Quantum error-correcting codes from matrix-product codes related to quasi-orthogonal matrices and quasi-unitary matrices

Meng Cao *

Yau Mathematical Sciences Center, Tsinghua University, Beijing, 100084, China

Abstract

Matrix-product codes over finite fields are an important class of long linear codes by combining several commensurate shorter linear codes with a defining matrix over finite fields. The construction of matrix-product codes with certain self-orthogonality over finite fields is an effective way to obtain good $q$-ary quantum codes of large length. Specifically, it follows from CSS construction (resp. Hermitian construction) that a matrix-product code over $\mathbb{F}_q$ (resp. $\mathbb{F}_{q^2}$) which is Euclidean dual-containing (resp. Hermitian dual-containing) can produce a $q$-ary quantum code. In order to obtain such matrix-product codes, a common way is to construct quasi-orthogonal matrices (resp. quasi-unitary matrices) as the defining matrices of matrix-product codes over $\mathbb{F}_q$ (resp. $\mathbb{F}_{q^2}$). The usage of NSC quasi-orthogonal matrices or NSC quasi-unitary matrices in this process enables the minimum distance lower bound of the corresponding quantum codes to reach its optimum. This article has two purposes: the first is to summarize some results of this topic obtained by the author of this article and his cooperators in [11–13]; the second is to add some new results on quasi-orthogonal matrices (resp. quasi-unitary matrices), Euclidean dual-containing (resp. Hermitian dual-containing) matrix-product codes and $q$-ary quantum codes derived from these newly constructed matrix-product codes.

Keywords: Quantum codes; matrix-product codes; quasi-orthogonal matrices; quasi-unitary matrices; NSC matrices

Mathematics Subject Classification (2010): 11T55, 11T71, 81P45, 94B05

*E-mail address: caom17@tsinghua.org.cn; mengcaomath@126.com (M. Cao).


## Contents

1. Introduction ................................................. 3

2. Preliminaries .............................................. 6
   2.1 Classical error-correcting codes .......................... 6
   2.2 GRS codes and extended GRS codes ......................... 8
   2.3 Matrix-product codes ..................................... 9
   2.4 Quantum codes .......................................... 10

3. Quantum codes from Euclidean dual-containing matrix-product codes 11
   3.1 Basic concepts and properties ............................. 11
   3.2 General approach for constructing quantum codes via Euclidean dual-containing matrix-product codes ......................... 13
   3.3 Quantum codes related to quasi-orthogonal matrices .............. 14
      3.3.1 The utilization of the theory of quadratic forms .......... 14
      3.3.2 The utilization of the theory of quadratic sum .......... 15
      3.3.3 The utilization of the Hadamard matrices ............... 16
   3.4 Quantum codes related to NSC quasi-orthogonal matrices ............. 17
   3.5 Quantum codes related to special matrices $A$ with $AA^T$ being monomial matrices 26

4. Quantum codes from Hermitian dual-containing matrix-product codes 27
   4.1 Basic concepts and properties ............................. 27
   4.2 General approach for constructing quantum codes via Hermitian dual-containing matrix-product codes ......................... 28
   4.3 Quantum codes related to quasi-unitary matrices .................. 29
      4.3.1 Quantum codes related to quasi-unitary matrices for odd prime power $q$ ........................................ 30
      4.3.2 Quantum codes related to a $2^m \times 2^m$ quasi-unitary matrices ........................................ 31
   4.4 Quantum codes related to NSC quasi-unitary matrices .............. 32
   4.5 Quantum codes related to $k \times k$ NSC quasi-unitary matrices for any $k < q$ ................. 37
   4.6 Quantum codes related to special matrices $A$ with $AA^\dagger$ being monomial matrices 40

5. Concluding remarks ........................................... 41
   5.1 Main results and remarks .................................. 41
   5.2 Further discussion ...................................... 43

References .................................................. 44
1 Introduction

It is well known that quantum error-correcting codes (quantum codes, for short) are indispensable to quantum computation and quantum communication. They were introduced to deal with the problems of decoherence and quantum noise in quantum information. After the pioneering research in [7, 47, 49], the theory of quantum codes has experienced a rapid development over the past two decades. A great deal of research are focused on finding quantum codes with good parameters. Usually, we use the notation $[[n, k, d]]_q$ to represent a $q$-ary quantum code with length $n$, dimension $q^k$ and minimum distance $d$. It has the abilities to detect up to $d - 1$ quantum errors and correct up to $\lfloor \frac{d - 1}{2} \rfloor$ quantum errors. Naturally, we know that for a fixed length $n$ and a fixed dimension $q^k$ (or $k$), the larger value of $d$ means the better performance of error detection and error correction of the quantum code.

As we know, constructing quantum codes with good parameters is significant and difficult. The CSS construction (see Theorem 3.1 for details), introduced by Calderbank and Shor [9] and Steane [50], is a powerful method to construct $q$-ary quantum codes from classical codes with self-orthogonality over the finite field $\mathbb{F}_q$. To be more specific, any Euclidean self-orthogonal or Euclidean dual-containing code over $\mathbb{F}_q$ will produce a $q$-ary $[[n, 2k - n, \geq d]]$ quantum code. The Hermitian construction is currently one of the most frequently-used methods for constructing good $q$-ary quantum codes from classical codes such as cyclic codes (e.g., see [1, 15, 34, 35, 57]), generalized Reed-Solomon (abbreviated to GRS) codes (e.g., see [31, 32, 38, 58]) and matrix-product codes (e.g., see [11, 13, 33, 40, 42, 56]). In brief, both CSS construction and Hermitian construction establish the close relationship between classical codes and quantum codes, which enable us to construct new quantum codes in a convenient way.

The matrix-product code

$$C(A) = [C_1, C_2, \ldots, C_k]A$$

over finite fields is an interesting classical linear code with larger length by combining several commensurate linear codes $C_1, C_2, \ldots, C_k$, i.e., constituent codes with the same length, with a defining matrix $A$ over finite fields. This concept was proposed by Blackmore and Norton [4] in 2001, the same year that the Hermitian construction was proposed. Let $C_i$ be an $[n, t_i, d_i]_q$ linear code for $i = 1, 2, \ldots, k$ and $A$ be an $k \times s$ matrix over $\mathbb{F}_q$ with $k \leq s$. It is known from [4]
that the matrix-product code $C(A)$ has length $sn$ and dimension $\sum_{i=1}^{k} t_i$ (see also [45]). Besides, the minimum distance of $C(A)$, denoted by $d(C(A))$, is investigated in the following cases.

- In [4], Blackmore and Norton proved that if the defining matrix $A$ is non-singular by columns (abbreviated to NSC, see Definition 3.6 for details), then $d(C(A)) \geq \min_{1 \leq i \leq k} \{(s + 1 - i)d_i\}$. Moreover, they proved that if $A$ is NSC and it is a column permutation of an upper triangular matrix, then $d(C(A)) = \min_{1 \leq i \leq k} \{(s + 1 - i)d_i\}$.

- In [45], Özbudak and Stichtenoth proved that $d(C(A)) \geq \min_{1 \leq i \leq k} \{D_i(A)d_i\}$ for any full-rank defining matrix $A$, where $D_i(A)$ denotes the minimum distance of the code on $F_{s^q}$ generated by the first $i$ rows of $A$.

- In [28], Hernando et al. proved that $d(C(A)) = \min_{1 \leq i \leq k} \{D_i(A)d_i\}$ if $C_1 \supset C_2 \supset \cdots \supset C_k$ and the defining matrix $A$ has full rank. They also deduced that $d(C(A)) = \min_{1 \leq i \leq k} \{(s + 1 - i)d_i\}$ if $C_1 \supset C_2 \supset \cdots \supset C_k$ and $A$ is NSC.

By CSS construction or Hermitian construction, we can construct new $q$-ary quantum codes of large lengths and dimensions from the matrix-product codes that are Euclidean dual-containing or Hermitian dual-containing. The minimum distance or minimum distance lower bound of a matrix-product code can be easily determined from the above three cases. Therefore, we desire to know under which condition the matrix-product codes will be Euclidean dual-containing or Hermitian dual-containing. This leads to a question: what is the Euclidean dual code (resp. Hermitian dual code) of a matrix-product code over $F_{q^2}$? To this end, the defining matrix of a matrix-product code is usually set to be a non-singular matrix.

The solution to the question is listed as follows.

- In [4], Blackmore and Norton proved that

\[(C_1, C_2, \ldots, C_k)A)_{\perp} = [C_1^\perp, C_2^\perp, \ldots, C_k^\perp](A^{-1})^T\]

for any non-singular matrix $A$ over $F_q$ (see Lemma 3.3).

- In [56], Zhang and Ge proved that

\[(C_1, C_2, \ldots, C_k)_{\perp}^n = [C_1^{\perp n}, C_2^{\perp n}, \ldots, C_k^{\perp n}](A^{-1})^\dagger\]

for any non-singular matrix $A$ over $F_{q^2}$ (see Lemma 4.2).

Therefore, we can deduce that: (i) a matrix-product code $C(A)$ over $F_q$ is Euclidean dual-containing if and only if $[C_1^\perp, C_2^\perp, \ldots, C_k^\perp](A^{-1})^T \subseteq [C_1, C_2, \ldots, C_k]A$; (ii) a matrix-product code $C(A)$ over $F_{q^2}$ is Hermitian dual-containing if and only if $[C_1^{\perp n}, C_2^{\perp n}, \ldots, C_k^{\perp n}](A^{-1})^\dagger \subseteq [C_1, C_2, \ldots, C_k]A$. 
With the help of the above facts and quasi-orthogonal matrices (resp. quasi-unitary matrices), the author of this article and his cooperator [11, 12] gave a sufficient condition under which a matrix-product code over $\mathbb{F}_q$ (resp. $\mathbb{F}_{q^2}$) is Euclidean dual-containing (resp. Hermitian dual-containing), which provides a general approach for constructing quantum codes via Euclidean dual-containing (resp. Hermitian dual-containing) matrix-product codes (see Theorems 3.2 and 4.1). Based on this approach, Refs [11–13] constructed many new classes of matrix-product codes satisfying Euclidean dual-containing (resp. Hermitian dual-containing) by quasi-orthogonal matrices (resp. quasi-unitary matrices) and NSC quasi-orthogonal matrices (resp. NSC quasi-unitary matrices), which are very useful to construct good $q$-ary quantum codes by CSS construction (resp. Hermitian construction). It is worth mentioning that the utilization of NSC quasi-orthogonal or NSC quasi-unitary matrices enables the minimum distance lower bound of the corresponding quantum codes to reach its optimum.

We have two purposes in writing this article: the first is to summarize some results of this topic obtained by the author of this article and his cooperators in [11–13]; the second is to add some new results on quasi-orthogonal matrices (resp. quasi-unitary matrices), Euclidean dual-containing (resp. Hermitian dual-containing) matrix-product codes and $q$-ary quantum codes derived from these newly constructed matrix-product codes and CSS construction (resp. Hermitian construction). The remainder of this article is organized as follows.

Section 2 recalls some basics on classical error-correcting codes (including generalized Reed-Solomon (GRS) codes, extended GRS codes and matrix-product codes) and quantum error-correcting codes.

Section 3 is devoted to the construction of quantum codes from Euclidean dual-containing matrix-product codes related to quasi-orthogonal matrices and NSC quasi-orthogonal matrices. Subsection 3.1 recalls some basic concepts and properties on Euclidean dual codes, CSS construction and matrix-product codes over $\mathbb{F}_q$. Subsection 3.2 gives a general approach for constructing quantum codes via Euclidean dual-containing matrix-product codes (see Theorem 3.2). Subsection 3.3 shows three constructions of quantum codes related to quasi-orthogonal matrices by using: (i) the theory of quadratic forms (see Theorem 3.3); (ii) the theory of quadratic sum (see Theorem 3.4) and (iii) the Hadamard matrices (see Theorem 3.5). Subsection 3.4 presents a constructive method for constructing general quasi-orthogonal matrices and NSC quasi-orthogonal matrices (see Theorem 3.6). The utilization of NSC quasi-orthogonal matrices enables the minimum distance lower bound of the corresponding quantum codes to reach its optimum (see Theorem 3.7). Subsection 3.5 considers the quantum codes related to special matrices $A$ with $AA^T$ being monomial matrices (see Theorem 3.8).

Section 4 focuses on the construction of quantum codes from Hermitian dual-containing
matrix-product codes related to quasi-unitary matrices and NSC quasi-unitary matrices. Subsection 4.1 reviews some basic concepts and properties on Hermitian dual codes, Hermitian construction and matrix-product codes over $\mathbb{F}_{q^2}$. Subsection 4.2 provides a general approach for constructing quantum codes via Hermitian dual-containing matrix-product codes (see Theorem 4.1). Subsection 4.3 discusses the constructions of quantum codes related to (i) quasi-unitary matrices over $\mathbb{F}_{q^2}$ for any odd prime power $q$ (see Theorem 4.2) and (ii) $2^m \times 2^m$ quasi-unitary matrices over any field $\mathbb{F}_{q^2}$ (see Theorem 4.3). Subsection 4.4 shows a constructive method for acquiring general quasi-unitary matrices and NSC quasi-unitary matrices (see Theorem 4.4).

The utilization of NSC quasi-unitary matrices enables the minimum distance lower bound of the corresponding quantum codes to reach its optimum (see Theorem 4.5). Subsection 4.5 constructs new classes of quantum codes related to $k \times k$ NSC quasi-unitary matrices for any $k < q$ (see Theorem 4.7). Subsection 4.6 considers the quantum codes related to special matrices $A$ with $AA^\dagger$ being monomial matrices (see Theorem 4.8).

Section 5 makes a summary of this article and proposes the prospect of the follow-up work.

2 Preliminaries

In this section, we will recall some basics on classical error-correcting codes, including generalized Reed-Solomon (GRS) codes, extended GRS codes and matrix-product codes. The concept of quantum error-correcting codes (quantum codes, for short) is also reviewed.

2.1 Classical error-correcting codes

Assume that $q$ is a prime power. Let $\mathbb{F}_q$ denote the finite field with $q$ elements and $\mathbb{F}^n_q$ denote the $n$-dimensional vector space over $\mathbb{F}_q$. Let us recall some basics on classical error-correcting codes. For more details on them, we refer the reader to [44].

**Definition 2.1** Any $q$-ary classical error-correcting code $C$ can be viewed as a nonempty set of some vector space $\mathbb{F}^n_q$. Any vector $c = (c_1, c_2, \ldots, c_n) \in C$ is called the codeword of $C$, where $c_i \in \mathbb{F}_q$ for each $i$. Then code $C$ is said to has length $n$. If $C$ has $K$ codewords, then $\frac{k}{n}$ is called the rate or efficiency of $C$, where $k := \log_q K$.

Since $C$ is nonempty and $C \subseteq \mathbb{F}^n_q$, we know that $1 \leq K \leq q^n$, i.e., $0 \leq \frac{k}{n} \leq 1$.

**Definition 2.2** Given two vectors $u = (u_1, u_2, \ldots, u_n), v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}^n_q$, their Hamming distance $d_H(u, v)$ is defined as

$$d_H(u, v) = \sum_{i=1}^{n} 1 \leq i \leq n, u_i \neq v_i.$$
The Hamming weight of \( v \) is defined as

\[
w_H(v) = \#\{i | 1 \leq i \leq n, 0 \neq v_i \in \mathbb{F}_q\}.
\]

By the above definition, we know that \( d_H(u, v) = w_H(u - v) \), and \( d_H(u, v) \) satisfies the following properties:

1. \( d_H(u, v) \geq 0 \).  
2. \( d_H(u, v) = 0 \iff u = v \).
3. \( d_H(u, v) \leq d_H(u, w) + d_H(w, v) \).

**Definition 2.3** Given a \( q \)-ary classical error-correcting code \( C \) of length \( n \) and codewords number \( K \geq 2 \). Then, the minimum distance of \( C \) is defined as

\[
d(C) = \min\{d_H(c, c') | c, c' \in C, c \neq c'\}.
\]

If \( C \) is a linear code, i.e., \( C \) is a \( \mathbb{F}_q \)-vector subspace of \( \mathbb{F}_q^n \), then the minimum distance of \( C \) is

\[
d(C) = \min\{w_H(c) | 0 \neq c \in C\}.
\]

**Definition 2.4** We denote by \( [n, K, d]_q \) (or \( [n, k, d]_q \)) a \( q \)-ary classical error-correcting code of length \( n \), codewords number \( K \) and minimum distance \( d \), where \( k = \log_q K \).

**Theorem 2.1** ([44]) A classical error-correcting code of minimum distance \( d \) can detect up to \( d - 1 \) errors and correct up to \( \left\lfloor \frac{d-1}{2} \right\rfloor \) errors. Here, \( \left\lfloor x \right\rfloor \) represents the greatest integer less than or equal to \( x \).

**Theorem 2.2** ([44], Singleton bound) An \( [n, k, d]_q \) error-correcting code satisfies \( d \leq n + 1 - k \).

**Definition 2.5** If an \( [n, k, d]_q \) error-correcting code \( C \) satisfies \( d = n + 1 - k \), then \( C \) is called a maximum distance separable (abbreviated to MDS) code.

From Theorem 2.1, we know that MDS codes have the optimal abilities of error detection and error correction among all \( [n, k, d]_q \) error-correcting codes for fixed parameters \( n \) and \( k \).

