d]_q$ code C if the rows of G form a basis for C.

Definition 2.23. An $(n - k) \times n$ matrix H over $\mathbb{F}_q$ is called a ***parity-check matrix*** of an $[n, k, d]_q$ code C if H is a generator matrix of $C^{\perp}$.

Example 2.24. Let $C = \{00000, 10010, 01001, 00111, 11011, 10101, 01110, 11100\}$ be a linear code of length 5 over $\mathbb{F}_2$. Then $C^{\perp} = \{00000, 10110, 01101, 11011\}$ is a linear code over $\mathbb{F}_2$. Since $\{10010, 01001, 00111\}$ and $\{10110, 01101\}$ are bases of C and $C^{\perp}$, respectively, it implies that

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

is a generator matrix for C and

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

is a parity-check matrix of C.

Definition 2.25. For an $m \times n$ matrix A over $\mathbb{F}_q$, by abuse of notation, the ***Gram matrix*** (or ***Gramian***) of A is defined to be AA^T.

Proposition 2.26 ([23, Proposition 3.1])**.** *Let C be an $[n, k]_q$ code over $\mathbb{F}_q$ with generator matrix G and parity-check matrix H. Then*

$$\operatorname{rank}(GG^T) = k - \dim(\operatorname{Hull}(C)),$$

and

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

Next, some well-known properties of Euclidean self-orthogonal codes and LECD codes are discussed.

Corollary 2.27 ([25, Lemma 2])**.** *Let C be an $[n, k]_q$ code over $\mathbb{F}_q$ with generator matrix G and parity-check matrix H. Then the following statements hold.*

1. *C is Euclidean self-orthogonal if and only if $GG^T = [\mathbf{0}]$.*

2. *C is LECD if and only if GG^T is invertible. In this case, HH^T is invertible.*

Example 2.28. Let C_1 and C_2 be $[6, 2]_2$ and $[6, 2]_2$ codes over with generator matrix

$$G_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \text{ and } G_2 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix},$$

respectively.

Since

$$G_1G_1^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}^T = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

C_1 is a Euclidean self-orthogonal. Since

$$G_2G_2^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

is invertible, C_2 is LECD.

For a square prime power $q = r^2$, we have the following parallel properties for Hermitian duals and Hermitian hulls.

Theorem 2.29 ([37, Theorem 2.5.10])**.** *Let C be a linear code of length n over $\mathbb{F}_q$. Then $C^{\perp_H}$ is a linear code,* $\dim(C) + \dim(C^{\perp_H}) = n$*, and* $(C^{\perp_H})^{\perp_H} = C$*.*

Example 2.30. Let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$ and let C be a linear code of length 4 over $\mathbb{F}_4$ defined by

$$\begin{aligned} C = \{&0000, 1010, 0101, 1111, \alpha 0 \alpha 0, 0 \alpha 0 \alpha, \alpha\alpha\alpha\alpha, \alpha^2 0 \alpha^2 0, 0 \alpha^2 0 \alpha^2, \\ &\alpha^2\alpha^2\alpha^2\alpha^2, 1\alpha 1\alpha, \alpha 1 \alpha 1, 1\alpha^2 1 \alpha^2, \alpha^2 1 \alpha^2 1, \alpha\alpha^2\alpha\alpha^2, \alpha^2\alpha\alpha^2\alpha\}. \end{aligned}$$

Then the Hermitian dual of C is

$$\begin{aligned} C^{\perp_H} &= \{\boldsymbol{u} \in \mathbb{F}_4^2 \mid \langle \boldsymbol{u}, \boldsymbol{c} \rangle_H = 0 \text{ for all } \boldsymbol{c} \in C\} \\ &= \{0000, 1010, 0101, 1111, \alpha 0 \alpha 0, 0 \alpha 0 \alpha, \alpha\alpha\alpha\alpha, \alpha^2 0 \alpha^2 0, 0 \alpha^2 0 \alpha^2, \\ &\quad \alpha^2\alpha^2\alpha^2\alpha^2, 1\alpha 1\alpha, \alpha 1 \alpha 1, 1\alpha^2 1 \alpha^2, \alpha^2 1 \alpha^2 1, \alpha\alpha^2\alpha\alpha^2, \alpha^2\alpha\alpha^2\alpha\}. \end{aligned}$$

In this case, $C^{\perp_H}$ is a linear code over $\mathbb{F}_4$ such that $\dim(C^{\perp_H}) = \dim(C) = 2$. Therefore, $\dim(C) + \dim(C^{\perp_H}) = 2 + 2 = 4 = n$ and $(C^{\perp_H})^{\perp_H} = C$.

Definition 2.31. Let C be a linear code over $\mathbb{F}_q$.

- C is said to be ***Hermitian self-orthogonal code*** if

$$C \subseteq C^{\perp_H}.$$

- C is said to be ***Hermitian self-dual*** if

$$C = C^{\perp_H}.$$

- C is called ***maximal Hermitian self-orthogonal*** if it is Hermitian self-orthogonal and it is not contained in any Hermitian self-orthogonal codes.

- C is said to be ***linear Hermitian complementary dual (LHCD)*** if

$$C \cap C^{\perp_H} = \{\mathbf{0}\}.$$

Example 2.32. Let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$ and let

$$C_1 = \{0000, 1010, 0101, 1111, \alpha 0 \alpha 0, 0 \alpha 0 \alpha, \alpha\alpha\alpha\alpha, \alpha^2 0 \alpha^2 0, 0 \alpha^2 0 \alpha^2, \alpha^2\alpha^2\alpha^2\alpha^2, 1\alpha 1\alpha, \alpha 1 \alpha 1, 1\alpha^2 1 \alpha^2, \alpha^2 1 \alpha^2 1, \alpha\alpha^2\alpha\alpha^2, \alpha^2\alpha\alpha^2\alpha\}$$

and

$$C_2 = \{0000, 1011, 0111, 1100, \alpha 0 \alpha\alpha, 0\alpha\alpha\alpha, \alpha\alpha 00, \alpha^2 0 \alpha^2\alpha^2, 0\alpha^2\alpha^2\alpha^2, \alpha^2\alpha^2 00, 1\alpha\alpha^2\alpha^2, \alpha 1 \alpha^2\alpha^2, 1\alpha^2\alpha\alpha, \alpha^2 1 \alpha\alpha, \alpha\alpha^2 11, \alpha^2\alpha 11\}$$

be linear codes of length 4 over $\mathbb{F}_4$. Then

$$C_1^{\perp_H} = \{0000, 1010, 0101, 1111, \alpha 0 \alpha 0, 0 \alpha 0 \alpha, \alpha\alpha\alpha\alpha, \alpha^2 0 \alpha^2 0, 0 \alpha^2 0 \alpha^2, \alpha^2\alpha^2\alpha^2\alpha^2, 1\alpha 1\alpha, \alpha 1 \alpha 1, 1\alpha^2 1 \alpha^2, \alpha^2 1 \alpha^2 1, \alpha\alpha^2\alpha\alpha^2, \alpha^2\alpha\alpha^2\alpha\}$$

and

$$C_2^{\perp_H} = \{0000, 1110, 1101, 1111, \alpha\alpha\alpha 0, \alpha\alpha 0 \alpha, \alpha\alpha\alpha\alpha, \alpha^2\alpha^2\alpha^2 0, \alpha^2\alpha^2 0 \alpha^2, \alpha^2\alpha^2\alpha^2\alpha^2, \alpha^2\alpha^2 1 \alpha, \alpha^2\alpha^2\alpha 1, \alpha\alpha 1 \alpha^2, \alpha\alpha\alpha^2 1, 11\alpha\alpha^2, 11\alpha^2\alpha\}.$$

It follows that $C_1 = C_1^{\perp_H}$ and $C_2 \cap C_2^{\perp_H} = \{0000\}$. Therefore, C_1 is Hermitian self-orthogonal and Hermitian self-dual, and C_2 is LHCD. Moreover, C_1 is maximal Hermitian self-orthogonal because $\dim(C_1) = 2 \geq 2 = n/2$.

Definition 2.33. The ***Hermitian Hull*** of a linear code C is defined by

$$\mathrm{Hull}_H(C) = C \cap C^{\perp_H}.$$

From above definition, the Hermitian hull can be viewed as a general notion of Hermitian self-orthogonal codes and Hermitian LCDs.

Remark 2.34. *It is not difficult to see that a linear code C is Hermitian self-orthogonal if*

$$\mathrm{Hull}_H(C) = C,$$

and it is LHCD if

$$\mathrm{Hull}_H(C) = \{\mathbf{0}\}.$$

Definition 2.35. For $q = r^2$ and an $n \times m$ matrix $A = [a_{ij}]$ over $\mathbb{F}_q$, let

$$A^\dagger = [a_{ji}^r].$$

Proposition 2.36 ([23, Proposition 3.1])**.** *Let C be a linear code of length n over $\mathbb{F}_q$ with generator matrix G and parity-check matrix H. Then*

$$\mathrm{rank}(GG^\dagger) = k - \dim(\mathrm{Hull}_H(C)),$$

and

$$\mathrm{rank}(HH^\dagger) = n - k - \dim(\mathrm{Hull}_H(C)).$$

Next, the well-known properties of Hermitian self-orthogonal codes and LHCD codes are showed.

Corollary 2.37 ([25, Lemma 2]). *Let C be an $[n,k]_q$ code over $\mathbb{F}_q$ with generator matrix G and parity-check matrix H. Then the following statements hold.*

1. *C is Hermitian self-orthogonal if and only if $GG^\dagger = [0]$.*

2. *C is LHCD if and only if $GG^\dagger$ is invertible. In this case, $HH^\dagger$ is invertible.*

Example 2.38. Let C_1 be a $[4,2]_4$ code over $\mathbb{F}_4$ defined in Example 2.32. Then

$$G_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

is a generator matrix of C_1. Since

$$G_1G_1^\dagger = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}^\dagger = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

C_1 is a Hermitian self-orthogonal.

Let C_2 be a $[4,2]_4$ code over $\mathbb{F}_4$ defined in Example 2.32. Then

$$G_2 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

is a generator matrix of C_2. Since

$$G_2G_2^\dagger = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

is invertible, C_2 is LHCD.

Chapter 3

Hulls of Linear Codes

Hulls of linear codes have been of interest and extensively studied due to their rich algebraic structures and wide applications. In this chapter, hulls of linear codes are studied with respect to Euclidean and Hermintian inner products. Characterizations and properties of hulls of linear codes are given together with linear codes with special hulls.

Properties of hulls of linear codes are given in terms of their Gramians (see Definition 2.25) of their generator and parity-check matrices. The Gramian of a generator or parity-check matrix of a linear code plays an important role in the study of self-orthogonal codes, complementary dual codes, and hulls of linear codes.

From Proposition 2.26, It can be seen that if the ranks of the Gramians HH^T and GG^T are independent of H and G then $\mathrm{rank}(HH^T) = n - k - \dim(\mathrm{Hull}(C)) = n - k - \dim(\mathrm{Hull}(C^{\perp}))$ and $\mathrm{rank}(GG^T) = k - \dim(\mathrm{Hull}(C)) = k - \dim(\mathrm{Hull}(C^{\perp}))$.

Using the definition of the gramian, it can be seen that

- a linear code with generator matrix G is Euclidean self-orthogonal if and only if the Gramian GG^T is zero, and

- it is Euclidean complementary dual if and only if the Gramian GG^T is non-singular.

From Proposition 2.26, it is not difficult to see that generator and parity-check matrices of linear codes can be chosen such that their Gramians are of the following special forms (cf. [31, Corollary 3.2]).

Proposition 3.1. *Let C be a linear $[n,k]_q$ code such that $\dim(\mathrm{Hull}(C)) = \ell$. Then the following statements hold.*

1. *There exist a generator matrix G of C and an invertible $(k-\ell)\times(k-\ell)$ symmetric matrix A over $\mathbb{F}_q$ such that the Gramian of G is of the form*

$$GG^T = \left[\begin{array}{c|c} A & 0 \\ \hline 0 & 0 \end{array}\right].$$

2. *There exist a parity-check matrix H of C and an invertible $(n-k-\ell)\times(n-k-\ell)$ symmetric matrix B over $\mathbb{F}_q$ such that the Gramian of H is of the form*

$$HH^T = \left[\begin{array}{c|c} B & 0 \\ \hline 0 & 0 \end{array}\right].$$

Clearly, the Gramians of generator and parity-check matrices of linear codes are always symmetric. Unlike real symmetric matrices, a square symmetric matrix over finite fields does not need to be diagonalizable. From Proposition 3.1, it is therefore interesting to ask whether the Gramian of a generator/parity-check matrix of a linear code is diagonalizable. Equivalently, does a linear code have a generator matrix whose Gramian is a diagonal matrix? In Proposition 3.5, we provide a solution to this problem for the case where q is an odd prime power. A partial solution for the case where q is an even prime power is given in Proposition 3.9.

