IEICE TRANSACTIONS

on Fundamentals of Electronics,
Communications
and Computer Sciences

DOI:10.1587/transfun.2024EAP1055

Publicized:2024/07/23

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY
The Institute of Electronics, Information and Communication Engineers
Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER

Ternary quantum codes constructed from a class of quasi-twisted codes

Zhihao LI[†a)], **Ruihu LI**[†b)], **Chaofeng GUAN**[††c)], **Liangdong LU**[†d)], **Hao SONG**[†e)], ***Nonmembers,***
and* Qiang FU**[†f)], ***Member

1**SUMMARY** In this paper, we propose a class of 1-generator quasi-twisted codes with special structures and investigate their application to construct ternary quantum codes. We discuss the algebraic structure of these 1-generator quasi-twisted codes and their dual codes. Moreover, sufficient conditions for these quasi-twisted codes to satisfy Hermitian self-orthogonality are given. Then, some ternary quantum codes exceeding the Gilbert-Varshamov bound are derived from such Hermitian self-orthogonal 1-generator quasi-twisted codes. In particular, sixteen quantum codes are new or have better parameters than those in the literatures, eight of which are obtained by the progapation rules.

key words: *Quantum codes, quasi-twisted codes, Hermitian construction.*

1. Introduction

Quantum error-correcting codes (or quantum codes) are one of the necessary guarantees for the implementation of quantum communication and quantum computing. In 1995, Shor [1] constructed the first binary [[9, 1, 3]] quantum code, which can correct 1 bit quantum error. This marks the emergence of quantum code theory. Subsequently, Calderbank, Shor [2], and Steane [3] designed methods for constructing quantum codes using classical binary codes, respectively, which largely contributed to the development of quantum code theory. Gottesman [4] articulates the theory of stabilizer quantum codes through mathematical tools such as group theory. In 1998, Calderbank et al. [5] proposed a systematic method for constructing binary quantum codes from classical self-orthogonal codes over $\mathbb{F}_4$. The research on non-binary quantum codes originated from Rains' work [6] in 1999. A q-ary quantum code Q of length n is a K-dimensional subspace of q^n-dimensional Hilbert space $(\mathbb{C}^q)^{\otimes n}$, where $\mathbb{C}$ represents the complex field and $(\mathbb{C}^q)^{\otimes n}$ is the n-fold tensor power of $\mathbb{C}^q$. If $K = q^k$ and Q can detect any $d - 1$ quantum errors, then Q is denoted as $[[n, k, d]]_q$. In 2000, Bierbrauer and Edel [7] gave a method for constructing q-ary quantum codes from q^2-ary Hermitian self-orthogonal codes. Then Ashikhmin et al. [8] and Ketkar et al. [9] extend the conclusions of [5] to q-ary quantum codes. According to the work of [5, 7–9], the famous Hermitian construction method was proposed, which gives the relationship between quantum codes and Hermitian self-orthogonal classical codes.

Theorem 1: [5, 8, Hermitian construction] If exists a Hermitian self-orthogonal $[n, k]_{q^2}$ linear code C such that there are no vectors of weight less than d in $C^{\perp_H}\backslash C$ yields a quantum code with parameter $[[n, n-2k, d]]_q$. In particular, if there are no codewords of weight $< d$ in $C^{\perp_H}$, then the quantum code is pure.

By using Hermitian construction method, the work on constructing quantum codes from classical codes over finite fields have been greatly enriched [9–16].

Quasi-twisted (QT) codes are an important class of linear codes with rich algebraic structures, which are extension of cyclic codes, constacyclic codes, and quasi-cyclic (QC) codes. QT and QC codes have been used to construct classical and quantum codes with good parameters. For works on constructing classical codes see [17–20]. The construction of quantum codes from QT and QC codes began with the work of Galindo. Galindo et al. [13] proposed a method for constructing quantum codes by QC codes in 2018, and following this work, many scholars have been attracted to work on constructing quantum codes by QC and QT codes. In 2019, Lv et al. [14] extended their theory to QT codes and constructed some quantum codes over small fields by QT codes. Subsequently, based on the work of [14], Yao et al. [15, 21] investigated special algebraic structure of 1-generator and 2-generator QT codes and constructed a number of quantum codes with good parameters. Recently, Guan et al. [16] utilize Hermitian dual-containing QC codes to produce quantum codes. Inspired by [13–16, 21], we propose a class of 1-generator QT codes and discuss self-orthogonal condition with respect to Hermitian inner product of such QT codes. Then we use such Hermitian self-orthogonal 1-generator QT codes to construct ternary quantum codes with good parameters.