**Definition 2.6** Let \( C \) be an \( [n, k, d]_q \) linear code. Let \( v_1, \ldots, v_n \) be a \( \mathbb{F}_q \)-basis of \( C \). Write \( v_i = (a_{i1}, a_{i2}, \ldots, a_{in}) \). Then, we call the row full rank matrix

\[
G = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{bmatrix}
\]
a generator matrix of code $C$. Moreover, we can regard $C$ as the solution space of the following homogeneous linear equations:

$$\begin{align*}
&b_{11}x_1 + b_{12}x_2 + \ldots + b_{1n}x_n = 0, \\
&b_{21}x_1 + b_{22}x_2 + \ldots + b_{2n}x_n = 0, \\
&\ldots \ldots \ldots \\
&b_{n-k,1}x_1 + b_{n-k,2}x_2 + \ldots + b_{n-k,n}x_n = 0.
\end{align*}$$

The row full rank matrix

$$H = \begin{bmatrix}
  b_{11} & b_{12} & \cdots & b_{1n} \\
  b_{21} & b_{22} & \cdots & b_{2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  b_{n-k,1} & b_{n-k,2} & \cdots & b_{n-k,n}
\end{bmatrix}$$

is called a check matrix of $C$.

### 2.2 GRS codes and extended GRS codes

Let $k$ and $n$ be two positive integers with $k \leq n \leq q$. Let $\mathbf{a} = (a_1, \ldots, a_n)$, where $a_1, \ldots, a_n$ are distinct elements in $\mathbb{F}_q$. Let $\mathbf{v} = (v_1, \ldots, v_n)$, where $v_1, \ldots, v_n$ are nonzero elements in $\mathbb{F}_q$. Define

$$GRS_k(\mathbf{a}, \mathbf{v}) = \{(v_1f(a_1), \ldots, v_nf(a_n))|f(x) \in \mathbb{F}_q[x], \deg(f(x)) \leq k - 1\}$$

the generalized Reed-Solomon code (abbreviated to GRS code) associated with $\mathbf{a}$ and $\mathbf{v}$. It is an $[n,k]_q$ MDS code and it has a generator matrix

$$\begin{bmatrix}
v_1 & v_2 & \cdots & v_n \\
v_1a_1 & v_2a_2 & \cdots & v_na_n \\
\vdots & \vdots & \ddots & \vdots \\
v_1a_1^{k-1} & v_2a_2^{k-1} & \cdots & v_na_n^{k-1}
\end{bmatrix}$$

Moreover, the extended generalized Reed-Solomon code (abbreviated to extended GRS code) associated with $\mathbf{a}$ and $\mathbf{v}$ is defined as

$$GRS_k(\mathbf{a}, \mathbf{v}, \infty) = \{(v_1f(a_1), \ldots, v_nf(a_n), f_{k-1})|f(x) \in \mathbb{F}_q[x], \deg(f(x)) \leq k - 1\},$$
where \( f_{k-1} \) represents the coefficient of \( x^{k-1} \) in \( f(x) \). It is easily verified that \( GRS_k(a, v, \infty) \) is an \([n+1, k]_q\) MDS code with a generator matrix

\[
\begin{bmatrix}
v_1 & v_2 & \cdots & v_n & 0 \\
v_1a_1 & v_2a_2 & \cdots & v_na_n & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
v_1a_1^{k-2} & v_2a_2^{k-2} & \cdots & v_na_n^{k-2} & 0 \\
v_1a_1^{k-1} & v_2a_2^{k-1} & \cdots & v_na_n^{k-1} & 1 \\
\end{bmatrix}.
\]

### 2.3 Matrix-product codes

In 2001, Blackmore and Norton [4] proposed an important class of codes called matrix-product codes, which is very useful for constructing good \( q \)-ary quantum error-correcting codes (see Subsection 2.4) of large lengths by CSS construction (see Theorem 3.1) or Hermitian construction (see Lemma 4.1). We denote by \( \mathcal{M}(\mathbb{F}_q, s \times l) \) the set of \( s \times l \) matrices with entries in \( \mathbb{F}_q \).

**Definition 2.7** ([4]) Let \( A = (a_{ij})_{i,j=1}^{s,l} \in \mathcal{M}(\mathbb{F}_q, s \times l) \) be row full rank with \( s \leq l \). Let \( C_1, C_2, \ldots, C_s \) be linear codes of the same length \( n \) over \( \mathbb{F}_q \). The matrix-product code is defined as

\[
C(A) = [C_1, C_2, \ldots, C_s]A,
\]

which can be regarded as the set of all matrix-products \([c_1, c_2, \cdots, c_s]A\), where each \( c_i = (c_{i1}, c_{i2}, \ldots, c_{in})^T \in C_i \) is an \( n \times 1 \) column vector. Clearly, \( C(A) \) is a linear code of length \( ln \).

Then, any codeword \( c = [c_1, c_2, \ldots, c_s]A \) of \( C(A) \) is an \( n \times l \) matrix as follows:

\[
c = \begin{bmatrix}
\sum_{i=1}^s c_{i1}a_{1l} & \sum_{i=1}^s c_{i1}a_{2l} & \cdots & \sum_{i=1}^s c_{i1}a_{ll} \\
\sum_{i=1}^s c_{i2}a_{1l} & \sum_{i=1}^s c_{i2}a_{2l} & \cdots & \sum_{i=1}^s c_{i2}a_{ll} \\
\vdots & \vdots & \ddots & \vdots \\
\sum_{i=1}^s c_{in}a_{1l} & \sum_{i=1}^s c_{in}a_{2l} & \cdots & \sum_{i=1}^s c_{in}a_{ll}
\end{bmatrix}.
\]

The matrix \( A \) is called the defining matrix of \( C(A) \). Note that \( c \) can be also viewed as an \( 1 \times ln \) row vector

\[
c = \left[ \sum_{i=1}^s a_{i1}c_{i1}, \sum_{i=1}^s a_{i2}c_{i1}, \ldots, \sum_{i=1}^s a_{il}c_{i1} \right],
\]

where \( c_i = (c_{i1}, c_{i2}, \ldots, c_{in}) \in C_i \) is regarded as an \( 1 \times n \) row vector for \( i = 1, 2, \ldots, s \).
If \( G_i \) is a generator matrix of the code \( C_i \) for \( i = 1, 2, \ldots, s \), then

\[
G(A) = \begin{bmatrix}
G_{11} & a_{12}G_1 & \cdots & a_{1l}G_1 \\
G_{21} & a_{22}G_2 & \cdots & a_{2l}G_2 \\
\vdots & \vdots & \ddots & \vdots \\
G_{s1} & a_{s2}G_s & \cdots & a_{sl}G_s
\end{bmatrix}
\]

is a generator matrix of the matrix-product code \( C(A) \).

2.4 Quantum codes

Let us recall some basic concepts and properties on quantum error-correcting codes (quantum codes, for short). We use \( \mathbb{C}^q \) to represent the \( q \)-dimensional complex vector space over the complex field \( \mathbb{C} \). For any pure 1-qudit \(|v\rangle \in \mathbb{C}^q\), it can be written as

\[
|v\rangle = \sum_{a \in \mathbb{F}_q} v_a |a\rangle,
\]

where \( \{|a\rangle : a \in \mathbb{F}_q\} \) is a basis of \( \mathbb{C}^q \), \( v_a \in \mathbb{C} \) and \( \sum_{a \in \mathbb{F}_q} |v_a|^2 = 1 \). Any \( n \)-qudit is a joint state of \( n \) qudits of the \( q^n \)-dimensional complex vector space \((\mathbb{C}^q)^\otimes n \cong \mathbb{C}^{q^n}\). We can write any pure \( n \)-qudit as

\[
|v\rangle = \sum_{a \in \mathbb{F}_{q^n}} v_a |a\rangle,
\]

where

\[
\{|a\rangle = |a_1\rangle \otimes \cdots \otimes |a_n\rangle : (a_1, \ldots, a_n) \in \mathbb{F}_{q^n}\}
\]

is a basis of \( \mathbb{C}^{q^n} \), \( v_a \in \mathbb{C} \) and \( \sum_{a \in \mathbb{F}_{q^n}} |v_a|^2 = 1 \).

Let \( \gamma \) be a complex primitive \( p \)-th root of unity. Let \( a = (a_1, \ldots, a_n) \), \( b = (b_1, \ldots, b_n) \in \mathbb{F}_{q^n} \).

Define the error operators \( T(a_i) \) and \( R(a_i) \) as

\[
T(a_i)|x\rangle = |x + a_i\rangle,
\]

\[
R(a_i)|x\rangle = \gamma^{\text{Tr}(a_i)}|x\rangle,
\]

respectively, where \( \text{Tr}(x) \) is the trace function from \( \mathbb{F}_q \) (where \( q = p^m \) for some \( m \in \mathbb{N}^+ \)) to \( \mathbb{F}_p \).

If we use

\[
T(a) = T(a_1) \otimes \cdots \otimes T(a_n),
\]

\[
R(a) = R(a_1) \otimes \cdots \otimes R(a_n)
\]

to represent the tensor products of \( n \) error operators, then the error set

\[
E_n = \{\gamma^i T(a)R(b)|0 \leq i \leq p - 1, a, b \in \mathbb{F}_{q^n}\}
\]

10
forms an error group. For any error \( e = \gamma^T(a)R(b) \in E_n \), its quantum weight is defined as
\[
w_Q(e) = \sharp\{i | (a_i, b_i) \neq (0, 0)\}.
\]
Let
\[
E_n(i) = \{ e \in E_n | w_Q(e) \leq i \}.
\]
For a \( q \)-ary quantum code \( Q \), if \( d \) is the largest positive integer such that \( \langle u | e | v \rangle = 0 \) holds for any \( |u⟩, |v⟩ \in Q \) with \( \langle u | v \rangle = 0 \) and \( e \in E_n(d - 1) \), then we say \( Q \) has minimum distance \( d \). Usually, we use the notation \([[n, k, d]]_q\) to represent a \( q \)-ary quantum code of length \( n \), dimension \( q^k \) and minimum distance \( d \). It has the abilities to detect up to \( d - 1 \) quantum errors and correct up to \( \lfloor \frac{d-1}{2} \rfloor \) quantum errors. The minimum distance \( d \) of a quantum code must satisfy the quantum Singleton bound, i.e., \( 2d \leq n + 2 - k \). Further, if \( 2d = n + 2 - k \), then such a quantum code is called a quantum MDS code. For more information on quantum codes, see [2,7–9,22,36,46–48,50].

3 Quantum codes from Euclidean dual-containing matrix-product codes

This section is organized as follows. In subsection 3.1, we recall some basic concepts and properties on Euclidean dual codes, CSS construction and matrix-product codes. Subsection 3.2 gives a general approach for constructing quantum codes via Euclidean dual-containing matrix-product codes over \( \mathbb{F}_q \). Subsection 3.3 in turn provides the constructions of quantum codes related to quasi-orthogonal matrices in three manners: (i) the theory of quadratic forms; (ii) the theory of quadratic sum; and (iii) the Hadamard matrices. Subsection 3.4 proposes a constructive method for acquiring general quasi-orthogonal matrices and NSC quasi-orthogonal matrices. The utilization of NSC quasi-orthogonal matrices enables the minimum distance lower bound of the corresponding quantum codes to reach its optimum. Subsection 3.5 studies the quantum codes related to a special kind of matrices \( A \) with \( AA^T \) being monomial matrices.

3.1 Basic concepts and properties

Assume \( q \) is a prime power. Let \( \mathbb{F}_q \) be the finite field with \( q \) elements and let \( \mathbb{F}_q^* \) denote the set of non-zero elements over \( \mathbb{F}_q \). Now let us recall some basics on the Euclidean dual codes, CSS construction and matrix-product codes over \( \mathbb{F}_q \).

Definition 3.1 For \( x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n \), define
\[
(x, y) = \sum_{i=1}^{n} x_i y_i
\]
as the *Euclidean inner product* of \( x \) and \( y \). For a linear code \( C \) of length \( n \) over \( \mathbb{F}_q \), define

\[
C^\perp = \{ x \in \mathbb{F}_q^n \mid (x, y) = 0 \text{ for all } y \in C \}
\]
as the *Euclidean dual code* of \( C \).

**Definition 3.2** Let \( C \) be a linear code over \( \mathbb{F}_q^n \). Then,

1. If \( C \subseteq C^\perp \), then \( C \) is called an *Euclidean self-orthogonal code*;
2. If \( C^\perp = C \), then \( C \) is called an *Euclidean self-dual code*;
3. If \( C^\perp \subseteq C \), then \( C \) is called an *Euclidean dual-containing code*.

The following CSS construction tells us how to produce \( q \)-ary quantum codes from the classical linear codes over \( \mathbb{F}_q \).

**Theorem 3.1** (CSS construction, [9, 50]) Let \( C \) be an \( [n, k, d]_q \) linear code with \( C^\perp \subseteq C \), then there exists an \( [n, 2k - n, \geq d]_q \) quantum code.

The following lemma characterizes the parameters of the matrix-product codes over \( \mathbb{F}_q \).

**Lemma 3.1** ([45]) Let \( C_i \) be an \( [n, t_i]_q \) linear code for \( i = 1, 2, \ldots, k \). Let \( A \in \mathcal{M}(\mathbb{F}_q, k \times s) \) be full-rank. Denote by \( D_i(A) \) the minimum distance of the code on \( \mathbb{F}_q^s \) generated by the first \( i \) rows of \( A \). Then, the matrix-product code

\[
C(A) = [C_1, C_2, \ldots, C_k]A
\]
is an \( [sn, \sum_{i=1}^{k} t_i, \geq d]_q \) linear code, where \( d = \min_{1 \leq i \leq k} \{ D_i(A)\} \).

Besides, it is easy to give the following basic property on matrix-product codes. We omit its proof here.

**Lemma 3.2** Let \( C_i \) be an \( [n, t_i, d_i]_q \) linear code for \( i = 1, 2, \ldots, k \). Then, for any two matrices \( V = (v_{ij})_{i,j=1}^{k,r}, W = (w_{ij})_{i,j=1}^{r,l} \) over \( \mathbb{F}_q \), we have

\[
[C_1, C_2, \ldots, C_k]VW = ([C_1, C_2, \ldots, C_k]V)W.
\]

**Example 3.1** Let \( C_i \) be an \( [n, t_i, d_i]_q \) linear code, where \( i = 1, 2, 3 \). Consider

\[
V_1 = \begin{bmatrix}
1 & 1 & 1 \\
0 & 0 & 1 \\
1 & 0 & 1 \\
\end{bmatrix}, \quad W_1 = \begin{bmatrix}
1 & 0 & 0 \\
0 & -1 & 0 \\
0 & 1 & 1 \\
\end{bmatrix}.
\]

Then,

\[
[C_1, C_2, C_3]V_1 = \{[c_1, c_2, c_3]V_1 | c_i \in C_i \}
\]
\[
(C_1, C_2, C_3)W_1 = \{[c_1 + c_3, c_1 + c_2 + c_3] | c_i \in C_i \},
\]

On the other hand, in terms of

\[
V_1W_1 = \begin{bmatrix}
1 & 0 & 1 \\
0 & 1 & 1 \\
1 & 1 & 1
\end{bmatrix},
\]

we have

\[
(C_1, C_2, C_3)V_1W_1 = \{[c_1, c_2, c_3]V_1W_1 | c_i \in C_i \}
= \{[c_1 + c_3, c_1 + c_2 + c_3] | c_i \in C_i \}.
\]

Thus, \((C_1, C_2, C_3)V_1W_1 = ((C_1, C_2, C_3)V_1)W_1.\)

The following lemma gives the Euclidean dual code of a matrix-product code over \(\mathbb{F}_q\).

**Lemma 3.3** (\cite{4}) Let \(C_i\) be an \([n, t_i, d_i]_q\) linear code, where \(i = 1, 2, \ldots, k\). Let \(A \in M(\mathbb{F}_q, k \times k)\) be non-singular. Then,

\[
([C_1, C_2, \ldots, C_k]A)^\perp = [C^\perp_1, C^\perp_2, \ldots, C^\perp_k](A^{-1})^T.
\]

### 3.2 General approach for constructing quantum codes via Euclidean dual-containing matrix-product codes

Let

\[
\tau = \begin{pmatrix}
1 & 2 & \cdots & k \\
i_1 & i_2 & \cdots & i_k
\end{pmatrix}
\]

denote a permutation on \(\{1, 2, \ldots, k\}\). Let \(P_\tau\) be the \(k \times k\) permutation matrix in which the \(i_j\)-th row of the identity matrix \(I_k\) is replaced with the \(j\)-th row of it for \(j = 1, 2, \ldots, k\). We introduce the following definition.

**Definition 3.3** Let \(B \in M(\mathbb{F}_q, k \times k)\). If \(B = DP_\tau\), where \(D = \text{diag}(d_{11}, \ldots, d_{kk})\) with \(d_{ii} \in \mathbb{F}_q^*\) for each \(i\), then the matrix \(B\) is called a *monomial matrix* with respect to the permutation \(\tau\).

**Definition 3.4** Let \(B \in M(\mathbb{F}_q, k \times k)\). If \(BB^T\) is diagonal over \(\mathbb{F}_q^*\), then we call \(B\) a *quasi-orthogonal matrix* over \(\mathbb{F}_q\). If \(BB^T = I_k\), then we call \(B\) an *orthogonal matrix* over \(\mathbb{F}_q\).