3.1 Euclidean Hulls of Linear Codes

In this section, properties of hulls of linear codes are discussed. Alternative characterizations of the hull and the hull dimension of linear codes are given. Conditions for generator and parity-check matrices of linear codes to have diagonalizable Gramians are provided.

3.1.1 Characterizations of Euclidean Hulls of Linear Codes

The Euclidean hull dimension of linear codes has been determined in terms of the rank of the Gramians of generator and parity-check matrices of linear codes in [23] (see Proposition 2.26).

In the following proposition, alternative characterizations of the Euclidean hull dimension of linear codes are given.

Proposition 3.2. *Let C be a linear $[n,k]_q$ code and let ℓ be a non-negative integer. Then the following statements are equivalent.*

1) $\dim(\mathrm{Hull}(C)) = \ell$.

2) $\mathrm{rank}(GG^T) = k - \ell$ *for every generator matrix G of C.*

3) $\mathrm{rank}(G_1G_2^T) = k - \ell$ *for all generator matrices G_1 and G_2 of C.*

4) $\mathrm{rank}(HH^T) = n - k - \ell$ *for every parity-check matrix H of C.*

5) $\mathrm{rank}(H_1H_2^T) = n - k - \ell$ *for all parity-check matrices H_1 and H_2 of C.*

Proof. From Proposition 2.26, we have the equivalences 1) $\Leftrightarrow$ 2) and 1) $\Leftrightarrow$ 4). It remains to prove the equivalences 2) $\Leftrightarrow$ 3) and 4) $\Leftrightarrow$ 5). Since the arguments of proofs are similar, only the detailed proof of 2) $\Leftrightarrow$ 3) is provided.

To prove 2) $\Rightarrow$ 3), let G, G_1 and G_2 be generator matrices of C and assume that $\mathrm{rank}(GG^T) = k - \ell$. Since the rows of G, G_1 and G_2 are base for C, there exist invertible $k \times k$ matrices E_1 and E_2 such that $G_1 = E_1G$ and $G_2 = E_2G$. Consequently, we have

$$G_1G_2^T = E_1G(E_2G)^T = E_1G(G^TE_2^T) = E_1(GG^T)E_2^T.$$

Since E_1 and E_2^T are invertible, we have

$$\mathrm{rank}(G_1G_2^T) = \mathrm{rank}(E_1(GG^T)E_2^T) = \mathrm{rank}(GG^T) = k - \ell$$

as desired.

The statement 3) $\Rightarrow$ 2) is obvious. □

Based on Proposition 3.2, we have the following characterizations.

Corollary 3.3. *Let C be a linear $[n,k]_q$ code and let ℓ be a non-negative integer. Then the following statements are equivalent.*

1) $\dim(\mathrm{Hull}(C)) = \ell$.

2) *There exist nonzero elements $a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_q$ and generator matrices G_1 and G_2 of C such that*

$$G_1G_2^T = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0).$$

3) *There exist nonzero elements $b_1, b_2, \ldots, b_{n-k-\ell}$ in $\mathbb{F}_q$ and parity-check matrices H_1 and H_2 of C such that*

$$H_1H_2^T = \mathrm{diag}(b_1, b_2, \ldots, b_{n-k-\ell}, 0, \ldots, 0).$$

By convention, the set $\{a_1, a_2, \ldots, a_{k-\ell}\}$ (resp., $\{b_1, b_2, \ldots, b_{n-k-\ell}\}$) will be referred to the empty set if $k - \ell = 0$ (resp., $n - k - \ell = 0$).

Proof. To prove 1) $\Leftrightarrow$ 2), assume that $\dim(\mathrm{Hull}(C)) = \ell$. Let G be a generator matrix of C. By Proposition 3.2, we have that $\mathrm{rank}(GG^T) = k - \ell$. Applying suitable elementary row and column operations, it follows that

$$(PG)(QG)^T = PGG^TQ^T = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0)$$

for some nonzero elements $a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_q$ and invertible $k \times k$ matrices P and Q over $\mathbb{F}_q$. Let $G_1 = PG$ and $G_2 = QG$. Then G_1 and G_2 are generator matrices of C such that $G_1G_2^T = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0)$. Conversely, assume that 2) holds. Then $\mathrm{rank}(G_1G_2^T) = k - \ell$ and hence $\dim(\mathrm{Hull}(C)) = \ell$ by Proposition 3.2. Since $\mathrm{Hull}(C) = \mathrm{Hull}(C^\perp)$, the equivalence of 1) $\Leftrightarrow$ 3) can be obtained similarly. $\square$

3.1.2 Diagonalizability of Gramians

From Subsection 3.1.1, it guarantees that for a given linear code C over $\mathbb{F}_q$, there exist generator matrices G_1 and G_2 of C such that $G_1G_2^T$ is a diagonal matrix. Here, we focus on the diagonalizability the Gramian of a generator matrix of a linear code. The results are given in two cases based on the characteristic of the underlying finite field.

3.1.2.1 Odd Characteristics

For an odd prime power q, the Gramian of a generator/parity-check matrix of a linear code over $\mathbb{F}_q$ will be shown to be diagonalizable. We begin with the following useful lemma.

Lemma 3.4. *Let C be a linear code of length n over $\mathbb{F}_q$. If q is odd and C is not Euclidean self-orthogonal, then there exists a codeword $\boldsymbol{v} \in C$ such that $\langle \boldsymbol{v}, \boldsymbol{v} \rangle \neq 0$. In this case, $\boldsymbol{v} \notin \mathrm{Hull}(C)$.*

Proof. Assume that q is an odd prime power and C is not Euclidean self-orthogonal. Then there exist $\boldsymbol{u}$ and $\boldsymbol{w}$ in C such that $\langle \boldsymbol{u}, \boldsymbol{w} \rangle \neq 0$. If $\langle \boldsymbol{u}, \boldsymbol{u} \rangle \neq 0$ or $\langle \boldsymbol{w}, \boldsymbol{w} \rangle \neq 0$, we are done. Assume that $\langle \boldsymbol{u}, \boldsymbol{u} \rangle = 0$ and $\langle \boldsymbol{w}, \boldsymbol{w} \rangle = 0$. Let $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w}$. Since q is odd, we have $\langle \boldsymbol{v}, \boldsymbol{v} \rangle = \langle \boldsymbol{u}, \boldsymbol{u} \rangle + 2\langle \boldsymbol{u}, \boldsymbol{w} \rangle + \langle \boldsymbol{w}, \boldsymbol{w} \rangle = 2\langle \boldsymbol{u}, \boldsymbol{w} \rangle \neq 0$ as desired. Clearly, the said codeword is not in $\mathrm{Hull}(C)$. □

Proposition 3.5. *Let C be a non-zero linear code of length n over $\mathbb{F}_q$. If q is odd, then the Gramian of a generator matrix of C is diagonalizable.*

Proof. Assume that q is an odd prime power. We prove by induction on the dimension of C. If $\dim(C) = 1$, then Gramian of a generator matrix of C is a 1×1 matrix over $\mathbb{F}_q$ which is always diagonalizable. Assume that $\dim(C) = k$ for some positive integer $k \geq 2$ and assume that the statement holds true for all linear codes of dimension $k-1$. If C is Euclidean self-orthogonal, then $GG^T = [0]$ is diagonalizable for all generator matrices G of C by Proposition 3.2. Assume that C is not Euclidean self-orthogonal. Since q is odd, there exist $\boldsymbol{v} \in C$ such that $\langle \boldsymbol{v}, \boldsymbol{v} \rangle \neq 0$ by Lemma 3.4. Let $D = \{\boldsymbol{c} \in C \mid \langle \boldsymbol{v}, \boldsymbol{c} \rangle = 0\}$. Since $\langle \boldsymbol{v}, \boldsymbol{v} \rangle \neq 0$, we have $C = D \oplus \langle \boldsymbol{v} \rangle$ which implies that $\dim(D) = k - 1$. By the induction hypothesis, there exists a generator matrix

$$G = \begin{bmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \\ \vdots \\ \boldsymbol{v}_{k-1} \end{bmatrix}$$

of D whose Gramian GG^T is diagonal. Since $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{k-1}\} \subseteq D$, $\langle \boldsymbol{v}_i, \boldsymbol{v} \rangle = 0$ for all $1 \leq i \leq k-1$. Hence, $G' = \begin{bmatrix} \boldsymbol{v} \\ G \end{bmatrix}$ is a generator matrix for C such that the Gramian $G'G'^T$ is a diagonal matrix. □

The following corollary is a direct consequence of Proposition 3.5. Since a parity-check matrix of a linear code is a generator matrix for its dual, the above results can be restated including the parity-check matrix easily.

Corollary 3.6. *Let C be a linear $[n,k]_q$ code such that* $\dim(\mathrm{Hull}(C)) = \ell$. *If q is odd, then the following statements hold.*

1. *There exist nonzero elements $a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_q$ and a generator matrix G of C such that*
$$GG^T = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0).$$
2. *There exist nonzero elements $b_1, b_2, \ldots, b_{n-k-\ell}$ in $\mathbb{F}_q$ and a parity-check matrix H of C such that*
$$HH^T = \mathrm{diag}(b_1, b_2, \ldots, b_{n-k-\ell}, 0, \ldots, 0).$$

Example 3.7. Let C be a linear $[6,3]_3$ code with generator matrix

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

Then

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

is a parity-check matrix of C. The Gramians of G and H are of the form

$$GG^T = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \mathrm{diag}(2, 0, 0)$$

and

$$HH^T = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \mathrm{diag}(2, 0, 0)$$

which are diagonal. Since $\mathrm{rank}(GG^T) = 1$, we have $\dim(\mathrm{Hull}(C)) = 3 - \mathrm{rank}(GG^T) = 3 - 1 = 2$.

Linear codes with orthogonal or orthonormal basis are good candidates in some applications. However, in general, an orthogonal or orthonormal basis does not need to be exist. The existence of an orthonormal basis of some Euclidean complementary dual codes has been studied in [10]. Here, characterization for the existence of an orthogonal basis of Euclidean complementary dual codes over finite fields of odd characteristic can be obtained directly from Proposition 3.5.

Corollary 3.8. *Let q be an odd prime power and let C be a linear code over $\mathbb{F}_q$. Then C is Euclidean complementary dual if and only if C has a Euclidean orthogonal basis.*

3.1.2.2 Even Characteristics

For an even prime power q, the Gramians of generator and parity-check matrices of linear codes over $\mathbb{F}_q$ do not need to be diagonalizable. We give a necessary condition for them to be diagonalizable. It turns out that this condition is necessary for an odd prime power as well. However, for an odd prime power q, we already have stronger results described in the previous subsection. Since the results in the subsection are independent of the parity of q, they are presented for arbitrary prime powers q as follows.

Proposition 3.9. *Let C be a linear $[n, k]_q$ code such that* $\dim(\mathrm{Hull}(C)) = \ell$. *If* $\mathrm{Hull}(C)$ *is maximal self-orthogonal in C, then there exist nonzero elements*

$a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_q$ and a generator matrix G of C such that

$$GG^T = \operatorname{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0).$$

Precisely, the Gramian of a generator matrix of a linear code C whose hull is maximal self-orthogonal in C is diagonalizable.

Proof. Let $\mathcal{B} = \{\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_\ell\}$ be a basis of $\operatorname{Hull}(C)$. Assume that $\operatorname{Hull}(C)$ is maximal self-orthogonal in C. If there exists a codeword $\boldsymbol{x} \in C \setminus \operatorname{Hull}(C)$ such that $\langle \boldsymbol{x}, \boldsymbol{x} \rangle = 0$, then $\langle \boldsymbol{x}, \boldsymbol{c} \rangle = 0$ for all $\boldsymbol{c} \in \operatorname{Hull}(C)$. This implies that $\operatorname{Hull}(C) + \langle \boldsymbol{x} \rangle$ is self-orthogonal in C which is containing $\operatorname{Hull}(C)$, a contradiction. Hence, $\langle \boldsymbol{x}, \boldsymbol{x} \rangle \neq 0$ for all $\boldsymbol{x} \in C \setminus \operatorname{Hull}(C)$. Extending $\mathcal{B}$ to a basis $\mathcal{B} \cup \{\boldsymbol{t}_{\ell+1}, \boldsymbol{t}_{\ell+2}, \ldots, \boldsymbol{t}_k\}$ of C. Using the Gram-Schmidt process, $\langle \boldsymbol{t}_{\ell+1}, \boldsymbol{t}_{\ell+2}, \ldots, \boldsymbol{t}_k \rangle$ contains an orthogonal basis, denoted by $\{\boldsymbol{r}_{\ell+1}, \boldsymbol{r}_{\ell+2}, \ldots, \boldsymbol{r}_k\}$. Hence $\mathcal{B}' = \{\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_\ell, \boldsymbol{r}_{\ell+1}, \boldsymbol{r}_{\ell+2}, \ldots, \boldsymbol{r}_k\}$ is a basis for C such that $\langle \boldsymbol{r}_i, \boldsymbol{r}_i \rangle \neq 0$ for all $\ell + 1 \leq i \leq k$ and $\langle \boldsymbol{r}_i, \boldsymbol{r}_j \rangle = 0$ for all $1 \leq i \leq k$ and $1 \leq j \leq k$ such that $i \neq j$ or $1 \leq i = j \leq \ell$.