The paper is organized as follows. In Section 2, some notations and preliminaries are introduced. Section 3 presents a class of 1-generator QT codes and gives sufficient conditions for such QT codes to be Hermitian self-orthogonal. In section 4, some good Hermitian self-orthogonal 1-generator QT codes and good ternary quantum

[†]Basic Sciences, Air Force Engineering University, Xi'an, China.
[††]Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, China.
a) E-mail: A1054851421@aliyun.com
b) E-mail: liruihu@aliyu.com
c) E-mail: gcf2020@yeah.net
d) E-mail: kelinglv@163.com
e) E-mail: songhao_kgd@163.com
f) E-mail: fuqiangkgd@163.com

codes derived from these QT codes are listed in two tables. Conclusions are given in Section 5.

2. Preliminaries

Let $\mathbb{F}_l$ be the Galois field with l elements and $\mathbb{F}_l^n$ be the n-dimensional vector space over $\mathbb{F}_l$. For any two vectors $\boldsymbol{u} = (u_0, \dots, u_{n-1})$ and $\boldsymbol{v} = (v_0, \dots, v_{n-1}) \in \mathbb{F}_l^n$, the Hamming weight $wt(\boldsymbol{u})$ is the number of nonzero components of $\boldsymbol{u}$ and minimum Hamming distance of a linear code C is $d(C) = \min\{wt(\boldsymbol{u} - \boldsymbol{v}) \mid \boldsymbol{u},\ \boldsymbol{v} \in C, \boldsymbol{u} \neq \boldsymbol{v}\}$. A $[n, k, d]_l$ linear code C is a k-dimensional subspace of $\mathbb{F}_l^n$ and the minimum Hamming distance of C is denoted as d. For $l = q^2$, the Hermitian inner product of $\boldsymbol{u}$ and $\boldsymbol{v}$ is defined as $\langle \boldsymbol{u}, \boldsymbol{v} \rangle_h = \sum_{i=0}^{n-1} u_i {v_i}^q$. The Hermitian dual code $C^{\perp_H}$ of a linear code C is defined as: $C^{\perp_H} = \{\boldsymbol{u} \in \mathbb{F}_{q^2}^n \mid \langle \boldsymbol{u}, \boldsymbol{v} \rangle_h = 0,\ \text{for all}\ \boldsymbol{v} \in C\}$. If $C \subset C^{\perp_H}$, then C (resp. $C^{\perp_H}$) is called a Hermitian self-orthogonal code (resp. Hermitian dual-containing code). Let A_i be the number of codewords in C with weight equal to i for $0 \leq i \leq n$, and the weight enumerator of the code C is denoted as $w(z) = \sum_{i=0}^{n} A_i z^i = A_0 + A_1 z + \cdots + A_n z^n$.

In the following, we will give a brief introduction of constacyclic and QT codes, for detail please see [11], [14] and [15].

Let $\mathbb{F}_{q^2}^* = \mathbb{F}_{q^2} \backslash \{0\}$ and $\lambda \in \mathbb{F}_{q^2}^*$. For any $c = (c_0, c_1, \dots, c_{n-1}) \in C$, if $c' = (\lambda c_{n-1}, c_0, \dots, c_{n-2}) \in C$, then the code C is called a λ-constacyclic code. Assumed that $\mathcal{R}_n = \mathbb{F}_{q^2}[x]/\langle x^n - \lambda \rangle$ is the quotient ring and define a $\mathbb{F}_{q^2}$-module isomorphism τ_1 from $\mathbb{F}_{q^2}^n$ to $\mathcal{R}_n$, i.e. $\tau_1(c_0, c_1, \dots, c_{n-1}) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$. Suppose that C is a constacyclic code of length n over $\mathbb{F}_{q^2}$. As $\mathcal{R}_n$ is a principle ideal ring, each λ-constacyclic code is generated by a polynomial $g(x)$, i.e. $C = \langle g(x) \rangle$.

If $\lambda^r = 1$, where $\lambda \in \mathbb{F}_{q^2}^*$ and r is the smallest positive integer that makes the equation true, then we call r the order of λ and denoted it as $\mathrm{ord}(\lambda) = r$. If $gcd(n, q) = 1$ and λ is an r-th unit root over $\mathbb{F}_{q^2}^*$, there exists a primitive rn-th unit root ζ over a extension field $\mathbb{F}_{q^{2v}}$ that satisfies $\zeta^n = \lambda$. Let $\xi = \zeta^r$, this yields ξ as the n-th unit root over the extended field $\mathbb{F}_{q^{2v}}$. In this way, roots of $x^n - \lambda$ over $\mathbb{F}_{q^{2v}}$ can be written as $\zeta \xi^r = \zeta^{1+jr}$, where $0 \leq j \leq n - 1$. According to [11], we set $\Omega = \{i = 1 + jr \mid 0 \leq j \leq n - 1\}$. For $i \in \Omega$, the q^2-cyclotomic cosets C_i of module rn containing element i can be defined as $C_i = \{i, iq^2, \dots, i(q^2)^{s-1}\} \bmod rn$, where s is the smallest positive integer satisfying $(q^2)^s i \equiv i \bmod rn$. If $C = \langle g(x) \rangle$ is a constacyclic code, $T = \{i \in \Omega \mid g(\zeta^i) = 0\}$ is the defining set of C.