In the following theorem, we give a general approach for constructing \(q\)-ary quantum codes via Euclidean dual-containing matrix-product codes over \(\mathbb{F}_q\).
Theorem 3.2 ([12]) Let $C_j$ be an $[n, t_j, d_j]_q$ linear code with $C_j^⊥ \subseteq C_j$, where $j = 1, 2, \ldots, k$. For any non-singular matrix $A \in \mathcal{M}(\mathbb{F}_q, k \times k)$, if $AA^T$ is a monomial matrix with respect to the permutation $\tau$, then the matrix-product code

$$C(A) = [C_1, C_2, \ldots, C_k]A$$

is an $[kn, \sum_{i=1}^k t_i, \geq d]_q$ Euclidean dual-containing code, where $d = \min_{1 \leq i \leq k} \{d_i D_i(A)\}$. Further, $C(A)$ generates an $[[kn, 2\sum_{i=1}^k t_i - kn, \geq d]]_q$ quantum code.

By Theorem 3.2, we can construct Euclidean dual-containing matrix-product code $C(A)$ over $\mathbb{F}_q$, as long as the following two conditions hold:

(a) $AA^T$ is a monomial matrix with respect to $\tau$, where $\tau$ maps each $j \in \{1, 2, \ldots, k\}$ to $i_j \in \{1, 2, \ldots, k\}$;

(b) The constituent codes $C_1, C_2, \ldots, C_k$ of $C(A)$ satisfy $C_j^⊥ \subseteq C_j$ for each $j = 1, 2, \ldots, k$.

Further, we can obtain $q$-ary quantum codes by the CSS construction. In fact, for a given permutation $\tau$, it is not difficult to find proper constituent codes satisfying (b). We emphasize that the main difficulty lies in condition (a). As far as we know, it is very difficult to give a general method (not by computer search) for finding the matrix $A$ in condition (a). Therefore, in the next subsections, we will investigate the constructions of quantum codes when the defining matrix $A$ of $C(A)$ in turn satisfies different cases: (i) $A$ is a quasi-orthogonal matrix; (ii) $A$ is a NSC quasi-orthogonal matrix; (iii) $AA^T$ is a special class of monomial matrices.

### 3.3 Quantum codes related to quasi-orthogonal matrices

When $\tau$ is an identity permutation, i.e., $\tau = (1)$, it follows from Theorem 3.2 that

**Corollary 3.1** Let $C_i$ be an $[n, t_i, d_i]_q$ linear code with $C_i^⊥ \subseteq C_i$ for $i = 1, 2, \ldots, k$. For any non-singular matrix $A \in \mathcal{M}(\mathbb{F}_q, k \times k)$, if $A$ is quasi-orthogonal, then the matrix-product code

$$C(A) = [C_1, C_2, \ldots, C_k]A$$

is an $[kn, \sum_{i=1}^k t_i, \geq d]_q$ Euclidean dual-containing code, where $d = \min_{1 \leq i \leq k} \{d_i D_i(A)\}$. Further, $C(A)$ generates an $[[kn, 2\sum_{i=1}^k t_i - kn, \geq d]]_q$ quantum code.

By Corollary 3.1, the next task is to find the quasi-orthogonal matrix $A$ for constructing quantum codes.

#### 3.3.1 The utilization of the theory of quadratic forms

Similar to the theory of real quadratic forms, any quadratic form in $\mathbb{F}_q$, where $q$ is an odd prime power, can be simplified into a diagonal form according to a linear invertible transform.
In other words, this property is equivalent to the following proposition, which is shown by the language of matrices. The reader can refer [3] for more information.

**Proposition 3.1 ([3])** Let \( q \) be an odd prime power. Then, for any symmetric matrix \( A \in \mathcal{M}(\mathbb{F}_q, k \times k) \), there exists a non-singular matrix \( M \in \mathcal{M}(\mathbb{F}_q, k \times k) \) such that \( M^TAM \) is a \( k \times k \) diagonal matrix over \( \mathbb{F}_q \).

By the above proposition, the following theorem constructs Euclidean dual-containing matrix-product codes and obtains quantum codes by CSS construction.

**Theorem 3.3 ([12])** Let \( q \) be an odd prime power and \( C_i \) be an \([n, t_i, d_i]_q \) linear code with \( C_i^⊥ \subseteq C_i \) for \( i = 1, 2, \ldots, k \). Then, for any non-singular matrix \( B \in \mathcal{M}(\mathbb{F}_q, k \times k) \), there exists a non-singular matrix \( N \in \mathcal{M}(\mathbb{F}_q, k \times k) \) such that the matrix-product code

\[
C(N^TB) = [C_1, C_2, \ldots, C_k]N^TB
\]

is an \([kn, \sum_{i=1}^k t_i, \geq d]_q \) Euclidean dual-containing code, where \( d = \min_{1 \leq i \leq k} \{d_i D_i(N^TB)\} \). Further, \( C(N^TB) \) yields an \([[kn, 2\sum_{i=1}^k t_i - kn, \geq d]]_q \) quantum code.

### 3.3.2 The utilization of the theory of quadratic sum

The following proposition gives an interesting property on the quadratic sum over finite fields.

**Proposition 3.2 ([18])** Let \( \mathbb{F} \) be a field and let \( c = c_1^2 + \cdots + c_{2^m}^2 \) with \( c_i \in \mathbb{F} \) for each \( i \). Then, there exist \( 4^m \) elements \( \{s_{i,j}|1 \leq i, j \leq 2^m\} \) over \( \mathbb{F} \), satisfying that

1. \( s_{1,j} = c_j, 1 \leq j \leq 2^m \);
2. \( \sum_{k=1}^{2^m} s_{i,k}s_{j,k} = \delta_{i,j}c \), where \( \delta_{i,j} \) is the Kronecker symbol for \( 1 \leq i, j \leq 2^m \).

In fact, Proposition 3.2 is equivalent to the following proposition through the form of matrix language.

**Proposition 3.3 ([18])** Let \( \mathbb{F} \) be a field and let \( c = c_1^2 + \cdots + c_{2^m}^2 \) with \( c_i \in \mathbb{F} \) for each \( i \). Then, there exists a matrix \( S = (s_{i,j}) \in \mathcal{M}(\mathbb{F}, 2^m \times 2^m) \), satisfying that

\[
S^TS = SS^T = cI_{2^m},
\]

where \( (c_1, \ldots, c_{2^m}) \) is the first row of \( S \).

By Proposition 3.3, we have the following theorem.
Theorem 3.4 Let $0 \neq c = c_1^2 + \cdots + c_{2^m}^2$, where $c_i \in \mathbb{F}_q$ for $i = 1, 2, \ldots, 2^m$. Let $C_i$ be an $[n, t_i, d_i]_q$ linear code with $C_i^\perp \subseteq C_i$ for $i = 1, 2, \ldots, 2^m$. Then, there exists a matrix $S = (s_{i,j}) \in \mathcal{M}(\mathbb{F}_q, 2^m \times 2^m)$ such that the matrix-product code

$$C(S) = [C_1, C_2, \ldots, C_{2^m}] S$$

is an $[2^m n, \sum_{i=1}^{2^m} t_i, \geq d]_q$ Euclidean dual-containing code, where $d = \min_{1 \leq i \leq 2^m} \{ d_i D_i(S) \}$. Further, $C(S)$ generates an $[[2^m n, 2^m \sum_{i=1}^{2^m} t_i - 2^m n, \geq d]]_q$ quantum code.

3.3.3 The utilization of the Hadamard matrices

The Hadamard matrices are a special class of quasi-orthogonal matrices. Let us recall its definition.

Definition 3.5 Assume $H = (h_{ij})$ is an $n \times n$ matrix with $h_{ij} = \pm 1$. If $H_n H_n^T = n I_n$, then we call $H_n$ a Hadamard matrix.

It is not difficult to verify that the following three matrices

$$H_1 = (1), H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

are all Hadamard matrices. The following proposition constructs a class of Hadamard matrices over $\mathbb{F}_q$.

Proposition 3.4 (\cite{39}) Let $\mathbb{F}_q = \{ a_1, a_2, \ldots, a_q \}$, $q \equiv 3 \mod 4$. Denote by $\eta$ the quadratic character of $\mathbb{F}_q$. Then,

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & -1 & b_{12} & b_{13} & \cdots & b_{1q} \\ 1 & b_{21} & -1 & b_{23} & \cdots & b_{2q} \\ 1 & b_{31} & b_{32} & -1 & \cdots & b_{3q} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & b_{q1} & b_{q2} & b_{q3} & \cdots & -1 \end{bmatrix}$$

is an $(q + 1) \times (q + 1)$ Hadamard matrix, where $b_{ij} = \eta(a_j - a_i)$ for $1 \leq i \neq j \leq q$.

Corollary 3.2 (\cite{39}) Assume $q \equiv 3 \mod 4$ and $H$ is defined as in Proposition 3.4. Define $H_0 = H$ and

$$H_w := \begin{bmatrix} H_{w-1} & H_{w-1} \\ H_{w-1} & -H_{w-1} \end{bmatrix}, w \geq 1.$$ 

Then, $H_w$ is an $2^w(q + 1) \times 2^w(q + 1)$ Hadamard matrix for any integer $w$. 
By Corollary 3.2, we immediately construct Euclidean dual-containing matrix-product codes and obtain the corresponding quantum codes in the following theorem.

**Theorem 3.5**

Assume \( q \equiv 3 \mod 4 \), \( w \geq 1 \) and \( H_w \) is defined as in Corollary 3.2. Write \( w' = 2^w(q + 1) \). Let \( C_i \) be an \([n, t_i, d_i]_q\) linear code with \( C_i^\perp \subseteq C_i \) for each \( i = 1, \ldots, w' \). Then, the matrix-product code 

\[
C(H_w) = [C_1, C_2, \ldots, C_w']H_w
\]

is an \([w' n, \sum_{i=1}^{w'} t_i, \geq d]_q\) Euclidean dual-containing code, where \( d = \min_{1 \leq i \leq w'} \{d_i D_i(H_w)\} \). Further, \( C(H_w) \) generates an \([w' n, 2 \sum_{i=1}^{w'} t_i - w'n, \geq d]\) quantum code.

### 3.4 Quantum codes related to NSC quasi-orthogonal matrices

In this subsection, we will construct NSC quasi-orthogonal matrices as the defining matrices of matrix-product codes. With the help of CSS construction, we can obtain some classes of good quantum codes.

Recall that in Corollary 3.1 when the defining matrix \( A \) is quasi-orthogonal, we can construct an Euclidean dual-containing matrix-product code. Further, it generates a \([kn, 2 \sum_{i=1}^{k} t_i - kn, \geq d]\) quantum code from the CSS construction, where \( d = \min_{1 \leq i \leq k} \{d_i D_i(A)\} \). Clearly, the length and dimension of the quantum code are irrelevant to the defining matrix \( A \), while the minimum distance is related to it and is determined by \( D_i(A) \). Moreover, it is not difficult to check that \( D_i(A) \leq k + 1 - i \).

For fixed length and dimension, the larger value of the minimum distance means the better performance of error detection and error correction of the quantum code. Given this fact, we wish to make the minimum distance lower bound \( \min_{1 \leq i \leq k} \{d_i D_i(A)\} \) of the quantum codes from our constructed matrix-product codes as large as possible. That is to say, we need to find the quasi-orthogonal matrix \( A \) such that \( D_i(A) = k + 1 - i \). For general quasi-orthogonal matrix \( A \), the computation of \( D_i(A) \) is more and more difficult as the order of \( A \) increases.

Let us consider the following matrices.

**Definition 3.6** ([4]) Let \( A = (a_{ij}) \in M(\mathbb{F}_q, k \times k) \). Denote by \( D_i(A) \) the minimum distance of the code on \( \mathbb{F}_q^k \) generated by the first \( i \) rows of \( A \). Write \( A^{(i)} \) the matrix consisting of the first \( i \) rows of \( A \) and \( A(j_1, \ldots, j_i) \) the matrix consisting of the \( j_1, \ldots, j_i \) columns of \( A^{(i)} \), where \( 1 \leq j_1 < \ldots < j_i \leq k \). If \( A(j_1, \ldots, j_i) \) is non-singular for all \( 1 \leq i \leq k \) and \( 1 \leq j_1 < \ldots < j_i \leq k \), then we call \( A \) non-singular by columns (NSC).

From Definition 3.6, one can verify that a NSC matrix \( A \) satisfies \( D_i(A) = k + 1 - i \) exactly. For a matrix \( A \), if it is both NSC and quasi-orthogonal, then we call \( A \) NSC quasi-orthogonal.
Next, we will give a constructive method for acquiring general quasi-orthogonal matrices and NSC quasi-orthogonal matrices.

**Theorem 3.6 (Constructive method)** Let $A \in \mathcal{M}(\mathbb{F}_q, k \times k)$ be non-singular. If all leading principal minors of $AA^T$ are nonzero, then there exists a lower unitriangular matrix $L$ such that $LA$ is quasi-orthogonal over $\mathbb{F}_q$. Further, if $A$ is NSC, then $LA$ is NSC quasi-orthogonal.

**Proof.** We can write $AA^T$ as
\[
AA^T = \begin{bmatrix} A_{k-1} & h \\
               h^T & c \end{bmatrix},
\]
where $A_{k-1} = A_{k-1}^T$. Take
\[
L_{k-1} = \begin{bmatrix} I_{k-1} & 0_{(k-1) \times 1} \\
                        -h^T A_{k-1}^{-1} & 1 \end{bmatrix},
\]
then we have
\[
L_{k-1} A A^T L_{k-1}^T = \begin{bmatrix} A_{k-1} & 0_{(k-1) \times 1} \\
                                0_{1 \times (k-1)} & c - h^T A_{k-1}^{-1} h \end{bmatrix}.
\]

Now we write $A_{k-1}$ as
\[
A_{k-1} = \begin{bmatrix} A_{k-2} & r \\
                           r^T & s \end{bmatrix},
\]
where $A_{k-2} = A_{k-2}^T$. Let
\[
B_{k-2} = \begin{bmatrix} I_{k-2} & 0_{(k-2) \times 1} \\
                        -r^T A_{k-2}^{-1} & 1 \end{bmatrix},
\]
then we obtain
\[
B_{k-2} A_{k-1} B_{k-2}^T = \begin{bmatrix} A_{k-2} & 0_{(k-2) \times 1} \\
                                0_{1 \times (k-2)} & s - r^T A_{k-2}^{-1} r \end{bmatrix}.
\]

Let
\[
L_{k-2} = \begin{bmatrix} B_{k-2} & 0_{(k-1) \times 1} \\
                        0_{1 \times (k-1)} & 1 \end{bmatrix},
\]
then we obtain
\[
L_{k-2} L_{k-1} A A^T L_{k-1}^T L_{k-2}^T = \begin{bmatrix} A_{k-2} & 0_{(k-2) \times 1} & 0_{(k-2) \times 1} \\
                                0_{1 \times (k-2)} & s - r^T A_{k-2}^{-1} r & 0 \\
                                0_{1 \times (k-2)} & 0 & c - h^T A_{k-1}^{-1} h \end{bmatrix}.
\]

Repeating the above procedure on $A_{k-2}, A_{k-3}, \ldots, A_2$, one can finally obtain lower unitriangular matrices $L_{k-3}, L_{k-4}, \ldots, L_1$ such that
\[
l_1 l_2 \cdots l_{k-1} A A^T l_{k-1}^T \cdots l_2^T l_1^T = \text{diag}(\mu_1, \ldots, \mu_k)
\]
with $\mu_i \in \mathbb{F}_q^*$ for each $i$. Set $L = L_1L_2 \cdots L_{k-1}$, then $L$ is a lower unitriangular matrix. Then, we have

$$LAA^T L^T = \text{diag}(\mu_1, \ldots, \mu_k).$$

Hence, $LA$ is quasi-orthogonal.

Now let us prove that $LA$ is NSC. Write $A = (a_{ij})_{i,j=1}^k$ and $L = (l_{ij})_{i,j=1}^k$. For any $1 \leq s \leq k$ and $1 \leq j_1 < \cdots < j_s \leq k$, we have

$$|(LA)(j_1, \ldots, j_s)| = \det \begin{vmatrix} a_{1j_1} & a_{1j_2} & \cdots & a_{1j_s} \\ \sum_{i=1}^2 l_{2i}a_{ij_1} & \sum_{i=1}^2 l_{2i}a_{ij_2} & \cdots & \sum_{i=1}^2 l_{2i}a_{ij_s} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^s l_{si}a_{ij_1} & \sum_{i=1}^s l_{si}a_{ij_2} & \cdots & \sum_{i=1}^s l_{si}a_{ij_s} \\ a_{sj_1} & a_{sj_2} & \cdots & a_{sj_s} \end{vmatrix} = |A(j_1, \ldots, j_s)|.
$$

When $A$ is NSC, we have $|(LA)(j_1, \ldots, j_s)| = |A(j_1, \ldots, j_s)| \neq 0$. By Definition 3.6, $LA$ is NSC as well. Therefore, $LA$ is NSC quasi-orthogonal. $\square$

**Remark 3.1** As far as we know, the constructive method for acquiring general quasi-orthogonal matrices and NSC quasi-orthogonal matrices in Theorem 3.6 is proposed for the first time in literature.

