COMPLEMENTARY DUAL SUBFIELD LINEAR CODES OVER FINITE FIELDS

By

Mr. Kriangkrai Boonniyom

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree
Master of Science Program in Mathematics
Department of Mathematics
Graduate School, Silpakorn University
Academic Year 2015

COMPLEMENTARY DUAL SUBFIELD LINEAR CODES
OVER FINITE FIELDS

By

Mr. Kriangkrai Boonniyom

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree
Master of Science Program in Mathematics
Department of Mathematics
Graduate School, Silpakorn University
Academic Year 2015

รหัสเชิงเส้นฟีลด์ย่อยซึ่งมีรหัสคู่กันแบบเติมเต็มบนฟีลด์จำกัด

โดย

นายเกรียงไกร บุญนิยม

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาคณิตศาสตร์

ภาควิชาคณิตศาสตร์

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

ปีการศึกษา 2558

The Graduate School, Silpakorn University has approved and accredited the Thesis title of “Complementary Dual Subfield Linear Codes over Finite Fields” submitted by Mr. Kriangkrai Boonniyom as a partial fulfillment of the requirements for the degree of Master of Science in Mathematics

…..

(Associate Professor Panjai Tantatsanawong, Ph.D.)

Dean of Graduate School

........../..................../..........

The Thesis Advisor

Somphong Jitman, Ph.D.

The Thesis Examination Committee

.... Chairman

(Associate Professor Nawarat Ananchuen, Ph.D.)

............/......................../.............

.... Member

(Professor Patanee Udomkavanich, Ph.D.)

............/......................../.............

.... Member

(Somphong Jitman, Ph.D.)

............/......................../.............

57305207: MAJOR: MATHEMATICS

KEY WORDS: COMPLEMENTARY DUAL CODES / HERMITIAN INNER PRODUCT / TRACE HERMITIAN INNER PRODUCT

KRIANGKRAI BOONNIYOM: COMPLEMENTARY DUAL SUBFIELD LINEAR CODES OVER FINITE FIELDS. THESIS ADVISOR: SOMPHONG JITMAN, Ph.D. 34 pp.

In this thesis, two families of complementary codes over finite fields $\mathbb{F}_q$ are studied, where $q = r^2$ is a prime power: 1) Hermitian complementary dual linear codes, and 2) trace Hermitian complementary dual subfield linear codes. Necessary and sufficient conditions for a linear code (resp., a subfield linear code) to be Hermitian complementary dual (resp., trace Hermitian complementary dual) are determined. Constructions of such codes are given together with their parameters. Some illustrative examples are provided as well.

Department of Mathematics Graduate School, Silpakorn University

Student's signature .... Academic Year 2015

Thesis Advisor's signature..

57305207: สาขาวิชาคณิตศาสตร์
คำสำคัญ: รหัสคู่กันแบบเติมเต็ม, ผลคูณภายในแบบแอร์มีต, ผลคูณภายในแบบเทรซแอร์มีต

เกรียงไกร บุญนิยม: รหัสเชิงเส้นฟีลด์ย่อยซึ่งมีรหัสคู่กันแบบเติมเต็มบนฟีลด์จำกัด. อาจารย์ที่ปรึกษาวิทยานิพนธ์: อ. ดร. สมพงค์ จิตต์มั่น. 34 หน้า.

ในวิทยานิพนธ์นี้ได้ศึกษารหัสคู่กันแบบเติมเต็มสองรูปแบบบนฟีลด์จำกัด $\mathbb{F}_q$ โดยที่ $q = r^2$ เป็นจำนวนเฉพาะยกกำลัง กล่าวคือ 1) รหัสเชิงเส้นคู่กันแบบเติมเต็มภายใต้ผลคูณภายในแบบแอร์มีตและ 2) รหัสเชิงเส้นฟีลด์ย่อยคู่กันแบบเติมเต็มภายใต้ผลคูณภายในแบบเทรซแอร์มีต ทั้งนี้ได้ให้เงื่อนไขที่จำเป็นและเพียงพอสำหรับการเป็นรหัสคู่กันแบบเติมเต็มภายใต้ผลคูณภายในแบบแอร์มีตของรหัสเชิงเส้น และเงื่อนไขที่จำเป็นและเพียงพอสำหรับการเป็นรหัสคู่กันแบบเติมเต็มภายใต้ผลคูณภายในแบบเทรซแอร์มีตของรหัสเชิงเส้นฟีลด์ย่อย พร้อมทั้งสร้างรหัสคู่กันแบบเติมเต็มทั้งสองรูปแบบและแสดงค่าพารามิเตอร์ของรหัสดังกล่าว ในส่วนสุดท้ายได้แสดงตัวอย่างการสร้างรหัสดังกล่าวอีกด้วย

ภาควิชาคณิตศาสตร์	บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ลายมือชื่อนักศึกษา..	ปีการศึกษา 2558
ลายมือชื่ออาจารย์ที่ปรึกษาวิทยานิพนธ์	

Acknowledgements

Firstly, I would like to thank Dr. Somphong Jitman, my advisor, for his helpful suggestion, valuable comments throughout the thesis, and immense depth of knowledge.

Besides my advisor, I would like to thank the rest of my thesis committee: Associate Professor Dr. Nawarat Ananchuen and Professor Dr. Patanee Udomkavanich, for their insightful comments and suggestions.

Finally, I would express my very profound gratitude to my beloved family and to my friends for their understanding, encouragement and moral support through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Table of Contents

Chapter 1

Introduction

Information media, such as communication systems and storage devices of data, are not 100 percent reliable in practice because of noise or other forms of introduced interference. The art of error correcting codes is a branch of Mathematics that has been introduced to deal with this problem since 1960s.

Linear codes with Euclidean complementary dual have been studied in [7]. The characterization and properties of such codes were given. These codes are interesting since they reach the maximum decoding capability of adder channel [7]. Moreover, in some cases, such codes can be decoded faster than other linear codes using nearest neighbor decoding. In [11], necessary and sufficient conditions for cyclic codes to be Euclidean complementary dual have been determined. Hermitian complementary dual cyclic codes over finite fields have been characterized in [9]. Subfield linear codes and their duals under the trace Hermitian inner product have been studied in [1] and [8]. Such codes have an application in constructing quantum codes in [1] and references therein.

To the best of our knowledge, Hermitian complementary dual linear codes and trace Hermitian complementary dual subfield linear codes have not been well studied. Therefore, it is of natural interest to studied complementary dual codes with respect to the Hermitian and trace Hermitian inner products.

In this thesis, we focus on Hermitian complementary dual linear codes and trace Hermitian complementary dual subfield linear codes. Characterizations, properties, and constructions of such codes are studied.

The thesis is organized as follows: Some basic concepts and preliminary results on complementary dual codes are recalled in Chapter 2. In Chapter 3, characterization of complementary dual codes with respect to the two inner products are given. Some constructions and illustrative examples of such complementary dual codes are established in Chapter 4.

Chapter 2

Preliminaries

In this chapter, we recall some basic properties of codes over finite fields and introduce the dual of a code with respect to the inner product.

2.1 Codes and Duals

Let r and $q = r^2$ be prime power integers and let $\mathbb{F}_r \subsetneq \mathbb{F}_q$ be finite fields. Let $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_r$ denote the *trace map* given by $\mathrm{Tr}(\beta) = \beta + \beta^r$. Some properties of the trace map can be found in [4, Theorem 2.23]. For $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n$, let $\overline{\boldsymbol{u}} = (\overline{u_1}, \overline{u_2}, \ldots, \overline{u_n})$, where $\overline{a} = a^r$ for all $a \in \mathbb{F}_q$. For each matrix A=$[a_{ij}] \in M_{m,n}(\mathbb{F}_q)$, let $\overline{A} = [\overline{a}_{ij}]$ and $\mathrm{Tr}(A) = [\mathrm{Tr}(\mathrm{a_{ij}})]$.

Given $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_q^n$, let $\mathrm{wt}(\boldsymbol{v})$ denote the *Hamming weight* of $\boldsymbol{v}$ and $d(\boldsymbol{u}, \boldsymbol{v})$ denote the *Hamming distance* between $\boldsymbol{u}$ and $\boldsymbol{v}$. A *code* of length n over $\mathbb{F}_q$ is defined to be a nonempty subset C of $\mathbb{F}_q^n$. The *minimum distance* $d(C)$ is given by

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

An $[n, k]_q$ *linear code* C is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$ and an $[n, k]_q$ code is called an $[n, k, d]_q$ linear code if its minimum distance is d. A $k \times n$ matrix G over $\mathbb{F}_q$ is called a *generator matrix* for an $[n, k, d]_q$ linear code C if the rows of G form a basis of C.

For a general, not necessarily linear, code $C \subseteq \mathbb{F}_q^n$, the notation $(n, M = |C|, d)_q$ is commonly used. A code C is said to be an $\mathbb{F}_r$-*linear code* over $\mathbb{F}_q$ if C is a subspace of the $\mathbb{F}_r$-vector space $\mathbb{F}_q^n$. When r is clear from the context, C is called a *subfield linear code* over $\mathbb{F}_q$. It is not difficult to see that if C is an $\mathbb{F}_r$-linear code of length n over $\mathbb{F}_q$, then $|C| = r^\ell$ for some $0 \le \ell \le 2n$ and $\dim_{\mathbb{F}_r}(C) = \ell$. An $\ell \times n$ matrix G over $\mathbb{F}_q$ is called a *generator matrix* for an $(n, r^\ell, d)_q$ $\mathbb{F}_r$-linear code C if the rows of G form a basis of C as an $\mathbb{F}_r$-vector space.