To study QT codes, we define a new mapping τ_2 from $\mathbb{F}_{q^2}^{ln}$ to $\mathcal{R}_n^l$, i.e. $\tau_2(c_0, c_1, \dots, c_{n-1}, \dots, c_{(l-1)n}, c_{(l-1)n+1}, \dots, c_{ln-1}) = (c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}, \dots, c_{(l-1)n} + c_{(l-1)n+1} x + \cdots + c_{ln-1} x^{n-1})$. For any $c = (c_0, c_1, \dots, c_{n-1}, \dots, c_{(l-1)n}, c_{(l-1)n+1}, \dots, c_{ln-1}) \in C$, if $c' = (\lambda c_{n-1}, c_0, \dots, c_{n-2}, \dots, \lambda c_{ln-1}, c_{(l-1)n}, \dots, c_{ln-2}) \in C$, then C is called a λ-QT code with index l. Therefore, it is easy to see that C is a λ-QT code with index l if and only if $\tau_2(c)$ is an $\mathcal{R}_n$-submodule of $\mathcal{R}_n^l$. Let C be a QT code over $\mathbb{F}_{q^2}$. If C is generated by $G(x)$, where $G(x) = (g_0(x), g_1(x), \dots, g_{l-1}(x)) \in \mathcal{R}_n^l$, then C is called a 1-generator QT code with index l. A generator matrix G of C is shown below, where G_i is the λ-constacyclic matrix generated by $g_i(x)$, for $0 \leq i \leq l - 1$, respectively.

$$G = (G_0, G_1, \dots, G_{l-1}).$$

Regarding the dimension of QT code C, we can get it from [22]. In [22], it is shown that the generator polynomial of C is given as $\mathbf{g(x)} = gcd(g_0(x), g_1(x), \dots, g_r(x), x^n - \lambda)$, and the dimension of C is $n - deg(\mathbf{g(x)})$. Similarly, a 2-generator QT code can be regarded as a QT code generated by juxtaposing the top and bottom of two 1-generator QT codes.

3. A class of Hermitian self-orthogonal 1-generator QT codes

According to [11], we are able to obtain that if a λ-constacyclic code is Hermitian self-orthogonal, then $\mathrm{ord}(\lambda) \mid (q + 1)$. From this section, we concentrate on Hermitian self-orthogonal QT codes, thus assume $\mathrm{ord}(\lambda) \mid (q + 1)$ and $g(x) \mid x^n - \lambda$. In the following, we define a class of special structured 1-generator QT codes with index 2.

Definition 1: Assumed that $v_j(x)$ are monic polynomials in $\mathcal{R}_n$ for $1 \leq j \leq 2$. If $gcd(v_j(x), (x^n - \lambda)/g(x)) = 1$ and $gcd(v_1(x), v_2(x)) = 1$, we denote the QT code over $\mathbb{F}_{q^2}$ of length $2n$ with index 2 generated by $(g(x)v_1(x), g(x)v_2(x))$ as $C_{q^2(g,v_1,v_2)}$.

Remark 1: [21, definition 1] Let $C_{q^2}(g, f)$ be a QT code over $\mathbb{F}_{q^2}$ of length $2n$ and index 2 generated by $(g(x), f(x)g(x))$, where $f(x)$ and $g(x)$ are monic polynomials in $\mathcal{R}_n$ such that $g(x) \mid x^n - 1$ and $gcd(f(x), (x^n - \lambda)/g(x)) = 1$.

The definition of 1-generated QT codes in [21] is a special case in our Definition 1.

Let $f(x) = f_0 + f_1 x + \cdots + f_{n-1} x^{n-1} \in \mathcal{R}_n$ and $[f(x)] = [f_0, f_1, \dots, f_{n-1}]$ denote vectors in $\mathbb{F}_{q^2}^n$ determined by the coefficient of $f(x)$ in an ascending order. To simplify writing, we define the following polynomials.

$$\bar{f}(x) = \lambda x^n f(x^{-1}) = \lambda^2 f_0 + \lambda f_{n-1} x + \cdots + \lambda f_1 x^{n-1},$$
$$f^q(x) = f_0^q + f_1^q x + \cdots + f_{n-1}^q x^{n-1}.$$

Let $h(x) = (x^n - \lambda)/g(x)$, then $g^{\perp}(x) = x^{deg(h(x))} h(\frac{1}{x})$. According to [11], the Hermitian dual code of a constacyclic code $\langle g(x) \rangle$ is $\langle g^{\perp q}(x) \rangle$. The following exchange law for Hermitian inner product between polynomials will play an important role in later theorem proving.

