Chamchuri Journal of Mathematics
Volume 9(2017), 35–51
http://www.math.sc.chula.ac.th/cjm

Matrix-Product Constructions for Hermitian Self-Orthogonal Codes

Somphong Jitman*,† and Todsapol Mankean

Received 25 October 2017
Revised 30 November 2017
Accepted 30 November 2017

Abstract: Self-orthogonal codes have been of interest due to there rich algebraic structures and wide applications. Euclidean self-orthogonal codes have been quite well studied in literature. Here, Hermitian self-orthogonal codes have been investigated. Constructions of such codes have been given based on the well-known matrix-product construction for linear codes. Criterion for the underlying matrix and the input codes required in such constructions have been determined. In many cases, the Hermitian self-orthogonality of the input codes and the assumption that the underlying matrix is unitary can be relaxed. Some special matrices used in the constructions and illustrative examples of good Hermitian self-orthogonal codes have been provided as well.

Keywords: matrix-product codes, Hermitian self-orthogonal codes, quasi-unitary matrices

2000 Mathematics Subject Classification: 94B05, 94B60

1 Introduction

Self-orthogonal codes constitute an important class of linear codes due to their rich algebraic structures and wide applications (see [8], [9], [15], [16], and references

* *Corresponding author*
† *The author is supported by the Thailand Research Fund under Research Grant MRG6080012.*

therein). In [2], a nice construction that can produce linear codes with explicit and good parameters has been introduced, namely, a matrix-product construction. The said construction can be viewed as a generalization of the well-known $(u|u+v)$-construction and $(u+v+w|2u+v|u)$-construction (see [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] has been shown to be sharped in [6].

In [5], the matrix-product construction has been applied in constructing Euclidean self-orthogonal codes in the case where the underlying matrix is a square orthogonal matrix. In the same fashion, this idea has been extended to construct Hermitian self-orthogonal codes in [13] and [16]. However, in both cases, the input codes are required to be self-orthogonal and the underlying matrix must be either orthogonal or unitary. For the Euclidean case, the Euclidean self-orthogonality of the input codes and the assumption that the matrix is orthogonal have been relaxed in [14].

In this paper, we extend the concept in [14] to cover the Hermitian case. The Hermitian self-orthogonality of the input codes and the assumption that the underlying is unitary can be relaxed in many cases. Matrices used in the constructions are studied together with examples of some good Hermitian self-orthogonal matrix-product codes.

The paper is organized as follows. Some basic properties of matrices, linear codes, self-orthogonal codes, and matrix-product codes are recalled in Section 2. Two matrix-product constructions for Hermitian self-orthogonal codes are discussed in Section 3. In Section 4, the study of special matrices over finite fields is given. Illustrative examples of good matrix-product Hermitian self-orthogonal codes are provided in Section 5.

2 Preliminaries

Let q be a prime power and let $\mathbb{F}_q$ denote the finite field of order q. Some properties of matrices and codes over $\mathbb{F}_q$ used in this paper are recalled in the following subsections.

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 from $\mathbb{F}_q$. 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.

Assume that $q = r^2$ is square. For a matrix $A = [a_{ij}] \in M_{s,l}(\mathbb{F}_q)$, let $A^\dagger := [\overline{a_{ji}}] \in M_{s,l}(\mathbb{F}_q)$, where $\overline{a} := a^r$ for all $a \in \mathbb{F}_q$. In this paper, a matrix $A \in M_{s,l}(\mathbb{F}_q)$ with the property that $AA^\dagger$ is diagonal or anti-diagonal is required in the constructions of Hermitian self-orthogonal codes. 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. A matrix $A \in M_{s,s}(\mathbb{F}_q)$ is called a *unitary matrix* if $AA^\dagger = I_s$ and it is called a *quasi-unitary matrix* if $AA^\dagger = \lambda I_s$ for some non-zero $\lambda \in \mathbb{F}_q$.

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 $\mathbb{F}_q$. 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 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 weight* $d(C)$ of C is

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

where $\mathrm{wt}(\boldsymbol{u})$ is the number of nonzero entries in $\boldsymbol{u}$. A $k \times n$ matrix G over $\mathbb{F}_q$ is called a *generator matrix* for an $[n, k, d]_q$ code C if the rows of G form a basis of C.