Lemma 2.1.1. *If $q = r^2$ is an odd prime power, then there exists $\alpha \in \mathbb{F}_q$ such that $\overline{\alpha} = -\alpha$.*

Proof. Assume that $q = r^2$ is an odd prime power. Since the trace function $\varphi : \mathbb{F}_q \to \mathbb{F}_r$ defined by $a \mapsto a + a^r$ is a surjective $\mathbb{F}_r$-linear map, there exists $\alpha \in \ker(\varphi) \backslash \{0\}$ such that $\varphi(\alpha) = 0$. Hence, $\overline{\alpha} = \alpha^r = -\alpha$ as desired. $\square$

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 inner products between $\boldsymbol{u}$ and $\boldsymbol{v}$ are defined as follows:

1. $\langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{E}} := \sum_{i=1}^n u_i v_i$ is the *Euclidean inner product* of $\boldsymbol{u}$ and $\boldsymbol{v}$.
2. $\langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{H}} := \sum_{i=1}^n u_i \overline{v_i} = \langle \boldsymbol{u}, \overline{\boldsymbol{v}} \rangle_{\mathrm{E}}$ is the *Hermitian inner product* of $\boldsymbol{u}$ and $\boldsymbol{v}$.
3. The *trace Hermitian inner product* are defined into two cases depending on the field characteristic:
   (a) For even q, $\langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{TrH}} := \mathrm{Tr}(\langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{H}})$.
   (b) For odd q, $\langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{TrH}} := \mathrm{Tr}(\alpha \langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{H}})$, where $\alpha \in \mathbb{F}_q \setminus \{0\}$ is such that $\overline{\alpha} = -\alpha$.

The *Euclidean dual* (resp., *Hermitian dual* and *trace Hermitian dual*) of a code C is defined to be the set

$$C^{\perp_{\mathrm{E}}} := \{\boldsymbol{u} \in \mathbb{F}_q^n \mid \langle \boldsymbol{u}, \boldsymbol{c} \rangle_{\mathrm{E}} = 0 \text{ for all } \boldsymbol{c} \in C\}$$

$$(\text{resp., } C^{\perp_{\mathrm{H}}} := \{\boldsymbol{u} \in \mathbb{F}_q^n \mid \langle \boldsymbol{u}, \boldsymbol{c} \rangle_{\mathrm{H}} = 0 \text{ for all } \boldsymbol{c} \in C\}$$

$$C^{\perp_{\mathrm{TrH}}} := \{\boldsymbol{u} \in \mathbb{F}_q^n \mid \langle \boldsymbol{u}, \boldsymbol{c} \rangle_{\mathrm{TrH}} = 0 \text{ for all } \boldsymbol{c} \in C\}).$$

A code C of length n over $\mathbb{F}_q$ is said to be *Euclidean* (resp., *Hermitian* and *trace Hermitian*) *complementary dual* if $C \cap C^{\perp_{\mathrm{E}}} = \{\boldsymbol{0}\}$ (resp., $C \cap C^{\perp_{\mathrm{H}}} = \{\boldsymbol{0}\}$ and $C \cap C^{\perp_{\mathrm{TrH}}} = \{\boldsymbol{0}\}$).

Next proposition is straight forward from the definitions.

Proposition 2.1.2. *Let C be a code of length n over $\mathbb{F}_q = \mathbb{F}_{r^2}$. Then the following statements hold.*

i) If C is a linear code, then C is Euclidean complementary dual if and only if

$$\mathbb{F}_q^n = C \oplus C^{\perp_{\mathrm{E}}}.$$

ii) If C is a linear code, then C is Hermitian complementary dual if and only if

$$\mathbb{F}_q^n = C \oplus C^{\perp_{\mathrm{H}}}.$$

iii) If C is an $\mathbb{F}_r$-linear code, then C is trace Hermitian complementary dual if and only if

$$\mathbb{F}_q^n = C \oplus C^{\perp_{\mathrm{TrH}}}.$$

The following properties of codes and their duals are discussed in [8, Chapter 3].

Proposition 2.1.3. *Let C be a code of length n over $\mathbb{F}_q = \mathbb{F}_{r^2}$. Then the following statements hold.*

i) If C is a linear code, then $\left(C^{\perp_{\mathrm{E}}}\right)^{\perp_{\mathrm{E}}} = C$ and $\left(C^{\perp_{\mathrm{H}}}\right)^{\perp_{\mathrm{H}}} = C$.

ii) If C is an $\mathbb{F}_r$-linear code, then $\left(C^{\perp_{\mathrm{TrH}}}\right)^{\perp_{\mathrm{TrH}}} = C$.

Note that the properties $\left(C^{\perp_{\mathrm{H}}}\right)^{\perp_{\mathrm{H}}} = C$ and $(C^{\perp_{\mathrm{E}}})^{\perp_{\mathrm{E}}} = C$ do not need to be true if C is not a linear code.

The following properties are a direct consequence of Proposition 2.1.3.

Corollary 2.1.4. *Let C be a code of length n over $\mathbb{F}_q = \mathbb{F}_{r^2}$. Then the following statements hold.*

i) *If C is a linear code, then $n = \dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(C^{\perp_{\mathrm{E}}})$ and $n = \dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(C^{\perp_{\mathrm{H}}})$.*

ii) *If C is an $\mathbb{F}_r$-linear code, then $2n = \dim_{\mathbb{F}_r}(C) + \dim_{\mathbb{F}_r}(C^{\perp_{\mathrm{TrH}}})$.*

From Corollary 2.1.4, to study complementary duality of codes, we focus on the Euclidean and Hermitian inner product if codes are linear, and the trace Hermitian inner product if codes are $\mathbb{F}_r$-linear over $\mathbb{F}_q$.

For an $[n,k]_q$ code C, a parity check matrix for C is defined to be an $(n-k)\times n$ matrix where rows form a basis of $C^{\perp}$. The following results are well known [5].

Theorem 2.1.5. *If $G = [I_k|A]$ is a generator matrix for an $[n,k]_q$ code C in standard form, then $H = [-A^T|I_{(n-k)}]$ is a parity check matrix for C.*

Remark 2.1.6. *If H is a parity check matrix for an $[n,k]_q$ linear code C , then $\overline{H}$ is a generator matrix for $C^{\perp_{\mathrm{H}}}$.*

Chapter 3

Characterization of Complementary Dual Subfield Linear Codes

The characterization and properties of Linear codes with Euclidean complementary dual have been established in [7]. In this chapter, characterizations of Hermitian complementary dual linear codes and trace Hermitian complementary dual subfield linear codes are given in terms of orthogonal projections.

Definition 3.0.7. *Let V be an inner product space over a field $\mathbb{F}$. An $\mathbb{F}$-linear map $T : V \to V$ is called an* $\mathbb{F}$-orthogonal projection *with respect to the prescribed inner product $\langle \cdot, \cdot \rangle$ if*

i) $T^2 = T$, *and*

ii) $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 0$ *for all* $\boldsymbol{u} \in \mathrm{Im}(T)$ *and* $\boldsymbol{v} \in \ker(T)$.

3.1 Characterization of Hermitian Complementary Dual Linear Codes

The following property of $\mathbb{F}_q$-orthogonal projection plays vital role in characterizing Hermitian complementary dual linear codes over $\mathbb{F}_q$

Lemma 3.1.1. *Let C be a linear code of length n over $\mathbb{F}_q = \mathbb{F}_{r^2}$ and let $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear map. Then T is an $\mathbb{F}_q$-orthogonal projection with respect to the Hermitian inner product onto C if and only if*

$$T(\boldsymbol{v}) = \begin{cases} \boldsymbol{v} & \textit{if } \boldsymbol{v} \in C, \\ \mathbf{0} & \textit{if } \boldsymbol{v} \in C^{\perp_{\mathrm{H}}}. \end{cases}$$

Proof. Suppose that $T : \mathbb{F}_q^n \to C$ is an $\mathbb{F}_q$-orthogonal projection with respect to the Hermitian inner product onto C. Let $\boldsymbol{v} \in C$ and $\boldsymbol{u} \in C^{\perp_H}$. Since T is onto C, $C = \mathrm{Im(T)}$. Then there exists $\boldsymbol{x} \in \mathbb{F}_q^n$ such that $T(\boldsymbol{x}) = \boldsymbol{v}$. and $\boldsymbol{v} = T(\boldsymbol{x}) = T^2(\boldsymbol{x}) = T(T(\boldsymbol{x})) = T(\boldsymbol{v})$. Since $\langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{H}} = 0$ for all $\boldsymbol{v} \in C = \mathrm{Im(T)}$, $\boldsymbol{u} \in \ker(\mathrm{T})$. So $T(\boldsymbol{u}) = \mathbf{0}$.

Conversely, assume that

$$T(\boldsymbol{v}) = \begin{cases} \boldsymbol{v} & \text{if } \boldsymbol{v} \in C, \\ \mathbf{0} & \text{if } \boldsymbol{v} \in C^{\perp_{\mathrm{H}}}. \end{cases}$$

Sicne T is a function, $C \cap C^{\perp_{\mathrm{H}}} = \{\mathbf{0}\}$. For each $\boldsymbol{v} \in \mathbb{F}_q^n$, it can be written uniquely as $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w}$, where $\boldsymbol{u} \in C$ and $\boldsymbol{w} \in C^{\perp_{\mathrm{H}}}$. Then $T(\boldsymbol{u}) = \boldsymbol{u}$ and $T(\boldsymbol{w}) = \mathbf{0}$. Hence, $T^2(\boldsymbol{u}) = T(T(\boldsymbol{u})) = T(\boldsymbol{u})$ and $T^2(\boldsymbol{w}) = T(T(\boldsymbol{w})) = T(\mathbf{0}) = \mathbf{0} = T(\boldsymbol{w})$. It follows that $T^2(\boldsymbol{v}) = T(\boldsymbol{v})$ for all $\boldsymbol{v} \in \mathbb{F}_q^n$. Let $\boldsymbol{u} \in \mathrm{Im}(T)$ and $\boldsymbol{v} \in \ker(T)$. Then $\boldsymbol{u} \in C$ and $T(\boldsymbol{v}) = \mathbf{0}$. It follows that $\boldsymbol{v} \in C^{\perp_{\mathrm{H}}}$ and $\langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{H}} = 0$. Hence, $\mathrm{Im(T)}$ and $\ker(\mathrm{T})$ are orthogonal with respect to the Hermitian inner product. □

Corollary 3.1.2. *Let C be a linear code of length n over $\mathbb{F}_q = \mathbb{F}_{r^2}$ and let $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear map. Then T is an $\mathbb{F}_q$-orthogonal projection with* *respect to the Hermitian inner product onto* $C^{\perp_{\mathrm{H}}}$ *if and only if*

$$T(\boldsymbol{v}) = \begin{cases} \boldsymbol{v} & \text{if } \boldsymbol{v} \in C^{\perp_{\mathrm{H}}}, \\ \boldsymbol{0} & \text{if } \boldsymbol{v} \in C. \end{cases}$$

Proof. Using arguments similar to those in Lemma 3.1.1. □

The characterization of Hermitian complementary dual linear codes is given as follows.