Lemma 1: [23] Let $f(x)$, $v(x)$ and $c(x)$ be monic polynomials in $\mathcal{R}_n$. Then the following equality of Hermitian inner product of vectors in $\mathbb{F}_{q^2}^n$ holds

$$\langle [v(x)f(x)], [c(x)] \rangle_H = \langle [f(x)], [\bar{v}^q(x)c(x)] \rangle_H.$$

From the work in [11] and Lemma 1, the following proposition can be obtained.

Proposition 1: The Hermitian dual code $C_{q^2}^{\perp_H}(g, v_1, v_2)$ of

$C_{q^2}(g, v_1, v_2)$ over $\mathbb{F}_{q^2}$ is generated by pairs $(g^{\perp_q}(x)\bar{v}_1^q(x), g^{\perp_q}(x))$ and $(-\bar{v}_2^q(x), \bar{v}_1^q(x))$.

Proof Let $c_1 = ([a(x)g(x)v_1(x)], [a(x)g(x)v_2(x)])$ be any codeword in $C_{q^2}(g, v_1, v_2)$ and $c_2 = ([b(x)g^{\perp q}(x)\bar{v}_1^q(x) - c(x)\bar{v}_2^q(x)], [b(x)g^{\perp_q}(x) + c(x)\bar{v}_1^q(x)])$ be any codeword in the code generated by $(g^{\perp_q}(x)\bar{v}_1^q(x), g^{\perp_q}(x))$ and $(-\bar{v}_2^q(x), \bar{v}_1^q(x))$, where $a(x), b(x)$ and $c(x) \in \mathcal{R}_n$. Then $\langle c_1, c_2\rangle_H$ is equal to

$$\begin{gathered}\Big\langle([a(x)g(x)v_1(x)], [a(x)g(x)v_2(x)]), ([b(x)g^{\perp q}(x)\bar{v}_1^q(x) - c(x)\bar{v}_2^q(x)], \\ [b(x)g^{\perp_q}(x) + c(x)\bar{v}_1^q(x)])\Big\rangle_H \\ = \Big\langle[a(x)g(x)v_1(x)], [b(x)g^{\perp q}(x)\bar{v}_1^q(x)]\Big\rangle_H - \\ \Big\langle[a(x)g(x)v_1(x)], [c(x)\bar{v}_2^q(x)]\Big\rangle_H \\ + \langle[a(x)g(x)v_2(x)], [b(x)g^{\perp_q}(x)]\rangle_H + \Big\langle[a(x)g(x)v_2(x)], [c(x)\bar{v}_1^q(x)]\Big\rangle_H.\end{gathered}$$

According to lemma 1 we can get

$$\Big\langle[a(x)g(x)v_2(x)], [c(x)\bar{v}_1^q(x)]\Big\rangle_H = \Big\langle[a(x)g(x)v_1(x)], [c(x)\bar{v}_2^q(x)]\Big\rangle_H.$$

Further, the Hermitian inner product of the codes generated by $g(x)$ and $g^{\perp q}(x)$ is 0, so that $\Big\langle[a(x)g(x)v_1(x)], [b(x)g^{\perp q}(x)\bar{v}_1^q(x)]\Big\rangle_H = 0$ and $\langle[a(x)g(x)v_2(x)], [b(x)g^{\perp_q}(x)]\rangle_H = 0$, i.e. $\langle c_1, c_2\rangle_H = 0$. Therefore, the Hermitian dual code $C_{q^2}^{\perp_H}(g, v_1, v_2)$ contains the code generated by $(g^{\perp_q}(x)\bar{v}_1^q(x), g^{\perp_q}(x))$ and $(-\bar{v}_2^q(x), \bar{v}_1^q(x))$. According to [22], one can check that the dimension of the code $C_{q^2}(g, v_1, v_2)$ is $n - deg(gcd((g(x)v_1(x), g(x)v_2(x)))) = n - deg(g(x))$. Hence, the dimension of $C_{q^2}^{\perp_H}(g, v_1, v_2)$ is $2n - (n - deg(g(x))) = n + deg(g(x))$. The dimension of code generated by $(g^{\perp_q}(x)\bar{v}_1^q(x), g^{\perp_q}(x))$ and $(-\bar{v}_2^q(x), \bar{v}_1^q(x))$ is $deg(gcd(g^{\perp_q}(x)\bar{v}_1^q(x), g^{\perp_q}(x))) + deg(gcd(-\bar{v}_2^q(x), \bar{v}_1^q(x))) = deg(g(x)) + n$, which is equal to the dimension of $C_{q^2}^{\perp_H}(g, v_1, v_2)$. Therefore, our conclusion holds. □

According to proposition 1, we find that the dual code of $C_{q^2}(g, v_1, v_2)$ is a 2-generator QT code. The following are sufficient conditions that in sure $C_{q^2}(g, v_1, v_2)$ are Hermitian self-orthogonal.

