SELF-ORTHOGONAL MATRIX PRODUCT CODES OVER FINITE FIELDS

By

Mr. Todsapol Mankean

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 2016

SELF-ORTHOGONAL MATRIX PRODUCT CODES OVER FINITE FIELDS

By

Mr. Todsapol Mankean

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 2016

รหัสผลคูณเมทริกซ์เชิงตั้งฉากในตัวบนฟีลด์จำกัด

โดย
นายทสพล แม้นเขียน

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์
ภาควิชาคณิตศาสตร์
บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ปีการศึกษา 2559

The Graduate School, Silpakorn University has approved and accredited the Thesis title of "Self-Orthogonal Matrix Product Codes over Finite Fields" submitted by Mr. Todsapol Mankean 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

(Chalermpong Worawannotai, Ph.D.)

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

.... Member

(Professor Patanee Udomkavanich, Ph.D.)

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

.... Member

(Somphong Jitman, Ph.D.)

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

57305203 : MAJOR : MATHEMATICS

KEY WORDS: SELF-ORTHOGONAL CODES / LINEAR CODES / MATRIX-PRODUCT CODES/ EUCLIDEAN INNER PRODUCT HERMITIAN INNER PRODUCT

TODSAPOL MANKEAN : SELF-ORTHOGONAL MATRIX PRODUCT CODES OVER FINITE FIELDS. THESIS ADVISOR : SOMPHONG JITMAN, Ph.D. 44 pp.

Self-orthogonal codes form an important class of linear codes due to their rich algebraic structures and wide applications. In this thesis, the well-known matrix-product construction for linear codes is applied to construct self-orthogonal codes under both the Euclidean and Hermitian inner products. Sufficient conditions on the input codes and matrices used in the construction of self-orthogonal matrix-product codes are given as well as some illustrative examples.

Department of Mathematics Graduate School, Silpakorn University

Student's signature .... Academic Year 2016

Thesis Advisor's signature ....

57305203: สาขาวิชาคณิตศาสตร์

คำสำคัญ: รหัสเชิงตั้งฉากในตัว / รหัสเชิงเส้น / รหัสผลคูณเมทริกซ์ / ผลคูณภายในแบบยุคลิด / คูณภายในแบบแอร์มีต

ทสพล แม้นเขียน : รหัสผลคูณเมทริกซ์เชิงตั้งฉากในตัวบนฟิลด์จำกัด. อาจารย์ที่ปรึกษาวิทยานิพนธ์ : ดร. สมพงค์ จิตต์มั่น. 44 หน้า.

รหัสเชิงตั้งฉากในตัวเป็นรหัสเชิงเส้นที่มีความสำคัญเนื่องจากเป็นรหัสที่มีโครงสร้างทางพีชคณิตที่ดีและยังสามารถประยุกต์ใช้ได้อีกหลากหลาย ในวิทยานิพนธ์นี้ได้นำเสนอการสร้างรหัสเชิงตั้งฉากในตัวภายใต้ผลคูณภายในแบบยุคลิดและแบบแอร์มีตโดยประยุกต์มาจากรหัสผลคูณเมทริกซ์ พร้อมทั้งให้เงื่อนไขที่เพียงพอสำหรับการเป็นรหัสและเมทริกซ์ที่ใช้ในการสร้างรหัสผลคูณเมทริกซ์ เชิงตั้งฉากในตัว

ภาควิชาคณิตศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

ลายมือชื่อนักศึกษา.. ปีการศึกษา 2559

ลายมือชื่ออาจารย์ที่ปรึกษาวิทยานิพนธ์ ....

Acknowledgements

First of all, I would like to express my gratitude to Dr. Somphong Jitman, my thesis advisor, for his help and support in all stages of my thesis studies.

In addition, I would like to thank Dr. Chalermpong Worawannotai and Professor Dr. Patanee Udomkavanich, the chairman and a member of the thesis committee, for their comments and suggestions.

I would like to thank the Department of Mathematics, Faculty of Science Silpakorn University for the facility support.

I would like to thank the Development and Promotion of Science and Technology Talents Project (DPST) for the financial support throughout my undergraduate and graduate studies.

Finally, special thanks to my beloved parents for understanding and support.

Table of Contents

Chapter 1

Introduction

Coding theory is the study of the properties of codes and deals 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 rich algebraic structures, various applications, and link with other objects as shown [14], [8] and references therein. Such codes have extensively been studied by many coding theorists. Self-orthogonal codes can be applied to construct quantum codes [8]. One interesting problem is to construct self-orthogonal codes with good parameters.

The matrix-product construction for linear codes has been introduced in [2]. Matrix-product codes are interesting since they can be viewed as a generalization of the well-known $(u|u+v)$-construction and $(u+v+w|2u+v|u)$-construction [2]. In [2], properties of matrix-product codes have been studied as well as a lower bound for the minimum distance of the output codes. In some cases, the lower bound given in [2] was shown to be sharped [6].

In [5], the matrix-product construction has been applied to obtain Euclidean self-orthogonal codes in the case where the underlying matrix is a square orthogonal matrix and the input codes are Euclidean self-orthogonal. Similarly, this idea has been extended to construct Hermitian self-orthogonal codes in [15] and [13]. However, the input codes are required to be Hermitian self-orthogonal.

In this thesis, we propose a more general set up for self-orthogonal matrix-product codes under the Euclidean and Hermitian inner products. In many cases, the self-orthogonality of the input codes can be relaxed. Some basic properties of matrices, linear codes, self-orthogonal codes and matrix-product codes are discussed in Chapter 2. Matrix-product constructions for Euclidean self-orthogonal codes are discussed in Chapter 3 as well as properties of matrices used for the constructions. In Chapter 4, we present matrix-product constructions for Hermitian self-orthogonal codes.

Chapter 2

Preliminaries

For a prime power q, let $\mathbb{F}_q$ denote the finite field of order q. In this chapter, some properties of matrices and codes over $\mathbb{F}_q$ used in this thesis are recalled.

2.1 Matrices

For positive integers $s \leq l$, denote by $M_{s,l}(\mathbb{F}_q)$ the set of $s \times l$ matrices whose entries are in $\mathbb{F}_q$. A matrix $A \in M_{s,l}(\mathbb{F}_q)$ is said to be *full-row-rank* if the rows of A are linearly independent. Denote by $\mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_s)$ the $s \times s$ *diagonal matrix* whose diagonal entries are $\lambda_1, \lambda_2, \ldots, \lambda_s$. Similarly, let $\mathrm{adiag}(\lambda_1, \lambda_2, \ldots, \lambda_s)$ denote the $s \times s$ *anti-diagonal matrix* whose anti-diagonal entries are $\lambda_1, \lambda_2, \ldots, \lambda_s$. Denote by I_s and J_s the matrices $\mathrm{diag}(1, 1, \ldots, 1)$ and $\mathrm{adiag}(1, 1, \ldots, 1)$, respectively. For $A = [a_{ij}] \in M_{s,l}(\mathbb{F}_q)$, and $q = r^2$, define $A^\dagger = [a_{ji}^r]$. A matrix $A \in M_{s,l}(\mathbb{F}_q)$ is said to be *semi-orthogonal* (resp., *semi-unitary*) if $AA^T = I_s$ (resp., $AA^\dagger = I_s$). A semi-orthogonal (resp., *semi-unitary*) matrix $A \in M_{s,l}(\mathbb{F}_q)$ is called an *orthogonal matrix* (resp., *unitary matrix*) if $s = l$. An $s \times s$ matrix A over $\mathbb{F}_q$ is said to be *quasi-orthogonal* (resp., *quasi-unitary*) if $AA^T = \lambda I_s$ (resp., $AA^\dagger = \lambda I_s$) for some non-zero element $\lambda \in \mathbb{F}_q$. These matrices are good ingredients in matrix-product constructions for self-orthogonal linear codes. The existence and properties of such matrices will be studied in Sections 3.2 and 4.2.

2.2 Linear Codes

For each positive integer n, denote by $\mathbb{F}_q^n$ the $\mathbb{F}_q$-vector space of all vectors of length n over $\mathbb{F}_q$. For $\boldsymbol{u}$ and $\boldsymbol{v}$ in $\mathbb{F}_q^n$, let $\mathrm{wt}_{\mathrm{H}}(\boldsymbol{u})$ and $\mathrm{d}_{\mathrm{H}}(\boldsymbol{u},\boldsymbol{v})$ denote the *Hamming weight* of $\boldsymbol{u}$ and the *Hamming distance* between $\boldsymbol{u}$ and $\boldsymbol{v}$, respectively. Precisely, for $\boldsymbol{u}=(u_1,u_2,\cdots,u_n)$ and $\boldsymbol{v}=(v_1,v_2,\cdots,v_n)$ in $\mathbb{F}_q^n$, $\mathrm{wt}_{\mathrm{H}}(\boldsymbol{u})=|\{i \mid u_i\neq 0\}|$ and $\mathrm{d}_{\mathrm{H}}(\boldsymbol{u},\boldsymbol{v})=|\{i \mid u_i\neq v_i\}|$. A set $C\subseteq \mathbb{F}_q^n$ is called a *linear code of length* n over $\mathbb{F}_q$ if it is a subspace of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$. A linear code C of length n over $\mathbb{F}_q$ is said to have parameters $[n,k,d]_q$ if the $\mathbb{F}_q$-dimension of C is k and the *minimum Hamming distance* of C is

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

For a linear code C, it is well-known (see [12, p. 48]) that

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

An $k\times n$ 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 of C.

For $\boldsymbol{u}=(u_1,u_2,\ldots,u_n)$ and $\boldsymbol{v}=(v_1,v_2,\ldots,v_n)$ in $\mathbb{F}_q^n$, we consider the following inner products between $\boldsymbol{u}$ and $\boldsymbol{v}$.

1. $\langle \boldsymbol{u},\boldsymbol{v}\rangle_E := \sum_{i=1}^n u_iv_i$ is called the *Euclidean inner product* between $\boldsymbol{u}$ and $\boldsymbol{v}$.

2. For $q=r^2$, $\langle \boldsymbol{u},\boldsymbol{v}\rangle_H := \sum_{i=1}^n u_i\overline{v_i}=\langle \boldsymbol{u},\overline{\boldsymbol{v}}\rangle_E$ is called the *Hermitian inner product* between $\boldsymbol{u}$ and $\boldsymbol{v}$, where $\overline{a}=a^r$ for all $a\in\mathbb{F}_q$.

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

$$C^{\perp_E}:=\{\boldsymbol{u}\in\mathbb{F}_q^n \mid \langle \boldsymbol{u},\boldsymbol{c}\rangle_E=0 \text{ for all } \boldsymbol{c}\in C\}$$
$$(\text{resp., } C^{\perp_H}:=\{\boldsymbol{u}\in\mathbb{F}_q^n \mid \langle \boldsymbol{u},\boldsymbol{c}\rangle_H=0 \text{ for all } \boldsymbol{c}\in C\}).$$

A code C is said to be *Euclidean* (resp., *Hermitian*) *self-orthogonal* if $C\subseteq C^{\perp_E}$ (resp., $C\subseteq C^{\perp_H}$). A linear code C is said to be *Euclidean* (resp., *Hermitian*) *self-dual* if $C=C^{\perp_E}$ (resp., $C=C^{\perp_H}$).