Lemma 3.1.3. *Let* C *be a linear code of length* n *over* $\mathbb{F}_q = \mathbb{F}_{r^2}$. *Then* C *is Hermitian complementary dual if and only if there exists an* $\mathbb{F}_q$*-orthogonal projection with respect to the Hermitian inner product from* $\mathbb{F}_q^n$ *onto* C.

Proof. Assume that Π_C is an $\mathbb{F}_q$-orthogonal projection with respect to the Hermitian inner product from $\mathbb{F}_q^n$ onto C. By Lemma 3.1.1, we have

$$\Pi_C(\boldsymbol{v}) = \begin{cases} \boldsymbol{v} & \text{if } \boldsymbol{v} \in C, \\ \boldsymbol{0} & \text{if } \boldsymbol{v} \in C^{\perp_{\mathrm{H}}}. \end{cases}$$

Suppose that C is not Hermitian complementary dual. Then the exists $\boldsymbol{u} \neq \boldsymbol{0}$ such that $\boldsymbol{u} \in C \cap C^{\perp_H}$, i.e., $\boldsymbol{u} \in C$ and $\boldsymbol{u} \in C^{\perp_{\mathrm{H}}}$. It follows that $\boldsymbol{0} \neq \boldsymbol{u} = \Pi_C(\boldsymbol{u}) = \boldsymbol{0}$, a contradiction. Therefore, C is Hermitian complementary dual.

Conversely, suppose C is Hermitian complementary dual. Let $\boldsymbol{v} \in \mathbb{F}_q^n$. Then there exists a unique pair $\boldsymbol{u} \in C$ and $\boldsymbol{w} \in C^{\perp_{\mathrm{H}}}$ such that $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w}$. Defined a map $\Pi_C : \mathbb{F}_q^n \to \mathbb{F}_q^n$ by

$$\Pi_C(\boldsymbol{v}) = \boldsymbol{u}.$$

It is not difficult to verify that Π_C is a linear map such that

$$\Pi_C(\boldsymbol{z}) = \begin{cases} \boldsymbol{z} & \text{if } \boldsymbol{z} \in C, \\ \boldsymbol{0} & \text{if } \boldsymbol{z} \in C^{\perp_{\mathrm{H}}}. \end{cases}$$

Hence, by Lemma 3.1.1, Π_C an $\mathbb{F}_q$-orthogonal projection with respect to the Hermitian inner product from $\mathbb{F}_q^n$ onto C. □

Corollary 3.1.4. *Let C be a linear code of length n over $\mathbb{F}_q = \mathbb{F}_{r^2}$. Then C is Hermitian complementary dual if and only if there exists an $\mathbb{F}_q$-orthogonal projection with respect to the Hermitian inner product from $\mathbb{F}_q^n$ onto $C^{\perp_{\mathrm{H}}}$.*

Proof. Using arguments similar to those in Lemma 3.1.3. □

Theorem 3.1.5. *Let C be a linear code of length n over $\mathbb{F}_q = \mathbb{F}_{r^2}$ with generator matrix G. Then C is Hermitian complementary dual if and only if $G\overline{G}^T$ is invertible.*

In this case, $\prod_C := \overline{G}^T(G\overline{G}^T)^{-1}G$ is an $\mathbb{F}_q$-orthogonal projection with respect to the Hermitian inner product from $\mathbb{F}_q^n$ onto C.

Proof. Suppose that $G\overline{G}^T$ is a non-invertible matrix. Since $G\overline{G}^T$ is a $k \times k$ matrix, we have $\mathrm{rank}(G\overline{G}^T) < k$. It follows that

$$k = \mathrm{null}(G\overline{G}^T) + \mathrm{rank}(G\overline{G}^T) < \mathrm{null}(G\overline{G}^T) + k.$$

Then $\mathrm{null}(G\overline{G}^T) > k - k = 0$, i.e., $\{\mathbf{0}\} \subsetneq \ker(G\overline{G}^T)$. Then there exists $\boldsymbol{u} \in \ker(G\overline{G}^T) \setminus \{\mathbf{0}\} \subseteq \mathbb{F}_q^k$. Hence, $\boldsymbol{u}G\overline{G}^T = \mathbf{0}$ and $\boldsymbol{u}G \in C \setminus \{\mathbf{0}\}$.

Each $\boldsymbol{v} \in C$ can be written as $\boldsymbol{v} = \boldsymbol{u'}G$ for some $\boldsymbol{u'} \in \mathbb{F}_q^k$. Hence,

$$\langle \boldsymbol{u}G, \boldsymbol{v}\rangle_{\mathrm{H}} = (\boldsymbol{u}G)\overline{\boldsymbol{v}}^T = (\boldsymbol{u}G)(\overline{\boldsymbol{u'}G})^T = \boldsymbol{u}G\overline{G}^T(\overline{\boldsymbol{u'}})^T = 0(\overline{\boldsymbol{u'}})^T = 0.$$

Therefore, $\boldsymbol{u}G \neq \mathbf{0}$ is also a vector in $C^{\perp_{\mathrm{H}}}$. It follows that $C \cap C^{\perp_{\mathrm{H}}} \neq \{\mathbf{0}\}$, i.e., C is not Hermitian complementary dual.

Conversely, assume that $G\overline{G}^T$ is invertible. Let $\boldsymbol{v} \in \mathbb{F}_q^n$. If $\boldsymbol{v} \in C$, then there exists $\boldsymbol{u} \in \mathbb{F}_q^k$ such that $\boldsymbol{v} = \boldsymbol{u}G$, and hence,

$$\begin{aligned}\boldsymbol{v}\overline{G}^T(G\overline{G}^T)^{-1}G &= \boldsymbol{u}G\overline{G}^T(G\overline{G}^T)^{-1}G\\ &= \boldsymbol{u}I_kG\\ &= \boldsymbol{u}G = \boldsymbol{v}.\end{aligned}$$

If $\boldsymbol{v} \in C^{\perp_{\mathrm{H}}}$, then $\boldsymbol{v}\overline{G}^T = \mathbf{0}$, and hence,

$$\boldsymbol{v}\overline{G}^T(G\overline{G}^T)^{-1}G = \mathbf{0}(G\overline{G}^T)^{-1}G = \mathbf{0}.$$

Therefore, $\overline{G}^T(G\overline{G}^T)^{-1}G$ is an $\mathbb{F}_q$-orthogonal projection with respect to the Hermitian inner product from $\mathbb{F}_q^n$ onto C. Therefore, C is Hermitian complementary dual. $\square$

Example 3.1.6. *Let C be a linear code of length 4 over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$ with generator matrix $G = \begin{bmatrix} 1 & 0 & \alpha & 0 \\ 0 & 1 & 1 & \alpha \end{bmatrix}$. Since*

$$G\overline{G}^T = \begin{bmatrix} 1 & 0 & \alpha & 0 \\ 0 & 1 & 1 & \alpha \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ \alpha^2 & 1 \\ 0 & \alpha^2 \end{bmatrix} = \begin{bmatrix} 1+\alpha^3 & \alpha \\ \alpha^2 & 2+\alpha^3 \end{bmatrix} = \begin{bmatrix} 0 & \alpha \\ \alpha^2 & 1 \end{bmatrix},$$

we have $\det(G\overline{G}^T) = 1$*. Then $G\overline{G}^T$ is invertible, and hence, C is Hermitian complementary dual by Theorem* 3.1.5*.*

The characterization of Hermitian complementary dual linear codes can be given in terms of the parity check matrix of the codes as well.

Corollary 3.1.7. *Let C be a linear code of length n over $\mathbb{F}_q = \mathbb{F}_{r^2}$ and let H be a parity check matrix for C. Then C is Hermitian complementary dual if and only if $\overline{H}H^T$ is invertible.*

In this case, $\prod_{C^{\perp_{\mathrm{H}}}} := H^T(\overline{H}H^T)^{-1}\overline{H}$ is an $\mathbb{F}_q$-orthogonal projection with respect to the Hermitian inner product from $\mathbb{F}_q^n$ onto $C^{\perp_{\mathrm{H}}}$.

Proof. First, we note that $\overline{H}$ is a generator matrix for $C^{\perp_{\mathrm{H}}}$. Then the first statement follows from Theorem 3.1.5 since C is Hermitian complementary dual if and only if $C^{\perp_{\mathrm{H}}}$ is Hermitian complementary dual. Consequently, $H^T(\overline{H}H^T)^{-1}\overline{H}$ is an $\mathbb{F}_q$-orthogonal projection with respect to the Hermitian inner product from $\mathbb{F}_q^n$ onto $C^{\perp_{\mathrm{H}}}$. $\square$

Example 3.1.8. *Let C be a linear code of length 4 over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 =$*

$\alpha+1\}$ *with parity-check matrix* $H = \begin{bmatrix} \alpha^2 & 1 & 1 & 0 \\ 0 & \alpha^2 & 0 & 1 \end{bmatrix}$. *Since*

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

we have $\det(\overline{H}H^T) = 1$. *Then* $\overline{H}H^T$ *is invertible, and hence,* C *is Hermitian complementary dual by Corollary* 3.1.7.

3.2 Characterization of Complementary Dual Subfield Linear Codes

Now, we focus on the characterization of trace Hermitian complementary dual subfield linear codes.