For $1 \leq i \leq k - \ell$, let $a_i = \langle \boldsymbol{r}_{\ell+i}, \boldsymbol{r}_{\ell+i} \rangle \neq 0$. Let $G_1 = \begin{bmatrix} \boldsymbol{r}_{\ell+1} \\ \vdots \\ \boldsymbol{r}_k \end{bmatrix}$, $G_2 = \begin{bmatrix} \boldsymbol{r}_1 \\ \vdots \\ \boldsymbol{r}_\ell \end{bmatrix}$ and $G = \begin{bmatrix} G_1 \\ G_2 \end{bmatrix}$. Then $G_1 G_1^T = \operatorname{diag}(a_1, a_2, \ldots, a_{k-\ell})$, $G_1 G_2^T = [0]$, $G_2 G_1^T = [0]$ and $G_2 G_2^T = [0]$. Hence,

$$GG^T = \left[\begin{array}{c|c} G_1G_1^T & G_1G_2^T \\ \hline G_2G_1^T & G_2G_2^T \end{array}\right] = \left[\begin{array}{ccc|c} a_1 & & & \\ & \ddots & & \mathbf{0} \\ & & a_{k-\ell} & \\ \hline & \mathbf{0} & & \mathbf{0} \end{array}\right] = \operatorname{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0)$$

as desired. $\square$

Similarly to the previous proposition, we can replace a generator matrix G by a parity-check matrix H of C and derive the following result.

Corollary 3.10. *Let C be a linear $[n,k]_q$ code such that $\dim(\mathrm{Hull}(C)) = \ell$. If $\mathrm{Hull}(C)$ is maximal self-orthogonal in $C^{\perp}$, then there exist nonzero elements $b_1, b_2, \dots, b_{n-k-\ell}$ in $\mathbb{F}_q$ and a parity-check matrix H of C such that*

$$HH^T = \mathrm{diag}(b_1, b_2, \dots, b_{n-k-\ell}, 0, \dots, 0).$$

In the case where C is maximal Euclidean self-orthogonal, then $\mathrm{Hull}(C) = C$ is maximal Euclidean self-orthogonal in $C^{\perp}$. Hence, we have the following corollary.

Corollary 3.11. *Let C be a linear $[n,k]_q$ code. If C is maximal Euclidean self-orthogonal, then there exist nonzero elements $b_1, b_2, \dots, b_{n-2k}$ in $\mathbb{F}_q$ and a parity-check matrix H of C whose Gramian is*

$$HH^T = \mathrm{diag}(b_1, b_2, \dots, b_{n-2k}, 0, \dots, 0).$$

Example 3.12. Let C be a linear $[6,3]_2$ code with parity-check matrix

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

Then

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

is parity-check matrix of C. Since $GG^T = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and Proposition 2.26, we get

$$\dim(C \cap C^{\perp}) = \dim(\mathrm{Hull}(C)) = k - \mathrm{rank}(GG^T) = 2 - 0 = 2 = \dim(C).$$

It implies that $\mathrm{Hull}(C)$ is maximal Euclidean self-orthogonal in $C^{\perp}$ and the Gramian of H is

$$HH^T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \mathrm{diag}(1, 1, 0, 0).$$

Lemma 3.13. *Let C be a linear $[n, k]_q$ code such that $\dim(\mathrm{Hull}(C)) = \ell$. Then the following statements hold.*

1) *If $k - \ell \leq 1$, then $\mathrm{Hull}(C)$ is maximal self-orthogonal in C.*

2) *If $n - k - \ell \leq 1$, then $\mathrm{Hull}(C)$ is maximal self-orthogonal in $C^{\perp}$.*

Proof. To prove 1), assume that $k - \ell \leq 1$. If $k - \ell = 0$, then we have $k = \ell$ which means $\mathrm{Hull}(C) = C$. Hence, $\mathrm{Hull}(C)$ is a Euclidean self-orthogonal in C, i.e., C is maximal Euclidean self-orthogonal in C. Assume that $k - \ell = 1$. Then there exists $\boldsymbol{v} \in C \backslash \mathrm{Hull}(C)$. Suppose that $\langle \boldsymbol{v}, \boldsymbol{v} \rangle = 0$. Then $C = \langle \boldsymbol{v} \rangle + \mathrm{Hull}(C)$. Since $\langle \boldsymbol{v}, \boldsymbol{c} \rangle = 0$ for all $\boldsymbol{c} \in C$, we have $\boldsymbol{v} \in \mathrm{Hull}(C)$ which is a contradiction. Hence, $\langle \boldsymbol{v}, \boldsymbol{v} \rangle \neq 0$. Therefore, $\mathrm{Hull}(C)$ is maximal Euclidean self-orthogonal in C. By replacing C with $C^{\perp}$ in 1), the result of 2) follows similarly. □

Corollary 3.14. *Let C be a linear $[n, k]_q$ code such that $\dim(\mathrm{Hull}(C)) = \ell$. If q is even, then the following statements hold.*

1) *$k - \ell \leq 1$ if and only if $\mathrm{Hull}(C)$ is maximal Euclidean self-orthogonal in C.*

2) *$n - k - \ell \leq 1$ if and only if $\mathrm{Hull}(C)$ is maximal Euclidean self-orthogonal in $C^{\perp}$.*

Proof. Assume that q is even. The sufficient part follows from Lemma 3.13. For necessity, assume that $k-\ell>1$. Then there exist two linearly independent elements $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ in $C\setminus \text{Hull}(C)$. Then $\langle \boldsymbol{v}_1,\boldsymbol{v}_1\rangle \neq 0$ and $\langle \boldsymbol{v}_2,\boldsymbol{v}_2\rangle\neq 0$. Since q is even, every element in $\mathbb{F}_q$ is square. Let a be an element in $\mathbb{F}_q$ such that $a^2=\frac{\langle \boldsymbol{v}_1,\boldsymbol{v}_1\rangle}{\langle \boldsymbol{v}_2,\boldsymbol{v}_2\rangle}$. Then $\langle \boldsymbol{v}_1+a\boldsymbol{v}_2,\boldsymbol{v}_1+a\boldsymbol{v}_2\rangle=\langle \boldsymbol{v}_1,\boldsymbol{v}_1\rangle+2a\langle \boldsymbol{v}_1,\boldsymbol{v}_2\rangle+a^2\langle \boldsymbol{v}_2,\boldsymbol{v}_2\rangle=2\langle \boldsymbol{v}_1,\boldsymbol{v}_1\rangle=0$ and $\boldsymbol{v}_1+a\boldsymbol{v}_2\in C\setminus \text{Hull}(C)$. Hence, $\text{Hull}(C)+\langle \boldsymbol{v}_1+a\boldsymbol{v}_2\rangle$ is Euclidean self-orthogonal and $\text{Hull}(C)\subsetneq \text{Hull}(C)+\langle \boldsymbol{v}_1+a\boldsymbol{v}_2\rangle\subseteq C$. Therefore, $\text{Hull}(C)$ is not maximal Euclidean self-orthogonal in C. The second statement follows immediately from 1). $\square$

Corollary 3.15. *Let C be a non-zero linear code of length n over $\mathbb{F}_q$. If q is even and* $\dim(C)-\dim(\text{Hull}(C))\leq 1$, *then the Gramian of a generator matrix of C is diagonalizable.*

The diagonalizabilty studied above will be useful in the applications in Chapter 5.

3.2 Hermitian Hulls of Linear Codes

Recall the *Hermitian hull* of a code C is $\text{Hull}_H(C)=C\cap C^{\perp_H}$. A code C is said to be *Hermitian self-orthogonal* if $C\subseteq C^{\perp_H}$ and it is said to be *Hermitian complementary dual* if $\text{Hull}_H(C)=\{\mathbf{0}\}$. Clearly, C is Hermitian self-orthogonal if $\text{Hull}_H(C)=C$.

In this section, a discussion on Hermitian hulls of linear codes is given. We note that most of the results in this section can be obtained using the arguments analogous to those in Section 3.1. Therefore, the proofs for those results will be omitted. Some proofs are provided if they are required and different from those in Section 3.1. For convenience, the theorem numbers are given in the form $3.1.N'$ if it corresponds to 3.1.N in Section 3.1.

The Hermitian hull dimension of linear codes has been characterized in [23]. Here, we provide an alternative characterizations of the Hermitian hull dimension of linear codes.

Proposition 3.16. *Let C be a linear $[n,k]_{q^2}$ code and let ℓ be a non-negative integer. Then the following statements are equivalent.*

1) $\dim(\mathrm{Hull}_H(C)) = \ell$.

2) $\mathrm{rank}(GG^\dagger) = k - \ell$ *for every generator matrix G of C.*

3) $\mathrm{rank}(G_1G_2^\dagger) = k - \ell$ *for all generator matrices G_1 and G_2 of C.*

4) $\mathrm{rank}(HH^\dagger) = n - k - \ell$ *for every parity-check matrix H of C.*

5) $\mathrm{rank}(H_1H_2^\dagger) = n - k - \ell$ *for all parity-check matrices H_1 and H_2 of C.*

From Proposition 3.16, the following characterizations can be obtained directly.

Corollary 3.17. *Let C be a linear $[n,k]_{q^2}$ code and let ℓ be a non-negative integer. Then the following statements are equivalent.*

1) $\dim(\mathrm{Hull}_H(C)) = \ell$.

2) *There exist nonzero elements $a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_{q^2}$ and generator matrices G_1 and G_2 of C such that*

$$G_1G_2^\dagger = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0).$$

3) *There exist nonzero elements $b_1, b_2, \ldots, b_{n-k-\ell}$ in $\mathbb{F}_{q^2}$ and parity-check matrices H_1 and H_2 of C such that*

$$H_1H_2^\dagger = \mathrm{diag}(b_1, b_2, \ldots, b_{n-k-\ell}, 0, \ldots, 0).$$

Example 3.18. Let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$ and C be a linear $[6, 3]_4$ code with generator matrix

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

Then

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & 0 & \alpha^2 & \alpha \\ 0 & 0 & 0 & 1 & \alpha & 1 \end{bmatrix}$$

is a parity-check matrix of C. Since $GG^\dagger = \begin{bmatrix} 1 & \alpha^2 & 1 \\ \alpha & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ and Proposition 2.36, we get

$$\dim(\mathrm{Hull}_H(C)) = k - \mathrm{rank}(GG^\dagger) = 3 - 2 = 1 = \ell.$$

Choose

$$G_1 = \begin{bmatrix} \alpha^2 & 0 & 1 & 1 & 0 & 1 \\ \alpha & \alpha^2 & \alpha^2 & \alpha & \alpha^2 & 0 \\ 0 & \alpha & \alpha^2 & 0 & 1 & \alpha^2 \end{bmatrix} \text{ and } G_2 = \begin{bmatrix} \alpha & 0 & 0 & 0 & \alpha^2 & \alpha \\ 1 & 0 & \alpha & \alpha & 0 & \alpha \\ 0 & 1 & \alpha & 0 & \alpha^2 & \alpha \end{bmatrix}.$$

Then $G_1 \sim G$ and $G_2 \sim G$. Moreover, G_1 and G_2 are generator matrices of C such that

$$G_1 G_2^\dagger = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \mathrm{diag}(1, 1, 0).$$

Choose

$$H_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & \alpha \\ 1 & 0 & 1 & 0 & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & 0 & \alpha^2 & \alpha \end{bmatrix} \text{ and } H_2 = \begin{bmatrix} \alpha^2 & \alpha & 0 & 0 & \alpha^2 & 1 \\ 0 & 0 & 0 & \alpha^2 & 1 & \alpha^2 \\ 0 & 1 & \alpha & 0 & \alpha^2 & \alpha \end{bmatrix}.$$

Then $H_1 \sim H$ and $H_2 \sim H$. It follows that H_1 and H_2 are parity-check matrices of C and

$$H_1H_2^\dagger = \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & 0 \end{bmatrix} = \mathrm{diag}(\alpha, \alpha, 0).$$

For an odd prime power q, we show that $GG^\dagger$ is always diagonalizable for every generator matrix G of a linear code over $\mathbb{F}_{q^2}$. We begin with the following useful lemma.