For linear codes C_1 and C_2 of the same length over $\mathbb{F}_q$, if C_i is generated by a generator matrix G_i for $i \in \{1,2\}$, then it is not difficult to see that ([12, p.67]), $G_1G_2^T = [\mathbf{0}]$ if and only if $C_1 \subseteq C_2^{\perp_E}$. In particular, $G_1G_1^T = [\mathbf{0}]$ if and only if C_1 is Euclidean self-orthogonal. For $q = r^2$, $G_1G_2^\dagger = [\mathbf{0}]$ if and only if $C_1 \subseteq C_2^{\perp_H}$. In particular, $G_1G_1^\dagger = [\mathbf{0}]$ if and only if C_1 is Hermitian self-orthogonal.

2.3 Matrix-Product Codes

The matrix-product construction for linear codes has been introduced in [2] and extensively studied in [6] and [3]. The major results are summarized as follows. For each integers $1 \leq s \leq l$, let $A = [a_{ij}] \in M_{s,l}(\mathbb{F}_q)$. For each integer $1 \leq i \leq s$, let C_i be a linear $[m, k_i, d_i]_q$ code over $\mathbb{F}_q$ with a generator matrix G_i. The *matrix-product code* $[C_1, C_2, \cdots, C_s] \cdot A$ is defined to be the linear code of length ml over $\mathbb{F}_q$ generated by

$$G = \begin{bmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{bmatrix}.$$

The matrix-product code $[C_1, C_2, \cdots, C_s] \cdot A$ is simply denoted by C_A if $C_1, C_2, \ldots, C_s$ are clear in the context.

For each $A \in M_{s,l}(\mathbb{F}_q)$ and for each $1 \leq i \leq s$, denote by $\delta_i(A)$ the minimum distance of the linear code of length l over $\mathbb{F}_q$ generated by the first i rows of A. Some properties of matrix-product codes (see [2] and [3]) can be summarized as follows.

Theorem 2.3.1. *With the notations given above, the following statements hold.*

1. *C_A is a linear code of length ml over $\mathbb{F}_q$.*
2. $\dim(C_A) \leq \sum_{i=1}^{s} k_i$.
3. *If A is full-row-rank, then*

$$\dim(C_A) = \sum_{i=1}^{s} k_i.$$

4. $\mathrm{d_H}(C_A) \geq \min_{1\leq i\leq s}\{d_i\delta_i(A)\}$.

5. If $C_1 \supseteq C_2 \supseteq \cdots \supseteq C_s$, *then*

$$\mathrm{d_H}(C_A) = \min_{1\leq i\leq s}\{d_i\delta_i(A)\}.$$

If A is an invertible square matrix, the Euclidean dual of a matrix-product code is again a matrix-product code and it is determined as follows.

Theorem 2.3.2 ([2, p. 19]). *With the notations given above and* $s = \ell$. *If* A *is an invertible* $s \times s$ *matrix, then*

$$([C_1, C_2, \cdots, C_s] \cdot A)^{\perp_E} = [C_1^{\perp_E}, C_2^{\perp_E}, \cdots, C_s^{\perp_E}] \cdot (A^{-1})^T.$$

From Theorem 2.3.2, the matrix-product construction for Euclidean self-orthogonal codes has been given, where A is a $s \times s$ orthogonal matrix and the input codes C_i are Euclidean self-orthogonal (see [5], [15] and [13]).

In general the dual of a matrix-product code does not need to be matrix-product. In this paper, we focus on a more general set up for Euclidean and Hermitian self-orthogonal matrix-product codes where the restriction on the self-orthogonality of the input codes are relaxed. The detailed constructions are given in the following chapters.

Chapter 3

Euclidean Self-Orthogonal Matrix-Product Codes

In this chapter, sufficient conditions for matrix-product codes to be Euclidean self-orthogonal are given. Two matrix-product constructions for Euclidean self-orthogonal linear codes are presented.

3.1 Constructions

In the following theorem, a matrix-product construction for Euclidean self-orthogonal codes whose input codes are self-orthogonal is discussed. This results is a bit more general than the ones in [5] since the underlying matrix does not need to be orthogonal.

Theorem 3.1.1. *Let $s \leq l$ be positive integers. Let $C_1, C_2, \ldots, C_s$ be linear codes of the same length over $\mathbb{F}_q$ and let $A \in M_{s\times l}(\mathbb{F}_q)$. If AA^T is diagonal and $C_i \subseteq C_i^{\perp_E}$ for all $1 \leq i \leq s$, then $C_A \subseteq C_A^{\perp_E}$.*

Proof. Assume that $AA^T = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_s)$ and $C_i \subseteq C_i^{\perp_E}$ for all $1 \leq i \leq s$. For each $1 \leq i \leq s$, let G_i be a generator matrix for the code C_i. Let $A =$

$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1l} \\ a_{21} & a_{22} & \cdots & a_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sl} \end{bmatrix}$, the matrix-product code C_A is generated by

$$G = \begin{bmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{bmatrix}.$$

It follows that

$$\begin{aligned} GG^T &= \begin{bmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{bmatrix} \begin{bmatrix} a_{11}G_1^T & a_{21}G_2^T & \cdots & a_{s1}G_s^T \\ a_{12}G_1^T & a_{22}G_2^T & \cdots & a_{s2}G_s^T \\ \vdots & \vdots & \ddots & \vdots \\ a_{1l}G_1^T & a_{2l}G_2^T & \cdots & a_{sl}G_s^T \end{bmatrix} \\ &= \begin{bmatrix} \lambda_1(G_1G_1^T) & 0(G_1G_2^T) & \cdots & 0(G_1G_s^T) \\ 0(G_2G_1^T) & \lambda_2(G_2G_2^T) & \cdots & 0(G_2G_s^T) \\ \vdots & \vdots & \ddots & \vdots \\ 0(G_sG_1^T) & 0(G_sG_2^T) & \cdots & \lambda_s(G_sG_s^T) \end{bmatrix}. \end{aligned}$$

Since $C_i \subseteq C_i^{\perp_E}$ for all $1 \leq i \leq s$, we have that $G_iG_i^T = [\mathbf{0}]$ for all $1 \leq i \leq s$. It follows that $GG^T = [\mathbf{0}]$. Hence, $C_A \subseteq C_A^{\perp_E}$ as desired. $\square$

Example 3.1.2. *Let* $A = \begin{bmatrix} 1 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 \end{bmatrix} \in M_{2,4}(\mathbb{F}_3)$. *Then A is full-row-rank,* $AA^T = \mathrm{diag}(1,2)$, $\delta_1(A) = 4$, *and* $\delta_2(A) = 2$. *Let C_1 and C_2 be the linear codes of length* 6 *over* $\mathbb{F}_3$ *generated by*

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

and

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

respectively. Then $C_2 \subseteq C_1$ *are Euclidean self-orthogonal with parameters* $[6, 2, 3]_3$ *and* $[6, 1, 6]_3$*, respectively. By Theorems 2.3.1 and 3.1.1,* C_A *is a Euclidean self-orthogonal code with parameters* $[24, 3, 12]_3$.

If A is a square quasi-orthogonal, then the next corollary can be deduced.

Corollary 3.1.3. *If* $A \in M_{s,s}(\mathbb{F}_q)$ *is such that* $AA^T = \lambda I_s$ *for some non-zero* λ *in* $\mathbb{F}_q$ *and* $C_i \subseteq C_i^{\perp_E}$ *for all* $1 \le i \le s$*, then* $C_A \subseteq C_A^{\perp_E}$.

Next, a matrix-product construction for Euclidean self-orthogonal codes is studied while the Euclidean self-orthogonality of the input codes is relaxed.

Theorem 3.1.4. *Let* $s \le l$ *be positive integers. Let* $C_1, C_2, \dots, C_s$ *be linear codes of the same length over* $\mathbb{F}_q$ *and let* $A \in M_{s\times l}(\mathbb{F}_q)$*. If* AA^T *is anti-diagonal and* $C_i \subseteq C_{s-i+1}^{\perp_E}$ *for all* $1 \le i \le s$*, then* $C_A \subseteq C_A^{\perp_E}$.

Proof. Assume that $AA^T = \mathrm{adiag}(\lambda_1, \lambda_2, \dots, \lambda_s)$ and $C_i \subseteq C_{s-i+1}^{\perp_E}$ for all $1 \le i \le s$. For each $1 \le i \le s$, let G_i be a generator matrix of the code C_i. Since $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1l} \\ a_{21} & a_{22} & \cdots & a_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sl} \end{bmatrix}$, the matrix-product code C_A is generated by

$$G = \begin{bmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{bmatrix}.$$

It follows that

$$GG^T = \begin{bmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{bmatrix} \begin{bmatrix} a_{11}G_1^T & a_{21}G_2^T & \cdots & a_{s1}G_s^T \\ a_{12}G_1^T & a_{22}G_2^T & \cdots & a_{s2}G_s^T \\ \vdots & \vdots & \ddots & \vdots \\ a_{1l}G_1^T & a_{2l}G_2^T & \cdots & a_{sl}G_s^T \end{bmatrix}$$

$$= \begin{bmatrix} 0(G_1G_1^T) & \cdots & 0(G_1G_{s-1}^T) & \lambda_1(G_1G_s^T) \\ 0(G_2G_1^T) & \cdots & \lambda_2(G_2G_{s-1}^T) & 0(G_2G_s^T) \\ \vdots & \cdots & \vdots & \vdots \\ \lambda_s(G_sG_1^T) & \cdots & 0(G_sG_{s-1}^T) & 0(G_sG_s^T) \end{bmatrix}.$$

Since $C_i \subseteq C_{s-i+1}^{\perp_E}$ for all $1 \leq i \leq s$, we have $G_iG_{s-i+1}^T = [\mathbf{0}]$ for all $1 \leq i \leq s$. Hence, $GG^T = [\mathbf{0}]$. Therefore, $C_A \subseteq C_A^{\perp_E}$ as desired. $\square$

Example 3.1.5. *Let* $A = \begin{bmatrix} 1 & 1 & 2 \\ 2 & 1 & 1 \end{bmatrix} \in M_{2,3}(\mathbb{F}_3)$. *Then* A *is full-row-rank,* $AA^T =$ adiag$(2,2)$, $\delta_1(A) = 3$, *and* $\delta_2(A) = 1$. *Let* C_1 *and* C_2 *be the linear codes of length* 6 *over* $\mathbb{F}_3$ *generated by*

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 \end{bmatrix}$$

and

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

respectively. Then C_1 *and* C_2 *have parameters* $[6,5,2]_3$ *and* $[6,1,6]_3$*, respectively. Since* $C_2 \subseteq C_1 \subseteq C_2^{\perp_E}$*, by Theorems 2.3.1 and 3.1.4,* C_A *is a Euclidean self-orthogonal code with parameters* $[18,6,6]_3$.