**Remark 3.2** In [19], the authors constructed several classes of Euclidean dual-containing matrix-product codes over $\mathbb{F}_q$ by choosing some special NSC orthogonal matrices as the defining matrices of matrix-product codes. By contrast, Theorem 3.6 actually offers an effective algorithm for constructing NSC quasi-orthogonal matrices. Besides, since the orthogonal matrices are just a special case of the quasi-orthogonal matrices, Theorem 3.6 gives us more freedom in the choice of the defining matrices with the same order. What’s more, Theorem 3.6 enables us to obtain more classes of good quantum codes from the corresponding Euclidean dual-containing matrix-product codes.

**Remark 3.3** Let $B_i$ denote the matrix consisting of the last $i$ rows and the last $i$ columns of $AA^T$. Assume that $B_i$ is non-singular for each $i = 1, \ldots, k$. Now we can write $AA^T$ as

$$AA^T = \begin{bmatrix} b & g^T \\ g & B_{k-1} \end{bmatrix},$$

where $b = (b_{ij})_{i,j=1}^k$, $g = (g_{ij})_{i,j=1}^k$, and $B_{k-1}$ is a lower unitriangular matrix with $b_{ij} = g_{ij}$ for $i < j$.
where $B_{k-1} = B_{k-1}^T$. Then, there exists an upper unitriangular matrix

$$U_{k-1} = \begin{bmatrix} 1 & -g^T B_{k-1}^{-1} \\ 0_{(k-1) \times 1} & I_{k-1} \end{bmatrix}$$

such that

$$U_{k-1} A A^T U_{k-1}^T = \begin{bmatrix} b - g^T B_{k-1}^{-1} g & 0_{1 \times (k-1)} \\ 0_{(k-1) \times 1} & B_{k-1} \end{bmatrix}.$$

Similar to the proof of Theorem 3.6, this finally produces an upper unitriangular matrix $U$ such that $UA$ is quasi-orthogonal. However, we check that $UA$ may not be NSC for certain NSC matrix $A$.

We give the following example to illustrate Theorem 3.6 and Remark 3.3.

**Example 3.2** In $\mathbb{F}_5$, let us consider the NSC matrix

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

We have

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

(a) It is easily verified that all leading principal minors of $A A^T$ are nonzero. By Theorem 3.6, there exists

$$L_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 2 & 1 \end{bmatrix}$$

such that

$$L_2 A A^T L_2^T = \begin{bmatrix} 1 & 3 & 0 \\ 3 & 3 & 2 \\ 0 & 0 & 1 \end{bmatrix} \triangleq \begin{bmatrix} A_2 & 0_{2 \times 1} \\ 0_{1 \times 2} & 1 \end{bmatrix}.$$  

Then, there exists $B_1 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ such that $B_1 A_2 B_1^T = \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}$. Let $L_1 = \begin{bmatrix} B_1 & 0_{2 \times 1} \\ 0_{1 \times 2} & 1 \end{bmatrix}$, then we obtain

$$L_1 L_2 A A^T L_2^T L_1^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$  

20
Let $L = L_1L_2$, then we obtain a lower unitriangular matrix $L$ such that $LAA^T L^T = \text{diag}(1, 4, 1)$. Hence, $LA$ is quasi-orthogonal over $\mathbb{F}_5$. Moreover, it is not difficult to find that

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

is NSC over $\mathbb{F}_5$. Therefore, $LA$ is NSC quasi-orthogonal over $\mathbb{F}_5$.

(b) One can verify that the matrix consisting of the last $i$ rows and the last $i$ columns of $AA^T$ is non-singular for each $i = 1, 2, 3$. By Remark 3.3, there exists

$$U_2 = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

such that

$$U_2AA^TU_2^T = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 2 \\ 0 & 2 & 2 \end{bmatrix} \triangleq \begin{bmatrix} 2 & 0_{1 \times 2} \\ 0_{2 \times 1} & V \end{bmatrix}.$$ 

Then, there exists $\tilde{V} = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}$ such that $\tilde{V} \tilde{V}^T = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. Let $U_1 = \begin{bmatrix} 1 & 0_{1 \times 2} \\ 0_{2 \times 1} & \tilde{V} \end{bmatrix}$, then we have

$$U_1U_2AA^TU_2^TU_1^T = \begin{bmatrix} 2 & 0 \\ 0 & 1 \\ 0 & 0 \\ 2 & 0 \end{bmatrix}.$$

Write $U = U_1U_2$, then we obtain an upper unitriangular matrix $U$ such that $UAA^TU^T = \text{diag}(2, 1, 2)$. Hence, $UA$ is quasi-orthogonal over $\mathbb{F}_5$. However, since

$$UA = \begin{bmatrix} 3 & 3 & 3 \\ 1 & 1 & 3 \\ 1 & 4 & 0 \end{bmatrix},$$

we know that $|(UA)(1, 2)| = 0$, which means that $UA$ is not NSC.

**Corollary 3.3** Let $k \leq q$. Assume $x_1, \ldots, x_k$ are $k$ distinct elements in $\mathbb{F}_q$. Let

$$V = \begin{bmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_k \\ \lambda_1 x_1 & \lambda_2 x_2 & \cdots & \lambda_k x_k \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1 x_1^{k-1} & \lambda_2 x_2^{k-1} & \cdots & \lambda_k x_k^{k-1} \end{bmatrix},$$

21
where $\lambda_i \in \mathbb{F}_q^*$. If all leading principal minors of $VV^T$ are nonzero, then there exists a lower unitriangular matrix $L$ such that $LV$ is NSC quasi-orthogonal over $\mathbb{F}_q$.

**Proof.** Since $k \leq q$, then for any $1 \leq s \leq k$ and $1 \leq j_1 < \cdots < j_s \leq k$, we have

$$[V(j_1, \ldots, j_s)] = \left( \sum_{i=1}^{s} \lambda_{j_i} \right) \prod_{1 \leq m < n \leq s} (x_{jm} - x_{jn}) \neq 0.$$  

Hence, $V$ is NSC. Then the result follows by Theorem 3.6. □

By Theorem 3.6, we obtain the following result.

**Theorem 3.7** Let $C_i$ be an $[n, t_i, d_i]_q$ linear code with $C_i \subseteq C_i$ for each $i = 1, 2, \ldots, k$. For any NSC matrix $A \in \mathcal{M}(\mathbb{F}_q, k \times k)$, if all leading principal minors of $AA^T$ are nonzero, then there exists a lower unitriangular matrix $L$ such that the matrix-product code

$$C(LA) = [C_1, C_2, \ldots, C_k]LA$$

is an $[kn, \sum_{i=1}^{k} t_i, \geq d_i]_q$ Euclidean dual-containing code, where $d = \min_{1 \leq i \leq k} \{(k+1-i)d_i\}$. Further, $C(LA)$ generates an $[[kn, 2 \sum_{i=1}^{k} t_i - kn, \geq d]]_q$ quantum code.

**Proof.** By Theorem 3.6, there exists a lower unitriangular matrix $L \in \mathcal{M}(\mathbb{F}_q, k \times k)$ such that $LAA^TL^T = R$, where $R = \text{diag}(r_{11}, \ldots, r_{kk})$ with each $r_{ii} \in \mathbb{F}_q^*$. Then, we have $[(LA)^{-1}]^T = R^{-1}LA$. By Lemma 3.3 we know

$$([C_1, C_2, \ldots, C_k]LA)\perp = [C_1^+, C_2^+, \ldots, C_k^+]R^{-1}LA.$$  

Besides, it follows from $r_{ii}^{-1}C_i = C_i^+$ that

$$[C_1^+, C_2^+, \ldots, C_k^+]R^{-1}LA = [r_{11}^{-1}C_1^+, r_{22}^{-1}C_2^+, \ldots, r_{kk}^{-1}C_k^+]LA$$  

$$= [C_1^+, C_2^+, \ldots, C_k^+]LA$$

$$\subseteq [C_1, C_2, \ldots, C_k]LA.$$  

Hence, $C(LA)$ is Euclidean dual-containing with parameters $[kn, \sum_{i=1}^{k} t_i, \geq d]_q$, where $d = \min_{1 \leq i \leq k} \{(k+1-i)d_i\}$. By CSS construction, it generates an $[[kn, 2 \sum_{i=1}^{k} t_i - kn, \geq d]]_q$ quantum code. □

According to Theorem 3.7 and Corollary 3.3, we immediately obtain the following corollary.

**Corollary 3.4** Let $k \leq q$. Let $C_i$ be an $[n, t_i, d_i]_q$ linear code with $C_i^+ \subseteq C_i$ for each $i = 1, 2, \ldots, k$. Let $V$ be defined as in Corollary 3.3, where $x_i \in \mathbb{F}_q, \lambda_i \in \mathbb{F}_q^*$. If all leading principal minors of $VV^T$ are nonzero, then there exists a lower unitriangular matrix $L$ such that the matrix-product code

$$C(LV) = [C_1, C_2, \ldots, C_k]LV$$

is an $[kn, \sum_{i=1}^{k} t_i, \geq d]_q$ Euclidean dual-containing code, where $d = \min_{1 \leq i \leq k} \{(k+1-i)d_i\}$. Further, $C(LV)$ generates an $[[kn, 2 \sum_{i=1}^{k} t_i - kn, \geq d]]_q$ quantum code by CSS construction.
Similarly to Example 3.2, we are able to construct the $2 \times 2$ NSC quasi-orthogonal matrix over $F_5$. Let us consider the NSC matrix

$$\tilde{A}_1 = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}.$$ 

We have $\tilde{A}_1^{\top} \tilde{A}_1 = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$ whose all leading principal minors are nonzero. By Theorem 3.6, there exists a lower unitriangular matrix $\tilde{L}_1 = \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}$ such that

$$\tilde{L}_1 \tilde{A}_1 \tilde{A}_1^{\top} \tilde{L}_1^{\top} = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}.$$ 

Thus, $\tilde{L}_1 \tilde{A}_1$ is NSC quasi-orthogonal.

For convenience, let us replace the $3 \times 3$ matrices $L$ and $A$ in Example 3.2 with $\tilde{L}_2$ and $\tilde{A}_2$, respectively. Then, we get the following proposition.

**Proposition 3.5** Let $C_i$ be an $[n, t_i, d_i]_5$ linear code with $C_i^\perp \subseteq C_i$, $i = 1, 2, 3$. Then,

1. The matrix-product code $C(\tilde{L}_1 \tilde{A}_1) = [C_1, C_2] \tilde{L}_1 \tilde{A}_1$ is an $[2n, t_1 + t_2, \geq d]_5$ Euclidean dual-containing code, where $d = \min\{2d_1, d_2\}$. Further, $C(\tilde{L}_1 \tilde{A}_1)$ generates an $[[2n, 2(t_1 + t_2 - n), \geq d]]_5$ quantum code;

2. The matrix-product code $C(\tilde{L}_2 \tilde{A}_2) = [C_1, C_2, C_3] \tilde{L}_2 \tilde{A}_2$ is an $[3n, t_1 + t_2 + t_3, \geq d]_5$ Euclidean dual-containing code, where $d = \min\{3d_1, 2d_2, d_3\}$. Further, $C(\tilde{L}_2 \tilde{A}_2)$ generates an $[[3n, 2(t_1 + t_2 + t_3) - 3n, \geq d]]_5$ quantum code.

**Proof.** Since $\tilde{L}_1 \tilde{A}_1$ and $\tilde{L}_2 \tilde{A}_2$ are both NSC quasi-orthogonal over $F_5$, we know

$$D_i(\tilde{L}_1 \tilde{A}_1) = 3 - i, i = 1, 2,$$

$$D_j(\tilde{L}_2 \tilde{A}_2) = 4 - j, j = 1, 2, 3.$$ 

Then the result follows from Theorem 3.7. □

Next let us construct the $2 \times 2$, $3 \times 3$ and $4 \times 4$ NSC quasi-orthogonal matrix over $F_7$. Denote by

$$\tilde{A}_3 = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}, \tilde{A}_4 = \begin{bmatrix} 1 & 3 & 4 \\ 0 & 1 & 2 \\ 2 & 3 & 5 \end{bmatrix}, \tilde{A}_5 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}.$$
One can see that $\tilde{A}_3$, $\tilde{A}_4$ and $\tilde{A}_5$ are all NSC, and all leading principal minors of $\tilde{A}_3 A_3^T$, $\tilde{A}_4 A_4^T$ and $\tilde{A}_5 A_5^T$ are nonzero. Then, it follows from Theorem 3.6 that there exist lower unitriangular matrices

$$\tilde{L}_3 = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \tilde{L}_4 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 5 & 1 \end{pmatrix}, \tilde{L}_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 2 & 4 & 2 & 1 \end{pmatrix}$$

such that $\tilde{L}_3 A_3 A_3^T \tilde{L}_3^T = \text{diag}(5, 3)$, $\tilde{L}_4 A_4 A_4^T \tilde{L}_4^T = \text{diag}(5, 6, 1)$, $\tilde{L}_5 A_5 A_5^T \tilde{L}_5^T = \text{diag}(2, 1, 1, 4)$. Hence

$$\tilde{L}_3 A_3 = \begin{pmatrix} 1 & 2 \\ 6 & 4 \end{pmatrix}, \tilde{L}_4 A_4 = \begin{pmatrix} 1 & 3 & 4 \\ 2 & 0 & 3 \\ 3 & 4 & 5 \end{pmatrix}, \tilde{L}_5 A_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 0 & 3 & 2 \\ 0 & 3 & 2 & 4 \\ 6 & 4 & 5 & 5 \end{pmatrix}$$

are all NSC quasi-orthogonal matrix over $\mathbb{F}_7$. Similarly to the above proposition, we have the following proposition.

**Proposition 3.6** Let $C_i$ be an $[n, t_i, d_i]_7$ linear code with $C_i \subseteq C_j$ for each $i = 1, 2, 3, 4$. Then,

1. The matrix-product code $C(L_3 A_3) = [C_1, C_2] L_3 A_3$ is an $[2n, t_1 + t_2, \geq d]_7$ Euclidean dual-containing code, where $d = \min\{2d_1, d_2\}$. Further, $C(L_3 A_3)$ generates an $[[2n, 2(t_1 + t_2 - n), \geq d]]_7$ quantum code;

2. The matrix-product code $C(L_4 A_4) = [C_1, C_2, C_3] L_4 A_4$ is an $[3n, t_1 + t_2 + t_3, \geq d]_7$ Euclidean dual-containing code, where $d = \min\{3d_1, 2d_2, d_3\}$. Further, $C(L_4 A_4)$ generates an $[[3n, 2(t_1 + t_2 + t_3) - 3n, \geq d]]_7$ quantum code;

3. The matrix-product code $C(L_5 A_5) = [C_1, C_2, C_3, C_4] L_5 A_5$ is an $[4n, t_1 + t_2 + t_3 + t_4, \geq d]_7$ Euclidean dual-containing code, where $d = \min\{4d_1, 3d_2, 2d_3, d_4\}$. Further, $C(L_5 A_5)$ generates an $[[4n, 2(t_1 + t_2 + t_3 + t_4 - 2n), \geq d]]_7$ quantum code.

Now we are able to construct the $2 \times 2$, $3 \times 3$ and $4 \times 4$ NSC quasi-orthogonal matrices over $\mathbb{F}_9$. Suppose $\xi$ is a primitive element of $\mathbb{F}_9$. Denote by

$$\tilde{A}_6 = \begin{pmatrix} \xi^2 & \xi^2 \\ 1 & \xi^2 \end{pmatrix}, \tilde{A}_7 = \begin{pmatrix} 1 & \xi^2 & 1 \\ 0 & 1 & \xi \\ 1 & \xi & \xi^2 \end{pmatrix}, \tilde{A}_8 = \begin{pmatrix} 1 & 1 & \xi^2 & 1 \\ 0 & 1 & 1 & \xi^2 \\ 1 & 0 & -1 & \xi^2 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$
\(\widetilde{A}_7 \widetilde{A}_7^T\) and \(\widetilde{A}_8 \widetilde{A}_8^T\) are nonzero. By Theorem 3.6, we obtain lower unitriangular matrices

\[
\widetilde{L}_6 = \begin{bmatrix} 1 & 0 \\ 1 - \xi^2 & 1 \end{bmatrix}, \quad \widetilde{L}_8 = \begin{bmatrix} 1 & 0 & 0 \\ -\xi^2 - \xi & 1 & 0 \\ \xi^3 + 1 & -\xi^2 - \xi & 1 \end{bmatrix},
\]

such that \(\widetilde{L}_6 \widetilde{A}_6 \widetilde{A}_6^T \widetilde{L}_6^T = \text{diag}(1, -\xi^2), \widetilde{L}_7 \widetilde{A}_7 \widetilde{A}_7^T \widetilde{L}_7^T = \text{diag}(1, \xi^3 - 1, \xi^3 - 1), \widetilde{L}_8 \widetilde{A}_8 \widetilde{A}_8^T \widetilde{L}_8^T = \text{diag}(-1, \xi^2 + 1, 1 - \xi^2, -1)\). Hence,

\[
\widetilde{L}_6 \widetilde{A}_6 = \begin{bmatrix} \xi^2 & \xi^2 \\ \xi^2 - 1 & 1 - \xi^2 \end{bmatrix}, \quad \widetilde{L}_7 \widetilde{A}_7 = \begin{bmatrix} 1 & \xi^2 & 1 \\ -\xi^2 - \xi & -\xi^3 - 1 & -\xi^2 \\ \xi^3 - 1 & -\xi & 1 \end{bmatrix},
\]

\[
\widetilde{L}_8 \widetilde{A}_8 = \begin{bmatrix} 1 & 1 & \xi^2 & 1 \\ 1 - \xi^2 & -1 - \xi^2 & \xi^2 - 1 & 1 \\ -\xi^2 & -\xi^2 & 1 - \xi^2 & \xi^2 - 1 \\ 1 & -\xi^2 - 1 & 1 - \xi^2 & -1 \end{bmatrix}
\]

are all NSC quasi-orthogonal matrix over \(\mathbb{F}_9\). This immediately derives the following proposition.