In addition, assume that $q = r^2$ is a square. For $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n$, let $\overline{\boldsymbol{v}} := (\overline{v_1}, \overline{v_2}, \ldots, \overline{v_n})$, where $\overline{a} := a^r$ for all $a \in \mathbb{F}_q$. 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 *Hermitian inner product* of $\boldsymbol{u}$ and $\boldsymbol{v}$ is defined by

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

The *Hermitian dual* of a linear code $C \subseteq \mathbb{F}_q^n$ is defined to be the set

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

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

For linear codes C_1 and C_2 of the same length over $\mathbb{F}_q$, it is well known that if C_i is generated by G_i for $i \in \{1, 2\}$, then $G_1 G_2^\dagger = [\mathbf{0}]$ if and only if $C_1 \subseteq C_2^{\perp_H}$. Especially, $G_1 G_1^\dagger = [\mathbf{0}]$ if and only if C_1 is Hermitian self-orthogonal.

2.3 Matrix-Product Codes

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

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

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 weight 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 are given in the following theorem.

Theorem 2.1. *Assume the notations above. Then 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 $\mathrm{d}(C_A) = \min_{1\leq i\leq s}\{d_i\delta_i(A)\}$.

From now on, we assume that $q = r^2$ is a square and focus on the dual of a matrix product code with respect to the Hermitian inner product. If A is an invertible square matrix, the Hermitian dual of a matrix-product codes is again matrix-product and determined as follows.

Theorem 2.2. *Assume the notation above and $s = \ell$. If A is a nonsingular $s \times s$ matrix, then*

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

From Theorem 2.2, a matrix-product construction has been applied for Hermitian self-orthogonal codes in [13] and [16], where A is a $s \times s$ unitary matrix and the input codes C_i' are Hermitian self-orthogonal.

In general the Hermitian dual of a matrix-product code does not need to be matrix-product. In this paper, we focus on this general set up for Hermitian self-orthogonal matrix-product codes. The restriction on the Hermitian self-orthogonality of the input codes and the condition that A is unitary can be relaxed in many cases. The detailed constructions are given in the next section.

3 Constructions

In this section, we focus on two types of matrix-product constructions for Hermitian self-orthogonal linear codes. Sufficient conditions on the matrix and the input codes for matrix-product codes to be Hermitian self-orthogonal are given.

In the following theorem, a matrix-product construction for Hermitian self-orthogonal codes whose input codes are Hermitian self-orthogonal is discussed. The results 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 3.1. *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. Assume that $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1l} \\ a_{21} & a_{22} & \cdots & a_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sl} \end{bmatrix}$. Then 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

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

Since $C_i \subseteq C_i^{\perp_H}$ for all $1 \leq i \leq s$, we have $G_iG_i^\dagger = [\mathbf{0}]$ 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 3.2. *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 3.3. Let β be a primitive element of $\mathbb{F}_4$ and let $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \beta & \beta^2 \\ 1 & \beta^2 & \beta \end{bmatrix}$. 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

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta^8 & \beta^{10} \end{bmatrix}, \quad G_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 \end{bmatrix},$$

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 2.1 and 3.1, C_A is a Hermitian self-orthogonal code with parameters $[18,6,6]_4$.

In the following theorem, a matrix-product construction for Hermitian self-orthogonal codes is studied in the case where the Hermitian self-orthogonality of the input codes are relaxed.

Theorem 3.4. *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 $AA^\dagger = \mathrm{adiag}(\lambda_1, \lambda_2, \ldots, \lambda_s)$ 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. Write $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1l} \\ a_{21} & a_{22} & \cdots & a_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sl} \end{bmatrix}$. Then 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

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

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

The following results can be deduced directly from Theorem 3.4. The proofs are omitted.