Lemma 3.2.1. *Let* C *be an* $\mathbb{F}_r$*-linear code of length* n *over* $\mathbb{F}_q = \mathbb{F}_{r^2}$ *and let* $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ *be an* $\mathbb{F}_r$*-linear map. Then* T *is an* $\mathbb{F}_r$*-orthogonal projection with respect to the trace Hermitian inner product onto* C *if and only if*

$$T(\boldsymbol{v}) = \begin{cases} \boldsymbol{v} & \textit{if } \boldsymbol{v} \in C, \\ \boldsymbol{0} & \textit{if } \boldsymbol{v} \in C^{\perp_{\mathrm{TrH}}}. \end{cases}$$

Proof. Using arguments similar to those in Lemma 3.1.1 and applying the trace Hermitian inner product instead of the Hermitian inner product, the statement is proved. □

Corollary 3.2.2. *Let* C *be an* $\mathbb{F}_r$*-linear code of length* n *over* $\mathbb{F}_q = \mathbb{F}_{r^2}$ *and let* $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ *be an* $\mathbb{F}_r$*-linear map. Then* T *is an* $\mathbb{F}_r$*-orthogonal projection with respect to the trace Hermitian inner product onto* $C^{\perp_{\mathrm{TrH}}}$ *if and only if*

$$T(\boldsymbol{v}) = \begin{cases} \boldsymbol{v} & \textit{if } \boldsymbol{v} \in C^{\perp_{\mathrm{TrH}}}, \\ \boldsymbol{0} & \textit{if } \boldsymbol{v} \in C. \end{cases}$$

Proof. Using arguments similar to those in Corollary 3.1.2 and applying the trace Hermitian inner product instead of the Hermitian inner product, the statement is proved. □

Lemma 3.2.3. *Let C be an $\mathbb{F}_r$-linear code of length n over $\mathbb{F}_q = \mathbb{F}_{r^2}$. Then C is trace Hermitian complementary dual if and only if there exists an $\mathbb{F}_r$-orthogonal projection with respect to the trace Hermitian inner product from $\mathbb{F}_q^n$ onto C.*

Proof. Assume that Λ_C is an $\mathbb{F}_r$-orthogonal projection with respect to the trace Hermitian inner product from $\mathbb{F}_q^n$ onto C. By Lemma 3.2.1, it follows that

$$\Lambda_C(\boldsymbol{v}) = \begin{cases} \boldsymbol{v} & \text{if } \boldsymbol{v} \in C, \\ \boldsymbol{0} & \text{if } \boldsymbol{v} \in C^{\perp_{\mathrm{TrH}}}. \end{cases}$$

Suppose that C is not trace Hermitian complementary dual. Then there exists $\boldsymbol{u} \neq \boldsymbol{0}$ such that $\boldsymbol{u} \in C \cap C^{\perp_{\mathrm{TrH}}}$. It follows that $\boldsymbol{0} \neq \boldsymbol{u} = \Pi_C(\boldsymbol{u}) = \boldsymbol{0}$, a contradiction. Hence, C is trace Hermitian complementary dual.

Conversely, suppose C is trace Hermitian complementary dual. Let $\boldsymbol{v} \in \mathbb{F}_q^n$. Then there exists a unique pair $\boldsymbol{u} \in C$ and $\boldsymbol{w} \in C^{\perp_{\mathrm{TrH}}}$ such that $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w}$. Defined a map $\Lambda_C : \mathbb{F}_q^n \to \mathbb{F}_q^n$ by

$$\Lambda_C(\boldsymbol{v}) = \boldsymbol{u}.$$

It is not difficult to see that Λ_C is an $\mathbb{F}_r$-linear map such that

$$\Lambda_C(\boldsymbol{z}) = \begin{cases} \boldsymbol{z} & \text{if } \boldsymbol{z} \in C, \\ \boldsymbol{0} & \text{if } \boldsymbol{z} \in C^{\perp_{\mathrm{TrH}}}. \end{cases}$$

Hence, by Lemma 3.1.1, Λ_C an $\mathbb{F}_r$-orthogonal projection with respect to the trace Hermitian inner product from $\mathbb{F}_q^n$ onto C. □

Corollary 3.2.4. *Let C be an $\mathbb{F}_r$-linear code of length n over $\mathbb{F}_q = \mathbb{F}_{r^2}$. Then C is trace Hermitian complementary dual if and only if there exists an $\mathbb{F}_r$-orthogonal projection with respect to the trace Hermitian inner product from $\mathbb{F}_q^n$ onto $C^{\perp_{\mathrm{TrH}}}$.*

Proof. Using arguments similar to those in Lemma 3.2.3. □

Theorem 3.2.5. *Let C be an $\mathbb{F}_r$-linear code of length n over $\mathbb{F}_q = \mathbb{F}_{r^2}$ with generator matrix G. Then C is trace Hermitian complementary dual if and only if $G\overline{G}^T - \overline{G}G^T$ is invertible.*

In this case, $\Lambda_C : \mathbb{F}_q^n \to C$ defined by

$$\Lambda_C(\boldsymbol{v}) = \begin{cases} \mathrm{Tr}(\boldsymbol{v}\overline{G}^T)(G\overline{G}^T - \overline{G}G^T)^{-1}G & \text{if } q \text{ is even,} \\ \alpha^{-1}\mathrm{Tr}(\alpha\boldsymbol{v}\overline{G}^T)(G\overline{G}^T - \overline{G}G^T)^{-1}G & \text{if } q \text{ is odd} \end{cases}$$

is an $\mathbb{F}_r$-orthogonal projection with respect to the trace Hermitian inner product from $\mathbb{F}_q^n$ onto C, where $\alpha \in \mathbb{F}_q \setminus \{0\}$ is such that $\overline{\alpha} = -\alpha$.

Proof. Assume that $G\overline{G}^T - \overline{G}G^T$ is not invertible. We separate the proof into two cases.

Case 1 q is even. Then $\mathrm{Tr}(G\overline{G}^T) = G\overline{G}^T - \overline{G}G^T$ is invertible. Since $\mathrm{Tr}(G\overline{G}^T)$ is a $k \times k$ matrix, we have $\mathrm{rank}(\mathrm{Tr}(G\overline{G}^T)) < k$. It follows that

$$k = \mathrm{null}(\mathrm{Tr}(G\overline{G}^T)) + \mathrm{rank}(\mathrm{Tr}(G\overline{G}^T)) < \mathrm{null}(\mathrm{Tr}(G\overline{G}^T)) + k.$$

Hence, $\mathrm{null}(\mathrm{Tr}(G\overline{G}^T)) > k - k = 0$, i.e., $\{\mathbf{0}\} \subsetneq \ker(\mathrm{Tr}(G\overline{G}^T))$. Then there exists $\boldsymbol{u} \in \ker(\mathrm{Tr}(G\overline{G}^T)) \setminus \{\mathbf{0}\} \subseteq \mathbb{F}_r^k$ such that $\boldsymbol{u}(\mathrm{Tr}(G\overline{G}^T)) = \mathbf{0}$ and $\boldsymbol{u}G \in C \setminus \{\mathbf{0}\}$. Hence,

$$\mathrm{Tr}(\boldsymbol{u}G\overline{G}^T) = (\boldsymbol{u}G)\overline{G}^T - \overline{\boldsymbol{u}G}G^T = \boldsymbol{u}(\mathrm{Tr}(G\overline{G}^T)) = 0.$$

Case 2 q is odd. Then $\mathrm{Tr}(\alpha G\overline{G}^T) = \alpha(G\overline{G}^T - \overline{G}G^T)$ is not invertible for all $\alpha \in \mathbb{F}_q \setminus \{\mathbf{0}\}$ such that $\overline{\alpha} = -\alpha$. Since $\mathrm{Tr}(\alpha G\overline{G}^T)$ is a $k \times k$ matrix, we have $\mathrm{rank}(\mathrm{Tr}(\alpha G\overline{G}^T)) < k$ and

$$\begin{aligned} k &= \mathrm{null}(\mathrm{Tr}(\alpha G\overline{G}^T)) + \mathrm{rank}(\mathrm{Tr}(\alpha G\overline{G}^T)) \\ &< \mathrm{null}(\mathrm{Tr}(\alpha G\overline{G}^T)) + k. \end{aligned}$$

It follows that $\mathrm{null}(\mathrm{Tr}(\alpha G\overline{G}^T)) > k-k = 0$, and hence, $\{\mathbf{0}\} \subsetneq \ker(\mathrm{Tr}(\alpha G\overline{G}^T))$. Then there exists $\boldsymbol{u} \in \ker(\mathrm{Tr}(\alpha G\overline{G}^T))\setminus\{\mathbf{0}\} \subseteq \mathbb{F}_r^k$ such that $\boldsymbol{u}(\mathrm{Tr}(\alpha G\overline{G}^T)) = \mathbf{0}$

and $\boldsymbol{u}G \in C \setminus \{\mathbf{0}\}$. We have

$$\mathrm{Tr}(\alpha\boldsymbol{u}G\overline{G}^T) = \alpha((\boldsymbol{u}G)\overline{G}^T - \overline{\boldsymbol{u}G}G^T) = \boldsymbol{u}(\mathrm{Tr}(\alpha G\overline{G}^T)) = 0.$$

From both cases, $\boldsymbol{u}G$ is also a vector in $C^{\perp_{\mathrm{TrH}}}$. It follows that $C \cap C^{\perp_{\mathrm{TrH}}} \neq \{\mathbf{0}\}$. Therefore, C is not is trace Hermitian complementary dual.

Conversely, assume that $G\overline{G}^T - \overline{G}G^T$ is invertible. Let $\Lambda_C : \mathbb{F}_q^n \to C$ defined by

$$\Lambda_C(\boldsymbol{v}) = \begin{cases} \mathrm{Tr}(\boldsymbol{v}\overline{G}^T)(G\overline{G}^T - \overline{G}G^T)^{-1}G \text{ if } q \text{ is even,} \\ \alpha^{-1}\mathrm{Tr}(\alpha\boldsymbol{v}\overline{G}^T)(G\overline{G}^T - \overline{G}G^T)^{-1}G \text{ if } q \text{ is odd.} \end{cases}$$

Let $\boldsymbol{v} \in \mathbb{F}_q^n$. If $\boldsymbol{v} \in C$, then there exists $\boldsymbol{u} \in \mathbb{F}_r^k$ such that $\boldsymbol{v} = \boldsymbol{u}G$, and hence,

$$\begin{aligned} \Lambda_C(\boldsymbol{v}) &= \begin{cases} \mathrm{Tr}(\boldsymbol{v}\overline{G}^T)(G\overline{G}^T - \overline{G}G^T)^{-1}G \text{ if } q \text{ is even,} \\ \alpha^{-1}\mathrm{Tr}(\alpha\boldsymbol{v}\overline{G}^T)(G\overline{G}^T - \overline{G}G^T)^{-1}G \text{ if } q \text{ is odd,} \end{cases} \\ &= \begin{cases} \mathrm{Tr}(\boldsymbol{u}G\overline{G}^T)(G\overline{G}^T - \overline{G}G^T)^{-1}G \text{ if } q \text{ is even,} \\ \alpha^{-1}\mathrm{Tr}(\alpha\boldsymbol{u}G\overline{G}^T)(G\overline{G}^T - \overline{G}G^T)^{-1}G \text{ if } q \text{ is odd,} \end{cases} \\ &= \begin{cases} (\boldsymbol{u}G\overline{G}^T - \overline{\boldsymbol{u}G}G^T)(G\overline{G}^T - \overline{G}G^T)^{-1}G \text{ if } q \text{ is even,} \\ \alpha^{-1}\alpha(\boldsymbol{u}G\overline{G}^T - \overline{\boldsymbol{u}G}G^T)(G\overline{G}^T - \overline{G}G^T)^{-1}G \text{ if } q \text{ is odd,} \end{cases} \\ &= \boldsymbol{u}(G\overline{G}^T - \overline{\boldsymbol{u}G}G^T)(G\overline{G}^T - \overline{G}G^T)^{-1}G \\ &= \boldsymbol{u}I_kG \\ &= \boldsymbol{u}G \\ &= \boldsymbol{v}. \end{aligned}$$