Proposition 2: If $g^{\perp q}(x) \mid g(x)$, $((\bar{v}_1^q(x))^2 + \bar{v}_2^q(x)) \mid (v_1(x)\bar{v}_1^q(x) + v_2(x)\bar{v}_2^q(x))$ and $((\bar{v}_1^q(x))^2 + \bar{v}_2^q(x)) \mid (v_2(x)\bar{v}_1^q(x) - v_1(x))$, then the 1-QT code $C_{q^2}(g, v_1, v_2)$ is Hermitian self-orthogonal.

Proof Assumed that $\lambda_1(x) = \frac{g(x)(v_1(x)\bar{v}_1^q(x)+v_2(x)\bar{v}_2^q(x))}{g^{\perp q}(x)((\bar{v}_1^q(x))^2+\bar{v}_2^q(x))}$ and $\lambda_2(x) = \frac{g(x)(v_2(x)\bar{v}_1^q(x)-v_1(x))}{(\bar{v}_1^q(x))^2+\bar{v}_2^q(x)}$, when $g^{\perp q}(x) \mid g(x)$, $((\bar{v}_1^q(x))^2 + \bar{v}_2^q(x)) \mid (v_1(x)\bar{v}_1^q(x) + v_2(x)\bar{v}_2^q(x))$ and $((\bar{v}_1^q(x))^2 + \bar{v}_2^q(x)) \mid (v_2(x)\bar{v}_1^q(x) - v_1(x))$, we are able to obtain $\lambda_1(x), \lambda_2(x) \in \mathcal{R}_n$. Furthermore, the equation

$$\begin{gathered}(g(x)v_1(x), g(x)v_2(x)) = \lambda_1(x)(g^{\perp q}(x)\bar{v}_1^q(x), g^{\perp_q}(x)) \\ +\lambda_2(x)(-\bar{v}_2^q(x), \bar{v}_1^q(x))\end{gathered}$$

can be hold. Therefore, $C_{q^2}(g, v_1, v_2) \subseteq C_{q^2}^{\perp_H}(g, v_1, v_2)$. □

Theorem 2 can be derived directly from Theorem 1, proposition 1 and proposition 2.

Theorem 2: If $C_{q^2}(g, v_1, v_2)$ satisfied the conditions of proposition 1 and proposition 2, then there exist a quantum code $[[2n, 2deg(g(x)), d]]_q$, where d denotes the distance of Hermitian dual code $C_{q^2}^{\perp_H}(g, v_1, v_2)$.

In addition, new quantum codes can be derived from existing ones by the following propagation rules, which will be used later.

Theorem 3: [5, 9] Assumed that an $[[n, k, d]]_q$ quantum code exists.

(1) If $k > 0$, then an $[[n + 1, k, d]]_q$ code exists.
(2) If the code is pure and $n \geq 2$, then an $[[n-1, k+1, d-1]]_q$ code exists.
(3) If $k > 1$ or if $k = 1$ and the code is pure, then an $[[n, k - 1, d]]_q$ code exists.
(4) If $n \geq 2$, then an $[[n - 1, k, d - 1]]$ code exists.

In order to determine whether a quantum code exists under given conditions, Feng et al. [24] proposed the quantum GV bound. A quantum code that exceeds the quantum GV bound is usually considered to be excellent.

Theorem 4: [24, quantum GV bound] Let $n > k \geq 2$ with $n \equiv k$ (mod 2), $d \geq 2$. If the inequality

$$\frac{q^{n-k+2} - 1}{q^2 - 1} > \sum_{i=1}^{d-1}(q^2 - 1)^{i-1}\binom{n}{i}$$

is met, there exists an $[[n, k, d]]_q$ pure quantum code.

4. Good ternary quantum codes derived from QT codes

In this section, some ternary quantum codes are constructed which improve the minimum distance lower bound in [12] and exceed the quantum GV bound. Moreover, according to Theorem 3, we derive some new ternary quantum codes from existing ones.

Since the construction of binary quantum codes is more studied, we focus on the construction of ternary quantum codes. Let $\mathbb{F}_3 = \{0, 1, 2\}$, $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 - x - 1) = \{0, 1, w, w^2, w^3, w^4, w^5, w^6, w^7\}$ and w be the root of $x^2 - x - 1$. It is easy to get $w^2 = w + 1, w^3 = 2w + 1, w^4 = 2, w^5 = 2w, w^6 = 2w + 2, w^7 = w + 2$. For the shift-constant λ of QT codes, we take $\lambda = w^2$ or w^4.

In the following, several examples are given to show that our construction method works, in which the algebraic software Magma [25] is used to compute the specific parameters of the QT codes.