The following corollaries can be obtained directly from Theorem 3.1.4. The proofs are omitted.

Corollary 3.1.6. *If $A \in M_{s,s}(\mathbb{F}_q)$ is such that $AA^T = \lambda J_s$ for some non-zero element λ in $\mathbb{F}_q$ and $C_i \subseteq C_{s-i+1}^{\perp_E}$ for all $1 \leq i \leq s$, then $C_A \subseteq C_A^{\perp_E}$.*

By choosing $C_i = C_{s-i+1}^{\perp_E}$ in Corollary 3.1.6, the next corollary follows.

Corollary 3.1.7. *If $A \in M_{s,s}(\mathbb{F}_q)$ is such that $AA^T = \lambda J_s$ for some non-zero element λ in $\mathbb{F}_q$ and $C_i = C_{s-i+1}^{\perp_E}$ for all $1 \leq i \leq s$, then C_A is Euclidean self-dual.*

3.2 Special Matrices and Applications

In order to apply the matrix-product constructions discussed in Section 3.1 to obtain Euclidean self-orthogonal codes, a matrix $A \in M_{s,l}(\mathbb{F}_q)$ with the property that AA^T is diagonal or anti-diagonal is required. To the best of our knowledge, there are no proper names for such matrices. For convenience, the following definitions are given. A matrix $A \in M_{s,l}(\mathbb{F}_q)$ is said to be *weakly semi-orthogonal* if AA^T is diagonal and it is said to be *weakly anti-semi-orthogonal* if AA^T is anti-diagonal. In the case where A is square, such matrices are called *weakly quasi-orthogonal* and *weakly anti-quasi-orthogonal*, respectively. These two families of matrices are studied in Subsections 3.2.1 and 3.2.2, respectively.

3.2.1 Weakly Quasi-Orthogonal Matrices

In this subsection, the existence of some weakly quasi-orthogonal matrices are given.

Lemma 3.2.1. *Let α be a primitive element of $\mathbb{F}_q$. Then the following statements hold.*

1. *If q is odd, then $A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is invertible and (weakly) quasi-orthogonal with $\delta_1(A) = 2$ and $\delta_2(A) = 1$.*
2. *If $q > 2$ is even, then $A = \begin{bmatrix} 1 & \alpha \\ \alpha & 1 \end{bmatrix}$ is invertible and (weakly) quasi-orthogonal with $\delta_1(A) = 2$ and $\delta_2(A) = 1$.*

Proof. To prove 1, assume that q is odd and $A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Clearly, A is invertible, $\delta_1(A) = 2$ and $\delta_2(A) = 1$. Since

$$AA^T = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \mathrm{diag}(2, 2),$$

A is (weakly) quasi-orthogonal.

To prove 2, assume that $q > 2$ is even and $A = \begin{bmatrix} 1 & \alpha \\ \alpha & 1 \end{bmatrix}$. Clearly, A is invertible, $\delta_1(A) = 2$ and $\delta_2(A) = 1$. Since

$$AA^T = \begin{bmatrix} 1 & \alpha \\ \alpha & 1 \end{bmatrix} \begin{bmatrix} 1 & \alpha \\ \alpha & 1 \end{bmatrix} = \begin{bmatrix} 1+\alpha^2 & 0 \\ 0 & 1+\alpha^2 \end{bmatrix} = \mathrm{diag}(1+\alpha^2, 1+\alpha^2),$$

A is (weakly) quasi-orthogonal. $\square$

Applying Theorem 3.1.1 and Lemma 3.2.1, we conclude the following corollary.

Corollary 3.2.2. *Let q be a prime power. If there exist Euclidean self-orthogonal $[m, k_1, d_1]_q$ and $[m, k_2, d_2]_q$ codes, then a Euclidean self-orthogonal $[2m, k_1 + k_2, d]_q$ code can be constructed with $d \geq \min\{2d_1, d_2\}$.*

Proof. Assume that there exist Euclidean self-orthogonal codes C_1 and C_2 with parameters $[m, k_1, d_1]_q$ and $[m, k_2, d_2]_q$. By Lemma 3.2.1, there exist a 2×2 invertible and weakly quasi-orthogonal matrix A over $\mathbb{F}_q$ with $\delta_1(A) = 2$ and $\delta_2(A) = 1$. By Theorems 2.3.1 and 3.1.1, the matrix-product code C_A is Euclidean self-orthogonal with parameters $[2m, k_1 + k_2, d]_q$ and $d \geq \min\{2d_1, d_2\}$. $\square$

Example 3.2.3. *Let α be a primitive element of $\mathbb{F}_4$. By Lemma 3.2.1, $A = \begin{bmatrix} 1 & \alpha \\ \alpha & 1 \end{bmatrix} \in M_{2,2}(\mathbb{F}_4)$ is invertible, $AA^T = \mathrm{diag}(1+\alpha^2, 1+\alpha^2)$, $\delta_1(A) = 2$, and $\delta_2(A) = 1$. Let C_1 and C_2 be the linear codes of length 4 over $\mathbb{F}_4$ generated by*

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

and

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

respectively. Then $C_2 \subseteq C_1$ *are Euclidean self-orthogonal with parameters* $[4,2,2]_4$ *and* $[4,1,4]_4$*, respectively. By Theorem 2.3.1 and Corollary 3.2.2,* C_A *is a Euclidean self-orthogonal code with parameters* $[8,3,4]_4$*.*

In the following theorem, the existence 3×3 (weakly) quasi-orthogonal matrices are given.

Theorem 3.2.4. *Let* $\mathbb{F}_q$ *be a finite field such that* $q \geq 4$ *and let* $a \in \mathbb{F}_q \setminus \{0,1,2\}$*. Then the following statements hold.*

1. *If* $Char(\mathbb{F}_q) = 2$*, then* $A := \begin{bmatrix} 1 & a & 1 \\ a & 1 & 0 \\ 1 & a & a^2+1 \end{bmatrix}$ *is invertible and weakly quasi-orthogonal with* $\delta_1(A) = 3$*,* $\delta_2(A) = 2$ *and* $\delta_3(A) = 1$*.*
2. *If* $Char(\mathbb{F}_q) = 3$*, then* $A := \begin{bmatrix} a & -a & 1 \\ 1 & 1 & 0 \\ -a & a & 2a^2 \end{bmatrix}$ *is invertible and weakly quasi-orthogonal with* $\delta_1(A) = 3$*,* $\delta_2(A) = 2$ *and* $\delta_3(A) = 1$*.*
3. *If* $Char(\mathbb{F}_q) \geq 5$*, then* $A := \begin{bmatrix} a & -a & a \\ 1 & 1 & 0 \\ -a & a & 2a \end{bmatrix}$ *is invertible and weakly quasi-orthogonal with* $\delta_1(A) = 3$*,* $\delta_2(A) = 2$ *and* $\delta_3(A) = 1$*.*

Proof. To prove 1, assume that $Char(\mathbb{F}_q) = 2$ and $A = \begin{bmatrix} 1 & a & 1 \\ a & 1 & 0 \\ 1 & a & a^2+1 \end{bmatrix}$. Clearly, $\delta_1(A) = 3$, $\delta_2(A) = 2$ and $\delta_3(A) = 1$. Since $\det(A) = a^2(a+1)^2$, $\det(A) \neq 0$ if and only if $a \notin \{0, 1\}$. Hence, A is invertible. Since

$$AA^T = \begin{bmatrix} 1 & a & 1 \\ a & 1 & 0 \\ 1 & a & a^2+1 \end{bmatrix} \begin{bmatrix} 1 & a & 1 \\ a & 1 & a \\ 1 & 0 & a^2+1 \end{bmatrix}$$

$$= \begin{bmatrix} a^2 & 0 & 0 \\ 0 & a^2+1 & 0 \\ 0 & 0 & a^4+a^2 \end{bmatrix} = \mathrm{diag}(a^2, a^2+1, a^4+a^2),$$

A is weakly quasi-orthogonal.

To prove 2, assume that $Char(\mathbb{F}_q) = 3$ and $A = \begin{bmatrix} a & -a & 1 \\ 1 & 1 & 0 \\ -a & a & 2a^2 \end{bmatrix}$. Clearly, $\delta_1(A) = 3$, $\delta_2(A) = 2$ and $\delta_3(A) = 1$. Since $\det(A) = a(a^2-1) = a(a-1)(a+1)$, $\det(A) \neq 0$ if and only if $a \notin \{0, 1, 2\}$. Hence, A is invertible. Since

$$AA^T = \begin{bmatrix} a & -a & 1 \\ 1 & 1 & 0 \\ -a & a & 2a^2 \end{bmatrix} \begin{bmatrix} a & 1 & -a \\ -a & 1 & a \\ 1 & 0 & 2a^2 \end{bmatrix}$$

$$= \begin{bmatrix} 2a^2+1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & a^4+2a^2 \end{bmatrix} = \mathrm{diag}(2a^2+1, 2, a^4+2a^2),$$

A is weakly quasi-orthogonal.

To prove 3, assume that $Char(\mathbb{F}_q) \geq 5$ and $A = \begin{bmatrix} a & -a & a \\ 1 & 1 & 0 \\ -a & a & 2a \end{bmatrix}$. Clearly, $\delta_1(A) = 3$, $\delta_2(A) = 2$ and $\delta_3(A) = 1$. Since $\det(A) = 6a^2$, $\det(A) \neq 0$ if and only if $a \neq 0$. Hence, A is invertible. Since

$$AA^T = \begin{bmatrix} a & -a & a \\ 1 & 1 & 0 \\ -a & a & 2a \end{bmatrix} \begin{bmatrix} a & 1 & -a \\ -a & 1 & a \\ a & 0 & 2a \end{bmatrix} = \begin{bmatrix} 3a^2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6a^2 \end{bmatrix} = \mathrm{diag}(3a^2, 2, 6a^2),$$

A is weakly quasi-orthogonal. $\square$

Theorem 3.2.4 can be applied to construct a Euclidean self-orthogonal code as follows.