**Proposition 3.7** Let \(C_i\) be an \([n, t_i, d_i]_{9}\) linear code with \(C_i^\perp \subseteq C_i\) for each \(i = 1, 2, 3, 4\). Then,

1. The matrix-product code \(C(\widetilde{L}_6 \widetilde{A}_6) = [C_1, C_2] \widetilde{L}_6 \widetilde{A}_6\) is an \([2n, 2 \{t_1 + t_2\}, \geq d]_9\) Euclidean dual-containing code, where \(d = \min\{2d_1, d_2\}\). Further, \(C(\widetilde{L}_6 \widetilde{A}_6)\) generates an \([2n, 2 (t_1 + t_2 - n), \geq d]_9\) quantum code;

2. The matrix-product code \(C(\widetilde{L}_7 \widetilde{A}_7) = [C_1, C_2, C_3] \widetilde{L}_7 \widetilde{A}_7\) is an \([3n, t_1 + t_2 + t_3, \geq d]_9\) Euclidean dual-containing code, where \(d = \min\{3d_1, 2d_2, d_3\}\). Further, \(C(\widetilde{L}_7 \widetilde{A}_7)\) generates an \([3n, 2 (t_1 + t_2 + t_3) - 3n, \geq d]_9\) quantum code;

3. The matrix-product code \(C(\widetilde{L}_8 \widetilde{A}_8) = [C_1, C_2, C_3, C_4] \widetilde{L}_8 \widetilde{A}_8\) is an \([4n, t_1 + t_2 + t_3 + t_4, \geq d]_9\) Euclidean dual-containing code, where \(d = \min\{4d_1, 3d_2, 2d_3, d_4\}\). Further, \(C(\widetilde{L}_8 \widetilde{A}_8)\) generates an \([4n, 2 (t_1 + t_2 + t_3 + t_4 - 2n), \geq d]_9\) quantum code.

**Remark 3.4** The \(4 \times 4\) NSC quasi-orthogonal matrix \(\widetilde{L}_5 \widetilde{A}_5\) over \(\mathbb{F}_7\) in Proposition 3.6(3) and the \(2 \times 2\), \(3 \times 3\) and \(4 \times 4\) NSC quasi-orthogonal matrices \(\widetilde{L}_6 \widetilde{A}_6, \widetilde{L}_7 \widetilde{A}_7\) and \(\widetilde{L}_8 \widetilde{A}_8\) over \(\mathbb{F}_9\) in
Proposition 3.7 are constructed for the first time by our constructive method in Theorem 3.6. These enable us to construct new classes of Euclidean dual-containing matrix-product codes and the corresponding good quantum codes, as shown in Proposition 3.6(3) and Proposition 3.7, respectively. By our constructive method, some other NSC quasi-orthogonal matrices in different finite fields can be also constructed, which will help us to obtain more classes of good quantum codes.

3.5 Quantum codes related to special matrices $A$ with $AA^T$ being monomial matrices

In this subsection, we consider the matrix $A$ which satisfies that $AA^T$ is a special class of monomial matrices. By applying the matrix $A$ into the defining matrices of matrix-product codes, we can naturally construct some new Euclidean dual-containing matrix-product codes and acquire some good quantum codes by CSS construction.

Let $\alpha$ be a primitive element of $\mathbb{F}_q$. Suppose $1 \leq k < q - 1$ and $k \mid (q - 1)$, then $\alpha^{\frac{q-1}{k}}$ generates a cyclic group with order $k$. For convenience, we write $\beta_i = \alpha^{\frac{i(q-1)}{k}}$, where $i = 0, 1, \ldots, k - 1$. For any $\gamma \in \mathbb{F}_q^*$, let $a = (\gamma \beta_0, \ldots, \gamma \beta_{k-1})$ and $w = (1, \ldots, 1)$. Then, $a$ and $w$ generate the GRS code $GRS_k(a, w)$ whose generator matrix is expressed as follows:

$$A_\gamma = \begin{bmatrix}
1 & 1 & \cdots & 1 \\
\gamma \beta_0 & \gamma \beta_1 & \cdots & \gamma \beta_{k-1} \\
\vdots & \vdots & \ddots & \vdots \\
(\gamma \beta_0)^{k-1} & (\gamma \beta_1)^{k-1} & \cdots & (\gamma \beta_{k-1})^{k-1}
\end{bmatrix}.$$

On the matrix $A_\gamma$, we have the following result.

**Lemma 3.4** ([14]) Assume $1 \leq k < q - 1$ and $k \mid (q - 1)$. For any $\gamma \in \mathbb{F}_q^*$, we have

$$A_\gamma A_\gamma^T = \hat{D}\tau,$$

where $\hat{D} = \text{diag}(k, \gamma k, \ldots, \gamma k)$ and

$$\tau = \begin{pmatrix} 1 & 2 & 3 & \cdots & k \\ 1 & k & k-1 & \cdots & 2 \end{pmatrix}.$$

Note that when $k \geq 3$, the permutation $\tau = \begin{pmatrix} 1 & 2 & 3 & \cdots & k \\ 1 & k & k-1 & \cdots & 2 \end{pmatrix}$ is nontrivial, i.e., $\tau \neq (1)$. Therefore, if we take $A_\gamma$ as the defining matrices of matrix-product codes, we can get a new class of Euclidean dual-containing matrix-product codes and obtain the corresponding good quantum codes by CSS construction.
Theorem 3.8 ([12]) Let $1 \leq k < q - 1$ and $k \mid (q - 1)$. Let $C_i$ be an $[n, t_i, d_i]_q$ linear code with $C_i^\perp \subseteq C_1$ and $C_{k+i}^\perp \subseteq C_i$ for $i = 2, 3, \ldots, k$. Then, the matrix-product code

$$C(A_γ) = [C_1, C_2, \ldots, C_k] A_γ$$

is an $[kn, \sum_{i=1}^k t_i, d]_q$ Euclidean dual-containing code, where $d = \min_{1 \leq i \leq k} \{(k+1-i)d_i\}$. Further, $C(A_γ)$ generates an $[[kn, 2 \sum_{i=1}^k t_i - kn, \geq d]]_q$ quantum code.

Remark 3.5 In Theorem 3.8, the constituent codes of the matrix-product code satisfy the conditions $C_1^\perp \subseteq C_1$ and $C_{k+i}^\perp \subseteq C_i$ where $j = 2, 3, \ldots, k$, which means that: 1) if $k = 2k' + 1$ for $k' \geq 1$, then $C_1^\perp \subseteq C_1$ while the remaining constituent codes $C_2, \ldots, C_k$ are not necessarily dual-containing; 2) if $k = 2k''$ for $k'' \geq 2$, then $C_1^\perp \subseteq C_1$, $C_{k''+1}^\perp \subseteq C_{k''+1}$ while the remaining constituent codes $C_2, \ldots, C_{k''+1}$ are not necessarily dual-containing. Therefore, constituent codes that are not complete Euclidean dual-containing can also generate an Euclidean dual-containing matrix-product code in certain cases.

4 Quantum codes from Hermitian dual-containing matrix-product codes

This section is organized as follows. In subsection 4.1, we recall some basic concepts and properties on Hermitian dual codes, Hermitian construction and matrix-product codes. Subsection 4.2 gives a general approach for constructing quantum codes via Hermitian dual-containing matrix-product codes over $\mathbb{F}_{q^2}$. Subsection 4.3 in turn provides the constructions of quantum codes related to (i) quasi-unitary matrices over $\mathbb{F}_{q^2}$ for any odd prime power $q$; (ii) $2^m \times 2^m$ quasi-unitary matrices over any field $\mathbb{F}_{q^2}$. Subsection 4.4 proposes a constructive method for acquiring general quasi-unitary matrices and NSC quasi-unitary matrices. The utilization of NSC quasi-unitary matrices enables the minimum distance lower bound of the corresponding quantum codes to reach its optimum. By using the constructive method in Subsection 4.4 and certain properties of the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_k]$, Subsection 4.5 constructs $k \times k$ NSC quasi-unitary matrices for any $k < q$ and obtains new classes of good quantum codes related to these matrices. Subsection 4.6 studies the quantum codes related to a special kind of matrices $A$ with $AA^\dagger$ being monomial matrices.

4.1 Basic concepts and properties

Assume that $q$ is a prime power. Let $\mathbb{F}_{q^2}$ be the finite field with $q^2$ elements and let $\mathbb{F}_{q^2}^*$ denote the set of non-zero elements over $\mathbb{F}_{q^2}$. Let $\mathcal{M}(\mathbb{F}_{q^2}, s \times t)$ be the set of $s \times t$ matrices over $\mathbb{F}_{q^2}$. 

27
For any \( a \in \mathbb{F}_{q^2} \), we define \( \overline{a} = a^q \) the conjugate of \( a \). For any matrix \( A = (a_{ij}) \in \mathcal{M}(\mathbb{F}_{q^2}, s \times t) \), we define \( A^\dagger = (a_{ji}) \) its conjugate transpose.

Next, we will recall some basics on the Hermitian dual codes, Hermitian construction and matrix-product codes over \( \mathbb{F}_{q^2} \).

**Definition 4.1** For two vectors \( x = (x_1, x_2, \ldots, x_n) \), \( y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_{q^2}^n \), define
\[
(x, y)_H = \sum_{i=1}^{n} x_i \overline{y}_i.
\]
as the *Hermitian inner product* of \( x \) and \( y \). For a linear code \( C \) of length \( n \) over \( \mathbb{F}_{q^2} \), define its *Hermitian dual code* as
\[
C^\perp_H = \{ x \in \mathbb{F}_{q^2}^n \mid (x, y)_H = 0 \text{ for all } y \in C \}.
\]

**Definition 4.2** Let \( C \) be a linear code over \( \mathbb{F}_{q^2}^n \). Then,
1. If \( C \subseteq C^\perp_H \), then \( C \) is called a *Hermitian self-orthogonal code*;
2. If \( C^\perp_H = C \), then \( C \) is called a *Hermitian self-dual code*;
3. If \( C^\perp_H \subseteq C \), then \( C \) is called a *Hermitian dual-containing code*.

For any vector \( v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_{q^2}^n \), we define \( v^q = (v_1^q, v_2^q, \ldots, v_n^q) \). Let \( S \) be a subset of \( \mathbb{F}_{q^2}^n \) and define \( S^q = \{ v^q \mid v \in S \} \). Then, one can verify that \( C^\perp_H = (C^q)^\perp \) holds for any linear code \( C \) over \( \mathbb{F}_{q^2} \). Therefore, we know that \( C \) is Hermitian dual-containing if and only if \( (C^q)^\perp \subseteq C \) if and only if \( C^\perp \subseteq C^q \).

The following result is called Hermitian construction, which is one of the most frequently-used methods for constructing quantum codes.

**Lemma 4.1** ([2], Hermitian construction) If \( C \) is an \([n, k, d]_{q^2}\) linear code with \( C^\perp_H \subseteq C \), then there exists an \([n, 2k-n, \geq d]_q\) quantum code.

For a matrix-product code over \( \mathbb{F}_{q^2} \), its Hermitian dual code has the following form.

**Lemma 4.2** ([56]) Let \( C_i \) be an \([n, t_i, d_i]_{q^2}\) linear code, where \( i = 1, 2, \ldots, k \). If \( A \in \mathcal{M}(\mathbb{F}_{q^2}, k \times k) \) is non-singular, then
\[
([C_1, C_2, \ldots, C_k]A)^\perp_H = [C_1^\perp_H, C_2^\perp_H, \ldots, C_k^\perp_H](A^{-1})^\dagger.
\]

### 4.2 General approach for constructing quantum codes via Hermitian dual-containing matrix-product codes

Let
\[
\tau = \begin{pmatrix}
1 & 2 & \cdots & k \\
i_1 & i_2 & \cdots & i_k
\end{pmatrix}
\]
denote a permutation on \{1, 2, \ldots, k\}. Let \( P_\tau \) be the \( k \times k \) permutation matrix in which the \( i_j \)-th row of the identity matrix \( I_k \) is replaced with the \( j \)-th row of it for \( j = 1, 2, \ldots, k \).

We give the following definition.

**Definition 4.3** Let \( B \in \mathcal{M}(\mathbb{F}_{q^2}, k \times k) \). If \( B = D P_\tau \), where \( D = \text{diag}(d_{11}, \ldots, d_{kk}) \) with \( d_{ii} \in \mathbb{F}_{q^2}^* \) for each \( i \), then we call \( B \) a monomial matrix with respect to the permutation \( \tau \).

**Definition 4.4** Let \( B \in \mathcal{M}(\mathbb{F}_{q^2}, k \times k) \). If \( BB^\dagger \) is diagonal over \( \mathbb{F}_{q^2}^* \), then we call \( B \) a quasi-unitary matrix over \( \mathbb{F}_{q^2} \). If \( BB^\dagger = I_k \), then we call \( B \) an unitary matrix over \( \mathbb{F}_{q^2} \).

The following theorem gives a general approach for constructing \( q \)-ary quantum codes via Hermitian dual-containing matrix-product codes over \( \mathbb{F}_{q^2} \).

**Theorem 4.1** ([11]) Let \( C_j \) be an \([n, t_j, d_j]_{q^2}\) linear code with \( C_i^\perp \subseteq C_j \) for \( j = 1, 2, \ldots, k \).

For any non-singular matrix \( A \in \mathcal{M}(\mathbb{F}_{q^2}, k \times k) \), if \( AA^\dagger \) is a monomial matrix with respect to the permutation \( \tau \), then the matrix-product code \( C(A) = [C_1, C_2, \ldots, C_k]A \)

is an \([kn, \sum_{i=1}^k t_i, \geq d]_{q^2}\) Hermitian dual-containing code, where \( d = \min_{1 \leq i \leq k} \{D_i(A)d_i\} \). Further, \( C(A) \) generates an \([kn, 2 \sum_{i=1}^k t_i - kn, \geq d]\) quantum code.

By Theorem 4.1, we can construct a Hermitian dual-containing matrix-product code \( C(A) \) over \( \mathbb{F}_{q^2} \), as long as the following two conditions hold:

(i) \( AA^\dagger \) is a monomial matrix with respect to \( \tau \), where \( \tau \) maps each \( j \in \{1, 2, \ldots, k\} \) to \( i_j \in \{1, 2, \ldots, k\} \);

(ii) The constituent codes \( C_1, C_2, \ldots, C_k \) of \( C(A) \) satisfy \( C_i^\perp \subseteq C_j \) for each \( j = 1, 2, \ldots, k \).

Further, we can obtain \( q \)-ary quantum codes by Hermitian construction. In fact, for a given permutation \( \tau \), it is not difficult to find proper constituent codes satisfying (ii). The main difficulty lies in condition (i). As far as we know, it is very difficult to give a general method (not by computer search) for finding the matrix \( A \) in condition (i). Therefore, in the remaining subsections of this section, we will investigate the constructions of quantum codes when the defining matrix \( A \) of \( C(A) \) in turn satisfies different cases: (1) \( A \) is a quasi-unitary matrix; (2) \( A \) is a NSC quasi-unitary matrix; (3) \( AA^\dagger \) is a special monomial matrix.

### 4.3 Quantum codes related to quasi-unitary matrices

When \( \tau \) is an identity permutation, i.e., \( \tau = (1) \), it follows from Theorem 4.1 that
Corollary 4.1 Let $C_i$ be an $[n_i, t_i, d_i]_q$ linear code with $C_i^{t_i} \subseteq C_i$ for $i = 1, 2, \ldots, k$. For any non-singular $A \in \mathcal{M}(\mathbb{F}_q^2, k \times k)$, if $A$ is quasi-unitary, then the matrix-product code

$$C(A) = [C_1, C_2, \ldots, C_k]A$$

is an $[kn, \sum_{i=1}^{k} t_i, \geq d]_q$ Hermitian dual-containing code, where $d = \min_{1 \leq i \leq k} \{d_i, D_i(A)\}$. Further, $C(A)$ generates an $[[kn, 2\sum_{i=1}^{k} t_i - kn, \geq d]]_q$ quantum code.

4.3.1 Quantum codes related to quasi-unitary matrices for odd prime power $q$

First, let us recall the following concepts.

Definition 4.5 ([20]) Let $K$ be a field with character $\text{char}(K) \neq 2$. Let $\sigma$ be a automorphism of $K$. If $\sigma \neq \text{id}$ and $\sigma^2 = \text{id}$, then $\sigma$ is called an involution.

Definition 4.6 ([20]) For any matrix $A = (a_{ij})$, define $A^\sigma = (\sigma(a_{ij}))$. Given a matrix $H \in \mathcal{M}(K, k \times k)$. If $H^T = H^\sigma$, then $H$ is called a Hermitian matrix with respect to the automorphism $\sigma$.