Assume that $\boldsymbol{v} \in C^{\perp_{\mathrm{TrH}}}$. Then

$$0 = \begin{cases} \mathrm{Tr}(\boldsymbol{v}\overline{G}^T) & \text{if } q \text{ is even,} \\ \mathrm{Tr}(\alpha\boldsymbol{v}\overline{G}^T) & \text{if } q \text{ is odd} \end{cases}$$

and

$$\Lambda_C(\boldsymbol{v}) = \begin{cases} \mathrm{Tr}(\boldsymbol{v}\overline{G}^T)(G\overline{G}^T - \overline{G}G^T)^{-1}G \text{ if } q \text{ is even,} \\ \alpha^{-1}\mathrm{Tr}(\alpha\boldsymbol{v}\overline{G}^T)(G\overline{G}^T - \overline{G}G^T)^{-1}G \text{ if } q \text{ is odd,} \end{cases}$$

$$= \begin{cases} 0(G\overline{G}^T - \overline{G}G^T)^{-1}G \text{ if } q \text{ is even,} \\ \alpha^{-1}0(G\overline{G}^T - \overline{G}G^T)^{-1}G \text{ if } q \text{ is odd,} \end{cases}$$

$$= 0.$$

Hence, Λ_C is an $\mathbb{F}_r$-orthogonal projection with respect to the trace Hermitian inner product from $\mathbb{F}_q^n$ onto C. Therefore, C is trace Hermitian complementary dual. $\square$

Example 3.2.6. *Let C be an $\mathbb{F}_3$-linear code of length 4 over $\mathbb{F}_9 = \mathbb{F}_3(\omega)$ where ω is a root of $x^2 + 2x + 2$ with generator matrix* $G = \begin{bmatrix} 1 & 0 & \omega^3 & 0 \\ 0 & 1 & 2\omega^2 & 2 \\ \omega & 0 & \omega^4 & 0 \\ 0 & \omega & 2\omega^3 & 2\omega \end{bmatrix}$.

Since

$$G\overline{G}^T - \overline{G}G^T = \begin{bmatrix} 0 & \omega^5 & 0 & 1 \\ \omega^7 & 0 & \omega^2 & 0 \\ 0 & \omega^6 & 0 & \omega \\ 1 & 0 & \omega^3 & 0 \end{bmatrix} - \begin{bmatrix} 0 & \omega^7 & 0 & 1 \\ \omega^5 & 0 & \omega^6 & 0 \\ 0 & \omega^2 & 0 & \omega^3 \\ 1 & 0 & \omega & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & \omega^2 & 0 & 0 \\ \omega^6 & 0 & \omega^6 & 0 \\ 0 & \omega^2 & 0 & \omega^6 \\ 0 & 0 & \omega^2 & 0 \end{bmatrix},$$

$G\overline{G}^T - \overline{G}G^T$ is invertible. Hence, by Theorem 3.2.8, C is trace Hermitian complementary dual.

Example 3.2.7. *Let C be an $\mathbb{F}_2$-linear code of length 4 over $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 =$*

$\omega+1\}$ with generator matrix $G = \begin{bmatrix} 1 & 0 & \omega & 0 \\ 0 & 1 & 1 & \omega \\ \omega & 0 & \omega^2 & 0 \\ 0 & \omega & \omega & \omega^2 \end{bmatrix}$. *Since*

$$G\overline{G}^T - \overline{G}G^T = \begin{bmatrix} 0 & \omega & 0 & 1 \\ \omega^2 & 1 & \omega & \omega^2 \\ 0 & \omega^2 & 0 & \omega \\ 1 & \omega & \omega^2 & 1 \end{bmatrix} - \begin{bmatrix} 0 & \omega^2 & 0 & 1 \\ \omega & 1 & \omega^2 & \omega \\ 0 & \omega & 0 & \omega^2 \\ 1 & \omega^2 & \omega & 1 \end{bmatrix}$$

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

$G\overline{G}^T - \overline{G}G^T$ is invertible. Therefore, by Theorem 3.2.5, C is trace Hermitian complementary dual.

Since C is trace Hermitian complementary dual if and only if $C^{\perp_{\mathrm{TrH}}}$ is trace Hermitian complementary dual, we have the following corollary.

Corollary 3.2.8. *Let C be an $\mathbb{F}_r$-linear code of length n over $\mathbb{F}_q = \mathbb{F}_{r^2}$ and let H be a generator of $C^{\perp_{\mathrm{TrH}}}$. Then C is trace Hermitian complementary dual if and only if $H\overline{H}^T - \overline{H}H^T$ is invertible.*

In this case, $\Lambda_{C^{\perp_{\mathrm{TrH}}}} : \mathbb{F}_q^n \to C^{\perp_{\mathrm{TrH}}}$ defined by

$$\Lambda_{C^{\perp_{\mathrm{TrH}}}}(\boldsymbol{v}) = \begin{cases} \mathrm{Tr}(\boldsymbol{v}\overline{H}^T)(H\overline{H}^T - \overline{H}H^T)^{-1}H & \text{if } q \text{ is even,} \\ \alpha^{-1}\mathrm{Tr}(\alpha\boldsymbol{v}\overline{H}^T)(H\overline{H}^T - \overline{H}H^T)^{-1}H & \text{if } q \text{ is odd} \end{cases}$$

is an $\mathbb{F}_r$-orthogonal projection with respect to the trace Hermitian inner product from $\mathbb{F}_q^n$ onto $C^{\perp_{\mathrm{TrH}}}$, where $\alpha \in \mathbb{F}_q \setminus \{0\}$ is such that $\overline{\alpha} = -\alpha$.

Example 3.2.9. *Let C be an $\mathbb{F}_2$-linear code of length 4 over $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 =$*

$\omega+1\}$ *such that* $H = \begin{bmatrix} \omega^2 & 1 & 1 & 0 \\ 0 & \omega^2 & 0 & 1 \\ \omega & \omega^2 & \omega^2 & 0 \\ 0 & \omega & 0 & \omega^2 \end{bmatrix}$ *is a generator matrix for* $C^{\perp_{\mathrm{TrH}}}$.

Since

$$H\overline{H}^T - \overline{H}H^T = \begin{bmatrix} 1 & \omega & \omega & \omega^2 \\ \omega^2 & 0 & 1 & 0 \\ \omega^2 & 1 & 1 & \omega \\ \omega & 0 & \omega^2 & 0 \end{bmatrix} - \begin{bmatrix} 1 & \omega^2 & \omega^2 & \omega \\ \omega & 0 & 1 & 0 \\ \omega & 1 & 1 & \omega^2 \\ \omega^2 & 0 & \omega & 0 \end{bmatrix}$$
$$= \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix},$$

$H\overline{H}^T - \overline{H}H^T$ *is invertible. Therefore, by Corollary* 3.2.8, C *is trace Hermitian complementary dual.*

Chapter 4

Constructions of Complementary Dual Subfield Linear Codes

In this chapter, some constructions of complementary dual codes with respect to the Hermitian and trace Hermitian inner product are given.

4.1 Constructions of Hermitian Complementary Dual Linear Codes

It is well known that, for a given $[n, k, d]_q$ code, there exists an equivalent code with the same parameters such that its generator matrix is of the form $G = [I_k \ A]$ for some $k \times (n-k)$ matrix over $\mathbb{F}_q$. The generator matrix of a linear code of this form plays an important role in constructing Hermitian complementary dual codes.

Lemma 4.1.1 ([10, p. 13])**.** *Let p be a positive integer. Then -1 is a quadratic modulo p if $p \equiv 1 \bmod 4$.*

Theorem 4.1.2. *Let C be an $[n, k, d]$ linear code of length n over $\mathbb{F}_q = \mathbb{F}_{r^2}$ with generator matrix $G = [I_k \ P]$. Then the following statement holds.*

i) *If* $\text{char}(\mathbb{F}_q) = 2$, *then a linear code* C' *with generator matrix* $G' = [I_k\ P\ P]$ *is Hermitian complementary dual with parameters* $[2n-k, k, d']_q$, *where* $d' \geq d$.

ii) *If* $\text{char}(\mathbb{F}_r) \equiv 1 \bmod 4$, *then there exists* $\lambda \in \mathbb{F}_q$ *such that* $\lambda^2 = -1$ *and a linear code* C' *with generator matrix* $G' = [I_k\ P\ \lambda P]$ *is Hermitian complementary dual with parameters* $[2n-k, k, d']_q$, *where* $d' \geq d$.

Proof. *i)* Assume that $\text{char}(\mathbb{F}_q)= 2$. Then

$$G'(\overline{G'})^T = I_k + P\overline{P}^T + P\overline{P}^T = I_k + 2P\overline{P}^T = I_k + 0 = I_k.$$

Therefore, $G'\overline{G'}^T$ is invertible. The code C' generated by G' is Hermitian complementary dual by Theorem 3.1.5.

Since C is a linear code of length n, G has n columns. Note that P has $n-k$ columns. It follows that $G' = [I_k\ P\ P]$ has $k+(n-k)+(n-k) = 2n-k$ columns. Hence, C' generated by G' is a linear code of length $2n-k$ and dimension k.

Next, we show that $d(C') \geq d_{min}$. Let $\boldsymbol{v} \in C' \setminus \{\mathbf{0}\}$. Then there exists $\boldsymbol{u} \in \mathbb{F}_q^k \setminus \{\mathbf{0}\}$ such that $\boldsymbol{v} = \boldsymbol{u}G' = [\boldsymbol{u}I_k\ \boldsymbol{u}P\ \boldsymbol{u}P]$ Hence,

$$\begin{aligned} wt(\boldsymbol{v}) &= wt([\boldsymbol{u}I_k\ \boldsymbol{u}P\ \boldsymbol{u}P]) \\ &\geq wt([\boldsymbol{u}I_k\ \boldsymbol{u}P]) \\ &= wt(\boldsymbol{u}[I_k\ P]) \\ &= wt(\boldsymbol{u}G) \\ &= d(\boldsymbol{u}G) \geq d(C) = d. \end{aligned}$$

Therefore, $d' = d(C') \geq d$

ii) Assume that $\text{char}(\mathbb{F}_r) \equiv 1 \bmod 4$. Then $r = 4k+1$ for some integer k.