Example 1: Let $n = 14$, $\lambda = w^2$ and $r = 4$, we can get $\Omega = \{1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53\}$. Consider the 9-cyclotomic cosets module 56 and choose $T = C_{17} \cup C_{29}$ as defining set of $\langle g(x)\rangle$, where $C_{17} = \{17, 33, 41\}$ and $C_{29} = \{29, 37, 53\}$. Then $g(x) = x^6 + wx^5 + w^3x^3 + w^5x + w^6$. We choose $v_1(x) = 2x^{13} + w^6x^{12} + w^3x^{11} + wx^{10} + wx^9 + x^8 + w^3x^7 + w^3x^6 + wx^5 + w^2x^4 + 2x^3 + w^3x^2 + w^3x + w^6$, $v_2(x) = w^3x^{13} + w^7x^{12} + x^{11} + 2x^9 + x^8 + 2x^7 + x^5 + w^5x^4 + wx^3 + 2x^2 + w^7x +$

w^5 and $g(x), v_1(x), v_2(x)$ satisfy the conditions in Theorem 2. This can generate a $[28, 8]_9$ Hermitian self-orthogonal code and its dual code is $[28, 20, 6]_9$, whose weight enumerator is $w(z) = 1 + 2240z^6 + 57680z^7 + 1219568z^8 + \cdots + 449344634493065760z^{28}$. Then, we can obtain a ternary quantum code with parameters $[[28, 12, 6]]_3$.

Example 2: Assume that $n = 20$, $\lambda = w^4$ and $r = 2$, we get $\Omega = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39\}$ and consider the 9-cyclotomic cosets module 40 and choose the defining set $T = C_1 \cup C_{11} \cup C_{17} \cup C_{31}$, where $C_1 = \{1, 9\}$, $C_{11} = \{11, 19\}$, $C_{17} = \{17, 23\}$ and $C_{31} = \{31, 39\}$. Hence $g(x) = x^8 + w^5x^7 + w^5x^6 + w^2x^5 + w^2x^4 + 2x^3 + wx^2 + w^3x + 1$. Let $v_1(x) = 2x^{19} + wx^{18} + w^6x^{16} + w^5x^{15} + w^5x^{14} + w^6x^{13} + wx^{12} + x^11 + w^3x^{10} + w^2x^9 + w^7x^8 + w^7x^7 + w^2x^6 + w^3x^4 + 2x^3 + w^2x^2 + w^2x + w^7$ and $v_2(x) = 2x^{19} + w^6x^{18} + x^{16} + w^7x^{15} + wx^{14} + x^{13} + w^6x^{12} + x^{11} + w^2x^{10} + x^9 + w^3x^8 + w^5x^7 + x^6 + w^2x^4 + 2x^3 + w^5x^2 + w^6$ satisfy Theorem 2, then a Hermitian self-orthogonal code $[40, 12]_9$ can be obtained. $[40, 28, 8]_9$ is the Hermitian dual code of $[40, 12]_9$, whose weight enumerator is $w(z) = 1 + 5520z^8 + 121120z^9 + 3189056z^{10} + \cdots + 4706405754676928917342976z^{40}$. Via Theorem 2, a $[[40, 16, 8]]_3$ quantum code is obtained which is superior to $[[40, 14, 8]]_3$ in [12].

Example 3: Let $n = 37$, $\lambda = w^4$ and $r = 2$, we get $\Omega = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 3 7, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73\}$. Consider the 9-cyclotomic cosets module 74 and select $T = C_1 \cup C_3 \cup C_{15}$, where $C_1 = \{1, 7, 9, 33, 47, 49, 53, 63, 71\}$, $C_3 = \{3, 11, 21, 25, 27, 41, 65, 67, 73\}$ and $C_{15} = \{15, 29, 31, 39, 51, 55, 57, 61, 69\}$. Hence $g(x) = x^{27} + wx^{26} + w^5x^{25} + 2x^{24} + w^2x^{23} + w^2x^{22} + wx^{21} + x^{20} + w^2x^{19} + wx^{18} + w^5x^{17} + 2x^{16} + 2x^{15} + w^6x^{14} + w^2x^{13} + 2x^{12} + 2x^{11} + w^7x^{10} + w^3x^9 + w^6x^8 + x^7 + w^3x^6 + w^6x^5 + w^6x^4 + 2x^3 + w^7x^2 + w^3x + 1$. Let $v_1(x) = w^7x^{36} + wx^{33} + w^3x^4 + w^5x + 1$, $v_2(x) = w^7x^{36} + wx^{35} + wx^{34} + w^5x^{33} + 2x^{32} + w^2x^{31} + w^6x^{30} + w^6x^{29} + wx^{28} + 2x^{27} + w^5x^{26} + w^2x^{24} + w^6x^{23} + w^5x^{22} + w^6x^{21} + w^3x^{20} + wx^{17} + w^2x^{16} + w^7x^{15} + w^2x^{14} + w^6x^{13} + w^7x^{11} + 2x^{10} + w^3x^9 + w^2x^8 + w^2x^7 + w^6x^6 + 2x^5 + w^7x^4 + w^3x^3 + w^3x^2 + w^5x + 1$. These will generate a Hermitian self-orthogonal code $[74, 10]_9$ and its dual code is $[74, 64, 6]_9$, whose weight enumerator is $w(z) = 1 + 27232z^6 + 1157952z^7 + 72281424z^8 + \cdots + 19330092978661515896424803845378071795525370876 48096527048z^{74}$. Then, the $[[74, 54, 6]]_3$ quantum code can be obtained by Theorem 2. the $[[74, 54, 6]]_3$ quantum code has a higher information rate than $[[73, 37, 6]]_3$ in [12]. According to Theorem 3, we can obtain quantum codes with parameters $[[74, 53, 6]]_3$, $[[75, 54, 6]]_3$, $[[73, 54, 5]]_3$, $[[73, 55, 5]]_3$, which are better than $[[73, 37, 6]]_3$, $[[73, 49, 5]]_3$ in [12].