Lemma 4.3 ([20]) Let $K$ be a field with character $\text{char}(K) \neq 2$. Let $\sigma$ be an involution of $K$ and let $K_0$ be the fixed subfield of $\sigma$ in $K$. If $H \in \mathcal{M}(K, k \times k)$ is a Hermitian matrix with respect to $\sigma$ and $\text{rank}(H) = k - t$, then there exists a non-singular matrix $M \in \mathcal{M}(K, k \times k)$ such that

$$M^\sigma H M^T = \text{diag}(h_1, \ldots, h_{k-t}, 0, \ldots, 0),$$

where $h_i \in K_0$ for $i = 1, 2, \ldots, k - t$.

Based on the above facts, we will prove that there exist quasi-unitary matrices and unitary matrices over $\mathbb{F}_{q^2}$ when $q$ is an odd prime power.

Proposition 4.1 Let $q$ be an odd prime power. Then, for any non-singular matrix $A \in \mathcal{M}(\mathbb{F}_{q^2}, k \times k)$, there exists a non-singular matrix $N \in \mathcal{M}(\mathbb{F}_{q^2}, k \times k)$ such that $N A^\dagger N^\dagger$ is diagonal over $\mathbb{F}_{q^2}$, i.e., $N A$ is quasi-unitary over $\mathbb{F}_{q^2}$. Moreover, there exists a non-singular matrix $N' \in \mathcal{M}(\mathbb{F}_{q^2}, k \times k)$ such that $N' A$ is unitary over $\mathbb{F}_{q^2}$.

Proof. In Definition 4.5, let $K = \mathbb{F}_{q^2}$ and $\sigma = \sigma_1 : x \mapsto x^q$. One can verify that $\sigma_1$ is an involution. Hence, $H$ is a Hermitian matrix with respect to $\sigma_1$ if and only if $H^\dagger = H$. Since $A^\dagger = (A^\sigma)^T$, we know $(AA^\dagger)^T = A^\sigma A^T = (AA^\dagger)^\sigma$. Then, $AA^\dagger$ is a Hermitian matrix with respect to $\sigma_1$. As $AA^\dagger$ is non-singular, it follows from Lemma 4.3 that there exists a non-singular matrix $N$ such that $NAA^\dagger N^\dagger$ is diagonal over $\mathbb{F}_{q^2}$. Write $NAA^\dagger N^\dagger = \text{diag}(r_1, r_2, \ldots, r_k)$, where each $r_i \in \mathbb{F}_{q^2}$. By $NAA^\dagger N^\dagger = (NAA^\dagger N^\dagger)^\dagger$ we know that $r_i = r_i^q$, then $r_i \in \mathbb{F}_q^\times$. Thus, $NAA^\dagger N^\dagger$ is diagonal over $\mathbb{F}_q^\times$, i.e., $NA$ is quasi-unitary over $\mathbb{F}_{q^2}$.
Moreover, by \( r_i \in \mathbb{F}_q^* \) we know that there exists \( s_i \in \mathbb{F}_q^* \) such that \( r_i = s_i^{q+1} \). Let \( N' = D_1 N \), where \( D_1 = \text{diag}(s_1^{-1}, s_2^{-1}, \ldots, s_k^{-1}) \). Then, \( N' A A^L(N')^\dagger = I_k \), i.e., \( N' A \) is unitary over \( \mathbb{F}_q^2 \). This completes the proof. \( \square \)

By Proposition 4.1, we can construct Hermitian dual-containing matrix-product codes and obtain the corresponding quantum codes in the following theorem.

**Theorem 4.2** Let \( q \) be an odd prime power. Let \( C_i \) be an \([n_i, t_i, d_i]_{q^2}\) linear code with \( C_i^{\perp_{H}} \subseteq C_i \) for \( i = 1, 2, \ldots, k \). Then, for any non-singular matrix \( A \in \mathcal{M}(\mathbb{F}_{q^2}, k \times k) \), there exist non-singular matrices \( N, N' \in \mathcal{M}(\mathbb{F}_{q^2}, k \times k) \) such that the matrix-product codes

\[
C(NA) = [C_1, C_2, \ldots, C_k]NA
\]

and

\[
C(N'A) = [C_1, C_2, \ldots, C_k]N'A
\]

are \([kn, \sum_{i=1}^{k} t_i, \geq d'_i]_{q^2}\) Hermitian dual-containing code and \([kn, \sum_{i=1}^{k} t_i, \geq d''_i]_{q^2}\) Hermitian dual-containing code, respectively, where \( d' = \min_{1 \leq i \leq k} \{d_i D_i(NA)\} \) and \( d'' = \min_{1 \leq i \leq k} \{d_i D_i(N'A)\} \).

Further, \( C(NA) \) and \( C(N'A) \) can generate quantum codes with parameters \([kn, 2 \sum_{i=1}^{k} t_i - kn, \geq d'_i]_{q} \) and \([kn, 2 \sum_{i=1}^{k} t_i - kn, \geq d''_i]_{q} \), respectively.

**Proof.** It is immediately obtained by Corollary 4.1 and Proposition 4.1. \( \square \)

**4.3.2 Quantum codes related to a \( 2^m \times 2^m \) quasi-unitary matrices**

Similar to Proposition 3.3, we now construct a special kind of quasi-unitary matrices.

**Proposition 4.2** In the finite field \( \mathbb{F}_{q^2} \), suppose \( c = c_1^{q+1} + \cdots + c_{2^m}^{q+1} \neq 0 \). Then, there exists a matrix \( S = (s_{i,j}) \in \mathcal{M}(\mathbb{F}_{q^2}, 2^m \times 2^m) \) such that \( S^\dagger S = SS^\dagger = c I_{2^m} \), i.e., \( S \) is quasi-unitary over \( \mathbb{F}_{q^2} \), where \( (c_1, \ldots, c_{2^m}) \) denotes the first row of \( S \).

**Proof.** Assume that the result holds for \( m-1 \). Write \( c = a + b \), where

\[
a = c_1^{q+1} + \cdots + c_{2^{m-1}}^{q+1},
\]

\[
b = c_{2^{m-1}+1}^{q+1} + \cdots + c_{2^m}^{q+1}.
\]

Then, there exist \( A, B \in \mathcal{M}(\mathbb{F}_{q^2}, 2^{m-1} \times 2^{m-1}) \) such that

\[
AA^\dagger = A^\dagger A = a I_{2^{m-1}},
\]

\[
BB^\dagger = B^\dagger B = b I_{2^{m-1}},
\]

where \( (c_1, \ldots, c_{2^{m-1}}) \) and \( (c_{2^{m-1}+1}, \ldots, c_{2^m}) \) are the first row of \( A \) and \( B \), respectively. 31
Now let us discuss the following two cases.

**Case (1):** When \( a \neq 0 \), take
\[
S = \begin{bmatrix}
A & B \\
-a^{-1}A^\dagger B^\dagger & A^\dagger
\end{bmatrix}.
\]
Then, we have \( S^\dagger S = SS^\dagger = cI_{2m} \), and \((c_1, \ldots, c_{2m})\) is the first row of \( S \).

**Case (2):** When \( b \neq 0 \), take
\[
S = \begin{bmatrix}
B & A \\
-b^{-1}B^\dagger A^\dagger & B^\dagger
\end{bmatrix}.
\]
Then, we have \( S^\dagger S = SS^\dagger = cI_{2m} \), and \((c_1, \ldots, c_{2m})\) is the first row of \( S \).

Therefore, \( S \) is quasi-unitary over \( \mathbb{F}_{q^2} \). This completes the proof.

By Corollary 4.1 and Proposition 4.2, we can directly obtain the following theorem.

**Theorem 4.3** Let \( C_i \) be an \([n, t_i, d_i]_q\) linear code with \( C_i^\perp \subseteq C_i \) for \( i = 1, 2, \ldots, 2^m \). In \( \mathbb{F}_{q^2} \), write \( c = c_{1}^{q+1} + \cdots + c_{2^m}^{q+1} \neq 0 \). Then, there exists a matrix \( S \in \mathcal{M}(\mathbb{F}_{q^2}, 2^m \times 2^m) \) such that the matrix-product code
\[
C(S) = [C_1, C_2, \ldots, C_{2^m}]S
\]
is an \([2^m n, \sum_{i=1}^{2^m} t_i, \geq d]_q\) Hermitian dual-containing code, where \( d = \min_{1 \leq i \leq 2^m} \{d_i D_i(S)\} \). Further, \( C(S) \) generates an \([[2^m n, 2 \sum_{i=1}^{2^m} t_i - 2^m n, \geq d]]_q\) quantum code.

### 4.4 Quantum codes related to NSC quasi-unitary matrices

In this subsection, we will construct NSC quasi-unitary matrices as the defining matrices of matrix-product codes. By Hermitian construction, we can obtain some classes of good quantum codes.

Recall that in Corollary 4.1 when the defining matrix \( A \) is quasi-unitary, we can construct a Hermitian dual-containing matrix-product code. Further, it can generate an \([kn, 2 \sum_{i=1}^{k} t_i - kn, \geq d]_q\) quantum code from Hermitian construction, where \( d = \min_{1 \leq i \leq k} \{d_i D_i(A)\} \). Here \( D_i(A) \leq k + 1 - i \). Similar to Subsection 3.4, we wish to make the minimum distance lower bound of the constructed matrix-product codes as large as possible. In other words, we need to find the quasi-unitary matrix \( A \) satisfying \( D_i(A) = k + 1 - i \). Similar to Subsection 3.4, we can consider NSC matrices. For a matrix \( A \), if it is both NSC and quasi-unitary, then we call \( A \) NSC quasi-unitary.

The following theorem gives a constructive method for constructing general quasi-unitary matrices and NSC quasi-unitary matrices.
Theorem 4.4 ([13], Constructive method) Let $A \in M(\mathbb{F}_{q^2}, k \times k)$ be non-singular. If all leading principal minors of $AA^\dagger$ are nonzero, then there exists a lower unitriangular matrix $L$ such that $LA$ is quasi-unitary over $\mathbb{F}_{q^2}$. Further, if $A$ is NSC, then $LA$ is NSC quasi-unitary.

Remark 4.1 As far as we know, the constructive method for acquiring general quasi-unitary matrices and NSC quasi-unitary matrices in Theorem 4.4 was proposed in [13] for the first time.

Remark 4.2 Let $B_i$ denote the matrix consisting of the last $i$ rows and the last $i$ columns of $AA^\dagger$. Suppose $B_i$ is non-singular for each $i = 1, \ldots, k$. We can write $AA^\dagger$ as

$$AA^\dagger = \begin{bmatrix} b & g^\dagger & B_{k-1} \\ g & B_{k-1} \end{bmatrix},$$

where $B_{k-1} = B_{k-1}^\dagger$ and $b = b^\theta$. Then, there exists an upper unitriangular matrix

$$U_{k-1} = \begin{bmatrix} 1 & -g^\dagger B_{k-1}^{-1} \\ 0_{(k-1) \times 1} & I_{k-1} \end{bmatrix}$$

such that

$$U_{k-1}AA^\dagger U_{k-1}^\dagger = \begin{bmatrix} b - g^\dagger B_{k-1}^{-1} g & 0_{1 \times (k-1)} \\ 0_{(k-1) \times 1} & B_{k-1} \end{bmatrix}.$$ 

Similar to the proof of Theorem 4.4, one can finally obtain an upper unitriangular matrix $U$ such that $UA$ is quasi-unitary. However, it can be checked that $UA$ may not be NSC for some NSC matrix $A$.

Corollary 4.2 Let $k \leq q^2$. Assume that $x_1, \ldots, x_k$ are $k$ distinct elements in $\mathbb{F}_{q^2}$. Let

$$V = \begin{bmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_k \\ \lambda_1 x_1 & \lambda_2 x_2 & \cdots & \lambda_k x_k \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1 x_1^{k-1} & \lambda_2 x_2^{k-1} & \cdots & \lambda_k x_k^{k-1} \end{bmatrix},$$

where $\lambda_i \in \mathbb{F}_{q^2}^*$. If all leading principal minors of $VV^\dagger$ are nonzero, then there exists a lower unitriangular matrix $L$ such that $LV$ is NSC quasi-unitary over $\mathbb{F}_{q^2}$.

Proof. Since $k \leq q^2$, then for any $1 \leq s \leq k$ and $1 \leq j_1 < \cdots < j_s \leq k$, we have

$$|V(j_1, \ldots, j_s)| = \prod_{i=1}^s \lambda_{j_i} \cdot \prod_{1 \leq n < m \leq s} (x_{j_m} - x_{j_n}) \neq 0.$$ 

Hence, $V$ is NSC. Then the result follows by Theorem 4.4. \qed

Next, let $\alpha$ be a primitive element of $\mathbb{F}_{q^2}$. Assume that $k \mid (q + 1)$ and write $\beta_i = \alpha^{\frac{q^2-1}{q^2-1}}$ for $i = 0, 1, \ldots, k - 1$. If we take $L = I_k$ in Theorem 4.4, then we get the following corollary.
Corollary 4.3 ([33]) Let $k | (q + 1)$ and $M = (\beta_{i,j}^{-1})_{i,j=1}^k$. Then, we have $MM^\dagger = kI_k$, i.e., $M$ is NSC quasi-unitary.

According to Theorem 4.4, we have the following theorem.

Theorem 4.5 ([13]) Let $C_i$ be an $[n, t_i, d_i]_q$ linear code with $C_i^{1:n} \subseteq C_i$ for each $i = 1, 2, \ldots, k$. For any NSC matrix $A \in M(\mathbb{F}_q, k \times k)$, if all leading principal minors of $AA^\dagger$ are nonzero, then there exists a lower unitriangular matrix $L$ such that the matrix-product code

$$C(LA) = [C_1, C_2, \ldots, C_k]LA$$

is an $[kn, \sum_{i=1}^k t_i, \geq d]_q$ Hermitian dual-containing code, where $d = \min_{1 \leq i \leq k} \{(k + 1 - i)d_i\}$. Further, $C(LA)$ generates an $[[kn, 2\sum_{i=1}^k t_i - kn, \geq d]]_q$ quantum code.

By Theorem 4.5 and Corollary 4.2, we obtain the following corollaries.

Corollary 4.4 Let $k \leq q^2$. Let $C_i$ be an $[n, t_i, d_i]_q$ linear code with $C_i^{1:n} \subseteq C_i$ for each $i = 1, 2, \ldots, k$. Let $V$ be defined as in Corollary 4.2. If all leading principal minors of $VV^\dagger$ are nonzero, then there exists a lower unitriangular matrix $L$ such that the matrix-product code

$$C(LV) = [C_1, C_2, \ldots, C_k]LV$$

is an $[kn, \sum_{i=1}^k t_i, \geq d]_q$ Hermitian dual-containing code, where $d = \min_{1 \leq i \leq k} \{(k + 1 - i)d_i\}$. Further, $C(LV)$ generates an $[[kn, 2\sum_{i=1}^k t_i - kn, \geq d]]_q$ quantum code by Hermitian construction.

Corollary 4.5 Let $k | (q + 1)$ and $M$ be defined as in Corollary 4.3. Let $C_i$ be an $[n, t_i, d_i]_q$ linear code with $C_i^{1:n} \subseteq C_i$ for each $i = 1, 2, \ldots, k$. Then, the matrix-product code

$$C(M) = [C_1, C_2, \ldots, C_k]M$$

is an $[kn, \sum_{i=1}^k t_i, \geq d]_q$ Hermitian dual-containing code, where $d = \min_{1 \leq i \leq k} \{(k + 1 - i)d_i\}$. Further, $C(M)$ generates an $[[kn, 2\sum_{i=1}^k t_i - kn, \geq d]]_q$ quantum code by Hermitian construction.

From Theorem 4.5, we have the following corollary.

Corollary 4.6 Let $C_i$ be an $[n, t_i, d_i]_q$ linear code with $C_i^{1:n} \subseteq C_i$ for $i = 1, 2, 3, 4$. Then,

(1) There exists an $2 \times 2$ NSC quasi-unitary matrix $\hat{L}_1A_1$ over $\mathbb{F}_q^2$, such that the matrix-product code

$$C(\hat{L}_1A_1) = [C_1, C_2]\hat{L}_1A_1$$

is an $[2n, t_1 + t_2, \geq d]_q^2$ Hermitian dual-containing code, where $d = \min \{2d_1, d_2\}$. Further, $C(\hat{L}_1A_1)$ generates an $[[2n, 2(t_1 + t_2 - n), \geq d]]_q$ quantum code.
(2) There exists an $3 \times 3$ NSC quasi-unitary matrix $\widehat{L_2A_2}$ over $\mathbb{F}_{q^2}$, such that the matrix-product code

$$C(\widehat{L_2A_2}) = [C_1, C_2, C_3]\widehat{L_2A_2}$$

is an $[3n, t_1 + t_2 + t_3, \geq d]_{q^2}$ Hermitian dual-containing code, where $d = \min\{3d_1, 2d_2, d_3\}$. Further, $C(\widehat{L_2A_2})$ generates an $[[3n, 2(t_1 + t_2 + t_3) - 3n, \geq d]]_q$ quantum code.

(3) When $q \geq 5$, there exists an $4 \times 4$ NSC quasi-unitary matrix $\widehat{L_3A_3}$ over $\mathbb{F}_{q^2}$, such that the matrix-product code

$$C(\widehat{L_3A_3}) = [C_1, C_2, C_3, C_4]\widehat{L_3A_3}$$

is an $[4n, t_1 + t_2 + t_3 + t_4, \geq d]_{q^2}$ Hermitian dual-containing code, where $d = \min\{4d_1, 3d_2, 2d_3, d_4\}$. Further, $C(\widehat{L_3A_3})$ generates an $[[4n, 2(t_1 + t_2 + t_3 + t_4) - 4n, \geq d]]_q$ quantum code.