By Lemma 4.1.1, there exists $\lambda \in \mathbb{F}_q$ such that $\lambda^2 = -1$. Then

$$\begin{aligned} G'(\overline{G'})^T &= I_k + P\overline{P}^T + \lambda^{r+1}P\overline{P}^T \\ &= I_k + P\overline{P}^T + \lambda^{4k+1+1}P\overline{P}^T \\ &= I_k + P\overline{P}^T + \lambda^{2(2k+1)}P\overline{P}^T \\ &= I_k + P\overline{P}^T + (-1)P\overline{P}^T \\ &= I_k \end{aligned}$$

Therefore, $G'\overline{G'}^T$ is invertible. Hence, by Theorem 3.1.5, C' generated by G' is Hermitian complementary dual.

Similar to i), we can prove that a code C' generated by G' has length $2n-k$ dimension k and $d' = d'(C') \geq d$. $\square$

Example 4.1.3. *Let C be a linear code of length 4 over $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = \omega + 1\}$ with the generator matrix $G = \begin{bmatrix} 1 & 0 & \omega & 0 \\ 0 & 1 & 1 & \omega \end{bmatrix}$. Then C is an $[4, 2, 2]_4$ code. By theorem 4.1.2, a code generated by $G' = \begin{bmatrix} 1 & 0 & \omega & 0 & \omega & 0 \\ 0 & 1 & 1 & \omega & 1 & \omega \end{bmatrix}$ is Hermitian complementary dual with parameters $[6, 2, 3]_4$.*

Example 4.1.4. *Let C be a linear code of length 4 over $\mathbb{F}_{25} = \mathbb{F}_5(\omega)$ where ω is a root of $x^2 + 4x + 2$ with the generator matrix $G = \begin{bmatrix} 1 & 0 & \omega^{22} & \omega^5 \\ 0 & 1 & \omega^{19} & \omega^{22} \end{bmatrix}$ and $2^2 \equiv -1 \mod 5$. By Theorem 4.1.2, a linear code C' generated by $G' = \begin{bmatrix} 1 & 0 & \omega^{22} & \omega^5 & 2\omega^{22} & 2\omega^5 \\ 0 & 1 & \omega^{19} & \omega^{22} & 2\omega^{19} & 2\omega^{22} \end{bmatrix}$ is Hermitian complementary dual with parameters $[6, 2, 5]_{25}$.*

For $i \in \{1, 2\}$, let C_i be an $[n_i, k_i, d_i]_q$ code. Then their direct sum $C_1 \oplus C_2 = \{(c_1, c_2) | c_1 \in C_1, c_2 \in C_2\}$ is an $[n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\}]_q$ code (For detail please see [5]).

If C_i has generator matrix G_i and parity check matrix H_i, then

$$G_1 \oplus G_2 := \begin{bmatrix} G_1 & \mathbf{0} \\ \mathbf{0} & G_2 \end{bmatrix} \text{ and } H_1 \oplus H_2 := \begin{bmatrix} H_1 & \mathbf{0} \\ \mathbf{0} & H_2 \end{bmatrix}$$

are generator and parity check matrices for $C_1 \oplus C_2$, respectively. The direct sum construction can be applied to obtain Hermitian complement dual codes as follows.

Proposition 4.1.5. *If C_1 and C_2 are Hermitian complementary dual with parameters $[n_1, k_1, d_1]_q$ and $[n_2, k_2, d_2]_q$ with generator matrix G_1 and G_2 respectively, then their direct sum $C_1 \oplus C_2$ is Hermitian complementary dual with parameters $[n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\}]_q$.*

Proof. Assume that C_1 and C_2 are Hermitian complementary dual. Then

$$(G_1 \oplus G_2)\overline{(G_1 \oplus G_2)}^T = \begin{bmatrix} G_1\overline{G_1}^T & \mathbf{0} \\ \mathbf{0} & G_2\overline{G_2}^T \end{bmatrix}$$

is invertible because C_1 and C_2 are Hermitian complementary dual so that $G_1\overline{G_1}^T$ and $G_2\overline{G_2}^T$ are invertible. Therefore, $C_1 \oplus C_2$ is Hermitian complementary dual by Theorem 3.1.5. □

Example 4.1.6. *Let C_1 and C_2 be Hermitian complementary dual over $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = \omega + 1\}$ with parameters $[4, 2, 2]_4$ and $[4, 2, 2]_4$ and the generator matrices $G_1 = \begin{bmatrix} 1 & 0 & \omega & 0 \\ 0 & 1 & 1 & \omega \end{bmatrix}$ and $G_2 = \begin{bmatrix} 1 & 0 & \omega & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$ respectively. Then $G_1 \oplus G_2 = \begin{bmatrix} 1 & 0 & \omega & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & \omega & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & \omega & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$ is a generator matrix for $C_1 \oplus C_2$. By Proposition* 4.1.5*, $C_1 \oplus C_2$ is Hermitian complementary dual with parameters* $[8, 4, 2]_4$.

Similar to the direct sum construction, two linear codes of the same length can be combined to form a third code of double in length, namely, $(\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v})$ construction. Let C_i be an $[n, k_i, d_i]_q$ code for i $\in \{1, 2\}$. The $(\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v})$ construction [5] produces an $[2n, k_1 + k_2, \min\{2d_1, d_2\}]_q$ code

$$C = \{(\boldsymbol{u}, \boldsymbol{u}+\boldsymbol{v}) | \boldsymbol{u} \in C_1, \boldsymbol{v} \in C_2\}.$$

If C_i has a generator matrix G_i and a parity check matrix H_i, then generator and parity check matrices H for C are

$$G = \begin{bmatrix} G_1 & G_1 \\ \mathbf{0} & G_2 \end{bmatrix} \text{ and } H = \begin{bmatrix} H_1 & \mathbf{0} \\ -H_2 & H_2 \end{bmatrix},$$

respectively.

The $(\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v})$ construction can be applied to obtain Hermitian complementary dual linear codes as follows.

Proposition 4.1.7. *Let C_1 and C_2 be linear codes over $\mathbb{F}_q$ where $\mathrm{char}(\mathbb{F}_q) = 2$ with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, respectively. If $C_2 \cap C_1^{\perp_{\mathrm{H}}}$ is Hermitian complementary dual and $C_1 \cap C_2^{\perp_{\mathrm{H}}} = \{\mathbf{0}\}$, then $C = \{(\boldsymbol{u}, \boldsymbol{u}+\boldsymbol{v}) | \boldsymbol{u} \in C_1, \boldsymbol{v} \in C_2\}$ is Hermitian complementary dual with parameters $[2n, k_1+k_2, \min\{2d_1, d_2\}]_q$.*

Proof. Assume that $C_2 \cap C_1^{\perp_{\mathrm{H}}}$ is Hermitian complementary dual and $C_1 \cap C_2^{\perp_{\mathrm{H}}} = \{\mathbf{0}\}$. Let $C = \{(\boldsymbol{u}, \boldsymbol{u}+\boldsymbol{v}) | \boldsymbol{u} \in C_1, \boldsymbol{v} \in C_2\}$ and $D = \{(\boldsymbol{a}, \boldsymbol{b}) | \boldsymbol{a}+\boldsymbol{b} \in C_1^{\perp_{\mathrm{H}}}, \boldsymbol{b} \in C_2^{\perp_{\mathrm{H}}}\}$. We show that $D = C^{\perp_{\mathrm{H}}}$. Let $(\boldsymbol{a}, \boldsymbol{b}) \in D$ and $(\boldsymbol{u}, \boldsymbol{u}+\boldsymbol{v}) \in C$. Then

$$\begin{aligned} \langle (\boldsymbol{a}, \boldsymbol{b}), (\boldsymbol{u}, \boldsymbol{u}+\boldsymbol{v}) \rangle_{\mathrm{H}} &= \langle \boldsymbol{a}, \boldsymbol{u} \rangle_{\mathrm{H}} + \langle \boldsymbol{b}, \boldsymbol{u}+\boldsymbol{v} \rangle_{\mathrm{H}} \\ &= \langle \boldsymbol{a}, \boldsymbol{u} \rangle_{\mathrm{H}} + \langle \boldsymbol{b}, \boldsymbol{u} \rangle_{\mathrm{H}} + \langle \boldsymbol{b}, \boldsymbol{v} \rangle_{\mathrm{H}} \\ &= \langle \boldsymbol{a}+\boldsymbol{b}, \boldsymbol{u} \rangle_{\mathrm{H}} + \langle \boldsymbol{b}, \boldsymbol{v} \rangle_{\mathrm{H}} \\ &= 0 + 0 = 0. \end{aligned}$$

It follows that $D \subseteq C^{\perp_{\mathrm{H}}}$. From the definition of D, we have $D = \{(\boldsymbol{c}-\boldsymbol{b}, \boldsymbol{b}) | \boldsymbol{c} \in C_1^{\perp_{\mathrm{H}}}, \boldsymbol{b} \in C_2^{\perp_{\mathrm{H}}}\}$. Let $\varphi : C_1^{\perp_{\mathrm{H}}} \oplus C_2^{\perp_{\mathrm{H}}} \to D$ be defined by $\varphi(\boldsymbol{a}, \boldsymbol{b}) = (\boldsymbol{a}-\boldsymbol{b}, \boldsymbol{b})$. Then φ is a surjective linear map.