In order to save space and intuitive view of results, we use coefficient simplification to represent the polynomials in Table 1, noting $0, 1, w^4, w, w^2, w^3, w^5, w^6, w^7$ as $0, 1, 2, 3, 4, 5, 6, 7, 8$. For example, $1 + x + 2x^2 + wx^4 + w^3x^7 + w^7x^8$ over $\mathbb{F}_9$ is denoted as $1^2 2030^2 58$. In Table 1, we give good Hermitian self-orthogonal 1-generator QT codes over $\mathbb{F}_9$. Table 2 gives some ternary quantum codes derived from these QT codes in Table 1. In Table 2, above the dashed line are the best known quantum codes in [23, 26–28] that we can construct with the same parameters as them using our method; the quantum codes labeled with $*$ are new and have better parameters than the ones in [12, 23].

5. Conclusion

In this work, we present a class of 1-generator QT codes with index 2 which can construct quantum codes with good parameters. Moreover, the structure of $C_{q^2}^{\perp_H}(g, v_1, v_2)$ and the sufficient conditions for $C_{q^2}(g, v_1, v_2)$ to be Hermitian self-orthogonal are provided. Furthermore, some ternary quantum codes are constructed with parameters superior to previous work.

In fact, quantum codes over other finite fields can also be obtained by our construction method. In the future, we will investigate multi-generator QT codes with multi-index and construct quantum codes over other finite fields from self-orthogonal QT codes with respect to Hermitian inner product.

Acknowledgment

This work was supported by National Natural Science Foundation of China under Grant No. U21A20428, Natural Science Foundation of Shaanxi under Grant No.2023-JC-YB-003, No.2024JC-YBMS-055 and Natural Science Basic Research Program of Shaanxi (Program No.2023-JC-QN-0033).

Conflict of interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] P.W. Shor, Scheme for reducing decoherence in quantum computer memory, Phys. Rev. A, vol. 52, no. 4, pp. R2493, 1995.

[2] A.R. Calderbank, P.M. Shor, Good quantum error-correcting codes exist, Phys. Rev. A, vol. 54, no. 2, pp. 1098, 1996.

[3] A.M. Steane, Error correcting codes in quantum theory, Phys. Rev. Lett., vol. 77, no. 5, pp. 793, 1996.

[4] D. Gottesman, Class of quantum error-correcting codes saturating the quantum Hamming bound, Phys. Rev. A, vol. 54, no. 3, pp. 1862, 1996.

[5] A.R. Calderbank, E.M. Rains, P.M. Shor, N.J. Sloane, Quantum error correction via codes over $GF(4)$, IEEE Trans. Inf. Theory, vol. 44, no. 4, pp. 1369-1387, 1998.

[6] E.M. Rains, Nonbinary quantum codes, IEEE Trans. Inf. Theory, vol. 45, no. 6, pp. 1827–1832, 1999.

[7] J. Bierbrauer and Y. Edel, Quantum twisted codes, J. Comb. Des., vol. 8, no. 3, pp. 174-188, 2000.

[8] A. Ashikhmin, E. Knill, Nonbinary quantum stabilizer codes, IEEE Trans. Inf. Theory, vol. 47, no. 7, pp. 3065-3072, 2001.

[9] A. Ketkar, A. Klappenecker, S. Kumar, P.K. Sarvepalli, Nonbinary stabilizer codes over finite fields, IEEE Trans. Inf. Theory, vol. 52, no. 11, pp. 4892-4914, 2006.