**Proof.** (1) Define

$$\mathcal{R}_1 = \{x|x \in \mathbb{F}_{q^2}^*, x^2 \neq 1, x^{q+1} \neq -1\}.$$  

Clearly, this set is nonempty. For any $a_1 \in \mathcal{R}_1$, take

$$\widehat{A}_1 = \begin{bmatrix} 1 & a_1 \\ a_1 & 1 \end{bmatrix},$$

then $\widehat{A}_1$ is NSC and all leading principal minors of $\widehat{A}_1\widehat{A}_1^\top$ are nonzero. By Theorem 4.4, there exists a lower unitriangular matrix

$$\widehat{L}_1 = \begin{bmatrix} 1 & 0 \\ -(a_1^q + a_1)(1 + a_1^{q+1})^{-1} & 1 \end{bmatrix}$$

such that

$$\widehat{L}_1\widehat{A}_1\widehat{A}_1^\top\widehat{L}_1^\top = \text{diag}(1 + a_1^{q+1}, (1 - a_1^q)(1 - a_1^{2q})(1 + a_1^{q+1})^{-1}).$$

Hence, $\widehat{L}_1\widehat{A}_1$ is an $2 \times 2$ NSC quasi-unitary matrix over $\mathbb{F}_{q^2}$. Using Theorem 4.5, we know that $C(\widehat{L}_1\widehat{A}_1)$ is an $[2n, t_1 + t_2, \geq d]_{q^2}$ Hermitian dual-containing code. Further, it generates an $[[2n, 2(t_1 + t_2 - n), \geq d]]_q$ quantum code by Hermitian construction, where $d = \min\{2d_1, d_2\}$.

(2) Define

$$\mathcal{R}_2 = \{x|x \in \mathbb{F}_{q^2}^* \setminus \{1\}, x^{q+1} + 2 \neq 0, x^{q+1} - x^q - x + 3 \neq 0\}.$$  

Clearly, this set is nonempty. For any $a_2 \in \mathcal{R}_2$, take

$$\widehat{A}_2 = \begin{bmatrix} 1 & 1 & a_2 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix},$$

Writing
then \( \widehat{A}_2 \) is NSC and all leading principal minors of \( \widehat{A}_2 \widehat{A}_2^\dagger \) are nonzero. By Theorem 4.4, there exists a lower unitriangular matrix

\[
\widehat{L}_2 = \begin{bmatrix}
1 & 0 & 0 \\
-(a_2^q + 1)(a_2^{q+1} + 2)^{-1} & 1 & 0 \\
(1 - a_2^q)p_1 & (a_2^q - 2)p_1 & 1
\end{bmatrix}
\]

such that

\[
\widehat{L}_2 \widehat{A}_2 \widehat{A}_2^\dagger \widehat{L}_2^{-1} = \text{diag}(a_2^{q+1} + 2, (a_2^{q+1} + 2)^{-1} p_1^{-1}, p_1),
\]

where \( p_1 = (a_2^{q+1} - a_2^q - a_2 + 3)^{-1} \). Hence, \( \widehat{L}_2 \widehat{A}_2 \) is an \( 3 \times 3 \) NSC quasi-unitary matrix over \( \mathbb{F}_{q^2} \). Using Theorem 4.5, we know that \( C(\widehat{L}_2 \widehat{A}_2) \) is an \( [3n, t_1 + t_2 + t_3, \geq d]_{q^2} \) Hermitian dual-containing code. Further, it generates an \( [[3n, 2(t_1 + t_2 + t_3) - 3n, \geq d]]_q \) quantum code by Hermitian construction, where \( d = \min\{3d_1, 2d_2, d_3\} \).

(3) When \( q \geq 5 \), define

\[
\mathcal{R}_3 = \{ x | x \in \mathbb{F}_{q^3}^* \setminus \{ \pm 1, 3 \}, x^{q+1} + 3 \neq 0, 2x^{q+1} + 9 \neq 0, x^{q+1} - 3x^q - 3x + 15 \neq 0 \}.
\]

Clearly, this set is nonempty. For any \( a_3 \in \mathcal{R}_3 \), take

\[
\widehat{A}_3 = \begin{bmatrix}
1 & 1 & 1 & a_3 \\
1 & 0 & -1 & 1 \\
0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1
\end{bmatrix},
\]

then \( \widehat{A}_3 \) is NSC and all leading principal minors of \( \widehat{A}_3 \widehat{A}_3^\dagger \) are nonzero. By Theorem 4.4, there exists a lower unitriangular matrix

\[
\widehat{L}_3 = \begin{bmatrix}
1 & 0 & 0 & 0 \\
-a_3^q p_4 & 1 & 0 & 0 \\
-3p_4 p_5 & a_3 p_4 p_5 & 1 & 0 \\
(3 - a_3^q)p_2 & (a_3^q - 5)p_2 & (2a_3^q - 9)p_2 & 1
\end{bmatrix}
\]

such that

\[
\widehat{L}_3 \widehat{A}_3 \widehat{A}_3^\dagger \widehat{L}_3^{-1} = \text{diag}(p_4^{-1}, p_4 p_5^{-1}, p_4 p_5^{-1}, p_2),
\]

where \( p_2 = (a_3^{q+1} - 3a_3^q - 3a_3 + 15)^{-1}, p_3 = (2a_3^{q+1} + 9)^{-1}, p_4 = (a_3^q + 3)^{-1} \) and \( p_5 = a_3^q + 1 \). Hence, when \( q \geq 5 \), \( \widehat{L}_3 \widehat{A}_3 \) is an \( 4 \times 4 \) NSC quasi-unitary matrix over \( \mathbb{F}_{q^2} \). Using Theorem 4.5, we know that \( C(\widehat{L}_3 \widehat{A}_3) \) is an \( [4n, t_1 + t_2 + t_3 + t_4, \geq d]_{q^2} \) Hermitian dual-containing code. Further, it generates an \( [[4n, 2(t_1 + t_2 + t_3 + t_4) - 4n, \geq d]]_q \) quantum code by Hermitian construction, where \( d = \min\{4d_1, 3d_2, 2d_3, d_4\} \). \( \square \)
Remark 4.3 In Remark 4.5, we will give a different manner to construct the $3 \times 3$ NSC quasi-unitary matrices over $\mathbb{F}_{q^2}$. Note that the minimum distance lower bound $\min\{4d_1, 3d_2, 2d_3, d_4\}$ of the quantum codes in Corollary 4.6(3) is superior to the minimum distance lower bound $\min\{4d_1, 2d_2, 2d_3, d_4\}$ of those in [40, Theorem 3.5] since our newly constructed $4 \times 4$ quasi-unitary matrix is NSC while it is not NSC in [40, Theorem 3.5].

4.5 Quantum codes related to $k \times k$ NSC quasi-unitary matrices for any $k < q$

In this subsection, we will provide several important properties related to the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_k]$. Combining these properties with Theorem 4.4, we can construct new classes of NSC quasi-unitary matrices, which enables us to construct new classes of Hermitian dual-containing matrix-product codes and further acquire good quantum codes by Hermitian construction.

For a nonzero polynomial $f(x_1, \ldots, x_k) \in \mathbb{F}_q[x_1, \ldots, x_k]$, we use $\deg(f; x_i)$ to denote the degree of $f(x_1, \ldots, x_k)$ in $x_i$. First, we obtain the following proposition.

Proposition 4.3 ([13]) For a nonzero polynomial $f(x_1, \ldots, x_k) \in \mathbb{F}_q[x_1, \ldots, x_k]$, the following two statements are equivalent:

1. For any $a_1, \ldots, a_k \in \mathbb{F}_q$, $f(a_1, \ldots, a_k) = 0$;
2. There exist polynomials $g_i(x_1, \ldots, x_k), i = 1, \ldots, k$ in $\mathbb{F}_q[x_1, \ldots, x_k]$ such that

$$f(x_1, \ldots, x_k) = \sum_{i=1}^{k} g_i(x_1, \ldots, x_k) \cdot (x_i^q - x_i)$$

with $\deg(g_j; x_i) < q$ for each $i < j$.

By Proposition 4.3, we obtain the following proposition.

Proposition 4.4 ([13]) Let $f_1(x_1, \ldots, x_k), f_2(x_1, \ldots, x_k), \ldots, f_v(x_1, \ldots, x_k)$ be $v$ nonzero polynomials in $\mathbb{F}_q[x_1, \ldots, x_k]$. If $\sum_{j=1}^{v} \deg(f_j; x_i) < q$ holds for each $i$, then there exist $a_1, \ldots, a_k \in \mathbb{F}_q$ such that $f_j(a_1, \ldots, a_k) \neq 0$ holds for each $j$.

Denote by $A^{(i_1 \cdots i_u)}_{(j_1 \cdots j_u)}$ the $u \times u$ matrix consisting of the $i_1, \ldots, i_u$ rows and the $j_1, \ldots, j_u$ columns of $A$. Obviously, $A^{(1 \cdots u)}_{(j_1 \cdots j_u)}$ is just the matrix $A(j_1, \ldots, j_u)$ in Definition 3.6.

Now let us recall the Cauchy-Binet formula.

Lemma 4.4 ([29], Cauchy-Binet formula) Let $X = (x_{ij})$ be an $s \times n$ matrix and $Y = (y_{ij})$ be an $n \times s$ matrix. Then, for any positive integer $u \leq s$,

1. If $u > n$, then all $u \times u$ sub-determinant of $XY$ is 0;
(2) If \( u \leq n \), then the \( u \times u \) sub-determinant consisting of the \( i_1, \ldots, i_u \) rows and the \( j_1, \ldots, j_u \) columns of \( XY \) is

\[
\begin{vmatrix} X \end{vmatrix}_{i_1 \cdots i_u \atop j_1 \cdots j_u} = \sum_{1 \leq v_1 < \cdots < v_u \leq n} \begin{vmatrix} X \end{vmatrix}_{v_1 \cdots v_u \atop v_1 \cdots v_u} \begin{vmatrix} Y \end{vmatrix}_{v_1 \cdots v_u \atop j_1 \cdots j_u}.
\]

Using Proposition 4.4 and Lemma 4.4, we can obtain the following proposition.

Proposition 4.5 ([13]) Let \( k \) be a positive integer with \( k < q \). Then, for any non-singular matrix \( A \in M(F_{q^2}, k \times k) \), there exist \( \lambda_1, \ldots, \lambda_k \in F_{q^2}^* \) such that all leading principal minors of \( BB^\dagger \) are nonzero, where \( B = A \cdot \text{diag}(\lambda_1, \ldots, \lambda_k) \).

By proposition 4.5, we give the following proposition.

Proposition 4.6 ([13]) Let \( k \) be a positive integer with \( k < q \). Then, for any NSC matrix \( A \in M(F_{q^2}, k \times k) \), there exist \( \lambda_1, \ldots, \lambda_k \in F_{q^2}^* \) such that the matrix \( B = A \cdot \text{diag}(\lambda_1, \ldots, \lambda_k) \) satisfies the following properties:

1. All leading principal minors of \( BB^\dagger \) are nonzero;
2. \( B \in M(F_{q^2}, k \times k) \) is NSC.

Now, by using Proposition 4.6 and Theorem 4.4 we obtain new classes of NSC quasi-unitary matrices as follows.

Theorem 4.6 ([13]) There exist \( k \times k \) NSC quasi-unitary matrices over \( F_{q^2} \) for each \( k < q \).

Remark 4.4 Up to now the known (NSC) quasi-unitary matrices over \( F_{q^2} \) for constructing \( q \)-ary quantum codes via Hermitian dual-containing matrix-product codes can be summarized as follows.

- Refs [33, 42, 56] constructed \( 2 \times 2 \) NSC quasi-unitary matrices;
- For any odd prime power \( q \), Refs [40, 42] constructed \( 4 \times 4 \) quasi-unitary matrices that are not NSC;
- Ref [33] constructed \( k \times k \) NSC quasi-unitary matrices for \( k|\( q + 1 \) \) (see also Corollary 4.3), which can be deduced by the constructive method in Theorem 4.4;
- In [13], the author of this article and his cooperators constructed \( 3 \times 3 \) NSC quasi-unitary matrices (see also Corollary 4.6(2)). What’s more, they constructed \( k \times k \) NSC quasi-unitary matrices for any \( k < q \) (see also Theorem 4.6).

Compared with the quasi-unitary matrices in [33, 40, 42, 56], quasi-unitary matrices in [13] are all NSC and their range of orders is much broader. We list these results in Table 1.
| $k$ | Field | NSC (Yes/No) | References |
|-----|-------|--------------|------------|
| 2   | $F_{q^2}, q \neq 2$ | Yes | [33,42,56] |
| 3   | $F_{q^2}$ | Yes | [13], see also Corollary 4.6(2) |
| 4   | $F_{q^2}, q$ odd prime power | No | [40,42] |
| $k \mid (q + 1)$ | $F_{q^2}$ | Yes | [33], see also Corollary 4.3 |
| $k < q$ | $F_{q^2}$ | Yes | [13], see also Theorem 4.6 |

**Remark 4.5** In Corollary 4.6(2), we prove the existence of the $3 \times 3$ NSC quasi-unitary matrices over $F_{q^2}$. Here, we give a new manner to construct them. The detailed procedures are as follows.

**Step (a):** By Corollary 4.3, we know that there exist $3 \times 3$ NSC quasi-unitary matrices over $F_{q^2}$;

**Step (b):** It follows from Theorem 4.6 that there exist $3 \times 3$ NSC quasi-unitary matrices over $F_{q^2}$ for any $q \geq 4$;

**Step (c):** Define

$$W = \{ x \in F_{q^2} \mid x^4 - 1 \neq 0, x^4 - x^3 - x \neq 0 \}.$$ 

We know this set is nonempty. Take any $a \in W$ and denote by

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

One can verify that $A$ is NSC and all leading principal minors of $AA^\dagger$ are nonzero. By Theorem 4.4, there exists a lower unitriangular matrix $L$ such that $LA$ is NSC quasi-unitary. Hence, there exist $3 \times 3$ NSC quasi-unitary matrices over $F_{q^2}$.

In terms of Steps (a)-(c), we know that there always exist $3 \times 3$ NSC quasi-unitary matrices in any finite field $F_{q^2}$.

Using Corollary 4.6(2), Theorem 4.6 and Hermitian construction, we can construct new classes of good quantum codes as follows.

**Theorem 4.7** ([13]) Let $C_i$ be an $[n, t_i, d_i]_{q^2}$ linear code with $C_i^{⊥,n} \subseteq C_i$ for $i = 1, \ldots, k$. Then,

1. For $k = 3$, there exists an $[[3n, 2 \sum_{i=1}^{3} t_i - 3n, \geq d]]_{q}$ quantum code, where $d = \min_{1 \leq i \leq 3} \{(4 - i)d_i\}$.

2. For each positive integer $k$ with $k < q$, there exists an $[[kn, 2 \sum_{i=1}^{k} t_i - kn, \geq d]]_{q}$ quantum code, where $d = \min_{1 \leq i \leq k} \{(k + 1 - i)d_i\}$.
4.6 Quantum codes related to special matrices $A$ with $AA^\dagger$ being monomial matrices

In this subsection, we consider the special matrices $A$ satisfying $AA^\dagger$ is a class of monomial matrices. By applying the matrices $A$ into the defining matrices of matrix-product codes, we can naturally construct some new Hermitian dual-containing matrix-product codes and acquire some good quantum codes by Hermitian construction.

Let $\alpha$ be a primitive element of $\mathbb{F}_{q^2}$. Assume that $k \mid (q^2 - 1)$ and $k \nmid (q + 1)$. Let

$$U_{q,k} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \beta_0 & \beta_1 & \cdots & \beta_{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_0^{k-1} & \beta_1^{k-1} & \cdots & \beta_{k-1}^{k-1} \end{bmatrix},$$

where $\beta_i = \alpha^{\frac{q^2-1}{k}i}$, $i = 0, 1, \ldots, k - 1$. Now one can verify that the following result holds.

**Lemma 4.5** Let $k \mid (q^2 - 1)$ and $k \nmid (q + 1)$. Then, $U_{q,k}^* U_{q,k}^\dagger = kP_{q,k}$, where

$$\omega_{q,k} = \begin{bmatrix} 1 & 2 & \cdots & k \\ j_0 + 1 & j_1 + 1 & \cdots & j_{k-1} + 1 \end{bmatrix}$$

in which $j_s$ is the unique solution of the equation $s + qx \equiv 0 \pmod{k}$ in $\{0, 1, \ldots, k - 1\}$ for each $s = 0, 1, \ldots, k - 1$.

Using Lemma 4.5, we obtain the following theorem.

**Theorem 4.8** ([11]) Let $k \mid (q^2 - 1)$ and $k \nmid (q + 1)$. Let $C_i$ be an $[n, t_i, d_i]_{q^2}$ linear code with $C_{s+1}^\perp \subseteq C_{j_s+1}$ for each $i = 1, 2, \ldots, k$, where $j_s \in \{0, 1, \ldots, k - 1\}$ is the unique solution of the equation $s + qx \equiv 0 \pmod{k}$ for each $s \in \{0, 1, \ldots, k - 1\}$. Then, the matrix-product code

$$C(U_{q,k}) = [C_1, C_2, \ldots, C_k]U_{q,k}$$

is an $[kn, \sum_{i=1}^k t_i, \geq d]_{q^2}$ Hermitian dual-containing code, where $d = \min_{1 \leq i \leq k} \{(k + 1 - i)d_i\}$. Further, $C(U_{q,k})$ generates an $[[kn, 2 \sum_{i=1}^k t_i - kn, \geq d]]_q$ quantum code.