Lemma 3.19. *Let C be a linear code of length n over $\mathbb{F}_{q^2}$. If q is odd and C is not Hermitian self-orthogonal, then there exists a codeword $\boldsymbol{v} \in C$ such that $\langle \boldsymbol{v}, \boldsymbol{v} \rangle_H \neq 0$.*

Proof. Assume that q is an odd prime power and C is not Hermitian self-orthogonal. Then there exist $\boldsymbol{u}$ and $\boldsymbol{w}$ in C such that $\langle \boldsymbol{u}, \boldsymbol{w} \rangle_H \neq 0$. If $\langle \boldsymbol{u}, \boldsymbol{u} \rangle_H \neq 0$ or $\langle \boldsymbol{w}, \boldsymbol{w} \rangle_H \neq 0$, we are done. Assume that $\langle \boldsymbol{u}, \boldsymbol{u} \rangle_H = 0$ and $\langle \boldsymbol{w}, \boldsymbol{w} \rangle_H = 0$. Let $\boldsymbol{v} = \boldsymbol{u} + \langle \boldsymbol{u}, \boldsymbol{w} \rangle_H \boldsymbol{w}$. Since q is odd, we have

$$\begin{aligned} \langle \boldsymbol{v}, \boldsymbol{v} \rangle_H &= \langle \boldsymbol{u}, \boldsymbol{u} \rangle_H + \langle \boldsymbol{u}, \boldsymbol{w} \rangle_H^q \langle \boldsymbol{u}, \boldsymbol{w} \rangle_H + \langle \boldsymbol{u}, \boldsymbol{w} \rangle_H \langle \boldsymbol{w}, \boldsymbol{u} \rangle_H + \langle \boldsymbol{u}, \boldsymbol{w} \rangle_H^{q+1} \langle \boldsymbol{w}, \boldsymbol{w} \rangle_H \\ &= \langle \boldsymbol{u}, \boldsymbol{w} \rangle_H^q \langle \boldsymbol{u}, \boldsymbol{w} \rangle_H + \langle \boldsymbol{u}, \boldsymbol{w} \rangle_H \langle \boldsymbol{u}, \boldsymbol{w} \rangle_H^q \\ &= 2\langle \boldsymbol{u}, \boldsymbol{w} \rangle_H^q \langle \boldsymbol{u}, \boldsymbol{w} \rangle_H \\ &\neq 0 \end{aligned}$$

as desired. □

Applying Lemma 3.19 instead of Lemma 3.4, the next proposition can be obtained using the arguments similar to those for the proof of Proposition 3.5.

Proposition 3.20. *Let C be a non-zero linear code of length n over $\mathbb{F}_{q^2}$. If q is odd, then $GG^\dagger$ is diagonalizable for every generator generator matrix G of C.*

The following corollary is a direct consequence of Proposition 3.20.

Corollary 3.21. *Let C be a linear $[n,k]_{q^2}$ code such that* $\dim(\mathrm{Hull}_H(C)) = \ell$. *If q is odd, then the following statements hold.*

1. *There exist nonzero elements $a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_q$ and a generator matrix G of C such that*

$$GG^{\dagger} = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0).$$

2. *There exist nonzero elements $b_1, b_2, \ldots, b_{n-k-\ell}$ in $\mathbb{F}_q$ and a parity-check matrix H of C such that*

$$HH^{\dagger} = \mathrm{diag}(b_1, b_2, \ldots, b_{n-k-\ell}, 0, \ldots, 0).$$

Example 3.22. Let $\mathbb{F}_9 = \{0, 1, \alpha, \alpha^2, \alpha^3, 2, \alpha^5, \alpha^6, \alpha^7 \mid \alpha^2 + 2\alpha^2 + 2 = 0\}$ and C be a linear $[6,3]_9$ code with generator matrix

$$G = \begin{bmatrix} \alpha^6 & \alpha^7 & \alpha^3 & 2 & \alpha & \alpha^5 \\ \alpha & \alpha & \alpha^5 & \alpha^6 & 2 & \alpha^3 \\ 0 & \alpha & \alpha^7 & \alpha^2 & \alpha^6 & \alpha^3 \end{bmatrix}.$$

Then

$$H = \begin{bmatrix} 1 & 0 & 0 & \alpha^3 & \alpha & \alpha^3 \\ \alpha & \alpha & 1 & 1 & \alpha^2 & 2 \\ \alpha^7 & 1 & 0 & \alpha^3 & 2 & 1 \end{bmatrix}$$

is a parity-check matrix of C. Since $GG^{\dagger} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}$ and Proposition 2.36, we get

$$\dim(\mathrm{Hull}_H(C)) = k - \mathrm{rank}(GG^{\dagger}) = 3 - 3 = 0.$$

Therefore, we have

$$GG^\dagger = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix} = \mathrm{diag}(1,1,2)$$

and

$$H_1H_1^\dagger = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \mathrm{diag}(1,2,1).$$

Corollary 3.23. *Let q be an odd prime power and let C be a linear code over $\mathbb{F}_{q^2}$. Then C is Hermitian complementary dual if and only if C has a Hermitian orthogonal basis.*

The following results hold true for every prime powers q. However, for an odd prime power q, we already have stronger results in discussion above.

Proposition 3.24. *Let C be a linear $[n,k]_{q^2}$ code such that $\dim(\mathrm{Hull}_H(C)) = \ell$. If $\mathrm{Hull}_H(C)$ is maximal Hermitian self-orthogonal in C, then there exist nonzero elements $a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_{q^2}$ and a generator matrix G of C such that*

$$GG^\dagger = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0).$$

We can replace a generator matrix G by a parity-check matrix H of C and derive the result as follows.

Corollary 3.25. *Let C be a linear $[n,k]_{q^2}$ code such that $\dim(\mathrm{Hull}_H(C)) = \ell$. If $\mathrm{Hull}_H(C)$ is maximal Hermitian self-orthogonal in $C^{\perp_H}$, then there exist nonzero elements $b_1, b_2, \ldots, b_{n-k-\ell}$ in $\mathbb{F}_{q^2}$ and a parity-check matrix H of C such that*

$$HH^\dagger = \mathrm{diag}(b_1, b_2, \ldots, b_{n-k-\ell}, 0, \ldots, 0).$$

Corollary 3.26. *Let C be a linear $[n,k]_{q^2}$ code. If C is maximal Hermitian self-orthogonal, then there exist nonzero elements $b_1, b_2, \ldots, b_{n-2k}$ in $\mathbb{F}_{q^2}$ and a parity-check matrix H of C such that*

$$HH^\dagger = \operatorname{diag}(b_1, b_2, \ldots, b_{n-2k}, 0, \ldots, 0).$$

Example 3.27. Let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 \mid \alpha^2 + \alpha + 1 = 0\}$ and C be a linear $[6,2]_4$ code with generator matrix

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

Then

$$H = \begin{bmatrix} 0 & 1 & 1 & \alpha^2 & 1 & \alpha \\ 1 & 1 & 1 & 0 & \alpha^2 & 1 \\ 1 & \alpha & \alpha & \alpha & \alpha & \alpha \\ 1 & 0 & \alpha & 0 & 1 & 1 \end{bmatrix}$$

is parity-check matrix of C. Since $GG^\dagger = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and Proposition 2.36, we get

$$\dim(\mathrm{Hull}_H(C)) = k - \operatorname{rank}(GG^\dagger) = 2 - 0 = 2 = \dim(C).$$

It implies that $\mathrm{Hull}_H(C)$ is maximal Hermitian self-orthogonal in $C^{\perp_H}$ and

$$HH^\dagger = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \operatorname{diag}(1,1,0,0)$$

is diagonal.

Corollary 3.28. *Let C be a linear $[n,k]_{q^2}$ code such that* $\dim(\mathrm{Hull}_H(C)) = \ell$. *If q is even, then the following statements hold.*

1) $k - \ell \leq 1$ *if and only if* $\mathrm{Hull}_H(C)$ *is maximal Hermitian self-orthogonal in* C.

2) $n - k - \ell \leq 1$ *if and only if* $\mathrm{Hull}_H(C)$ *is maximal Hermitian self-orthogonal in* $C^{\perp_H}$.

Corollary 3.29. *Let C be a non-zero linear code of length n over $\mathbb{F}_{q^2}$. If q is even and* $\dim(C) - \dim(\mathrm{Hull}_H(C)) \leq 1$, *then $GG^\dagger$ is diagonalizable for every generator matrix G of C.*

Chapter 4

Linear ℓ-Intersection Pairs of Codes

Linear complementary pairs (LCPs) of codes have been of interest and extensively studied due to their rich algebraic structure and wide applications in cryptography. For example, in [12] and [13], it was shown that these pairs of codes can be used to counter passive and active side-channel analysis attacks on embedded cryptosystems. Several construction of LCPs of codes were also given.

In this chapter, we introduce a linear ℓ-Intersection pairs of codes as a generalization of the LCP of codes in [13]. A characterization of such pairs of codes is given in terms of generator and parity-check matrices of codes. Linear ℓ-Intersection pairs of codes has showed and constructed. Including of links between this concept and known families of codes such as complementary dual codes, self-orthogonal codes, and linear complementary pairs of codes, ℓ-Intersection pairs of codes have been seen as a generalization of hulls of code.

Definition 4.1. Two of linear codes C and D of length n over $\mathbb{F}_q$ are called a ***linear complementary pair (LCP)*** if

$$C \cap D = \{\mathbf{0}\} \ \ and \ \ C + D = \mathbb{F}_q^n.$$

Clearly, C and $C^\perp$ form a linear complementary pair for all LECD codes.

Example 4.2. Let C and D be linear $[6,2]_2$ and $[6,4]_2$ codes with generator matrices

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

and

$$G_D = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix},$$

respectively. Then $\dim(C) + \dim(D) = 2 + 4 = 6$. Since the rows of G_C and G_D are linearly independent, $C \cap D = \{\mathbf{0}\}$. Hence, the codes C and D form a LCP.

Definition 4.3. For an integer $\ell \geq 0$, linear codes C and D of length n over $\mathbb{F}_q$ are called a ***linear ℓ-intersection pair*** if

$$\dim(C \cap D) = \ell.$$

Example 4.4. Let $C = \{000000, 101010, 010101, 111111\}$ and $D = \{000000, 110011, 001100, 111111\}$ be linear codes of length 6 over $\mathbb{F}_2$. Then $C \cap D = \{000000, 111111\}$ has dimension one. Hence, C and D form a linear 1-intersection pair.

From the definition above, we have the following observations.

- A linear 0-intersection pair with $\dim(C) + \dim(D) = n$ is an LCP (see [13]).
- A linear 0-intersection pair with $D = C^\perp$ is an LCD code (see [33]).
- The study of a linear ℓ-intersection pair with $D = C^\perp$ is equivalent to that of the hull of C (see [23]).

Therefore, linear ℓ-intersection pairs of codes can be viewed as a generalization of LCPs of codes, LCD codes, and the hulls of codes.

4.1 Characterizations of Linear ℓ-Intersection Pairs of Codes

In this section, properties of linear ℓ-intersection pairs of codes are established in terms of their generator and parity-check matrices. In some cases, links between this concept and known families of codes such as complementary dual codes, self-orthogonal codes, and linear complementary pairs of codes, as well as hulls of codes, are discussed.

Theorem 4.5. *For $i \in \{1,2\}$, let C_i be a linear $[n,k_i]_q$ code with parity check matrix H_i and generator matrix G_i and let ℓ be a non-negative integer. Then* $\mathrm{rank}(H_1G_2^T)$ *and* $\mathrm{rank}(G_1H_2^T)$ *are independent of H_i and G_i and the following statements are equivalent.*

1. *C_1 and C_2 are a linear ℓ-intersection pair.*

2. $\mathrm{rank}(G_1H_2^T) = \mathrm{rank}(H_2G_1^T) = k_1 - \ell$.

3. $\mathrm{rank}(G_2H_1^T) = \mathrm{rank}(H_1G_2^T) = k_2 - \ell$.

Proof. First, we prove that $\mathrm{rank}(H_1G_2^T)$ and $\mathrm{rank}(G_1H_2^T)$ are independent of H_i and G_i. Let $\dim(C_1 \cap C_2) = m$. We prove that $\mathrm{rank}(G_1H_2^T) = \mathrm{rank}(H_2G_1^T) = k_1 - m$. Since $(G_1H_2^T)^T = H_2G_1^T$, it suffices to show that $\mathrm{rank}(G_1H_2^T) = k_1 - m$.