Corollary 3.2.5. *Let $q \geq 4$ be a prime power. If there exist Euclidean self-orthogonal $[m, k_1, d_1]_q$, $[m, k_2, d_2]_q$ and $[m, k_3, d_3]_q$ codes, then a Euclidean self-orthogonal $[3m, k_1 + k_2 + k_3, d]_q$ code can be constructed with $d \geq \min\{3d_1, 2d_2, d_3\}$.*

Proof. Assume that there are three Euclidean self-orthogonal codes with parameters $[m, k_1, d_1]_q$, $[m, k_2, d_2]_q$ and $[m, k_3, d_3]_q$. By Theorem 3.2.4, there exist a 3×3 invertible and weakly quasi-orthogonal matrix A over $\mathbb{F}_q$ with $\delta_1(A) = 3$, $\delta_2(A) = 2$ and $\delta_3(A) = 1$. By Theorems 2.3.1 and 3.1.1, the matrix-product code C_A is Euclidean self-orthogonal $[3m, k_1 + k_2 + k_3, d]_q$ with $d \geq \min\{3d_1, 2d_2, d_3\}$. $\square$

Example 3.2.6. *Let α be a primitive element of $\mathbb{F}_9$. By Theorem 3.2.4,* $A = \begin{bmatrix} \alpha & -\alpha & 1 \\ 1 & 1 & 0 \\ -\alpha & \alpha & 2\alpha^2 \end{bmatrix} \in M_{3,3}(\mathbb{F}_9)$ *is invertible,* $AA^T = \mathrm{diag}(2\alpha^2 + 1, 2, \alpha^4 + 2\alpha^2)$, $\delta_1(A) = 3$, $\delta_2(A) = 2$ *and* $\delta_3(A) = 1$. *Let C_1, C_2 and C_3 be the linear codes of length* 6 *over* $\mathbb{F}_9$ *generated by*

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha^6 & \alpha^5 & \alpha^5 & \alpha^7 & \alpha^3 & 1 \\ 1 & 2 & 1 & 2 & 1 & 2 \end{bmatrix},$$

$$G_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha^6 & \alpha^5 & \alpha^5 & \alpha^7 & \alpha^3 & 1 \end{bmatrix}$$

and

$$G_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

respectively. Then $C_3 \subseteq C_2 \subseteq C_1$ are Euclidean self-orthogonal codes with parameters $[6, 3, 3]_9$, $[6, 2, 4]_9$ *and* $[6, 1, 6]_9$, *respectively. By Theorem 2.3.1 and Corollary 3.2.5, C_A is a Euclidean self-orthogonal code with parameters* $[18, 6, 6]_9$.

3.2.2 Weakly Anti-Quasi-Orthogonal Matrices

In this subsection, we focus on the existence of weakly anti-quasi-orthogonal matrices. In a finite field $\mathbb{F}_q$ of characteristic p, it is well-known (Quadratic Reciprocity Law) (see [12, p. 185]) that if $p \equiv 1 \bmod 4$, or q is square and $p \equiv 3 \bmod 4$, then -1 is square in $\mathbb{F}_q$. Precisely, there exists $b \in \mathbb{F}_q$ such that $b^2 + 1 = 0$. Hence, we have the following results.

Lemma 3.2.7. *Let $\mathbb{F}_q$ be a finite field of characteristic p. If $p \equiv 1 \bmod 4$, or q is square and $p \equiv 3 \bmod 4$, then there exists $b \in \mathbb{F}_q$ such that $b^2 + 1 = 0$ and $A = \begin{bmatrix} 1 & b \\ 1 & -b \end{bmatrix}$ is invertible and (weakly) anti-quasi-orthogonal with $\delta_1(A) = 2$ and $\delta_2(A) = 1$.*

Proof. From the discussion above, there exists $b \in \mathbb{F}_q$ such that $b^2 + 1 = 0$. Let $A = \begin{bmatrix} 1 & b \\ 1 & -b \end{bmatrix}$. Clearly, A is invertible, $\delta_1(A) = 2$ and $\delta_2(A) = 1$. Since

$$AA^T = \begin{bmatrix} 1 & b \\ 1 & -b \end{bmatrix} \begin{bmatrix} 1 & 1 \\ b & -b \end{bmatrix} = \begin{bmatrix} 0 & 1 - b^2 \\ 1 - b^2 & 0 \end{bmatrix} = \mathrm{adiag}(1 - b^2, 1 - b^2),$$

A is (weakly) anti-quasi-orthogonal. □

Corollary 3.2.8. *Let $\mathbb{F}_q$ be a finite field of characteristic p such that $p \equiv 1 \bmod 4$, or q is square and $p \equiv 3 \bmod 4$. If there exist linear codes C_1 and C_2 with parameters $[m, k_1, d_1]_q$ and $[m, k_2, d_2]_q$ such that $C_1 \subseteq C_2^{\perp_E}$, then a Euclidean self-orthogonal $[2m, k_1 + k_2, d]_q$ code can be constructed with $d \geq \min\{2d_1, d_2\}$.*

Proof. Assume that there exist linear codes C_1 and C_2 with parameters $[m, k_1, d_1]_q$ and $[m, k_2, d_2]_q$ such that $C_1 \subseteq C_2^{\perp_E}$. By Lemma 3.2.7, there exist a 2×2 invertible and anti-quasi-orthogonal matrix A over $\mathbb{F}_q$ with $\delta_1(A) = 2$ and $\delta_2(A) = 1$. By Theorems 2.3.1 and 3.1.1, the matrix-product code C_A is Euclidean self-orthogonal with parameters $[2m, k_1 + k_2, d]_q$ with $d \geq \min\{2d_1, d_2\}$. □

Example 3.2.9. *Let $q = 5$. By Quadratic Reciprocity Law, there exists $b \in \mathbb{F}_5$ such that $b^2 + 1 = 0$. By Lemma 3.2.7 and $b := 2$, we have that $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \in M_{2,2}(\mathbb{F}_5)$ is invertible, $AA^T = \mathrm{adiag}(2,2)$, $\delta_1(A) = 2$, and $\delta_2(A) = 1$. Let C_1 and C_2 be the linear codes of length 5 over $\mathbb{F}_5$ generated by*

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 2 & 2 & 3 \end{bmatrix}$$

and

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

respectively. Then C_1 and C_2 have parameters $[5,3,3]_5$ and $[5,1,5]_5$, respectively. Since $C_2 \subseteq C_1 \subseteq C_2^{\perp_E}$, by Theorem 2.3.1 and Corollary 3.2.8, C_A is a Euclidean self-orthogonal code with parameters $[10,4,6]_5$.

By choosing $C_2 = C_1^{\perp_E}$ in Corollary 3.2.8, the next corollary follows.

Corollary 3.2.10. *Let $\mathbb{F}_q$ be a finite field of characteristic p such that $p \equiv 1 \bmod 4$, or q is square and $p \equiv 3 \bmod 4$. If there exists an $[m,k,d]_q$ code C, then a Euclidean self-dual $[2m,m,d']_q$ code can be constructed with $d' \geq \min\{2d, d^{\perp_E}\}$ and $d^{\perp_E} = d(C^{\perp_E})$.*

Example 3.2.11. *From Example 3.2.9, the matrix $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \in M_{2,2}(\mathbb{F}_5)$ is invertible, $AA^T = \mathrm{adiag}(2,2)$, $\delta_1(A) = 2$, and $\delta_2(A) = 1$. Let C be linear codes of length 5 over $\mathbb{F}_5$ generated by*

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

Then C and $C^{\perp_E}$ have parameters $[5,3,3]_5$ and $[5,2,4]_5$, respectively. By Corollary 3.2.7 , C_A is a Euclidean self-dual code with parameters $[10,5,d']_5$ where $d' \geq 4$.

Let p be a prime. In [10, p. 50], it has been shown that 1) if $p \equiv 1 \bmod 8$ or $p \equiv 3 \bmod 8$, then -2 is a square in $\mathbb{F}_p$, and 2) if $p \equiv -1 \bmod 8$ or $p \equiv -3 \bmod 8$, then -2 is not square in $\mathbb{F}_p$. In an extension field $\mathbb{F}_q$ of $\mathbb{F}_p$, we have the following results.

Proposition 3.2.12. *Let p be odd prime and $\mathbb{F}_q$ be a finite field of characteristic p. Then -2 is a square if one of the following statements hold.*

1. $p \equiv 1 \bmod 8$.
2. $p \equiv 3 \bmod 8$.
3. *q is square and* $p \equiv -1 \bmod 8$.
4. *q is square and* $p \equiv -3 \bmod 8$.

Proof. Assume that one of the four statements holds. We consider the proof into four cases.

Case 1 $p \equiv 1 \bmod 8$. We have that -2 is square $\mathbb{F}_p \subseteq \mathbb{F}_q$.

Case 2 $p \equiv 3 \bmod 8$. The proof is similar to Case 1.

Case 3 q is a square and $p \equiv -1 \bmod 8$. Since -2 is not square in $\mathbb{F}_p$, we have that $x^2 + 2$ is irreducible over $\mathbb{F}_p$. So, $K = \mathbb{F}_p[x]/\langle x^2 + 2\rangle$ is a field. It is known that K contains the roots of $x^2 + 2$. We have that $[K : \mathbb{F}_p] = 2$. So, $|K| = p^2$. Since q is a square, $K = \mathbb{F}_{p^2} \subseteq \mathbb{F}_q$.

Case 4 q is square and $p \equiv -3 \bmod 8$. The proof is similar to Case 3.

From the four cases, -2 is square in $\mathbb{F}_q$. □

Proposition 3.2.12 can be applied to construct anti-diagonal 3×3 matrices. Then the next theorem can be deduced.

Theorem 3.2.13. *Let $\mathbb{F}_q$ be a finite field of characteristic p. If $p \equiv 1 \bmod 8$, or $p \equiv 3 \bmod 8$, or q is a square and $p \equiv -1 \bmod 8$, or q is a square and $p \equiv -3 \bmod 8$, then there exists $b \in \mathbb{F}_q$ such that $b^2 + 2 = 0$ and $A = \begin{bmatrix} 1 & -1 & b \\ 1 & 1 & 0 \\ -1 & 1 & b \end{bmatrix}$ is invertible and anti-quasi-orthogonal with $\delta_1(A) = 3$, $\delta_2(A) = 2$ and $\delta_3(A) = 1$.*

Proof. From Proposition 3.2.12, there exists $b \in \mathbb{F}_q$ such that $b^2 + 2 = 0$. Let $A =$

$\begin{bmatrix} 1 & -1 & b \\ 1 & 1 & 0 \\ -1 & 1 & b \end{bmatrix}$. Clearly, A is invertible, $\delta_1(A) = 3$, $\delta_2(A) = 2$ and $\delta_3(A) = 1$. Since

$$AA^T = \begin{bmatrix} 1 & -1 & b \\ 1 & 1 & 0 \\ -1 & 1 & b \end{bmatrix} \begin{bmatrix} 1 & 1 & -1 \\ -1 & 1 & 1 \\ b & 0 & b \end{bmatrix} = \begin{bmatrix} 0 & 0 & b^2-2 \\ 0 & 2 & 0 \\ b^2-2 & 0 & 0 \end{bmatrix},$$

$AA^T = \mathrm{adiag}(b^2-2, 2, b^2-2)$. So, A is weakly anti-quasi-orthogonal. $\square$

Theorem 3.2.13 can be applied to construct a Euclidean self-orthogonal code as follows.