Corollary 3.5. *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 $1 \leq i \leq s$, then $C_A \subseteq C_A^{\perp_H}$.*

Example 3.6. Let β be a primitive element of $\mathbb{F}_4$. Then $A = \begin{bmatrix} 1 & \beta \\ \beta & 1 \end{bmatrix}$ 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

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

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 Theorem 2.1 and Corollary 3.5, C_A is a Hermitian self-orthogonal code with parameters $[8,3,4]_4$.

By choosing $C_i = C_{s-i+1}^{\perp_H}$ in Corollary 3.5, we have the following result.

Corollary 3.7. *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 $1 \leq i \leq s$, then C_A is Hermitian self-dual.*

4 Special Matrices and Applications

As discussed in Section 3, a full-row-rank matrix $A \in M_{s,l}(\mathbb{F}_q)$ with the property that $AA^\dagger$ is diagonal or anti-diagonal is required in the matrix-product construction for Hermitian self-orthogonal codes. From Theorem 2.1, the minimum Hamming weight of the output code depends on the sequence $\{\delta_i(A)\}_{i=1,2,\ldots,s}$. In most cases, the output code has large minimum Hamming weight if the sequence $\{\delta_i(A)\}_{i=1,2,\ldots,s}$ is decreasing.

In this section, a certification for the existence of weakly quasi-unitary and weakly anti-quasi-unitary matrices A over some finite fields with the property that $\{\delta_i(A)\}_{i=1,2,\ldots,s}$ is a decreasing sequence. Precise applications of such matrices in constructing Hermitian self-orthogonal codes are explained.

4.1 Weakly Quasi-Unitary Matrices

In this subsection, some weakly quasi-unitary matrices with the property that the sequence $\{\delta_i(A)\}_{i=1,2,\ldots,s}$ is decreasing are given as well as their applications in a matrix-product construction of Hermitian self-orthogonal codes.

First, we consider 2×2 (weakly) quasi-unitary matrices over an arbitrary finite field of square order greater than 4.

Lemma 4.1. *Let r be a prime power and $q = r^2$. Let α be a primitive element of $\mathbb{F}_q$. Then one of the following statements holds.*

1. *If q is odd, then $A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \in M_{2,2}(\mathbb{F}_q)$ is invertible and (weakly) quasi-unitary with $\delta_1(A) = 2$ and $\delta_2(A) = 1$.*
2. *If $q \geq 16$ is even, then $A = \begin{bmatrix} 1 & \alpha \\ \alpha^r & 1 \end{bmatrix} \in M_{2,2}(\mathbb{F}_q)$ is invertible and (weakly) quasi-unitary with $\delta_1(A) = 2$ and $\delta_2(A) = 1$.*

Proof. To prove (1), assume that q is odd. Let $A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. 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.

To prove (2), assume that $q > 2$ is even. 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

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

A is (weakly) quasi-unitary. □

Remark 4.2. We note that for every 2×2 matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ over $\mathbb{F}_4$, if $\delta_1(A) = 2$, then a and b are non-zeros. Hence, the top-left conner of $AA^\dagger$ is $a^3 + b^3 = 1 + 1 = 0$. Hence, A cannot be weakly quasi-unitary. Therefore, there are no weakly quasi-unitary matrices in $M_{2,2}(\mathbb{F}_4)$ with $\delta_1(A) = 2$ and $\delta_2(A) = 1$.

Quasi-unitary matrices in Lemma 4.1 can be applied to construct Hermitian self-orthogonal codes as follows.

Corollary 4.3. *Let $r \geq 3$ be a prime power and let $q = r^2$. 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-orthogonal codes C_1 and C_2 with parameters $[m, k_1, d_1]_q$ and $[m, k_2, d_2]_q$. By Lemma 4.1, 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 2.1 and 3.1, the matrix-product code C_A is Hermitian self-orthogonal with parameters $[2m, k_1 + k_2, d]_q$ with $d \geq \min\{2d_1, d_2\}$. □

Example 4.4. Let β be a primitive element of $\mathbb{F}_{16}$. By Lemma 4.1, we have that $A = \begin{bmatrix} 1 & \beta \\ \beta^2 & 1 \end{bmatrix}$ is invertible, $AA^\dagger = \mathrm{diag}(1+\beta^5, 1+\beta^5)$, $\delta_1(A) = 2$ and $\delta_2(A) = 1$. Let C_1 and C_2 be the linear codes of length 4 over $\mathbb{F}_{16}$ generated by

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

respectively. Then C_1 and C_2 are Hermitian self-orthogonal with parameters $[4, 2, 2]_{16}$ and $[4, 2, 1]_{16}$ respectively. Since $C_2 \subseteq C_1$, by Theorem 2.1 and Corollary 4.3, C_A is a Hermitian self-orthogonal code with parameters $[8, 3, 4]_{16}$.