Since $m = \dim(C_1 \cap C_2)$, we have $n \geq \dim(C_1 + C_2) = k_1 + k_2 - m$ which implies that $n - k_2 \geq k_1 - m$ and $n - k_1 \geq k_2 - m$. Let $B = \{g_1, g_2, \ldots, g_m\}$ be a basis of $C_1 \cap C_2$. If $m = k_1$, then $B \subsetneq C_2$ and $G_1H_2^T = [0]$, and hence $\mathrm{rank}(G_1H_2^T) = 0 = k_1 - m$ as desired. Assume that $m < k_1$ and extend B to be a basis $\{g_1, g_2, \ldots, g_m, g_{m+1}, \ldots, g_{k_1}\}$ for C_1. Then

$$J_1 = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_m \\ g_{m+1} \\ \vdots \\ g_{k_1} \end{bmatrix}$$

is a generator matrix for C_1. Applying a suitable sequence of elementary row operations gives an invertible $k_1 \times k_1$ matrix A over $\mathbb{F}_q$ such that $G_1 = AJ_1$ and hence

$$G_1 H_2^T = AJ_1 H_2^T.$$

Since A is invertible, we have

$$\operatorname{rank}(G_1 H_2^T) = \operatorname{rank}(J_1 H_2^T). \tag{4.1}$$

As $g_i \in C_2$ for all $i = 1, 2, \ldots, m$, we have $g_i H_2^T = 0$ for all $i = 1, 2, \ldots, m$ so then

$$J_1 H_2^T = \left[\begin{array}{c} \mathbf{0} \\ \hline \begin{bmatrix} g_{m+1} \\ \vdots \\ g_{k_1} \end{bmatrix} H_2^T \end{array} \right].$$

The matrix $\begin{bmatrix} g_{m+1} \\ \vdots \\ g_{k_1} \end{bmatrix} H_2^T$ has dimensions $(k_1 - m) \times (n - k_2)$ with $n - k_2 \geq k_1 - m$

so it follows that

$$\operatorname{rank}\left(\begin{bmatrix} g_{m+1} \\ \vdots \\ g_{k_1} \end{bmatrix} H_2^T\right) \leq (k_1 - m).$$

Suppose that $\operatorname{rank}\left(\begin{bmatrix} g_{m+1} \\ \vdots \\ g_{k_1} \end{bmatrix} H_2^T\right) < k_1 - m$. Then there exists a non-zero vector $\boldsymbol{u} \in \mathbb{F}_q^{k_1-m}$ such that

$$\boldsymbol{u}\begin{bmatrix} g_{m+1} \\ \vdots \\ g_{k_1} \end{bmatrix} H_2^T = [0],$$

so then $\boldsymbol{u}\begin{bmatrix} g_{m+1} \\ \vdots \\ g_{k_1} \end{bmatrix} \in C_2 \setminus \{\mathbf{0}\}$. Since $\operatorname{span}\{g_{m+1}, g_{m+2}, \ldots, g_{k_1}\} \cap C_2 = \{\mathbf{0}\}$, we have $\boldsymbol{u}\begin{bmatrix} g_{m+1} \\ \vdots \\ g_{k_1} \end{bmatrix} \notin C_2$, which is a contradiction. Therefore, $\operatorname{rank}(G_1H_2^T) = \operatorname{rank}(J_1H_2^T) = k_1 - m$ which is independent of G_1 and H_2 as required.

To prove 1) $\Leftrightarrow$ 2), assume that C_1 and C_2 are a linear ℓ-intersection pair. Then $\dim(C_1 \cap C_2) = \ell$. Hence, $\operatorname{rank}(G_1H_2^T) = \operatorname{rank}(J_1H_2^T) = k_1 - \ell$ which is independent of G_1 and H_2 as required. Conversely, assume that 2) holds. Then $k_1 - \ell = k_1 - m$. It implies that $\dim(C_1 \cap C_2) = m = \ell$, i.e., C_1 and C_2 are a linear ℓ-intersection pair as desired.

By swapping C_1 and C_2, the equivalent 1) $\Leftrightarrow$ 3) can be obtained similarly. $\square$

Example 4.6. Let C_1 and C_2 be linear $[6,2]_2$ and $[6,3]_2$ codes with generator matrices

$$G_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

and

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

respectively. Then

$$H_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

and

$$H_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

are parity-check matrices of C_1 and C_2, receptively. It follows that

$$G_1H_2^T = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}^T = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

and

$$G_2H_1^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}^T = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

which implies that $\mathrm{rank}(G_1H_2^T) = 2-2 = 0$ and $\mathrm{rank}(G_2H_1^T) = 3-2 = 1$. Hence, C_1 and C_2 form a linear 2-intersection pair by Theorem 4.5.

In the case where the sum of the two codes cover the entire space $\mathbb{F}_q^n$, we have the following corollary.

Corollary 4.7. *For $i \in \{1,2\}$, let C_i be a linear $[n,k_i]_q$ code with parity check matrix H_i and generator matrix G_i and let ℓ be a non-negative integer. Then the following statements are equivalents.*

1. *C_1 and C_2 are a linear ℓ-intersection pair such that $C_1 + C_2 = \mathbb{F}_q^n$.*

2. $\mathrm{rank}(G_1H_2^T) = \mathrm{rank}(H_2G_1^T) = n - k_2 = k_1 - \ell$.

3. $\mathrm{rank}(G_2H_1^T) = \mathrm{rank}(H_1G_2^T) = n - k_1 = k_2 - \ell$.

Proof. Since $C_1 + C_2 = \mathbb{F}_q^n$, we have that $n = k_1 + k_2 - \ell$. Then $n - k_2 = k_1 - \ell$ and $n - k_1 = k_2 - \ell$, and the equivalent follow from Theorem 4.5. □

By setting $\ell = 0$ in the above corollary, we have the following characterization of LCPs of codes.

Corollary 4.8. *For $i \in \{1,2\}$, let C_i be a linear $[n,k_i]_q$ code with parity check matrix H_i and generator matrix G_i. Then the following statements are equivalents.*

1. *C_1 and C_2 are a LCP.*

2. $\mathrm{rank}(G_1H_2^T) = \mathrm{rank}(H_2G_1^T) = k_1$.

3. $\mathrm{rank}(G_2H_1^T) = \mathrm{rank}(H_1G_2^T) = k_2$.

Example 4.9. Let C_1 and C_2 be linear $[6,2]_2$ and $[6,4]_2$ codes with generator matrices

$$G_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \text{ and } G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Then

$$H_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \text{ and } H_2 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

are parity-check matrices for C_1 and C_2 respectively. It follows that

$$G_1 H_2^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and

$$G_2 H_1^T = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}^T = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Since $\mathrm{rank}(G_1 H_2^T) = 2 = \dim(C)_1$ and $\mathrm{rank}(G_2 H_1^T) = 4 = \dim(C_2)$, C_1 and C_2 form a LCP by Corollary 4.8.

In the case where C_2 is the dual code of C_1, we have $C_1 \cap C_2 = \mathrm{Hull}(C_1) = \mathrm{Hull}(C_2)$ and the following result in [23] can be obtained from Theorem 4.5.

Remark 4.10. *In general, we may relate a linear ℓ-intersection pair of codes with the Galois dual of a linear code [18]. For $q = p^e$ and $0 \leq h < e$, the*

p^h-inner product (Galois inner product) *between* $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ *and* $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ *in* $\mathbb{F}_q$ *is defined to be*

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle_h = \sum_{i=1}^{n} u_i v_i^{p^h}.$$

The p^h-dual (Galois dual) $C^{\perp_h}$ *of a linear code* C *is defined as*

$$C^{\perp_h} = \{\boldsymbol{u} \in \mathbb{F}_q^n \mid \langle \boldsymbol{u}, \boldsymbol{c} \rangle_h = 0 \text{ for all } \boldsymbol{c} \in C\}.$$

Note that $C^{\perp_0}$ *is the Euclidean dual* $C^{\perp}$*. If* e *is even, the* $C^{\perp_{\frac{e}{2}}}$ *is the well-known Hermitian dual.*

Using statements similar to those in the proof of Theorem 4.5, the following result can be concluded. For $i \in \{1, 2\}$*, let* C_i *be a linear* $[n, k_i]_q$ *code with generator matrix* G_i *and let* H_i *be a generator matrix for the Galois dual* $C_i^{\perp_h}$*. If* C_1 *and* C_2 *are a linear* ℓ*-intersection pair then*

$$\operatorname{rank}(G_1 H_2^*) = \operatorname{rank}(H_2 G_1^*) = k_1 - \ell,$$

and

$$\operatorname{rank}(G_2 H_1^*) = \operatorname{rank}(H_1 G_2^*) = k_2 - \ell,$$

where $A^* = [a_{ji}^{p^h}]$ *for a matrix* $A = [a_{ij}]$ *over* $\mathbb{F}_q$*.*

4.2 Constructions of Linear ℓ-Intersection Pairs of Codes

In this section, a discussion on constructions of linear ℓ-intersection pairs is given. From the characterizations in the previous section, the value ℓ for which two linear codes of length n over $\mathbb{F}_q$ form a linear ℓ-intersection pair can be easily determined. Here, constructions of linear ℓ-intersection pairs will be given using the concept of equivalent codes and some propagation rules.

We note that constructions of linear 0-intersection pairs of linear codes C_1 and C_2 with $\dim(C_1) + \dim(C_2) = n$, LCPs of codes, have been given in [13]. Various constructions of linear 0-intersection pairs of linear codes C_1 and $C_2 = C_1^{\perp}$, LCD codes, have been discussed in [8], [9], [27], [33] and [35]. Constructions of some linear codes with prescribed hull dimension have been given in [23] and [32].

First of all, equivalent of two codes and weighted permutation matrix are used (see Remark 2.21). Using Definition 2.19 and Definition 2.20, It is not difficult to see that linear codes C_1 and C_2 of length n over $\mathbb{F}_q$ are equivalent if and only if there exists an $n \times n$ weighted permutation matrix A over $\mathbb{F}_q$ such that $C_2 = \{\boldsymbol{c}A \mid \boldsymbol{c} \in C_1\}$.

Lemma 4.11. *Let C_1 and C_2 be $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ codes, respectively. Let A be an $n \times n$ weighted permutation matrix over $\mathbb{F}_q$ and let G_1 and H_2 be a generator matrix of C_1 and a parity-check matrix of C_2, respectively. Then their exists a linear ℓ-intersection pair of $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ codes, where $\ell = k_1 - \operatorname{rank}(G_1 A H_2^T)$.*

Proof. Let C_1' be the linear code generated by G_1A. By the discussion above, C_1' is equivalent to C_1. Hence, C_1' is an $[n, k_1, d_1]_q$ code. By Theorem 4.5, C_1' and C_2 form a linear ℓ-intersection pair of $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ codes, where $\ell = k_1 - \operatorname{rank}((G_1A)H_2^T) = k_1 - \operatorname{rank}(G_1AH_2^T)$. □

In Lemma 4.11, the value ℓ depends on the choices of A. In applications, a suitable weighted permutation matrix A is required. Illustrative examples are given as follows.

Example 4.12. Let C_1 and C_2 be $[7, 4, 3]_2$ and $[7, 3, 4]_2$ codes with generator matrices

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \text{ and } G_2 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Using the computer algebra system MAGMA [3] and Theorem 4.5, it can be seen that C_1 and C_2 form a linear 3-intersection pair of $[7, 4, 3]_2$ and $[7, 3, 4]_2$ codes. Let

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \ A_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

and

$$A_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

be 7×7 (weighted) permutation matrices over $\mathbb{F}_2$. Let C_1', C_1'' and C_1''' be linear codes generated by G_1A_1, G_1A_2 and G_1A_3, respectively. Using the computer algebra system MAGMA [3] and Lemma 4.11, we have the result as follows;

- C_1' and C_2 form a linear 2-intersection pair of $[7, 4, 3]_2$ and $[7, 3, 4]_2$ codes.

- C_1'' and C_2 form a linear 1-intersection pair of $[7,4,3]_2$ and $[7,3,4]_2$ codes.

- C_1''' and C_2 form a linear 0-intersection pair of $[7,4,3]_2$ and $[7,3,4]_2$ codes.

Next, useful recursive constructions of linear ℓ-intersection pairs are given.