**Remark 4.6** By the condition $C_{s+1}^\perp \subseteq C_{j_s+1}$ in Theorem 4.8 we know that $C_{s+1}^\perp \subseteq C_{s+1}$ holds for each positive integer $s$ satisfying $k \mid (q + 1)s$, while the remaining constituent codes are not required to be Hermitian dual-containing. This reveals that constituent codes that are not complete Hermitian dual-containing can also generate an Hermitian dual-containing matrix-product code in certain cases.
In Theorem 4.8, if the defining matrix $U_{q,k}$ is replaced with $P_{q,k}U_{q,k}$, then we can prove that the corresponding matrix-product code $C(P_{q,k}U_{q,k})$ is also Hermitian dual-containing. The detailed process is shown in [11].

**Theorem 4.9 ([11])** Let $k \mid (q^2 - 1)$ and $k \nmid (q + 1)$. Let $C_i$ be an $[n, t_i, d_i]_{q^2}$ linear code with $C_{s+1}^+ \subseteq C_{j+1}$ for each $i = 1, 2, \ldots, k$, where $j_s \in \{0, 1, \ldots, k - 1\}$ is the unique solution of the equation $s + qx \equiv 0 \pmod{k}$ for each $s \in \{0, 1, \ldots, k - 1\}$. Then, the matrix-product code

$$C(P_{q,k}U_{q,k}) = [C_1, C_2, \ldots, C_k]P_{q,k}U_{q,k}$$

is an $[kn, \sum_{i=1}^{k} t_i, \geq d]_{q^2}$ Hermitian dual-containing code, where $d = \min_{1 \leq i \leq k} \{(k + 1 - i)d_i\}$, and $\varsigma_{q,k}$ is defined as in Lemma 4.5. Further, $C(P_{q,k}U_{q,k})$ generates an $[[kn, 2 \sum_{i=1}^{k} t_i - kn, \geq d]]_{q}$ quantum code.

## 5 Concluding remarks

In this section, we will make a summary of this article and propose the prospect of the follow-up work.

### 5.1 Main results and remarks

We explored the constructions of $q$-ary quantum codes by constructing Euclidean and Hermitian dual-containing matrix-product codes related to (NSC) quasi-orthogonal matrices and (NSC) quasi-unitary matrices, respectively. These work can be summarized as follows.

On the quantum codes derived from the Euclidean dual-containing matrix-product codes over $\mathbb{F}_q$,

- A general approach for constructing quantum codes via Euclidean dual-containing matrix-product codes was presented (see Theorem 3.2).

- The constructions of quantum codes related to quasi-orthogonal matrices through three tools, i.e., (i) the theory of quadratic forms (see Theorem 3.3); (ii) the theory of quadratic sum (see Theorem 3.4); (iii) the Hadamard matrices (see Theorem 3.5), were introduced in turn.

- A constructive method for acquiring general quasi-orthogonal matrices and NSC quasi-orthogonal matrices was given (see Theorem 3.6). The utilization of NSC quasi-orthogonal matrices enables the minimum distance lower bound of the corresponding quantum codes to reach its optimum (see Theorem 3.7).
• The quantum codes related to special matrices $A$ with $AA^T$ being monomial matrices were considered (see Theorem 3.8).

On the quantum codes derived from the Hermitian dual-containing matrix-product codes over $\mathbb{F}_{q^2}$,

• A general approach for constructing quantum codes via Hermitian dual-containing matrix-product codes was listed (see Theorem 4.1).

• The constructions of quantum codes related to (i) quasi-unitary matrices over $\mathbb{F}_{q^2}$ for any odd prime power $q$ (see Theorem 4.2) and (ii) $2^m \times 2^m$ quasi-unitary matrices over any field $\mathbb{F}_{q^2}$ (see Theorem 4.3) were given.

• A constructive method for acquiring general quasi-unitary matrices and NSC quasi-unitary matrices was shown (see Theorem 4.4). The utilization of NSC quasi-unitary matrices enables the minimum distance lower bound of the corresponding quantum codes to reach its optimum (see Theorem 4.5).

• New classes of quantum codes related to $k \times k$ NSC quasi-unitary matrices for each $k < q$ were constructed (see Theorem 4.7).

• The quantum codes related to special matrices $A$ with $AA^\dagger$ being monomial matrices were considered (see Theorem 4.8).

Remark 5.1 It should be pointed out that the constructive methods in Theorems 3.6 and 4.4 and the newly constructed NSC quasi-orthogonal (resp. NSC quasi-unitary) matrices from them can be also applied to the following topics.

• They can be used to construct good $q$-ary entanglement-assisted quantum error-correcting codes (abbreviated to EAQECCs) from matrix-product codes. One can verify that many of these EAQECCs will show better performance of error detection and error correction than those in some relevant literature. For more information on EAQECCs, see [5, 10, 27, 30, 37, 41, 43, 53–55].

• They can be used to construct linear codes with complementary duals (abbreviated to LCD codes). By using the newly constructed NSC quasi-orthogonal (resp. NSC quasi-unitary) matrices, we can obtain many new classes of Euclidean LCD (resp. Hermitian LCD) MDS codes, some of which improve those shown in [14] because of the less restrictions on the newly constructed matrices.
We believe that Theorems 3.6 and 4.4 and those matrices constructed by them would yield more applications in other fields.

**Remark 5.2** In [6], Brun et al. shown that any \([n, k, d; c]_q\) EAQECC with \(k > c\) can produce an \([n, k - c, d; c]_C\) catalytic quantum error-correcting codes (abbreviated to CQECCs). Naturally, many EAQECCs derived from the newly constructed matrix-product codes in this article can be applied to produce new and good CQECCs, which is very useful in quantum computation and quantum communication.

### 5.2 Further discussion

For \(q = 2\), it is not difficult to check that there are no \(2 \times 2\) and \(4 \times 4\) NSC quasi-unitary matrices over \(\mathbb{F}_2^2\). Further, one can check that there are no \(2n \times 2n\) NSC quasi-unitary matrices over \(\mathbb{F}_2^2\) for any positive integer \(n\). By Corollary 4.3, Corollary 4.6(2) (or Remark 4.5) and Theorem 4.6, we now propose the following problem.

**Problem 5.1** (a) Suppose \(q \neq 2, 3\). For \(k = q\), do \(k \times k\) NSC quasi-unitary matrices exist over \(\mathbb{F}_q^2\)?

(b) Suppose \(q \neq 2\). For \(q + 2 \leq k \leq q^2\), do \(k \times k\) NSC quasi-unitary matrices exist over \(\mathbb{F}_q^2\)?

**Remark 5.3** We guess that the \(k \times k\) NSC quasi-unitary matrices in Problem 5.1 always exist. It will be very exciting if this problem is solved by a general method (similar to the method reflected in Theorems 4.4 and 4.6) rather than by computer search. To this end, some other mathematical tools, such as the theory of classical group [21,52] and combinatorial design [16,51], might be necessary.

We have presented the constructive methods on NSC quasi-orthogonal matrices and NSC quasi-unitary matrices. Naturally, we desire to know if it is feasible to explore more general cases. Therefore, we propose the following problem.

**Problem 5.2** (a) How to construct the NSC matrix \(A\) over \(\mathbb{F}_q\) such that \(AA^T\) is monomial, i.e., \(AA^T = DP_\tau\) for certain non-singular diagonal matrix \(D\) over \(\mathbb{F}_q\) and permutation \(\tau\)?

(b) How to construct the NSC matrix \(A\) over \(\mathbb{F}_q^2\) such that \(AA^\dagger\) is monomial, i.e., \(AA^\dagger = DP_\tau\) for certain non-singular diagonal matrix \(D\) over \(\mathbb{F}_q^2\) and permutation \(\tau\)?

**Remark 5.4** We give some notes on Problem 5.2.

- To the best of our knowledge, a general method (not by computer search) for constructing such matrices is lacking at the present. In a sense, once Problem 5.2 is solved, the work for constructing quantum codes (including EAQECCs) derived from matrix-product codes...
over finite fields will be unified. By that time, a wider variety of good quantum codes
(including EAQECCs) with parameters better than many existing ones will be yielded.

- Once Problem 5.2 is solved, a great many potential CQECCs will be generated by the
  corresponding EAQECCs derived from matrix-product codes, as mentioned in Remark
  5.2.

- It will be interesting to explore the enumeration problems on some special matrices over
  finite fields, such as NSC matrices, NSC quasi-orthogonal matrices, NSC quasi-unitary
  matrices and those proposed in Problem 5.2, by using the theory of geometry of classical
  groups over finite fields and some related knowledge.

References

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. On quantum and classical BCH codes. *IEEE
Transactions on Information Theory*, 53(3):1183–1188, 2007.

[2] A. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Transactions on Infor-
mation Theory*, 47(7):3065–3072, 2001.

[3] G. Birkhoff and S. Mac Lane. A survey of modern algebra. *Universities Press*, 1998.

[4] T. Blackmore and G. H. Norton. Matrix-product codes over \( \mathbb{F}_q \). *Applicable Algebra in Engineering, Communication and Computing*, 12(6):477–500, 2001.

[5] T. A. Brun, I. Devetak, and M.-H. Hsieh. Correcting quantum errors with entanglement. *Science*,
314(5798):436–439, 2006.

[6] T. A. Brun, I. Devetak, and M.-H. Hsieh. Catalytic quantum error correction. *IEEE Transactions
on Information Theory*, 60(6):3073–3089, 2014.

[7] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. Sloane. Quantum error correction via codes
over GF(4). *IEEE Trans. Inf. Theory*, 44(4):1369–1387, 1998.

[8] A. R. Calderbank, E. M. Rains, and P. W. Shor N. J. Sloane. Quantum error correction and
orthogonal geometry. *Physical Review Letters*, 78(3):405, 1997.

[9] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Physical Review
A*, 54(2):1098, 1996.

[10] M. Cao. Galois hulls of MDS codes and their quantum error correction. *arXiv:2002.12892v2*, 2020.

[11] M. Cao and J. Cui. Construction of new quantum codes via Hermitian dual-containing matrix-
product codes. *Quantum Information Processing*, 19(12):1–26, 2020.

[12] M. Cao and J. Cui. New stabilizer codes from the construction of dual-containing matrix-product
codes. *Finite Fields and Their Applications*, 63:101643, 2020.
[13] M. Cao, H. Wang, and J. Cui. Construction of quantum codes from matrix-product codes. *IEEE Communications Letters*, 24(4):706–710, 2020.

[14] C. Carlet, S. Mesnager, C. Tang, and Y. Qi. Euclidean and Hermitian LCD MDS codes. *Designs, Codes and Cryptography*, 86(11):2605–2618, 2018.

[15] B. Chen, S. Ling, and G. Zhang. Application of constacyclic codes to quantum MDS codes. *IEEE Transactions on Information Theory*, 61(3):1474–1484, 2015.

[16] C. J. Colbourn and J. H. Dinitz. Handbook of combinatorial designs. *CRC Press*, 2006.

[17] M. F. Ezerman, S. Jitman, H. M. Kiah, and S. Ling. Pure asymmetric quantum MDS codes from CSS construction: A complete characterization. *International Journal of Quantum Information*, 11(03):1350027, 2013.

[18] K. Feng. Quadratic sum. *Harbin institute of technology press, Harbin (in Chinese)*, 2011.

[19] C. Galindo, F. Hernando, and D. Ruano. New quantum codes from evaluation and matrix-product codes. *Finite Fields and Their Applications*, 36:98–120, 2015.

[20] L. Giuzzi. Hermitian varieties over finite fields. *University of Sussex, USA*, 2000.

[21] R. Goodman and N. R. Wallach. Representations and invariants of the classical groups. *Cambridge University Press*, 2000.

[22] D. Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. *NASA International Conference on Quantum Computing and Quantum Communications*, pages 302–313, 1998.

[23] M. Grassl, T. Beth, and M. Roetteler. On optimal quantum codes. *International Journal of Quantum Information*, 2(01):55–64, 2004.

[24] M. Grassl and M. Roetteler. Quantum MDS codes over small fields. *IEEE International Symposium on Information Theory*, pages 1104–1108, 2015.

[25] G. G. La Guardia. Constructions of new families of nonbinary quantum codes. *Physical Review A*, 80(4):042331, 2009.

[26] G. G. La Guardia. On the construction of nonbinary quantum BCH codes. *IEEE Transactions on Information Theory*, 60(3):1528–1535, 2014.

[27] K. Guenda, S. Jitman, and T. A. Gulliver. Constructions of good entanglement-assisted quantum error correcting codes. *Designs, Codes and Cryptography*, 86(1):121–136, 2018.

[28] F. Hernando, K. Lally, and D. Ruano. Construction and decoding of matrix-product codes from nested codes. *Applicable Algebra in Engineering, Communication and Computing*, 20:497–507, 2009.

[29] R. A. Horn and C. R. Johnson. Matrix analysis. *Cambridge University Press*, 2012.

[30] M.-H. Hsieh, I. Devetak, and T. A. Brun. General entanglement-assisted quantum error-correcting codes. *Physical Review A*, 76(6):062313, 2007.
[31] L. Jin, H. Kan, and J. Wen. Quantum MDS codes with relatively large minimum distance from Hermitian self-orthogonal codes. *Designs, Codes and Cryptography*, 84(3):463–471, 2017.

[32] L. Jin and C. Xing. A construction of new quantum MDS codes. *IEEE transactions on information theory*, 60(5):2921–2925, 2014.

[33] S. Jitman and T. Mankean. Matrix-product constructions for Hermitian self-orthogonal codes. *arXiv:1710.04999*, 2017.

[34] X. Kai and S. Zhu. New quantum MDS codes from negacyclic codes. *IEEE Transactions on Information Theory*, 59(2):1193–1197, 2012.

[35] X. Kai, S. Zhu, and P. Li. Constacyclic codes and some new quantum MDS codes. *IEEE Transactions on Information Theory*, 60(4):2080–2086, 2014.

[36] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Transactions on Information Theory*, 52(11):4892–4914, 2006.

[37] R. Li, G. Xu, and L. Lu. Decomposition of defining sets of BCH codes and its applications. *J. Air Force Eng. Univ.(Nat. Sci. Ed.)*, 14(2):86–89, 2013.

[38] Z. Li, L. Xing, and X. Wang. Quantum generalized Reed-Solomon codes: Unified framework for quantum maximum-distance-separable codes. *Physical Review A*, 77(1):012308, 2008.

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

[40] X. Liu, H. Q. Dinh, H. Liu, and L. Yu. On new quantum codes from matrix product codes. *Cryptography and Communications*, 10(4):579–589, 2018.

[41] X. Liu and H. Liu. $\sigma$-LCD codes over finite chain rings. *Designs, Codes and Cryptography*, 88(4):727–746, 2020.

[42] X. Liu, H. Liu, and L. Yu. Entanglement-assisted quantum codes from matrix-product codes. *Quantum Information Processing*, 18(6):183, 2019.

[43] X. Liu, H. Liu, and L. Yu. New EAQEC codes constructed from Galois LCD codes. *Quantum Information Processing*, 19(1):20, 2020.

[44] F. J. MacWilliams and N. J. A. Sloane. The theory of error-correcting codes. *Elsevier*, 16, 1997.

[45] F. ¨Ozbudak and H. Stichtenoth. Note on Niederreiter-Xing’s propagation rule for linear codes. *Applicable Algebra in Engineering, Communication and Computing*, 13(1):53–56, 2002.

[46] E. M. Rains. Nonbinary quantum codes. *IEEE Transactions on Information Theory*, 45(6):1827–1832, 1999.

[47] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):R2493, 1995.

[48] A. M. Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77(5):793, 1996.

[49] A. M. Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996.
[50] A. M. Steane. Simple quantum error-correcting codes. *Physical Review A*, 54(6):4741, 1996.

[51] D. Stinson. Combinatorial designs: constructions and analysis. *Springer Science & Business Media*, 2007.

[52] H. Weyl. The classical groups: Their invariants and representations. *Princeton University Press*, 1946.

[53] M. M. Wilde and T. A. Brun. Optimal entanglement formulas for entanglement-assisted quantum coding. *Physical Review A*, 77(6):064302, 2008.

[54] M. M. Wilde and T. A. Brun. Entanglement-assisted quantum convolutional coding. *Physical Review A*, 81(4):042333, 2010.

[55] M. M. Wilde, M.-H. Hsieh, and Z. Babar. Entanglement-assisted quantum turbo codes. *IEEE Transactions on Information Theory*, 60(2):1203–1222, 2014.

[56] T. Zhang and G. Ge. Quantum codes from generalized Reed-Solomon codes and matrix-product codes. *arXiv:1508.00978*, 2015.

[57] T. Zhang and G. Ge. Some new classes of quantum MDS codes from constacyclic codes. *IEEE Transactions on Information Theory*, 61(9):5224–5228, 2015.

[58] T. Zhang and G. Ge. Quantum MDS codes with large minimum distance. *Designs, Codes and Cryptography*, 83(3):503–517, 2017.

[59] S. Zhu, Z. Sun, and P. Li. A class of negacyclic BCH codes and its application to quantum codes. *Designs, Codes and Cryptography*, 86(10):2139–2165, 2018.