Next, we show that φ is injective. Let $\boldsymbol{c_1}, \boldsymbol{c_2} \in C_1^{\perp_{\mathrm{H}}}$ and $\boldsymbol{d_1}, \boldsymbol{d_2} \in C_2^{\perp_{\mathrm{H}}}$. Assume that $(\boldsymbol{c}_1 - \boldsymbol{d}_1, \boldsymbol{d}_1) = (\boldsymbol{c}_2 - \boldsymbol{d}_2, \boldsymbol{d}_2)$. Then $\boldsymbol{d}_1 = \boldsymbol{d}_2$ and $\boldsymbol{c}_1 - \boldsymbol{d}_1 = \boldsymbol{c}_2 - \boldsymbol{d}_2 = \boldsymbol{c}_2 - \boldsymbol{d}_1$ which implies that $\boldsymbol{c}_1 = \boldsymbol{c}_2$. We have $(\boldsymbol{c}_1, \boldsymbol{d}_1) = (\boldsymbol{c}_2, \boldsymbol{d}_2)$, i.e., φ is injective. Therefore, φ is a bijection. Thus, $\dim(D) = n - k_1 + n - k_2 = 2n - (k_1 + k_2)$. Since $\dim(C^{\perp_{\mathrm{H}}}) = 2n - (k_1 + k_2)$ and $D \subseteq C^{\perp_{\mathrm{H}}}$, we have $D = C^{\perp_{\mathrm{H}}}$.

Next, we show that $C \cap C^{\perp_{\rm H}} = \{\mathbf{0}\}$. Let $(\boldsymbol{a}, \boldsymbol{b}) \in C \cap C^{\perp_{\rm H}}$. Since $(\boldsymbol{a}, \boldsymbol{b}) \in C$, we have $\boldsymbol{a} \in C_1$ and $\boldsymbol{a} + \boldsymbol{b} = \boldsymbol{b} - \boldsymbol{a} \in C_2$. Since $(\boldsymbol{a}, \boldsymbol{b}) \in C^{\perp_{\rm H}}$, we have $\boldsymbol{a} + \boldsymbol{b} \in C_1^{\perp_{\rm H}}$ and $\boldsymbol{b} \in C_2^{\perp_{\rm H}}$. Then $\boldsymbol{a} + \boldsymbol{b} \in C_1^{\perp_{\rm H}} \cap C_2 = (C_1 + C_2^{\perp_{\rm H}})^{\perp_{\rm H}}$. Since $\boldsymbol{a} \in C_1$ and $\boldsymbol{b} \in C_2^{\perp_{\rm H}}$, we have $\boldsymbol{a} + \boldsymbol{b} \in C_1 + C_2^{\perp_{\rm H}}$. Thus $\boldsymbol{a} + \boldsymbol{b} \in (C_1 + C_2^{\perp_{\rm H}}) \cap (C_1 + C_2^{\perp_{\rm H}})^{\perp_{\rm H}}$. Since $C_2 \cap C_1^{\perp_{\rm H}} = (C_1 + C_2^{\perp_{\rm H}})^{\perp_{\rm H}}$ is Hermitian complementary dual, it follows that $\boldsymbol{a} + \boldsymbol{b} = \mathbf{0}$ and $\boldsymbol{a} = \boldsymbol{b} \in C_1 \cap C_2^{\perp_{\rm H}} = \{\mathbf{0}\}$. Hence, $\boldsymbol{a} = \boldsymbol{b} = \mathbf{0}$. Therefore, C is Hermitian complementary dual. $\square$

Example 4.1.8. *Let C_1 and C_2 be linear codes over $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = \omega + 1\}$ with parameters $[4, 1, 2]_4$ and $[4, 2, 3]_4$ and generator matrices $G_1 = \begin{bmatrix} 1 & 0 & \omega & 0 \end{bmatrix}$ and $G_2 = \begin{bmatrix} 1 & 0 & 1 & \omega \\ 0 & 1 & \omega & \omega \end{bmatrix}$, respectively. Then $C_2 \cap C_1^{\perp_{\rm H}}$ is Hermitian complementary dual and $C_1 \cap C_2^{\perp_{\rm H}} = \{\mathbf{0}\}$. Therefore, $C = \{(\boldsymbol{u}, \boldsymbol{u} + \boldsymbol{v}) | \boldsymbol{u} \in C_1, \boldsymbol{v} \in C_2\}$ is Hermitian complementary dual with parameters $[8, 3, 3]_4$, by Proposition 4.1.7.*

4.2 Constructions of Complementary Dual Subfield Linear Codes

Given an $(n, r^\ell, d)_q$ $\mathbb{F}_r$-linear code C over $\mathbb{F}_{q=r^2} = \mathbb{F}_r(\omega)$, a generator matrix of C is an $\ell \times n$ matrix over $\mathbb{F}_q$. In [1], using elementary row operations, there exists an equivalent $\mathbb{F}_r$-linear code with the same parameters such that its generator matrix is of the form

$$G = \begin{bmatrix} I_k & A \\ \omega I_k & \omega A \\ \mathbf{0} & B \end{bmatrix}$$

for some nonnegative integer $k \leq \frac{\ell}{2}$, $k \times (n-k)$ matrix A over $\mathbb{F}_q$, and $(\ell - 2k) \times (n-k)$ matrix B over $\mathbb{F}_q$, where $\mathbf{0}$ denotes the $(\ell - 2k) \times k$ matrix whose entries are 0. Construction of trace Hermitian complementary dual codes are given via the generator matrix of this form.

Theorem 4.2.1. *Let C be an $(n, r^\ell, d)_q$ $\mathbb{F}_r$-linear code over $\mathbb{F}_{q=r^2} = \mathbb{F}_r(\omega)$ with generator matrix*

$$G = \begin{bmatrix} I_k & A \\ \omega I_k & \omega A \\ \mathbf{0} & B \end{bmatrix}$$

such that $B\overline{B}^T - \overline{B}B^T$ is invertible, for some non-negative integer k. Then the following statements hold.

i) *If $\mathrm{char}(\mathbb{F}_q) = 2$, then an $\mathbb{F}_r$-linear code C' with generator matrix*

$$G' = \begin{bmatrix} I_k & A & A & \mathbf{0} \\ \omega I_k & \omega A & \omega A & \mathbf{0} \\ \mathbf{0} & B & B & B \end{bmatrix}$$

is trace Hermitian complementary dual with parameters $(3n - 2k, r^\ell, d')_q$, where $d' \geq d$.

ii) *If $\mathrm{char}(\mathbb{F}_q) = 2$, then an $\mathbb{F}_r$-linear code C' with generator matrix*

$$G' = \begin{bmatrix} I_k & A & A \\ \omega I_k & \omega A & \omega^{r+1} A \\ \mathbf{0} & B & \omega^{-1} B \end{bmatrix}$$

such that $\overline{A}A^T = A\overline{A}^T$. C' is trace Hermitian complementary dual with parameters $(2n - k, r^\ell, d')_q$, where $d' \geq d$.

iii) *If $\mathrm{char}(\mathbb{F}_r) \equiv 1 \bmod 4$, then there exists $\lambda \in \mathbb{F}_q$ such that $\lambda^2 = -1$ and an $\mathbb{F}_r$-linear code C' with generator matrix*

$$G' = \begin{bmatrix} I_k & A & \lambda A & \mathbf{0} \\ \omega I_k & \omega A & \lambda \omega A & \mathbf{0} \\ \mathbf{0} & B & \lambda B & B \end{bmatrix}$$

is trace Hermitian complementary dual with parameters $(3n - 2k, r^\ell, d')_q$, where $d' \geq d$.

iv) *If* $\mathrm{char}(\mathbb{F}_r) \equiv 1 \bmod 4$, *then there exists* $\lambda \in \mathbb{F}_q$ *such that* $\lambda^2 = -1$ *and an* $\mathbb{F}_r$*-linear code* C' *with generator matrix*

$$G' = \begin{bmatrix} I_k & A & \lambda A \\ \omega I_k & \omega A & \lambda \omega^{r+1} A \\ \mathbf{0} & B & \lambda \omega^{-1} B \end{bmatrix}$$

such that $\overline{A}A^T = A\overline{A}^T$. C' *is trace Hermitian complementary dual with parameters* $(2n-k, r^\ell, d')_q$, *where* $d' \geq d$.

Proof. In cases $i) - iv)$, the parameters can be verified using argument similar to those in Theorem 4.1.2.

Next, we show that C' is trace Hermitian complementary dual.

i) Assume that char($\mathbb{F}_q$)= 2. Then

$$G'\overline{G'}^T = \begin{bmatrix} I_k & \overline{\omega} I_k & \mathbf{0} \\ \omega I_k & \omega^{r+1} I_k & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & B\overline{B}^T \end{bmatrix}.$$

It follows that

$$G'\overline{G'}^T - \overline{G'}G'^T = \begin{bmatrix} \mathbf{0} & (\omega + \overline{\omega}) I_k & \mathbf{0} \\ (\omega + \overline{\omega}) I_k & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & B\overline{B}^T - \overline{B}B^T \end{bmatrix}.$$

Since $B\overline{B}^T - \overline{B}B^T$ is invertible, $G'\overline{G'}^T - \overline{G'}G'^T$ is nonsingular. By Theorem 3.2.5, C' generated by G' is trace Hermitian complementary dual.

ii) Assume that char($\mathbb{F}_q$)= 2. Then we have $G'\overline{G'}^T$ as in (4.1). It follows that the matrix $G\overline{G'}^T - \overline{G'}G'^T$ is of the form (4.2). Since $B\overline{B}^T - \overline{B}B^T$ is invertible, $G'\overline{G'}^T - \overline{G'}G'^T$ is nonsingular. By Theorem 3.2.5, C' generated by G' is trace Hermitian complementary dual.

iii) Assume that $\mathrm{char}(\mathbb{F}_{\boldsymbol{r}}) \equiv 1 \bmod 4$. Then $r = 4k+1$ for some positive integer k. By Lemma 4.1.1, there exists $\lambda \in \mathbb{F}_q$ such that $\lambda^2 = -1$. Then $\lambda^{r+1} = \lambda^{2(2k+1)} = -1$, and hence, we get that $G'\overline{G'}^T$ is of the form (4.3).