Theorem 4.13. *Let $\ell \geq 0$ be an integer. If there exists a linear ℓ-intersection pair of $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ codes, then the following statements hold.*

1. *There exists a linear γ-intersection pair of $[n, k_1, d_1]_q$ and $[n, k_2 - \ell + \gamma, D_2]_q$ codes for all $0 \leq \gamma \leq \ell$, where $D_2 \geq d_2$.*

2. *There exists a linear γ-intersection pair of $[n + \ell - \gamma, k_1, d_1]_q$ and $[n + \ell - \gamma, k_2, D_2]_q$ codes for all $0 \leq \gamma \leq \ell$, where $D_2 \geq d_2$.*

Proof. Assume that there exists a linear ℓ-intersection pair of $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ codes, denoted by C_1 and C_2, respectively. Let $A = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_\ell\}$ be a basis of $C_1 \cap C_2$. Let B_1 and B_2 be bases of C_1 and C_2 extended respectively from A. For $\gamma = \ell$, the two statements are obvious. Assume that $0 \leq \gamma < \ell$.

To prove 1, let C_2' be the linear code generated by $B_2 \setminus \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{\ell-\gamma}\}$. Then C_2' is an $[n, k_2 - \ell + \gamma]_q$ code. Since C_2' is a subcode of C_2, we have $d(C_2') = D_2$ for some $D_2 \geq d_2$. It is clear that C_1 and C_2' form a linear γ-intersection pair.

To prove 2, let $\varphi_1 : B_1 \to \mathbb{F}_q^{n+1}$ and $\varphi_2 : B_2 \to \mathbb{F}_q^{n+1}$ be concatenated maps defined by

$$\varphi_1(\boldsymbol{u}) = \boldsymbol{u}|0$$

for all $\boldsymbol{u} \in B_1$, and

$$\varphi_2(\boldsymbol{u}) = \begin{cases} \boldsymbol{u}|1 & \text{if } \boldsymbol{u} = \boldsymbol{v}_\ell, \\ \boldsymbol{u}|0 & \text{otherwise} \end{cases}$$

for all $\boldsymbol{u} \in B_2$. Let C_1' and C_2' be the linear codes generated by $\varphi_1(B_1)$ and $\varphi_2(B_2)$. Clearly, C_1' and C_2' form a linear $(\ell-1)$-intersection pair of $[n+1, k_1, d_1]_q$ and $[n+1, k_2, D_2]_q$ codes for some $D_2 \geq d_2$. Continue this process, a linear γ-intersection pair of $[n+\ell-\gamma, k_1, d_1]_q$ and $[n+\ell-\gamma, k_2, D_2]_q$ codes can be constructed for all $0 \leq \gamma < \ell$, where $D_2 \geq d_2$. $\square$

Based on the characterizations given in section 4.1, Lemma 4.11 and some well known properties in linear codes [21], some linear ℓ-intersection pair of good codes over small finite fields can be constructed using the following steps:

1) Fix two best known linear codes C_1 and C_2 of length n over $\mathbb{F}_q$ from [21].

2) Fix an $n \times n$ weighted permutation matrix A over $\mathbb{F}_q$.

3) Compute $C_1' = \{\boldsymbol{c}A \mid \boldsymbol{c} \in C_1\}$.

4) Compute the value ℓ for which C_1' and C_2 form a linear ℓ-intersection pair using Lemma 4.11.

   Output: linear ℓ-intersection pair.

5) Apply recursive constructions given in Theorem 4.13.

   Output: linear γ-intersection pair, where $0 \leq \gamma \leq \ell$.

We note that a linear ℓ-intersection pair of linear codes with best known parameters is obtained in Step 4 while the minimum distance of the second code in a linear γ-intersection pair obtained in Step 5 might be lower than the best known ones.

Example 4.14. Using the computer algebra system MAGMA [3] and Theorem 4.13, the following linear γ-intersection pairs of codes $C_{\gamma 1}$ and $C_{\gamma 2}$ are derived from ℓ-intersection pairs of linear codes in Example 4.12.

- γ-intersection pairs derived from the linear 2-intersection pair of C_1' and C_2 with parameters $[7,4,3]_2$ and $[7,3,4]_2$, respectively.

γ	$C_{\gamma 1}$	$C_{\gamma 2}$
0	$[7,4,3]_2$	$[7,1,7]_2$
0	$[9,4,3]_2$	$[9,3,7]_2$
1	$[7,4,3]_2$	$[7,2,4]_2$
1	$[8,4,3]_2$	$[8,3,4]_2$
2	$[7,4,3]_2$	$[7,3,4]_2$

- γ-intersection pairs derived from the linear 1-intersection pair of C_1'' and C_2 with parameters $[7,4,3]_2$ and $[7,3,4]_2$, respectively.

γ	$C_{\gamma 1}$	$C_{\gamma 2}$
0	$[7,4,3]_2$	$[7,2,4]_2$
0	$[8,4,3]_2$	$[8,3,4]_2$
1	$[7,4,3]_2$	$[7,3,4]_2$

- γ-intersection pair derived from the linear 0-intersection pair of C_1''' and C_2 with parameters $[7,4,3]_2$ and $[7,3,4]_2$, respectively.

γ	$C_{\gamma 1}$	$C_{\gamma 2}$
0	$[7,4,3]_2$	$[7,3,4]_2$.

Using basic linear algebra, we have the following result.

Lemma 4.15. *If there exists a linear ℓ-intersection pair of $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$ codes, then $k_1+k_2-n \leq \ell \leq \min\{k_1,k_2\}$.*

Note that Lemma 4.15 does not guarantee the existence of a linear ℓ-intersection pair of $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$ codes for all ℓ satisfying $k_1+k_2-n \leq \ell \leq \min\{k_1,k_2\}$.

Conjecture 1. There exists a linear ℓ-intersection pair of $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ codes for all ℓ satisfying $k_1 + k_2 - n \leq \ell \leq \min\{k_1, k_2\}$ provided that there exist $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ codes.

The other cases remain an open problem. In our view, the concept of equivalent codes in Lemma 4.11 might be useful in solving Conjecture 1 as discussed in Example 4.12.

As an application, linear ℓ-intersection pairs of codes are employed to construct entanglement-assisted quantum error correcting codes. It will be discussed in Chapter 5.

Chapter 5

Applications

Applications of hulls in constructions of entanglement-assisted quantum error-correcting codes are discussed. In this chapter, hulls and linear ℓ-intersection pairs of codes discussed in Chapter 3 and Chapter 4 are applied in constructions of Entanglement-Assisted Quantum Error Correcting Codes (EAQECCs). EAQECCs were introduced in [26] which can be constructed from classical linear codes. The performance of the resulting quantum codes can be determined by the performance of the underlying classical codes. Precisely, an $[[n, k, d; c]]_q$ EAQECC encodes k logical qudits into n physical qudits using c copies of maximally entangled states and its performance is measured by its rate $\frac{k}{n}$ and net rate $(\frac{k-c}{n})$. As shown in [5], the net rate of an EAQECC is positive, it is possible to obtain catalytic codes. The readers may refer to [6], [23], and the references therein for more details on EAQECCs.

5.1 EAQECCs from Hulls of Linear Codes

The following results from [23] are useful for constructions of EAQECCs from classical linear codes and their hulls.

Proposition 5.1 ([23, Corollary 3.1]). *Let C be a classical $[n, k, d]_q$ linear code and $C^\perp$ its Euclidean dual with parameters $[n, n-k, d^\perp]_q$. Then there exist $[[n, k - \dim(\mathrm{Hull}(C)), d; n - k - \dim(\mathrm{Hull}(C))]]_q$ and $[[n, n - k - \dim(\mathrm{Hull}(C)), d^\perp; k - \dim(\mathrm{Hull}(C))]]_q$ EAQECCs.*

Proposition 5.2 ([23, Corollary 3.2]). *Let C be a classical $[n,k,d]_{q^2}$ code and let $C^{\perp_H}$ be its Hermitian dual with parameters $[n,n-k,d^{\perp_H}]_{q^2}$. Then there exists $[[n,k-\dim(\mathrm{Hull}_H(C)),d;n-k-\dim(\mathrm{Hull}_H(C))]]_q$ and $[[n,n-k-\dim(\mathrm{Hull}_H(C)),d^{\perp};k-\dim(\mathrm{Hull}_H(C))]]_q$ EAQECCs.*

Based on the diagonalizability of Gramians studied in Sections 3.1 and 3.2, EAQECCs can be constructed from all linear codes over finite fields of odd characteristic as follows.

Proposition 5.3. *Let $q \geq 5$ be an odd prime power and let C be a classical $[n,k,d]_q$ linear code such that $\dim(\mathrm{Hull}(C)) = \ell$. Then there exists an $[[n+r,k-\ell,d';n-k-\ell+r]]_q$ EAQECC with $d \leq d' \leq d+r$ for each $0 \leq r \leq k-\ell$.*

Proof. If $r=0$ or $k=\ell$, then the result follows directly from Proposition 5.1. Next, assume that $1 \leq r \leq k-\ell$. Since q is odd, there exists a generator matrix G for C such that the Gramian GG^T is diagonalizable by Proposition 3.5. Precisely, there exist linearly independent codewords $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{k-\ell}$ in C such that $\boldsymbol{x}_i\boldsymbol{x}_i^T \neq 0$ for all $1 \leq i \leq n-k$ and $\boldsymbol{x}_i\boldsymbol{x}_j^T = 0$ for all $1 \leq i < j \leq k-\ell$. Since $q \geq 5$, we have that $\{a^2 \mid a \in \mathbb{F}_q^*\}$ contains at least 2 elements. Hence, for each $i \in \{1,2,\ldots,k-\ell\}$, there exists $\alpha_i \in \mathbb{F}_q^*$ such that $\alpha_i^2 \neq -\boldsymbol{x}_i\boldsymbol{x}_i^T$. Let H be a parity check matrix for C and let C' be the code with parity check matrix

$$H' = \left[\begin{array}{ccc|c} & 0 & & H \\ \hline \alpha_1 & & & \boldsymbol{x}_1 \\ & \ddots & & \vdots \\ & & \alpha_r & \boldsymbol{x}_r \end{array}\right].$$

Then

$$H'(H')^T = \begin{bmatrix} HH^T & 0 & \dots & 0 \\ 0 & \alpha_1^2 + \boldsymbol{x}_1\boldsymbol{x}_1^T & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & \alpha_r^2 + \boldsymbol{x}_r\boldsymbol{x}_r^T \end{bmatrix}.$$

Since $\alpha_i^2 \neq -\boldsymbol{x}_i\boldsymbol{x}_i^T$ for all $1 \leq i \leq r$ and $\mathrm{rank}(HH^T) = n-k-\ell$, we have that $\mathrm{rank}(H'(H')^T) = n-k-\ell+r \geq 0$ since $\ell \leq \min\{k, n-k\}$ and $r \geq 0$. Equivalently, $\dim(\mathrm{Hull}(C')) = \ell$. Since every $d-1$ columns of H are linearly independent and $\alpha_i \neq 0$ for all $i \in \{1, 2, \dots, r\}$, every $d-1$ columns of H' are linearly independent. It follows that C' is an $[n+r, k, d']_q$ code where $d \leq d' \leq d+r$. Then by Proposition 5.1, there exists an $[[n+r, k-\ell, d'; n-k-\ell+r]]_q$ EAQECC. $\square$

In the same fashion, the Hermitian hulls of linear codes can be applied in constructions of EAQECCs in the following proposition.