Next, we focus on $M \times M$ (weakly) quasi-unitary matrices over $\mathbb{F}_q$, where $M \geq 2$ is an integer.

Lemma 4.5. *Let r be a prime power and $q = r^2$. Let M be a positive integer. If $M|(r+1)$, then there exists an $M \times M$ (weakly) quasi-unitary matrix over $\mathbb{F}_q$ with $\delta_i(A) = M - i + 1$ for all $1 \leq i \leq M$.*

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

Corollary 4.6. *Let r be a prime power and $q = r^2$. Let M be a 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 4.5, there exist an $M \times M$ 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 2.1 and 3.1, 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 4.7. Let α be a primitive element of $\mathbb{F}_4$. Then α is primitive 3th root unity in $\mathbb{F}_4$. By Lemma 4.5, it follows that $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix}$ is invertible, $AA^\dagger = \mathrm{diag}(1, 1, 1)$, $\delta_1(A) = 3, \delta_2(A) = 2$ 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

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \quad G_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha \end{bmatrix}$$

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 2.1 and 4.6 C_A is a Hermitian self-orthogonal code with parameters $[18, 6, 6]_4$.

4.2 Weakly Anti-Quasi-Unitary Matrices

In this subsection, we focus on the existence of weakly anti-quasi-unitary matrices with the property that the sequence $\{\delta_i(A)\}_{i=1,2,\ldots,s}$ is decreasing. Their applications in constructing Hermitian self-orthogonal codes are discussed as well.

In a finite field $\mathbb{F}_q$ with $q = r^2$, 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, the following lemma and corollaries can be deduced.

Lemma 4.8. *Let r be a prime power and $q = r^2$. 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 $q \geq 4$ 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. To prove (1), assume that q is odd. Since the norm is surjective, there exists $b \in \mathbb{F}_q$ such that $N(b) = b^{r+1} = -1$. Let $A = \begin{bmatrix} 1 & b \\ b & 1 \end{bmatrix}$. Clearly, A is invertible, $\delta_1(A) = 2$ and $\delta_2(A) = 1$. Since

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

A is (weakly) anti-quasi-unitary.

To prove (2), assume that $q \geq 4$ is even. 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

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

A is (weakly) anti-quasi-unitary. □

Corollary 4.9. *Let r be a prime power and $q = r^2$. 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 4.8, 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 2.1 and 3.4, the matrix-product code C_A is Hermitian self-orthogonal with parameters $[2m, k_1 + k_2, d]_q$ with $d \geq \min\{2d_1, d_2\}$. □

Example 4.10. Let β be a primitive element of $\mathbb{F}_4$. By Lemma 4.8, 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

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \beta & \beta^2 & \beta^3 & \beta^3 & \beta^4 & \beta^5 \end{bmatrix} \quad \text{and} \quad G_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

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 2.1 and 3.4, C_A is a Hermitian self-orthogonal code with parameters $[12,3,6]_4$.

5 Examples

In this section, examples of Hermitian self-orthogonal matrix-product codes with good parameters are given.

Using Corollary 4.3 and Hermitian self-orthogonal codes form various sources, Hermitian self-orthogonal matrix product codes can be constructed. Here, Hermitian self-orthogonal codes given in [8] are applied in Corollary 4.3, and hence, Hermitian self-orthogonal matrix-product codes with good parameters are obtained.