Consequently, we have

$$G'\overline{G'}^T - \overline{G'}G'^T = \begin{bmatrix} \mathbf{0} & (\omega+\overline{\omega})I_k & \mathbf{0} \\ (\omega+\overline{\omega})I_k & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & B\overline{B}^T - \overline{B}B^T \end{bmatrix}$$

which is invertible if and only if $B\overline{B}^T - \overline{B}B^T$ is invertible. Therefore, the code C' generated by G' is trace Hermitian complementary dual by Theorem 3.2.5.

iv) Assume that $\mathrm{char}(\mathbb{F}_{\boldsymbol{r}}) \equiv 1 \bmod 4$. Then $r = 4k+1$ for some positive integer k. By Lemma 4.1.1, there exists $\lambda \in \mathbb{F}_q$ such that $\lambda^2 = -1$. Then $\lambda^{r+1} = \lambda^{2(2k+1)} = -1$, and hence, we get that $G'\overline{G'}^T$ is of the form (4.4). It follows that $G'\overline{G'}^T - \overline{G'}G'^T$ in (4.5) is invertible if and only if $B\overline{B}^T - \overline{B}B^T$ is invertible. Therefore, the code C' generated by G' is trace Hermitian complementary dual by Theorem 3.2.5.

$$G'\overline{G'}^T = \begin{bmatrix} I_k + (1+\omega^{r+1})A\overline{A}^T & \overline{\omega} I_k + (\overline{\omega} + \omega^{2r+1})A\overline{A}^T & \mathbf{0} \\ \omega I_k + (\omega + \omega^{r+2})A\overline{A}^T & \omega^{r+1} I_k + (\omega^{r+1} + \omega^{2r+2})A\overline{A}^T & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & B\overline{B}^T + \omega^{-(r+1)} B\overline{B}^T \end{bmatrix}. \tag{4.1}$$

$$G'\overline{G'}^T - \overline{G'}G'^T = \begin{bmatrix} \mathbf{0} & (\overline{\omega} - \omega) I_k + (\overline{\omega} + \omega^{2r+1} - \omega - \omega^{r+2})A\overline{A}^T & \mathbf{0} \\ (\omega - \overline{\omega}) I_k + (\omega + \omega^{r+2} - \overline{\omega} - \omega^{2r+1})A\overline{A}^T & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 1 + \omega^{-(r+1)}(B\overline{B}^T - \overline{B}B^T) \end{bmatrix}. \tag{4.2}$$

$$G'\overline{G'}^T = \begin{bmatrix} I_k + (1+\lambda^{r+1})A\overline{A}^T & \overline{\omega}(I_k + (1+\lambda^{r+1})A\overline{A}^T) & (1+\lambda^{r+1})A\overline{B}^T \\ \omega(I_k + (1+\lambda^{r+1})A\overline{A}^T) & \omega^{r+1}(I_k + (1+\lambda^{r+1})A\overline{A}^T) & \omega(1+\lambda^{r+1})A\overline{B}^T \\ (1+\lambda^{r+1})A\overline{B}^T & \omega(1+\lambda^{r+1})A\overline{B}^T & (1+\lambda^{r+1})A\overline{B}^T + B\overline{B}^T \end{bmatrix} = \begin{bmatrix} I_k & \overline{\omega} I_k & \mathbf{0} \\ \omega I_k & \omega^{r+1} I_k & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & B\overline{B}^T \end{bmatrix}. \tag{4.3}$$

$$G'\overline{G'}^T = \begin{bmatrix} I_k + (1+\lambda^{r+1}\omega^{r+1})A\overline{A}^T & \overline{\omega}I_k + (\overline{\omega}+\lambda^{r+1}\omega^{2r+1})A\overline{A}^T & \mathbf{0} \\ \omega I_k + (\omega+\lambda^{r+1}\omega^{r+2})A\overline{A}^T & \omega^{r+1}I_k + (\omega^{r+1}+\lambda^{r+1}\omega^{2r+2})A\overline{A}^T & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & B\overline{B}^T + \lambda^{r+1}\omega^{-(r+1)})B\overline{B}^T \end{bmatrix}. \tag{4.4}$$

$$G'\overline{G'}^T - \overline{G'}G'^T = \begin{bmatrix} \mathbf{0} & (\overline{\omega}-\omega)I_k + (\overline{\omega}-\omega^{2r+1}-\omega+\omega^{r+2})A\overline{A}^T & \mathbf{0} \\ (\omega-\overline{\omega})I_k + (\omega-\omega^{r+2}-\overline{\omega}+\omega^{2r+1})A\overline{A}^T & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & (\omega^{-(r+1)}-1)(B\overline{B}^T - \overline{B}B^T) \end{bmatrix} \tag{4.5}$$

□

Example 4.2.2. *Let C be an $\mathbb{F}_2$-linear code of length 4 over $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = \omega + 1\}$ with the generator matrix* $G = \begin{bmatrix} 1 & 0 & \omega & 0 \\ 0 & 1 & 0 & \omega \\ \omega & 0 & \omega^2 & 0 \\ 0 & \omega & 0 & \omega^2 \\ 0 & 0 & 1 & \omega \\ 0 & 0 & \omega^2 & 1 \end{bmatrix}$. *Then C is a $(4, 2^6, 2)_4$ $\mathbb{F}_2$-linear code.*

Since

$$\begin{bmatrix} 1 & \omega \\ \omega^2 & 1 \end{bmatrix}\begin{bmatrix} 1 & \omega \\ \omega^2 & 1 \end{bmatrix} - \begin{bmatrix} 1 & \omega^2 \\ \omega & 1 \end{bmatrix}\begin{bmatrix} 1 & \omega^2 \\ \omega & 1 \end{bmatrix} = \begin{bmatrix} \omega + \overline{\omega} & 0 \\ 0 & \omega + \overline{\omega} \end{bmatrix}$$

is invertible, the $\mathbb{F}_2$-linear code C' generated by

$$G' = \begin{bmatrix} 1 & 0 & \omega & 0 & \omega & 0 & 0 & 0 \\ 0 & 1 & 0 & \omega & 0 & \omega & 0 & 0 \\ \omega & 0 & \omega^2 & 0 & \omega^2 & 0 & 0 & 0 \\ 0 & \omega & 0 & \omega^2 & 0 & \omega^2 & 0 & 0 \\ 0 & 0 & 1 & \omega & 1 & \omega & 1 & \omega \\ 0 & 0 & \omega^2 & 1 & \omega^2 & 1 & \omega^2 & 1 \end{bmatrix}$$

is trace Hermitian complementary dual with parameters $(8, 2^6, d(C') \geq 2)_4$ by Theorem 4.2.1. By direct calculation, we have $d(C') = 3$.

Example 4.2.3. *Let C be an $\mathbb{F}_2$-linear code of length 4 over $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = \omega + 1\}$ with the generator matrix* $G = \begin{bmatrix} 1 & 0 & \omega & 0 \\ 0 & 1 & 0 & \omega \\ \omega & 0 & \omega^2 & 0 \\ 0 & \omega & 0 & \omega^2 \\ 0 & 0 & 1 & \omega \\ 0 & 0 & \omega^2 & 1 \end{bmatrix}$. *Then C is a $(4, 2^6, 2)_4$ $\mathbb{F}_2$-linear code.*

Since

$$\begin{bmatrix} 1 & \omega \\ \omega^2 & 1 \end{bmatrix}\begin{bmatrix} 1 & \omega \\ \omega^2 & 1 \end{bmatrix} - \begin{bmatrix} 1 & \omega^2 \\ \omega & 1 \end{bmatrix}\begin{bmatrix} 1 & \omega^2 \\ \omega & 1 \end{bmatrix} = \begin{bmatrix} \omega+\overline{\omega} & 0 \\ 0 & \omega+\overline{\omega} \end{bmatrix}$$

is invertible and

$$\begin{bmatrix} \omega^2 & 0 \\ 0 & \omega^2 \end{bmatrix}\begin{bmatrix} \omega & 0 \\ 0 & \omega \end{bmatrix} = \begin{bmatrix} \omega & 0 \\ 0 & \omega \end{bmatrix}\begin{bmatrix} \omega^2 & 0 \\ 0 & \omega^2 \end{bmatrix},$$

the $\mathbb{F}_2$*-linear code* C' *generated by*

$$G' = \begin{bmatrix} 1 & 0 & \omega & 0 & \omega & 0 \\ 0 & 1 & 0 & \omega & 0 & \omega \\ \omega & 0 & \omega^2 & 0 & \omega & 0 \\ 0 & \omega & 0 & \omega^2 & 0 & \omega \\ 0 & 0 & 1 & \omega & \omega^{-1} & 1 \\ 0 & 0 & \omega^2 & 1 & \omega & \omega^{-1} \end{bmatrix}$$

is trace Hermitian complementary dual with parameters $(6, 2^6, d(C') \geq 2)_4$ *by Theorem* 4.2.1*. By direct calculation, we have* $d(C') = 2$*.*

References

[1] M. F. Ezerman, S. Jitman, S. Ling, D. V. Pasechnik, "CSS-like constructions of asymmetric quantum codes," *IEEE Trans. Inf. Theory*, 59, 6732–6754(2013).

[2] R. J. Faudree, R. H. Schelp, "Path-path Ramsey-type number for the complete bipartite graph," *Journal of Combinatorial Theory Series B,* 19(2), 161–173(1975).

[3] W. Goddard, M. A. Henning, O. R. Oellermann, "Bipartite Ramsey number and Zarankiewicz," *Journal of Discrete Mathematics,* 219, 85–95 (2000).

[4] R. Lidl, H. Niederreiter, Finite Fields, *Encyclopedia of Mathematics and its Applications,* vol. 20. Cambridge: Cambridge Univ. Press, 1997.

[5] S. Ling, C. Xing, Coding Theory : A First Course, *Cambridge University Press,* 2004.

[6] L. Maherani, G.R. Omidi, G. Raeisi, M. Shahsiah, O. R. Oellermann, "On three-color Ramsey number of paths," *Graphs and Combinatorics,* (2015)DOI 10.1007/s00373-014-1507-0.

[7] J. L. Massey, "Linear codes with complementary duals," *Discrete Mathematics,* 106/107, 337–342(1992).

[8] G. Nebe, E. M. Rains, and N. J. A. Sloane, Self-Dual Codes and Invariant Theory, *Springer*, Berlin, 2006.

[9] E. Sangwisut, S. Jitman, S. Ling, P. Udomkavanich, "Hulls of cyclic and negacyclic codes over finite fields," *Finite Fields and Their Applications*, 33, 232–257(2015).

[10] J.H. van Lint, Introduction to Coding Theory, *Springer*, Berlin, 1965.

[11] X. Yang, J. L. Massey, "The condition for a cyclic code to have a complementary dual," *Discrete Math,* 126, 391–393(1994).

Biography

Name	Mr. Kriangkrai Boonniyom
Address	60 Village No. 3 Donkrabuang Sub-district, Banpong District, Ratchaburi, 70110
Date of Birth	07 June 1990
Education	
2013	Bachelor of Science in Mathematics, Silpakorn University
2015	Master of Science in Mathematics, Silpakorn University