Proposition 5.4. *Let $q \geq 3$ be an odd prime power and let C be a classical $[n, k, d]_{q^2}$ linear code such that $\dim(\mathrm{Hull}_H(C)) = \ell$. Then there exists an $[[n+r, k-\ell, d'; n-k-\ell+r]]_q$ EAQECC with $d \leq d' \leq d+r$ for each $0 \leq r \leq k-\ell$.*

Proof. If $r = 0$ or $k = \ell$, then the result follows directly from Proposition 5.2. Next, assume that $1 \leq r \leq k-\ell$. Since q is odd, there exists a generator matrix G for C such that $GG^\dagger$ is diagonalizable by Proposition 3.20. Precisely, there exist linearly independent codewords $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_{k-\ell}$ in C such that $\boldsymbol{x}_i\boldsymbol{x}_i^\dagger \neq 0$ for all $1 \leq i \leq n-k$ and $\boldsymbol{x}_i\boldsymbol{x}_j^\dagger = 0$ for all $1 \leq i < j \leq k-\ell$. For each $i \in \{1, 2, \dots, r\}$, there exist $\alpha_i \in \mathbb{F}_{q^2}^*$ such that ${\alpha_i}^{q+1} \neq -\boldsymbol{x}_i\boldsymbol{x}_i^\dagger$ since $q \geq 3$. Let H be a generator matrix for $C^{\perp_H}$ and let C' be the code with parity check matrix

$$H' = \left[\begin{array}{ccc|c} & 0 & & H \\ \hline \alpha_1 & & & \boldsymbol{x}_1 \\ & \ddots & & \vdots \\ & & \alpha_r & \boldsymbol{x}_r \end{array}\right].$$

Then

$$H'(H')^\dagger = \left[\begin{array}{c|cccc} HH^\dagger & 0 & & \dots & 0 \\ \hline 0 & \alpha_1^{q+1} + \boldsymbol{x}_1\boldsymbol{x}_1^\dagger & & & 0 \\ \vdots & & & \ddots & \\ 0 & 0 & & & \alpha_r^{q+1} + \boldsymbol{x}_r\boldsymbol{x}_r^\dagger \end{array}\right].$$

Since $\alpha_i^{q+1} \neq -\boldsymbol{x}_i\boldsymbol{x}_i^\dagger$ for all $1 \leq i \leq r$ and $\text{rank}(HH^\dagger) = n-k-\ell$, we have that $rank(H'(H')^\dagger) = n-k-\ell+r \geq 0$ since $\ell \leq \min\{k, n-k\}$ and $r \geq 0$. Equivalently, $\dim(\text{Hull}_H(C')) = \ell$. It is easily seen that very $d-1$ columns of H' are linearly independent. Hence, C' is an $[n+r, k, d']_{q^2}$ code where $d \leq d' \leq d+r$. By Proposition 5.2, there exists an $[[n+r, k-\ell, d'; n-k-\ell+r]]_q$ EAQECC. □

Observe that linear $[n,k]_q$ and $[n,k]_{q^2}$ codes with $\frac{n}{2} < k \leq n$ have hull dimension $\ell \leq \min\{k, n-k\} \leq n-k$ which implies that $k-\ell \geq 2k-n$. From the constructions in Propositions 5.3 and 5.4, we have an EAQECC Q with parameters $[[n+r, k-\ell, d'; n-k-\ell+r]]_q$ for all $0 \leq r \leq k-\ell$. Hence, the net rate of Q is

$$\frac{(k-\ell)-(n-k-\ell+r)}{n+r} = \frac{2k-n-r}{n+r} > 0$$

for all classical linear codes with $k > \frac{n}{2}$ and $0 \leq r < 2k-n$ since $2k-n \leq k-\ell$. In addition, if the dimension of the input linear code is

$$k \geq \frac{3n+r}{4}, \tag{5.1}$$

its hull dimension is $\ell \leq \min\{k, n-k\} \leq n-k \leq n - \frac{3n+r}{4} = \frac{n-r}{4}$ which implies that $k - \ell \geq k - \frac{n-r}{4} \geq \frac{3n+r}{4} - \frac{n-r}{4} = \frac{n+r}{2}$, and hence, the rate of Q is

$$\frac{k-\ell}{n+r} \geq \frac{1}{2}.$$

To obtain EAQECCs with good minimum distances, the input linear code using Propositions 5.3 and 5.4 can be chosen from the best-known linear codes in the database of [3]. Moreover, the required number of maximally entangled states $c := n - k - \ell + r$ can be adjusted by the parameter r.

Remark 5.5. *We have the following observations and suggestions for the constructions of EAQECCs in Propositions 5.3 and 5.4.*

1. *By choosing best-known linear codes in [3] satisfy the condition $k \geq \frac{3n+r}{4}$ in* (5.1)*, all the EAQECCs obtained in Propositions 5.3 and 5.4 are good in the sense that they have good rate and positive net rate. Moreover, some of them have good minimum distances.*

2. *Under the assumption $\ell \leq k - \frac{n+r}{2}$, EAQECCs constructed in Propositions 5.3 and 5.4 have good rate*
$$\frac{k-\ell}{n+r} \geq \frac{1}{2}$$
and positive net rate
$$\frac{(k-\ell)-(n-k-\ell+r)}{n+r} = \frac{2k-n-r}{n+r} > 0$$
for all $0 \leq r < 2k-n$. It is easily seen that the condition $\ell \leq k - \frac{n+r}{2}$ is slightly lighter than (5.1) *and it is equivalent to finding classical linear codes with large dimension and small Euclidean/Hermitian hull dimension. Therefore, linear complementary dual codes studied in [8], [9], [10], [11], [23], and [33] would be good candidates in constructions of EAQECCs.*

Example 5.6. Let C be a linear $[6,3,4]_5$ code with generator matrix

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

Then

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

is a parity-check matrix of C. Since

$$GG^T = \begin{bmatrix} 4 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \text{ and } HH^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

we have $\dim(\mathrm{Hull}(C)) = 3 - \mathrm{rank}(GG^T) = 3 - 2 = 1$ by Proposition 2.26.

Choose $\boldsymbol{x}_1 = 240122$ and $\boldsymbol{x}_2 = 320202$. Then $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ are in C such that

$$\boldsymbol{x}_1\boldsymbol{x}_1^T = 4 \neq 0,\ \boldsymbol{x}_2\boldsymbol{x}_2^T = 1 \neq 0 \text{ and } \boldsymbol{x}_1\boldsymbol{x}_2^T = 0.$$

Since $\{a^2 \mid a \in \mathbb{F}_5^*\} = \{1^2, 2^2, 3^2, 4^2\} = \{1, 4\}$, choose $\alpha_1 = 2$ and $\alpha_2 = 1$. Then $\alpha_1, \alpha_2 \in \mathbb{F}_q^*$ and

$$\alpha_1^2 = 4 \neq -4 = -\boldsymbol{x}_1\boldsymbol{x}_1^T \quad \text{and} \quad \alpha_2^2 = 1 \neq -1 = -\boldsymbol{x}_2\boldsymbol{x}_2^T.$$

Let C' be a linear code with parity-check matrix

$$H' = \left[\begin{array}{cc|c} \mathbf{0} & \mathbf{0} & H \\ \hline \alpha_1 & 0 & \boldsymbol{x}_1 \\ 0 & \alpha_2 & \boldsymbol{x}_2 \end{array}\right]$$

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

Then

$$H'(H')^T = \left[\begin{array}{c|cc} HH^T & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \alpha_1^2 + \boldsymbol{x}_1\boldsymbol{x}_1^T & 0 \\ \mathbf{0} & 0 & \alpha_2^2 + \boldsymbol{x}_2\boldsymbol{x}_2^T \end{array}\right]$$

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

It follows that C' is an $[8,3,4]_5$ code with $\dim(\mathrm{Hull}(C')) = 1$. By Proposition 5.3, there exists an $[[8,2,4;4]]_5$ EAQECC.

Using the arguments in the computer algebra system MAGMA [3] shown below and the assumption $\ell \leq k - \frac{n+r}{2}$, EAQECCs can be constructed as in the proof of Propositions 5.3 and examples of EAQECCs are given in Table 5.1.

```
q:= (the cardinality of the finite field);
a:= (the starting point for the length);
b:= (the end point for the length);
for n in [a..b] do
  for r in [1..Floor((n-1)/2)] do
   for k2 in [n-r..n] do
    for k1 in [r..n-r-1] do
     Cperp:=BKLC(GF(q),n,k2);
     C1:=Dual(BKLC(GF(q),n,n-k1));
     l:=Dimension(C1 meet Cperp);
     d:=MinimumDistance(Cperp);
     if l le n/2-r then
      "C1=[",n,k1, MinimumDistance(C1),"]",
      "Cperp=[",n,k2, MinimumDistance(Cperp),"]",
      "Q=[[",n,k2-l, d, k1-l,"]]";
     end if;
    end for;
   end for;
  end for;
end for;
```

5.2 EAQECCs from Linear ℓ-Intersection Pairs of Codes

Linear ℓ-intersection pairs of codes can be used to construct EAQECCs using the following Propositions.

q	C $[n,k,d]_q$	Q $[[n,k,d;c]]_q$
5	$[8,4,4]$	$[[8,4,4;3]]$
5	$[8,5,3]$	$[[8,4,3;2]]$
5	$[8,6,2]$	$[[9,6,3;3]]$
5	$[9,7,2]$	$[[10,7,2;2]]$
5	$[10,7,3]$	$[[12,6,4;4]]$
5	$[10,8,2]$	$[[13,8,3;3]]$
7	$[8,5,4]$	$[[8,4,4;2]]$
7	$[8,6,3]$	$[[9,5,3;2]]$
7	$[9,6,3]$	$[[10,5,3;3]]$
7	$[9,7,2]$	$[[10,7,3;3]]$

q	C $[n,k,d]_q$	Q $[[n,k,d;c]]_q$
7	$[10,7,3]$	$[[10,6,3;2]]$
7	$[10,8,2]$	$[[11,8,3;3]]$
9	$[8,5,4]$	$[[8,5,4;4]]$
9	$[8,6,3]$	$[[9,6,4;3]]$
9	$[9,6,4]$	$[[10,6,4;4]]$
9	$[9,7,3]$	$[[10,6,3;2]]$
9	$[9,5,5]$	$[[10,5,5;5]]$
9	$[10,7,4]$	$[[10,7,4;3]]$
9	$[10,8,3]$	$[[11,8,4;3]]$
9	$[10,6,5]$	$[[10,6,5;4]]$

Table 5.1: EAQECCs constructed using Proposition 5.3.

Proposition 5.7 ([41, Corollary 1]). *Let H_1 and H_2 be parity-check matrices of two linear codes D_1 and D_2 with parameters $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$, respectively. Then an $[[n,k_1+k_2-n+c,\min\{d_1,d_2\};c]]_q$ EAQECC can be obtained where $c=\operatorname{rank}(H_1{H_2}^T)$ is the required number of maximally entangled states.*

Proposition 5.8. *Let $\ell \geq 0$ be an integer and C_1 and C_2 be a linear ℓ-intersection pair of codes with parameters $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$, respectively. Then there exists an $[[n,k_2-\ell,\min\{d_1^{\perp},d_2\};k_1-\ell]]_q$ EAQECC with $d_1^{\perp}=d(C_1^{\perp})$.*

Proof. If $D_1=C_1^{\perp}$ and $D_2=C_2$ in Proposition 5.7, then the result follows from Proposition 5.7 and Theorem 4.5. □

Corollary 5.9. *Let n and r be positive integers such that $r<\frac{n}{2}$. Let k_1 and k_2 be integers such that $r \leq k_1 < n-r \leq k_2 \leq n$. If there exists an $[n,k_2,d]_q$ code, then there exists a positive net rate $[[n,k_2-\ell,d;k_1-\ell]]_q$ EAQECC Q for some*

$0 \leq \ell \leq k_1$. *In addition, if* $\ell \leq \frac{n}{2} - r$, *the rate of EAQECC* Q *is greater than or equal to* $\frac{1}{2}$.

Proof. Assume that there exists an $[n, k_2, d]_q$ code, denoted by C_2. Since $n - k_1 \leq k_2$, there exisits a linear code D with parameters $[n, n - k_1, d_1^{\perp}]_q$ and $d_1^{\perp} \geq d$. Let $C_1 = D^{\perp}$. Then C_1 and C_2 form a linear ℓ-intersection pair of $[n, k_1]_q$ and $[n, k_2, d]_q$ for some $0 \leq \ell \leq k_1$ and $d(C_1^{\perp}) = d_1^{\perp} \geq d$. By Proposition 5.8, there exists an $[[n, k - \ell, \min\{d_1^{\perp}, d\}; k_1 - \ell]]_q = [[n, k - \ell, d; k_1 - \ell]]_q$ EAQECC Q. Consequently, the net rate of Q is

$$\frac{(k_2 - \ell) - (k_1 - \ell)}{n} = \frac{k_2 - k_1}{n} > 0.$$

In addition, assume that $\ell \leq \frac{n}{2} - r$. Then the rate of Q is

$$\frac{k_2 - \ell}{n} \geq \frac{(n - r) - (n/2 - r)}{n} = \frac{1}{2}$$

as desired. $\square$

To obtain an EAQECC with good minimum distances, the input linear code in Corollary 5.9 can be chosen from the best-known linear codes in [21] or in the database of [3]. Moreover, the required number of maximally entangled states $c = k_1 - \ell$ can be adjusted using a weighted permutation matrix as in Lemma 4.11 and Example 4.12.

Using the arguments in MAGMA shown below, it can be easily seen that a large number of linear ℓ-intersection pairs of best-known linear codes constructed as in the proof of Corollary 5.9 satisfy the condition $\ell \leq \frac{n}{2} - r$. Consequently, many EAQECCs obtained in Corollary 5.9 are good in the sense that they have good rate and positive net rate.

```
q:= (the cardinality of the finite field);
a:= (the starting point for the length);
b:= (the end point for the length);
for n in [a..b] do
  for r in [1..Floor((n-1)/2)] do
   for k2 in [n-r..n] do
    for k1 in [r..n-r-1] do
     C2:=BKLC(GF(q),n,k2);
     C1:=Dual(BKLC(GF(q),n,n-k1));
     l:=Dimension(C1 meet C2);
     d:=MinimumDistance(C2);
     if l le n/2-r then
      "[[",n,k2-l, d, k1-l,"]]";
     end if;
    end for;
   end for;
  end for;
end for;
```

By Theorem 4.5, the statement “`l := k1-rank(G1*Transpose(H2));`” can be replaced by “`G1:= GeneratorMatrix(C1); H2:= ParityCheckMatrix(H2); l := k1-rank(G1*Transpose(H2));`”.