In [8, Theorem 2.6], it has been shown that there exists a Hermitian self-orthogonal $[q+1, k, q-k+2]_q$ code for all $2 \le k \le \frac{r}{2}$, where $q = r^2$. By setting C_1 and C_2 be Hermitian self-orthogonal codes with parameter $[q+1, \lfloor \frac{r}{2} \rfloor, q - \lfloor \frac{r}{2} \rfloor + 2]_q$ and $[q+1, \lfloor \frac{r}{2} \rfloor - 1, q - \lfloor \frac{r}{2} \rfloor + 3]_q$ in Corollary 4.3, we have the following result.

Corollary 5.1. *Let r be a prime power and $q = r^2$. Then a Hermitian self-orthogonal $[2(q+1), 2\lfloor \frac{r}{2} \rfloor - 1, d]_q$ code can be constructed with $d \ge q - \lfloor \frac{r}{2} \rfloor + 3$.*

From Corollary 5.1, some examples of Hermitian self-orthogonal matrix-product codes over $\mathbb{F}_q$ are given in Table 5.

Next, we focus on examples of Hermitian self-orthogonal matrix-product codes derived from Corollary 4.9. For this case, good input codes can be chosen from the family of Generalized Reed-Solomon (GRS) codes recalled as follows.

For each positive integer $n \le q$, let $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n)$ and $w = (w_1, w_2, \ldots, w_n)$ where γ_i is a non-zero element and $w_1, w_2, \ldots w_n$ are distinct elements in $\mathbb{F}_q$. For each $0 \le k \le n$, denote by $\mathbb{F}_q[X]_k$ the set of all polynomials of degree less than k over $\mathbb{F}_q$. For convenience, the degree of the zero polynomial is defined to be -1.

q	Parameters		
	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 $d \geq 119$

Table 1: Hermitian Self-Orthogonal Matrix-Product Codes over $\mathbb{F}_q$

A *GRS code* of length $n \leq q$ and dimension $k \leq n$ is defined to be

$$GRS_{n,k}(\gamma, w) := \{(\gamma_1 f(w_1), \gamma_2 f(w_2), \ldots, \gamma_n f(v_n)) \mid f(X) \in \mathbb{F}_q[X]_k\}. \quad (1)$$

It is well known (see [8]) that the $GRS_{n,k}(w, \gamma)$ is a linear code with parameters $[n, k, n-k+1]_q$ and the Hermitian dual $(GRS_{n,k}(w, \gamma))^{\perp_H}$ of $GRS_{n,k}(w, \gamma)$ is also a GRS code with parameters are $[n, n-k, k+1]_q$. Moreover, $GRS_{n,k}(w, \gamma) \subsetneq GRS_{n,k+1}(w, \gamma)$. By letting $C_1 = GRS_{n,k}(w, \gamma)$ and $C_2 = (GRS_{n,k+i}(w, \gamma))^{\perp_H}$ (with $0 \leq i \leq n-k$) in Corollary 4.9, we have the following corollary.

Corollary 5.2. *Let r be a prime power and let $q = r^2$. Let $0 \leq k \leq n \leq q$ be integers. Then there exists a Hermitian self-orthogonal matrix-product code with parameters $[2n, n-i, d]_q$ for all $0 \leq i \leq n-k$, where $d \geq \min\{2(n-k+1), k+i+1\}$.*

Some examples of good Hermitian self-orthogonal codes over small finite fields derived from Corollary 5.2 of length $2q$ are given in Table 5.

For the special case where $i = 0$, or equivalently, $C_1 = GRS_{n,k}(w, \gamma)$ and $C_2 = C_1^{\perp_H} = (GRS_{n,k}(w, \gamma))^{\perp_H}$, a Hermitian self-dual matrix-product code can be constructed via Corollaries 3.7 and 5.2.