Corollary 3.2.14. *Let $\mathbb{F}_q$ be a finite field of characteristic p such that $p \equiv 1 \bmod 8$, or $p \equiv 3 \bmod 8$, or q is a square and $p \equiv -1 \bmod 8$, or q is a square and $p \equiv -3 \bmod 8$. If there exist codes C_1, C_2 and C_3 with parameters $[m, k_1, d_1]_q$, $[m, k_2, d_2]_q$ and $[m, k_3, d_3]_q$ such that $C_1 \subseteq C_3^{\perp_E}$ and C_2 is Euclidean self-orthogonal code, then there exists a Euclidean self-orthogonal $[3m, k_1 + k_2 + k_3, d]_q$ code with $d \geq \min\{3d_1, 2d_2, d_3\}$.*

Proof. Assume that there are three linear codes with parameters $[m, k_1, d_1]_q$, $[m, k_2, d_2]_q$ and $[m, k_3, d_3]_q$ such that $C_1 \subseteq C_3^{\perp_E}$ and C_2 is Euclidean self-orthogonal. By Theorem 3.2.13, there exist a 3×3 invertible and weakly quasi-orthogonal matrix A over $\mathbb{F}_q$ with $\delta_1(A) = 3$, $\delta_2(A) = 2$ and $\delta_3(A) = 1$. By Theorems 2.3.1 and 3.1.4, the matrix-product code C_A is Euclidean self-orthogonal $[3m, k_1 + k_2 + k_3, d]_q$ with $d \geq \min\{3d_1, 2d_2, d_3\}$. $\square$

Example 3.2.15. *Let $q = 9$. Then $p \equiv 3 \bmod 8$. By Proposition 3.2.12, we have that -2 is a square in $\mathbb{F}_9$. Precisely, by chosen $b = 1$, we have that $b^2 + 2 = 0$ and $A := \begin{bmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix} \in M_{3,3}(\mathbb{F}_9)$ is invertible, $AA^T = \mathrm{adiag}(2,2,2)$, $\delta_1(A) = 3$, $\delta_2(A) = 2$ and $\delta_2(A) = 1$. Let α be a primitive element of $\mathbb{F}_9$ and C_1, C_2 and C_3 be linear codes* *of length* 6 *over* $\mathbb{F}_3$ *generated by*

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 \end{bmatrix}$$

,

$$G_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha & 2\alpha & \alpha & 2\alpha & \alpha & 2\alpha \end{bmatrix}$$

and

$$G_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

respectively. Then C_1, C_2 *and* C_3 *have parameters* $[6,5,2]_9, [6,2,4]_9$ *and* $[6,1,6]_9$*, respectively. Since* $C_1 \subseteq C_3^{\perp_E}$ *and* C_2 *is Euclidean self-orthogonal code, by Theorem 2.3.1 and Corollary 3.2.14, we have that* C_A *is a Euclidean self-orthogonal code with parameters* $[18,8,d]_9$ *with* $d \geq \min\{2\cdot 3, 4\cdot 2, 6\cdot 1\} = 6$.

3.2.3 Summary

In this subsection, we summarize the existence of weakly quasi-orthogonal and weakly anti-quasi-orthogonal discussed in Subsection 3.2.1 and 3.2.2. These matrices play an important role in the matrix-product construction for Euclidean self-orthogonal codes. However, the construction where the matrices have larger size or where the matrices are non-square is an interesting problem as well.

Table 3.1: Existence of Weakly Quasi-Orthogonal Matrices.

s \ q	$\mathbb{F}_2$	$\mathbb{F}_3$	$\mathbb{F}_q, q \geq 4$
2	Lemma 3.2.1	Lemma 3.2.1	Lemma 3.2.1
3	?	?	Theorem 3.2.4
$s \geq 4$	?	?	?

Note that ? indicates the case where such matrices are not studied in this work.

Table 3.2: Existence of Weakly Anti-Quasi-Orthogonal Matrices

s \ q	$p \equiv 1 \bmod 4$	q is square and $p \equiv 3 \bmod 4$	$p \equiv 1 \bmod 8$	$p \equiv 3 \bmod 8$	q is square and $p \equiv -1 \bmod 8$	q is square and $p \equiv -3 \bmod 8$	q is even.
2	Lemma 3.2.7	Lemma 3.2.7	?	?	?	?	?
3	?	?	Theorem 3.2.13	Theorem 3.2.13	Theorem 3.2.13	Theorem 3.2.13	?
$s \geq 4$	?	?	?	?	?	?	?

3.3 Examples

In this part, we focus on applications of Corollaries 3.2.2, 3.2.8 and 3.2.10 in constructing Euclidean self-orthogonal and Euclidean self-dual codes.

First, we consider applications of Corollary 3.2.2 to Euclidean self-orthogonal codes in [1] and Euclidean self-orthogonal Reed-Solomon codes.

In [1], it has been shown that for any $q \equiv 1 \bmod 4$ such that $q \leq 113$, there exists a Euclidean self-dual code over $\mathbb{F}_q$ with parameter $[q-1, \frac{q-1}{2}, \frac{q-1}{2}]_q$.

In order to determine the algebraic structures and properties of Reed-Solomon codes, a brief introduction to cyclic codes is given as follows. A linear code C of length n over $\mathbb{F}_q$ is said to be *cyclic* if $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ provided that $(c_0, c_1, \ldots, c_{n-1})$ is a codeword in C. It is well-known that there is a one-to-one correspondence between a vector $c = (c_0, c_1, \ldots, c_{n-1})$ in $\mathbb{F}_q^n$ and the polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ in $\mathbb{F}_q[x]$ of degree at most $n-1$. Under this correspondence, a code C of length n over $\mathbb{F}_q$ can be considered as a principal ideal in the quotient ring $R_n := \mathbb{F}_q / \langle x^n - 1 \rangle$. Here, C is regarded as an ideal in R_n. Among all the generators of ideal C, there exists a unique monic one with minimal degree that divides $x^n - 1$. It is called the *generator polynomial* C and denoted by $G(x)$. Let

$$H(x) = \frac{x^n - 1}{G(x)}.$$

The polynomial $H(x)$ is called the *check polynomial* of C. Since $H(0) \neq 0$, the *reciprocal polynomial* of $H(x)$ can be defined and it is defined to be

$$H^*(x) = (H(0))^{-1}[x^{degH(x)} H(x^{-1})].$$

The polynomial $H(x)$ is said to be *self-reciprocal* over $\mathbb{F}_q$ is $H(x) = H^*(x)$. Note that $H^*(x)$ is a monic divisor of $x^n - 1$ over $\mathbb{F}_q$ and it is the generator polynomial of $C^{\perp_E}$ (see [12, p. 142]).

Lemma 3.3.1 ([12, p. 154]). *Let $g_1(x)$ and $g_2(x)$ be the generator polynomials of q-ary cyclic codes C_1 and C_2 of the same length, respectively. Then $C_1 \subseteq C_2$ if and only if $g_1(x)$ is divisible by $g_2(x)$.*

A *Reed-Solomon code* over $\mathbb{F}_q$ is a cyclic code of length $q-1$ over $\mathbb{F}_q$ generated by $G(x) = (x-\alpha^a)(x-\alpha^{a+1})\cdots(x-\alpha^{a+\delta-2})$, where α is a primitive element of $\mathbb{F}_q$, $a \geq 0$ and $2 \leq \delta \leq q-2$. From [12, Theorem 8.2.3], the Reed-Solomon code of length $q-1$ over $\mathbb{F}_q$ with the generator polynomial $G(x)$ has parameters $[q-1, q-\delta, \delta]_q$. In some cases, Reed-Solomon codes are Euclidean self-orthogonal.

Lemma 3.3.2. *Let $q \geq 8$ be a prime power and let α be a primitive element of $\mathbb{F}_q$. Let C be a Reed Solomon code of length $q-1$ over $\mathbb{F}_q$ with parity check polynomial $H(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)$. Then C is a Euclidean self-orthogonal code with parameters $[q-1, 3, q-3]_q$.*

Proof. Note that $H^*(x) = (x-\alpha)^*(x-\alpha^2)^*(x-\alpha^3)^*$ is a generator polynomial of a code $C^{\perp_E}$. Then

$$
\begin{aligned}
G(x) &= \left(\frac{x^n-1}{H(x)}\right) \\
&= \frac{(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{q-1})}{(x-\alpha)(x-\alpha^2)(x-\alpha^3)} \\
&= (x-\alpha^4)(x-\alpha^5)\cdots(x-\alpha^{q-1})
\end{aligned}
$$

is the generator polynomial for C. Hence, C is a $[q-1, 3, q-3]_q$ code.

Since $\alpha^{q-1} = 1$ and $q \geq 8$, we have that $(x-\alpha)^*, (x-\alpha^2)^*, (x-\alpha^3)^*, [(x-\alpha)(x-\alpha^2)]^*, [(x-\alpha)(x-\alpha^3)]^*$ and $[(x-\alpha^2)(x-\alpha^3)]^*$ are not self-reciprocal. Since

$$G^*(x) = (x-\alpha^4)^*(x-\alpha^5)^*\cdots(x-\alpha^{q-1})^*,$$

it follows that $H(x)|G^*(x)$. This implies that $H^*(x)|G(x)$. By Lemma 3.3.1, we have that $C \subseteq C^{\perp_E}$. Hence, C is a Euclidean self-orthogonal code. $\square$

By setting C_1 and C_2 to be $q-$ary Euclidean self-orthogonal code with parameters $[q-1, \frac{q-1}{2}, \frac{q-1}{2}]_q$ and $[q-1, 3, q-3]_q$, respectively, in Corollary 3.2.2, we have the following result.

Corollary 3.3.3. *Let $q \equiv 1 \bmod 4$ such that $8 \leq q \leq 113$. Then there exists a Euclidean self-orthogonal $[2(q-1), \frac{q-1}{2}+3, d]_q$ code can be constructed with $d \geq q-3$.*

Based on Corollary 3.3.3 and Reed-Solomon codes explained above, some examples of Euclidean self-orthogonal matrix-product codes over $\mathbb{F}_q$ with good parameters are given in Table 3.3.

Table 3.3: Euclidean self-Orthogonal Matrix-Product Codes over $\mathbb{F}_q$

q	Parametes		
	C_1	C_2	C_A
9	$[8, 4, 4]_9$	$[8, 3, 6]_9$	$[16, 7, d]_9$ with $d \geq 6$
13	$[12, 6, 6]_{13}$	$[12, 3, 10]_{13}$	$[24, 9, d]_{13}$ with $d \geq 10$
17	$[16, 8, 8]_{17}$	$[16, 3, 14]_{17}$	$[32, 11, d]_{14}$ with $d \geq 14$
25	$[24, 12, 12]_{25}$	$[24, 3, 22]_{25}$	$[48, 15, d]_{25}$ with $d \geq 22$

Based on Euclidean self-orthogonal codes in [9] and nested pairs of Generalized Reed-Solomon codes characterized in [4] and Corollaries 3.2.8 and 3.2.10, self-orthogonal and self-dual codes with good parameters can be obtained.