Based on the algorithm above, some illustrative examples are shown in Table 5.2.

q	C_1 $[n,k,d]_q$	C_2 $[n,k,d]_q$	Q $[[n,k,d;c]]_q$
3	$[8,3,4]$	$[8,5,3]$	$[[8,5,3;3]]$
3	$[8,4,4]$	$[8,5,3]$	$[[8,4,3;3]]$
4	$[7,3,4]$	$[7,4,3]$	$[[7,4,3;3]]$
4	$[8,3,4]$	$[8,5,3]$	$[[8,5,3;3]]$
5	$[6,2,5]$	$[6,4,3]$	$[[6,4,3;2]]$
5	$[6,3,4]$	$[6,4,3]$	$[[6,3,3;2]]$
5	$[7,3,3]$	$[7,4,3]$	$[[7,4,3;3]]$
5	$[8,3,4]$	$[8,5,3]$	$[[8,4,3;2]]$
5	$[8,4,4]$	$[8,5,3]$	$[[8,4,3;3]]$
7	$[5,2,4]$	$[5,3,3]$	$[[5,3,3;2]]$
7	$[6,3,4]$	$[6,4,3]$	$[[6,4,3;2]]$
7	$[6,3,4]$	$[6,4,3]$	$[[6,3,3;2]]$
7	$[7,2,6]$	$[7,5,3]$	$[[7,5,3;2]]$
7	$[7,3,5]$	$[7,5,3]$	$[[7,4,3;2]]$
7	$[7,5,3]$	$[7,4,4]$	$[[7,4,4;3]]$
7	$[8,2,7]$	$[8,6,3]$	$[[8,5,3;1]]$
7	$[8,3,6]$	$[8,6,3]$	$[[8,5,3;2]]$
7	$[8,4,5]$	$[8,6,3]$	$[[8,4,3;2]]$
7	$[8,3,6]$	$[8,5,4]$	$[[8,4,4;2]]$
7	$[8,4,5]$	$[8,5,4]$	$[[8,4,4;3]]$
7	$[8,3,6]$	$[8,6,3]$	$[[8,5,3;2]]$

q	C_1 $[n,k,d]_q$	C_2 $[n,k,d]_q$	Q $[[n,k,d;c]]_q$
8	$[6,3,4]$	$[6,4,3]$	$[[6,3,3;2]]$
8	$[7,3,5]$	$[7,5,3]$	$[[7,4,3;2]]$
8	$[7,5,3]$	$[7,4,4]$	$[[7,4,4;3]]$
8	$[7,2,6]$	$[7,5,3]$	$[[7,5,3;2]]$
8	$[7,3,5]$	$[7,4,4]$	$[[7,4,4;3]]$
8	$[8,2,7]$	$[8,6,3]$	$[[8,6,3;2]]$
8	$[8,3,6]$	$[8,6,3]$	$[[8,5,3;2]]$
8	$[8,4,5]$	$[8,6,3]$	$[[8,4,3;2]]$
8	$[8,3,6]$	$[8,5,4]$	$[[8,5,4;3]]$
8	$[8,4,5]$	$[8,5,4]$	$[[8,4,4;3]]$
8	$[8,3,6]$	$[8,6,3]$	$[[8,5,3;2]]$
9	$[5,2,4]$	$[5,3,3]$	$[[5,3,3;2]]$
9	$[6,2,5]$	$[6,4,3]$	$[[6,3,3;1]]$
9	$[6,3,4]$	$[6,4,3]$	$[[6,3,3;2]]$
9	$[7,2,6]$	$[7,5,3]$	$[[7,5,3;2]]$
9	$[7,3,5]$	$[7,5,3]$	$[[7,4,3;2]]$
9	$[7,3,5]$	$[7,4,4]$	$[[7,4,4;3]]$
9	$[8,2,7]$	$[8,6,3]$	$[[8,6,3;2]]$
9	$[8,3,6]$	$[8,6,3]$	$[[8,5,3;2]]$
9	$[8,4,5]$	$[8,6,3]$	$[[8,4,3;2]]$
9	$[8,3,6]$	$[8,5,4]$	$[[8,5,4;3]]$

Table 5.2: EAQECCs constructed using Proposition 5.8 for $q \in \{3,4,5,7,8,9\}$, $a = 5$, and $b = 8$.

References

[1] E. F. Assmus and J. D. Key, Affine and projective planes, *Discrete Math.*, vol. 83, pp. 161–187, 1990.

[2] M. Borello, J. D. L. Cruz and W. Willems, A note on linear complementary pairs of group codes, *Discrete Math.*, vol. 343, ID 111905, 2020.

[3] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, vol. 24, pp. 235–265, 1997.

[4] J. Bringer, C. Carlet, H. Chabanne, D. Guilley and H. Maghrebi, Orthogonal direct sum masking: a smartcard friendly computation paradigm in a code, with builtin protection against side-channel and fault attacks, *WISTP*, pp. 40–56, 2014.

[5] T. Brun, I. Devetak and M. H., Catalytic quantum error correction,*IEEE Trans. Inform. Theory*, vol. 60, pp. 3073–3089, 2014.

[6] T. Brun, I. Devetak and H. M. Hsieh, Correcting quantum errors with entanglement, *Science*, vol. 314, pp. 436–439, 2006.

[7] C. Carlet and S. Guilley, Coding Theorem and Applications, *Math. Science.*, vol. 3, pp. 97–105, 2015.

[8] C. Carlet and S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, *Adv. Math. Commun.*, vol. 10, pp. 131–150, 2016.

[9] C. Carlet, S. Mesnager, C. Tang and Y. Qi, Euclidean and Hermitian LCD MDS codes, *Des. Codes Cryptogr.*, vol. 86, pp. 2606–2618, 2018.

[10] C. Carlet, S. Mesnager, C. Tang and Y. Qi, New characterization and parametrization of LCD codes, *IEEE Trans. Inform. Theory*, vol. 65, pp. 39–49, 2019.

[11] C. Carlet, S. Mesnager, C. Tang, Y. Qi and R. Pellikaan, Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$, *IEEE Trans. Inform. Theory*, vol. 64, pp. 3010–3017, 2018.

[12] C. Carlet, C. Güneri, S. Mesnager and F. Özbudak, Construction of some codes suitable for both side channel and fault injection attacks, *Proceedings of International Workshop on the Arithmetic of Finite Fields (WAIFI 2018)*, Bergen, 2018.

[13] C. Carlet, C. Güneri, F. Özbudak, B. Özkaya and P. Solé, On linear complementary pairs of codes, *IEEE Trans. Inform. Theory*, vol. 64, pp. 6583–6589, 2018.

[14] D. Crnkovi, Classes of self-orthogonal or self-dual codes from orbit matrices of Menon designs, *Discrete Math.*, vol. 327, pp. 91–95, 2014.

[15] D. Crnkovi, N. Mostarac and S. Rukavina, Self-dual codes from quotient matrices of symmetric divisible designs with the dual property, *Discrete Math.*, vol. 339, Issue 2, pp. 91–95, 2016.

[16] S. T. Dougherty, J. L. Kim, H. Kulosman and H. Liuc, Self-dual codes over commutative Frobenius rings, *Discrete Math.*, vol. 16, Issue 1, pp. 14–26, 2010.

[17] M. F. Ezerman, S. Jitman, H. M. Kiah and S. Ling, Pure asymmetric quantum MDS codes from CSS construction: A complete characterization, *Int. J. of Quantum Information*, vol.11, ID 350027, 2013.

[18] Y. Fan and L. Zhang, Galois self-dual constacyclic codes, *Des. Codes Cryptogr.*, vol. 84, pp. 473–492, 2017.

[19] L. Galvez, J-L Kim, N. Lee, Y.G. Roe and B-S Won, Some Bounds on Binary LCD Codes, *Des. Codes Cryptogr.*, vol. 10, pp. 719–728, 2018.

[20] J. Gildea, A. Kaya, R. Taylor and B. Yildiz, Constructions for self-dual codes induced from group rings, *Discrete Math.*, vol. 51, pp. 71–92, 2018.

[21] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, Online available at http://www.codetables.de.Accessed on 2020-11-03.

[22] M. Grassl and M. Harada, New self-dual additive -codes constructed from circulant graphs, *Discrete Math.*, vol. 340, pp. 399–403, 2017.

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

[24] T. A. Gulliver, J. L. Kim, Y. Lee and C. Xing, New MDS or near-MDS self-dual codes, *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4354–4360, 2008.

[25] M. Harada and K. Saiti, Remark on subcodes of linear complimentary dual codes, *Information Processing Letters*, vol. 159-160, ID 105963, 2020.

[26] M. H. Hsich, I. Devetak and T. Brun, General entanglement-assisted quantum error-correcting codes, *Phys. Rev. A*, vol. 76, ID 062313, 2007.

[27] L. Jin, Construction of MDS codes with complementary duals, *IEEE Trans. Inf. Theory*, vol. 63, pp. 2843–2847, 2017

[28] L. Jin, S. Ling, J. Luo and C. Xing, Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes, *IEEE Trans. Inform. Theory*, vol.56, pp. 4735–4740, 2010.

[29] L. Jin and C. Xing, Euclidean and Hermitian self-orthogonal algebraic geometry and their application to quantum codes, *IEEE Trans. Inform. Theory*, vol. 58, pp. 5484–5489, 2012.

[30] R. Lidl and H. Niederreiter, Finite fields, *Cambridge University Press*, 1997.

[31] H. Liu and X. Pan, Galois hulls of linear codes over finite fields, *Des. Codes Cryptogr.*, vol. 88, pp. 241–255, 2020.

[32] G. Luo, X. Cao and X. Chen, MDS codes with hulls of arbitrary dimensions and their quantum error correction, *IEEE Trans. Inform. Theory*, vol. 65, pp. 2944–2952, 2019.

[33] J. L. Massey, Linear codes with complementary duals, *Discrete Math.*, vol. 106–107, pp 337–342, 1992.

[34] V. Pless, A classification of self-orthogonal codes over GF(2), *Discrete Math.*, vol. 3, pp. 209–246, 1972.

[35] J. Qian and L. Zhang, On MDS linear complementary dual codes and entanglement-assisted quantum codes, *Des. Codes Cryptogr.*, vol. 86, pp. 1565–1572, 2018.

[36] J. Qian and L. Zhang, Entanglement-assisted quantum codes from arbitrary binary linear codes, *Des. Codes Cryptogr.*, vol. 77, pp. 193–202, 2015.

[37] S. Ling and C. Xing, Coding theory : A first course, *Cambridge University Press*, 2004.

[38] N. Sendrier, Linear codes with complementary duals meet the Gilbert-Varshamov bound, *Discrete Math.*, vol. 285, pp. 345–347, 2004.

[39] N. Sendrier, On the dimension of the hull, *SIAM J. Appl. Math.*, vol. 10, pp. 282–293, 1997.

[40] C. E. Shannon, A mathematical theory of communication, *Bell System Tech. J.*, vol. 27, pp. 379–423, 1948.

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

DISSEMINATIONS

Publications

1. Kenza Guenda, T. Aaron Gulliver, Sompong Jitman, and Satanan Thipworawimon. "Linear ℓ-Intersection Pairs of Codes and Their Applications." *Des. Codes Cryptogr.*, vol. 88, 133–152, 2020.

2. Satanan Thipworawimon and Sompong Jitman. "Hulls of Linear Codes Revisited with Applications." *J. Appl. Math. Comput.*, vol. 62, 325–340, 2020.

VITA

Name	Miss Satanan Thipworawimon
Home Address	44/45 Village No.7 Sangchuto Road, Don-Khamin Sub-district, Tha-Maka District, Kanchanaburi, 71120, Thailand.
Institutions attended	2009 - 2012 Bachelor of Science in Mathematics, (First Class Honors), Silpakorn University 2013 - 2015 Master of Science in Mathematics, Silpakorn University 2016 - 2020 Doctor of Philosophy Program in Mathematics, Silpakorn University
Scholarship	The Development and Promotion of Science and Technology Talented Project (DPST) (Bachelor Degree, Master Degree and Doctoral Degree)
Experiences	2013 - 2018 Teaching Assistant in Calculus course, Silpakorn University -Calculus I,II -Calculus for Engineers I,II -Calculus for Computation Scientists I,II 2019 - 2020 Graduate visiting research student, University of Victoria, Cananda (1 year)