Corollary 5.3. *Let r be a prime power and let $q = r^2$. Let $0 \leq l \leq n \leq q$ be integers. Then there exists a Hermitian self-orthogonal matrix-product code with parameters $[2n, n, d]_q$ with $d \geq \min\{2(n-k+1), k+1\}$.*

6 Conclusion and Remarks

The well-known matrix-product construction for linear codes has been applied to construct Hermitian self-orthogonal codes. Criterion for the underlying matrices

q	n	k	i	Parameters
9	9	5	4	$[18, 5, d]_9$ with $d \geq 10$
		6	1	$[18, 8, d]_9$ with $d \geq 8$
16	16	9	6	$[32, 10, d]_{16}$ with $d \geq 16$
		10	3	$[32, 13, d]_{16}$ with $d \geq 14$
		11	0	$[32, 16, d]_{16}$ with $d \geq 12$
25	25	13	12	$[50, 13, d]_{25}$ with $d \geq 26$
		14	9	$[50, 16, d]_{25}$ with $d \geq 24$
		15	6	$[50, 19, d]_{25}$ with $d \geq 22$
		16	3	$[50, 22, d]_{25}$ with $d \geq 20$
		17	0	$[50, 25, d]_{25}$ with $d \geq 18$
49	49	25	24	$[98, 25, d]_{49}$ with $d \geq 50$
		26	21	$[98, 28, d]_{49}$ with $d \geq 48$
		27	18	$[98, 31, d]_{49}$ with $d \geq 46$
		28	15	$[98, 34, d]_{49}$ with $d \geq 44$
		29	12	$[98, 37, d]_{49}$ with $d \geq 42$
		30	9	$[98, 40, d]_{49}$ with $d \geq 40$
		31	6	$[98, 43, d]_{49}$ with $d \geq 38$
		32	3	$[98, 46, d]_{49}$ with $d \geq 36$
		33	0	$[98, 49, d]_{49}$ with $d \geq 34$

Table 2: Hermitian Self-Orthogonal Matrix-Product Codes over $\mathbb{F}_q$

and the input codes required in the constructions have been determined. In many cases, the Hermitian self-orthogonality of the input codes and the assumption that the underlying matrix is unitary can be relaxed. Illustrative examples of good Hermitian self-orthogonal codes have been given as well.

Some special matrices used in the constructions such as weakly quasi-unitary and weakly anti-quasi-unitary matrices have been given in some cases. In general, the study of a matrix $A \in M_{s,l}(\mathbb{F}_q)$ such that $AA^\dagger$ is diagonal or anti-diagonal is also an interesting problem.

For applications, it is well know that Hermitian self-orthogonal codes can be applied in constructing symmetric quantum codes (see, for example, [8], [9], [16], and [13]). Hence, the codes obtained in this paper can be applied in the such constructions as well.

References

[1] T. Aaron, J. L. Kim, Y. Lee, and C. Xing, New MDS or near-MDS self-dual codes, *IEEE Trans. Inf. Theory*, **54**(2008), 4735–4740.

[2] T. Blackmore and G. H. Norton, Matrix-product code over $\mathbb{F}_q$, *Appl. Algebra Eng., Commun. Comput.*, **12**(2001), 477–500.

[3] M. Bouye and M. Saïd, Matrix product codes over $\mathbb{F}_p$, *Gulf j. math.*, **3** (2015) 44–48.

[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*, **11**(2013), 1350027.

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

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

[7] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 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*, **53**(2010), 4735–4740.

[9] L. Jin and C. Xing, Euclidean and Hermitian self-orthogonal algebraic geometry and their application to quantum codes, *IEEE Trans. Inf. Theory*, **58**(2012), 5484–5489.

[10] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, 1994.

[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. Q. Dinh H. Liu, and L. Yu, On new quantum codes from matrix product codes, *Cryptography and Communications,* (in press, 2017).

[14] T. Mankean and S. Jitman, Matrix-product constructions for self-orthogonal linear codes, in *IEEE Conference Publications, 2016* 12*th International Conference on Mathematics, Statistics, and Their Applications (ICMSA)*, Banda Aceh, Indonesia (2016), 6-10.

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

[16] T. Zhang and G. Ge, Quantum codes from generalized Reed-Solomon codes and matrix-product codes [Online]. Available: http://arxiv.org/abs/1508.00978.

Somphong Jitman
Department of Mathematics, Faculty of Science, Silpakorn University
Nakhon Pathom 73000, Thailand
Email: sjitman@gmail.com

Todsapol Mankean
Department of Mathematics, Faculty of Science, Silpakorn University
Nakhon Pathom 73000, Thailand
Email: tong.todsapol2@gmail.com