For $1 \leq m \leq q$ and $1 \leq k \leq m$, let $\mathbb{F}_q[x]_k$ denote the set of all polynomials over $\mathbb{F}_q$ of degree less than k and let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be distinct elements in $\mathbb{F}_q$. A *generalized Reed-Solomon code* of length n and dimension k over $\mathbb{F}_q$ is defined to be the set

$$GRS_q(m, k) := \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_m)) \mid f(x) \in \mathbb{F}_q[x]_k\}.$$

In [4], it has been shown that there exist a pair of generalized Reed-Solomon codes $GRS_q(m, k) =: C \subseteq D := GRS_q(m, k+i)$ with parameters $[m, k, m-k+1]_q$ and $[m, k+i, m-k-i+1]_q$ for all $1 \leq k \leq m-1$ and $0 \leq i \leq m-k$. Moreover, $D^{\perp_E}$ has parameters $[m, m-k-i, k+i+1]_q$.

By setting $C_1 = C$ and $C_2 = D^{\perp_E}$ in Corollary 3.2.8, we have the following result.

Corollary 3.3.4. *Let $\mathbb{F}_q$ be a finite field of characteristic p such that $p \equiv 1 \bmod 4$, or q is square and $p \equiv 3 \bmod 4$. Then there exists a matrix-product Euclidean self-*

orthogonal code $[2m, m-i, d]_q$ *with* $d \geq \min\{2(m-k+1), k+i+1\}$ *for all* $1 \leq k \leq m-1$ *and* $0 \leq i \leq m-k$.

Based on Corollary 3.3.4 and a pair of generalized Reed-Solomon codes explained above, some examples of Euclidean self-orthogonal matrix-product codes over $\mathbb{F}_5$ with good parameters are given in Table 3.4.

Table 3.4: Euclidean Self-Orthogonal Matrix-Product Codes over $\mathbb{F}_5$

m	k	i	parameters
2	1	0	$[4, 2, d]_5$ with $d \geq 2$
3	2	0	$[6, 3, d]_5$ with $d \geq 3$
		1	$[6, 2, d]_5$ with $d \geq 4$
4	1	2	$[8, 2, d]_5$ with $d \geq 4$
	2	1	$[8, 3, d]_5$ with $d \geq 4$
	3	0	$[8, 4, d]_5$ with $d \geq 4$
5	2	0	$[10, 3, d]_5$ with $d \geq 6$
	3	0	$[10, 5, d]_5$ with $d \geq 4$
		1	$[10, 4, d]_5$ with $d \geq 5$
		2	$[10, 3, d]_5$ with $d \geq 6$

By setting $C_1 = C$ and $C_2 = C^{\perp}$ in Corollary 3.2.10, we have the following result.

Corollary 3.3.5. *Let* $\mathbb{F}_q$ *be a finite field of characteristic* p *such that* $p \equiv 1 \bmod 4$, *or* q *is square and* $p \equiv 3 \bmod 4$. *Then there exists a matrix-product Euclidean self-dual code* $[2m, m, d]_q$ *with* $d \geq \min\{2(m-k+1), k+1\}$ *for all* $1 \leq k \leq m-1$.

Based on Corollary 3.3.5 and generalized Reed-Solomon codes discussed above, some examples of Euclidean self-dual matrix-product codes over $\mathbb{F}_5$ with good parameters are given in Table 3.5.

Table 3.5: Euclidean Self-Dual Matrix-Product Codes over $\mathbb{F}_5$

m	k	parameters
2	1	$[4,2,d]_5$ with $d \geq 2$
3	2	$[6,3,d]_5$ with $d \geq 3$
4	3	$[8,4,d]_5$ with $d \geq 4$
5	3	$[10,5,d]_5$ with $d \geq 4$

Chapter 4

Hermitian Self-Orthogonal Matrix-Product Codes

In this section, we assume that $q = r^2$, where r is a prime power. Sufficient conditions for matrix-product codes to be Hermitian self-orthogonal are given. Two types of matrix-product constructions for Hermitian self-orthogonal linear codes are introduced.

4.1 Constructions

In the following theorem, a matrix-product construction for Hermitian self-orthogonal codes whose input codes are Hermitian self-orthogonal is discussed. The results in this part are a bit more general than the ones in [5] since the underlying matrix does not need to be unitary. The construction is given as follows.

Theorem 4.1.1. *Let $s \leq l$ be positive integers. Let $C_1, C_2, \ldots, C_s$ be linear codes of the same length over $\mathbb{F}_q$ and let $A \in M_{s\times l}(\mathbb{F}_q)$. If $AA^\dagger$ is diagonal and $C_i \subseteq C_i^{\perp_H}$ for all $1 \leq i \leq s$, then $C_A \subseteq C_A^{\perp_H}$.*

Proof. Assume that $AA^\dagger = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_s)$ and $C_i \subseteq C_i^{\perp_H}$ for all $1 \leq i \leq s$. For each $1 \leq i \leq s$, let G_i be a generator matrix for the code C_i. Since $A =$

$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1l} \\ a_{21} & a_{22} & \cdots & a_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sl} \end{bmatrix}$, the matrix-product code C_A is generated by

$$G = \begin{bmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{bmatrix}.$$

It follows that

$$GG^\dagger = \begin{bmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{bmatrix} \begin{bmatrix} a_{11}^rG_1^\dagger & a_{21}^rG_2^\dagger & \cdots & a_{s1}^rG_s^\dagger \\ a_{12}^rG_1^\dagger & a_{22}^rG_2^\dagger & \cdots & a_{s2}^rG_s^\dagger \\ \vdots & \vdots & \ddots & \vdots \\ a_{1l}^rG_1^\dagger & a_{2l}^rG_2^\dagger & \cdots & a_{sl}^rG_s^\dagger \end{bmatrix}.$$

$$= \begin{bmatrix} \lambda_1(G_1G_1^\dagger) & 0(G_1G_2^\dagger) & \cdots & 0(G_1G_s^\dagger) \\ 0(G_2G_1^\dagger) & \lambda_2(G_2G_2^\dagger) & \cdots & 0(G_2G_s^\dagger) \\ \vdots & \vdots & \ddots & \vdots \\ 0(G_sG_1^\dagger) & 0(G_sG_2^\dagger) & \cdots & \lambda_s(G_sG_s^\dagger) \end{bmatrix}.$$

Since $C_i \subseteq C_i^{\perp_H}$ for all $1 \leq i \leq s$, we have that $G_iG_i^\dagger = [\mathbf{0}]$ for all $1 \leq i \leq s$. It follows that $GG^\dagger = [\mathbf{0}]$. Hence, $C_A \subseteq C_A^{\perp_H}$ as desired. □

If A is a square quasi-unitary, then the following corollary can be deduced.

Corollary 4.1.2. *If $A \in M_{s,s}(\mathbb{F}_q)$ is such that $AA^\dagger = \lambda I_s$ for some non-zero λ in $\mathbb{F}_q$ and $C_i \subseteq C_i^{\perp_H}$ for all $1 \leq i \leq s$, then $C_A \subseteq C_A^{\perp_H}$.*

Example 4.1.3. *Let β be a primitive element of $\mathbb{F}_4$ and Let $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \beta & \beta^2 \\ 1 & \beta^2 & \beta \end{bmatrix} \in M_{3,3}(\mathbb{F}_4)$. Then A is invertible, $AA^\dagger = \mathrm{diag}(1,1,1)$, $\delta_1(A) = 3, \delta_2(A) = 2$ and $\delta_3(A) =$*

1 . *Let C_1, C_2 and C_3 be the linear codes of length 6 over $\mathbb{F}_4$ generated by*

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta^8 & \beta^{10} \end{bmatrix},$$

$$G_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 \end{bmatrix},$$

and

$$G_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

respectively. Then C_1, C_2 and C_3 are Hermitian self-orthogonal with parameters $[6,3,2]_4, [6,2,4]_4$ and $[6,1,6]_4$ respectively. Since $C_3 \subseteq C_2 \subseteq C_1$, by Theorems 2.3.1 and 4.1.1, C_A is a Hermitian self-orthogonal code with parameters $[18,6,6]_4$.

Next, a matrix-product construction for Hermitian self-orthogonal codes is studied while the Hermitian self-orthogonality of the input codes is relaxed.

Theorem 4.1.4. *Let $s \leq l$ be positive integers. Let $C_1, C_2, \ldots, C_s$ be linear codes of the same length over $\mathbb{F}_q$ and let $A \in M_{s\times l}(\mathbb{F}_q)$. If $AA^\dagger$ is anti-diagonal and $C_i \subseteq C_{s-i+1}^{\perp_H}$ for all $1 \leq i \leq s$, then $C_A \subseteq C_A^{\perp_H}$.*

Proof. Assume that $AA^\dagger = \text{adiag}(\lambda_1, \lambda_2, \ldots, \lambda_s)$ and $C_i \subseteq C_{s-i+1}^{\perp_H}$ for all $1 \leq i \leq s$. For each $1 \leq i \leq s$, let G_i be a generator matrix of the code C_i. Since $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1l} \\ a_{21} & a_{22} & \cdots & a_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sl} \end{bmatrix}$, the matrix-product code C_A is generated by

$$G = \begin{bmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{bmatrix}.$$

It follows that

$$GG^\dagger = \begin{bmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{bmatrix} \begin{bmatrix} a_{11}^rG_1^\dagger & a_{21}^rG_2^\dagger & \cdots & a_{s1}^rG_s^\dagger \\ a_{12}^rG_1^\dagger & a_{22}^rG_2^\dagger & \cdots & a_{s2}^rG_s^\dagger \\ \vdots & \vdots & \ddots & \vdots \\ a_{1l}^rG_1^\dagger & a_{2l}^rG_2^\dagger & \cdots & a_{sl}^rG_s^\dagger \end{bmatrix}$$

$$= \begin{bmatrix} 0(G_1G_1^\dagger) & \cdots & 0(G_1G_{s-1}^\dagger) & \lambda_1(G_1G_s^\dagger) \\ 0(G_2G_1^\dagger) & \cdots & \lambda_2(G_2G_{s-1}^\dagger) & 0(G_2G_s^\dagger) \\ \vdots & \cdots & \vdots & \vdots \\ \lambda_s(G_sG_1^\dagger) & \cdots & 0(G_sG_{s-1}^\dagger) & 0(G_sG_s^\dagger) \end{bmatrix}.$$

Since $C_i \subseteq C_{s-i+1}^{\perp_H}$ for all $1 \le i \le s$, we have $G_iG_{s-i+1}^\dagger = [\mathbf{0}]$ for all $1 \le i \le s$. Hence, $GG^\dagger = [\mathbf{0}]$. Therefore, $C_A \subseteq C_A^{\perp_H}$ as desired. $\square$

The following corollaries can be obtained directly from Theorem 4.1.4. The proofs are omitted.

Corollary 4.1.5. *If $A \in M_{s,s}(\mathbb{F}_q)$ is such that $AA^\dagger = \lambda J_s$ for some non-zero λ in $\mathbb{F}_q$ and $C_i \subseteq C_{s-i+1}^{\perp_H}$ for all $1 \le i \le s$, then $C_A \subseteq C_A^{\perp_H}$.*

Example 4.1.6. *Let β be a primitive element of $\mathbb{F}_4$ and let $A = \begin{bmatrix} 1 & \beta \\ \beta & 1 \end{bmatrix} \in M_{2,2}(\mathbb{F}_4)$ is invertible, $AA^\dagger = \mathrm{adiag}(1,1)$, $\delta_1(A) = 2$, and $\delta_2(A) = 1$. Let C_1 and C_2 be the linear codes of length 4 over $\mathbb{F}_4$ generated by*

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

and

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

respectively. Then C_1 and C_2 have parameters $[4,2,2]_4$ and $[4,1,4]_4$, respectively. Since $C_2 \subseteq C_1 \subseteq C_2^{\perp_H}$, by Theorems 2.3.1 and 4.1.4, C_A is a Hermitian self-orthogonal code with parameters $[8,3,4]_4$.

By choosing $C_i = C_{s-i+1}^{\perp_E}$ in Corollary 4.1.5, we have the following results.

Corollary 4.1.7. *If $A \in M_{s,s}(\mathbb{F}_q)$ is such that $AA^\dagger = \lambda J_s$ for some non-zero λ in $\mathbb{F}_q$ and $C_i = C_{s-i+1}^{\perp_H}$ for all $1 \le i \le s$, then C_A is Hermitian self-dual.*

4.2 Special Matrices and Applications

In order to apply the matrix-product constructions discussed in Section 4.1 to obtain Hermitian self-orthogonal codes, a matrix $A \in M_{s,l}(\mathbb{F}_q)$ with the property that $AA^\dagger$ is diagonal or anti-diagonal is required. To the best of our knowledge, there are no proper names for such matrices. For convenience, the following definitions are given. A matrix $A \in M_{s,l}(\mathbb{F}_q)$ is said to be *weakly semi-unitary* if $AA^\dagger$ is diagonal and it is said to be *weakly anti-semi-unitary* if $AA^\dagger$ is anti-diagonal. In the case where A is square, such matrices are called *weakly quasi-unitary* and *weakly anti-quasi-unitary*, respectively.

The existence and properties of such matrices are given as follows.

4.2.1 Weakly Quasi-Unitary Matrices

In this subsection, the existence of weakly quasi-unitary matrices defined are given as follows.

Lemma 4.2.1. *Let α be a primitive element of $\mathbb{F}_q$, where $q = r^2$ is a prime power. Then the following statements holds.*

1. *If q is odd, then $A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is invertible and (weakly) quasi-unitary with $\delta_1(A) = 2$ and $\delta_2(A) = 1$.*

2. *If $q > 2$ is even, then $A = \begin{bmatrix} 1 & \alpha \\ \alpha^r & 1 \end{bmatrix}$ is invertible and (weakly) quasi-unitary with $\delta_1(A) = 2$ and $\delta_2(A) = 1$.*

Proof. 1. Assume that q is odd and $A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Clearly, A is invertible, $\delta_1(A) = 2$ and $\delta_2(A) = 1$. Since

$$AA^T = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \mathrm{diag}(2,2),$$

A is (weakly) quasi-unitary.

2. Assume that $q > 2$ is even and let $A = \begin{bmatrix} 1 & \alpha \\ \alpha^r & 1 \end{bmatrix}$. Clearly, A is invertible, $\delta_1(A) = 2$ and $\delta_2(A) = 1$. Since

$$\begin{aligned} AA^\dagger &= \begin{bmatrix} 1 & \alpha \\ \alpha^r & 1 \end{bmatrix} \begin{bmatrix} 1 & \alpha^{r^2} \\ \alpha^r & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1+\alpha^{r+1} & \alpha^{r^2}+\alpha \\ \alpha^r+\alpha^r & 1+\alpha^{r+1} \end{bmatrix} \\ &= \begin{bmatrix} 1+\alpha^{r+1} & 0 \\ 0 & 1+\alpha^{r+1} \end{bmatrix} \\ &= \mathrm{diag}(1+\alpha^{r+1}, 1+\alpha^{r+1}), \end{aligned}$$

A is (weakly) quasi-unitary. □

Unitary matrices in Lemma 4.2.1 can be applied to construct Hermitian self-orthogonal codes as follows.

Corollary 4.2.2. *Let $\mathbb{F}_q$ be a finite field. If there exist Hermitian self-orthogonal $[m, k_1, d_1]_q$ and $[m, k_2, d_2]_q$ codes, then a Hermitian self-orthogonal $[2m, k_1 + k_2, d]_q$ code can be constructed with $d \geq \min\{2d_1, d_2\}$.*

Proof. Assume that there exist Hermitian self-orthogomal codes C_1 and C_2 with parameters $[m, k_1, d_1]_q$ and $[m, k_2, d_2]_q$. By Lemma 4.2.1, there exist a 2×2 invertible and (weakly) quasi-unitary matrix A over $\mathbb{F}_q$ with $\delta_1(A) = 2$ and $\delta_2(A) = 1$. By Theorems 2.3.1 and 4.1.1, the matrix-product code C_A is Hermitain self-orthogonal with parameters $[2m, k_1 + k_2, d]_q$ with $d \geq \min\{2d_1, d_2\}$. □

Example 4.2.3. *Let β be a primitive element of $\mathbb{F}_4$. By Lemma 4.2.1, we have that* $A = \begin{bmatrix} 1 & \beta \\ \beta^2 & 1 \end{bmatrix} \in M_{2,2}(\mathbb{F}_4)$ *is invertible,* $AA^\dagger = \operatorname{diag}(1+\beta^4, 1+\beta^4)$, $\delta_1(A) = 2$ *and* $\delta_2(A) = 1$. *Let C_1 and C_2 be the linear codes of length 4 over $\mathbb{F}_4$ generated by*

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

and

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

respectively. Then C_1 and C_2 are Hermitian self-orthogonal with parameters $[4,2,2]_4$ *and* $[4,2,1]_4$ *respectively. Since $C_2 \subseteq C_1$, by Theorem 2.3.1 and Corollary 4.2.2, C_A is a Hermitian self-orthogonal code with parameters* $[8,3,4]_4$.

Lemma 4.2.4. *Let M be a positive integer and let $q = r^2$ be a prime power. If $M|(r+1)$, then there exists a (weakly) quasi-unitary $M \times M$ matrix over $\mathbb{F}_q$ with $\delta_i(A) = M - i + 1$ for all $1 \le i \le M$.*

Proof. Assume that $M|(r+1)$. Then $\mathbb{F}_q$ contains a primitive M-th root unity. Let α be a fixed primitive M-th root unity in $\mathbb{F}_q$. Since $r \equiv -1 \bmod M$, we have

$$\overline{\alpha} = \alpha^r = \alpha^{-1}.$$

Define

$$A = \begin{bmatrix} (\alpha^0)^0 & (\alpha^1)^0 & \cdots & (\alpha^{M-1})^0 \\ (\alpha^0)^1 & (\alpha^1)^1 & \cdots & (\alpha^{M-1})^1 \\ \vdots & \vdots & \ddots & \vdots \\ (\alpha^0)^{M-1} & (\alpha^1)^{M-1} & \cdots & (\alpha^{M-1})^{M-1} \end{bmatrix}.$$

Let $B = AA^{\dagger}$. Then, for all $1 \leq i, j \leq M$, we have

$$\begin{aligned} b_{ij} &= \sum_{k=0}^{M-1} (\alpha^k)^{i-1} \overline{(\alpha^k)^{j-1}} = \sum_{k=0}^{M-1} (\alpha^k)^{i-1} \overline{(\alpha^k)}^{j-1} \\ &= \sum_{k=0}^{M-1} (\alpha^k)^{i-1} (\alpha^{-k})^{j-1} = \sum_{k=0}^{M-1} (\alpha^{i-j})^k \\ &= \begin{cases} M \neq 0 & \text{if } i = j, \\ 0 & \text{if otherwise.} \end{cases} \end{aligned}$$

Hence, $AA^{\dagger} = \operatorname{diag}(M, M, \ldots, M)$. Therefore, A is (weakly) quasi-unitary. From [2, Theorem 3.2], we have $\delta_i(A) = M - i + 1$ for all $1 \leq i \leq M$. □

Corollary 4.2.5. *Let q be a prime power and let M be positive integer such that $M|(r+1)$. If there exist Hermitian self-orthogonal $[m, k_1, d_1]_q$, $[m, k_2, d_2]_q, \ldots, [m, k_M, d_M]_q$ codes, then a Hermitian self-orthogonal $[Mm, k_1 + k_2 + \cdots + k_M, d]_q$ code can be constructed with $d \geq \min\{Md_1, (M-1)d_2, \ldots, d_M\}$.*

Proof. Assume that there are M Hermitian self-orthogonal codes with parameters $[m, k_1, d_1]_q$, $[m, k_2, d_2]_q, \ldots, [m, k_M, d_M]_q$. By Lemma 4.2.4, there exist a $M \times M$ invertible and quasi-unitary matrix A over $\mathbb{F}_q$ with $\delta_1(A) = M, \delta_2(A) = (M-1), \ldots, \delta_M(A) = 1$. By Theorems 2.3.1 and 4.1.1, the matrix-product code C_A is Hermitian self-orthogonal with parameters $[Mm, k_1 + k_2 + \cdots + k_M, d]_q$ with $d \geq \min\{Md_1, (M-1)d_2, \ldots, d_M\}$. □

Example 4.2.6. *Let α be a primitive element of $\mathbb{F}_4$. Then, α is primitive 3-root unity in $\mathbb{F}_4$. By lemma 4.2.4, we have that $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix}$ is invertible, $AA^{\dagger} =$ $\operatorname{diag}(1,1,1)$, $\delta_1(A) = 3, \delta_2(A) = 2$ and $\delta_1(A) = 1$. Let C_1 ,C_2 and C_3 be the linear codes of length 6 over $\mathbb{F}_4$ generated by*

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

,

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

and

$$G_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

respectively. Then $C_3 \subseteq C_2 \subseteq C_1$ *are Hermitian self-orthogonal with parameters* $[6,3,2]_4, [6,2,4]_4$ *and* $[6,1,6]_4$*, respectively. By Theorems 2.3.1 and 4.2.5* C_A *is a Hermitian self-orthogonal code with parameters* $[18,6,6]_4$*.*

4.2.2 Weakly Anti-Quasi-Unitary Matrices

In this subsection, we focus on the existence of weakly anti-quasi-unitary matrices. In a finite field $\mathbb{F}_q$ where $q = r^2$, the norm function $N : \mathbb{F}_q \to \mathbb{F}_r$ is defined by $N(\alpha) = \alpha^{r+1}$ for all α in $\mathbb{F}_q$. In [11, p. 57], it has been shown that N is surjective. Hence, we have the following lemma and corollaries can be deduced.

Lemma 4.2.7. *Let* α *be a primitive element of* $\mathbb{F}_q$*. Then the following statements hold.*

1. *If* q *is odd, then there exists* $b \in \mathbb{F}_q$ *such that* $b^{r+1} = -1$ *and* $A = \begin{bmatrix} 1 & b \\ b & 1 \end{bmatrix}$ *is invertible and (weakly) anti-quasi-unitary with* $\delta_1(A) = 2$ *and* $\delta_2(A) = 1$*.*

2. *If* $q > 2$ *is even, then* $A = \begin{bmatrix} \alpha & \alpha^r \\ 1 & 1 \end{bmatrix}$ *is invertible and (weakly) anti-quasi-unitary with* $\delta_1(A) = 2$ *and* $\delta_2(A) = 1$*.*

Proof. 1. Since the norm is surjective and $-1 \in \mathbb{F}_q$, there exists $b \in \mathbb{F}_q$ such that

$b^{r+1} = -1$. Let $A = \begin{bmatrix} 1 & b \\ b & 1 \end{bmatrix}$. Clearly, A is invertible, $\delta_1(A) = 2$ and $\delta_2(A) = 1$. Since

$$
\begin{aligned}
AA^{\dagger} &= \begin{bmatrix} 1 & b \\ b & 1 \end{bmatrix} \begin{bmatrix} b & b^r \\ b^r & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 + b^{r+1} & b + b^r \\ b + b^r & 1 + b^{r+1} \end{bmatrix} \\
&= \begin{bmatrix} 0 & b + b^r \\ b + b^r & 0 \end{bmatrix} \\
&= \operatorname{adiag}(b + b^r, b + b^r),
\end{aligned}
$$

A is (weakly) anti-quasi-unitary.

2. Assume that $q > 2$ is even and let $A = \begin{bmatrix} \alpha & \alpha^r \\ 1 & 1 \end{bmatrix}$. Clearly, A is invertible, $\delta_1(A) = 2$ and $\delta_2(A) = 1$. Since

$$
\begin{aligned}
AA^{\dagger} &= \begin{bmatrix} \alpha & \alpha^r \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \alpha^r & 1 \\ \alpha^{r^2} & 1 \end{bmatrix} \\
&= \begin{bmatrix} \alpha^{r+1} + \alpha^{r+1} & \alpha^r + \alpha \\ \alpha^r + \alpha & 1 + 1 \end{bmatrix} \\
&= \begin{bmatrix} 0 & \alpha^r + \alpha \\ \alpha^r + \alpha & 0 \end{bmatrix} \\
&= \operatorname{adiag}(\alpha^r + \alpha, \alpha^r + \alpha),
\end{aligned}
$$

A is (weakly) anti-quasi-unitary. □

Corollary 4.2.8. *Let $\mathbb{F}_q$ be a finite field of order $q > 2$. If there exist codes C_1 and C_2 with parameters $[m, k_1, d_1]_q$ and $[m, k_2, d_2]_q$ such that $C_1 \subseteq C_2^{\perp_H}$, then a Hermitian self-orthogonal $[2m, k_1 + k_2, d]_q$ code can be constructed with $d \geq \min\{2d_1, d_2\}$.*

Proof. Assume that there exist linear codes C_1 and C_2 with parameters $[m, k_1, d_1]_q$ and $[m, k_2, d_2]_q$ such that $C_1 \subseteq C_2^{\perp_H}$. By Lemma 4.2.7, there exist a 2×2 invertible and anti-quasi-orthogonal matrix A over $\mathbb{F}_q$ with $\delta_1(A) = 2$ and $\delta_2(A) = 1$. By Theorems 2.3.1 and 4.1.4, the matrix-product code C_A is Hermitian self-orthogonal with parameters $[2m, k_1 + k_2, d]_q$ with $d \geq \min\{2d_1, d_2\}$. $\square$

Example 4.2.9. *Let β be a primitive element of $\mathbb{F}_4$. By Lemma 4.2.7, we have that* $A = \begin{bmatrix} \beta & \beta^2 \\ 1 & 1 \end{bmatrix} \in M_{2,2}(\mathbb{F}_4)$ *is invertible,* $AA^\dagger = \mathrm{adiag}(1,1)$, $\delta_1(A) = 2$, *and* $\delta_2(A) = 1$. *Let C_1 and C_2 be the linear codes of length 6 over $\mathbb{F}_4$ generated by*

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \beta & \beta^2 & \beta^3 & \beta^3 & \beta^4 & \beta^5 \end{bmatrix}$$

and

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

respectively. Then C_1 and C_2 have parameters $[6, 2, 4]_4$ and $[6, 1, 6]_4$, respectively. Since $C_2 \subseteq C_1 \subseteq C_2^{\perp_H}$, by Theorems 2.3.1 and 4.1.4, C_A is a Hermitian self-orthogonal code with parameters $[12, 3, 6]_4$.

4.2.3 Summary

In this subsection, we summarize the existence of weakly quasi-unitary and weakly anti-quasi-unitary discussed in Subsections 4.2.1 and 4.2.2. These matrices play an important role in the matrix-product construction for Hermitain self-orthogonal codes. However, the existence of such matrices where the matrices have larger size or where the matrices are non-square is an interesting problem as well.

Table 4.1: Existence of Weakly Quasi-Unitary Matrices over $\mathbb{F}_q$, $q = r^2$

s \ r	$r \geq 2$
2	Lemma 4.2.1
$s \mid (r+1)$	Lemma 4.2.4
$s \neq 2 \wedge s \nmid (r+1)$	?

Note that ? indicates the case where such matrices are not studied in this work.

Table 4.2: Existence of Weakly Anti-Quasi-Unitary Matrices

$s \backslash q$	even	odd
2	Lemma 4.2.7	Lemma 4.2.7
$s \geq 3$	?	?

4.3 Examples

In this part, we focus on applications of Corollary 4.2.2. Based on Hermitian self-orthogonal codes in [8] and Corollary 4.2.2, Hermitian self-orthogonal codes with good parameters can be obtained.

In [8, Theorem 2.6], it has been shown that there exists a q-ary Hermitian self-orthogonal $[q+1, k, q-k+2]_q$ for all $2 \leq k \leq \frac{r}{2}$.

By setting C_1 and C_2 be a q-ary Hermitian self-orthogonal codes with parameter $[q+1, \lfloor \frac{r}{2} \rfloor, q - \lfloor \frac{r}{2} \rfloor + 2]$ and $[q+1, \lfloor \frac{r}{2} \rfloor - 1, q - \lfloor \frac{r}{2} \rfloor + 3]$ in Corollary 4.2.2, we have the following result.

Corollary 4.3.1. *Let $q = r^2$ be a prime power. Then a Hermitian self-orthogonal $[2(q+1), 2\lfloor \frac{r}{2} \rfloor - 1, d]_q$ code can be constructed with $d \geq q - \lfloor \frac{r}{2} \rfloor + 3$.*

Based on Corollary 4.3.1 and Hermitian self-orthogonal codes in [8], some examples of Hermitian self-orthogonal matrix-product codes over $\mathbb{F}_q$ with good parameters are given in Table 4.3.

Table 4.3: Hermitian self-Orthogonal Matrix-Product Codes over $\mathbb{F}_q$

q	Parametes		
	C_1	C_2	C_A
49	$[50, 3, 48]_{49}$	$[50, 2, 49]_{49}$	$[100, 5, d]_{49}$ with $d \geq 49$
64	$[65, 4, 62]_{64}$	$[65, 3, 63]_{64}$	$[130, 7, d]_{64}$ with $d \geq 63$
81	$[82, 4, 79]_{81}$	$[82, 3, 80]_{81}$	$[164, 7, d]_{81}$ with $d \geq 80$
121	$[122, 5, 118]_{121}$	$[122, 4, 119]_{121}$	$[244, 9, d]_{121}$ with $d \geq 119$

References

[1] T. Aaron, 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. 4735–4740, 2008.

[2] T. Blackmore and G. H. Norton, "Matrix-product code over $\mathbb{F}_q$," *Appl. Algebra Eng., Commun. Comput,* vol. 12, no. 6, pp. 477–500, 2001.

[3] M. Bouye and M. Saïd, "Matrix product codes over $\mathbb{F}_p$," *Gulf j. math.,* vol. 3, no. 2, pp. 44–48, 2015.

[4] 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, no. 3, p. 1350027, 2013.

[5] C. Galindo, F. Hernando, and D. Ruano, " New quantum codes from evaluation and matrix-product codes," *Finite Fields Appl.,* vol. 36, pp. 98–120, 2015.

[6] F. Hernando, K. Lally, and D. Ruano, "Construction and decoding of matrix-product codes from nested codes," *Appl. Algebra Eng., Commun. Comput,* vol. 20, pp. 497–507, 2009.

[7] W. C. Human and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.

[8] L. Jin, S. Ling, J. Luo, and C. Xing, "Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes," *IEEE Trans. Inf. Theory,* vol. 53, no. 9, pp. 4735–4740, 2010.

[9] L. Jin and C. Xing, "Euclidean and Hermitian self-orthogonal algebraic geometry and their application to quantum codes," *IEEE Trans. Inf. Theory,* vol. 58, no. 8, pp. 5484–5489, 2012.

[10] N. Koblitz, A Course in Number Theory and Cryptography. 2d ed. New York: Springer-Verlag.

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

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

[13] X. Liu, H. Liu, and L. Yu. (2016, Aug. 1). *On new quantum codes from matrix product codes* [Online]. Available: https://arxiv.org/abs/1604.05823.

[14] V. Pless, "A classification of self-orthogonal codes over GF(2)," *Discrete Math,* vol. 3, no. 1–3, pp. 209–246, 1972.

[15] T. Zhang and G. Ge. (2016, Aug. 1). *Quantum codes from generalized Reed-Solomon codes and matrix-product codes.* [Online]. Available: http://arxiv.org/abs/1508.00978.

Presentations and Publications

Presentations

● M. Todsapol and S. Jitman, *Matrix-Product construction for self-orthogonal linear codes*, Proceedings of the 12^{th} International Conference On Mathematics, Statistics and Their Applications, Syiah Kuala University, Banda Aceh Indonesia, 4-6 October, 2016.

Publications

● M. Todsapol and S. Jitman, *Matrix-product construction for self-orthogonal linear codes*, Proceedings of the International Conference On Mathematics, Statistics and Their Applications (ICMSA), Banda Aech, Indonesia, accepted.

Biography

Name	Mr. Todsapol Mankeamn
Address	81/5 Village No.5, Banleam Sub-district, Banleam District, Phetchaburi, 76110.
Date of Birth	13 July 1991
Education	
2013	Bachelor of Science in Mathematics, (First Class Honors), Silpakorn University.
2016	Master of Science in Mathematics, Silpakorn University.
Scholarship	Development and Promotion of Science and Technology Talents Project (DPST).