Table 1 Hermitian self-orthogonal 1-generator QT codes

λ	$g(x), v_1(x), v_2(x)$	C	$d(C^{\perp_H})$
w^2	$5621, 7343^20874, 87327517$	$[20, 7]_9$	6
w^4	$26061, 67^2676215, 387^208123$	$[20, 6]_9$	5
w^4	$1^22^21, 7^26368010685, 408210714012$	$[24, 8]_9$	6
w^4	$1021^2, 161010^41018, 1365760^284385$	$[26, 9]_9$	7
w^4	$1021201, 140510^41307, 1868351^235686$	$[26, 7]_9$	6
w^2	$15261, 1787^248674^2641, 32380686806525$	$[28, 10]_9$	7
w^2	$7605031, 75^22435^213^2572, 68236102120185$	$[28, 8]_9$	6
w^2	$187308431, 872513^278415, 785475812851$	$[28, 6]_9$	5
w^2	$18651, 103740^6745, 12432430^2572572$	$[30, 11]_9$	8
w^2	$4^25321, 174310^61574, 148787574346467$	$[30, 10]_9$	7
w^2	$737127^2181, 140^{14}7, 18121784^27^2641216$	$[34, 8]_9$	6
w^2	$8307641, 75^24361542^212^2731857, 5^2321636167148185812$	$[40, 14]_9$	9
w^4	$15324^26^21, 84^225048^2451376^27032, 7062401651417 1381072$	$[40, 12]_9$	8
w^4	$7803041^2671, 2028607351618 1354086, 4782084^3161817^3602$	$[40, 10]_9$	7
w^2	$7131867163681, 18082402081^36020726, 7054^2136^2471478^2517^2$	$[40, 8]_9$	6
w^2	$7574656^2862181, 104830^{12}567, 14340203^247475^2020757$	$[42, 8]_9$	5
w^4	$40410141427271, 505^284^27^248315674^27^263$ $30307^205^24^25137^23^204^2$	$[44, 9]_9$	6
w^4	$171014202410171, 3038460768231526840876$ $607^2620414^27147^2170284$	$[44, 8]_9$	5
w^2	$7141404070^21, 1^30^{18}1^2, 1420581^23060^28051^263027$	$[46, 12]_9$	8
w^4	$102717202717201, 642106352308^267812127626$ 802826865674817^28^45816	$[52, 12]_9$	7
w^4	$15827^2517582^2472^2634134^22631, 160^250^{28}30^28$ $165^28274^25280748430^25767406237^24263^28$	$[74, 10]_9$	6

Table 2 Good ternary quantum codes

C	Q	rate	codes in [12]	rate	codes in [23]	previous work
$[20, 7]_9$	$[[20, 6, 6]]_3$	-	-	-	-	[26]
$[20, 6]_9$	$[[20, 8, 5]]_3$	-	-	-	-	[26]
$[24, 8]_9$	$[[24, 8, 6]]_3$	-	-	-	-	[28]
$[26, 9]_9$	$[[26, 8, 7]]_3$	-	-	-	-	[28]
$[26, 7]_9$	$[[26, 12, 6]]_3$	-	-	-	-	[28]
$[28, 10]_9$	$[[28, 8, 7]]_3$	-	-	-	-	[28]
$[28, 8]_9$	$[[28, 12, 6]]_3$	-	-	-	-	[28]
$[28, 6]_9$	$[[28, 16, 5]]_3$	-	-	-	-	[28]
$[30, 11]_9$	$[[30, 8, 8]]_3$	-	-	-	-	[28]
$[30, 10]_9$	$[[30, 10, 7]]_3$	-	-	-	-	[28]
$[34, 8]_9$	$[[34, 18, 6]]_3$	-	-	-	-	[23]
$[46, 12]_9$	$[[46, 22, 8]]_3$	-	-	-	-	[27]
$[52, 12]_9$	$[[52, 28, 7]]_3$	-	-	-	-	[27]
$[40, 14]_9$	$^*[[40, 12, 9]]_3$	0.3	-	-	-	-
$[40, 12]_9$	$^*[[40, 16, 8]]_3$	0.4	$[[40, 14, 8]]_3$	0.35	-	-
$[40, 10]_9$	$^*[[40, 20, 7]]_3$	0.5	$[[40, 18, 7]]_3$	0.45	-	-
$[40, 8]_9$	$^*[[40, 24, 6]]_3$	-	$[[40, 24, 5]]_3$	-	-	-
$[42, 8]_9$	$^*[[42, 26, 5]]_3$	0.619	-	-	-	-
$[44, 9]_9$	$^*[[44, 26, 6]]_3$	0.591	$[[41, 23, 6]]_3$	0.561	$[[44, 24, 6]]_3$	-
-	$^*[[43, 26, 5]]_3$	0.605	$[[40, 24, 5]]_3$	0.6	$[[44, 24, 6]]_3$	-
-	$^*[[43, 27, 5]]_3$	0.628	$[40, 24, 5]]_3$	0.6	$[[44, 24, 6]]_3$	-
-	$^*[[44, 25, 6]]_3$	0.568	$[[41, 23, 6]]_3$	0.561	$[[44, 24, 6]]_3$	-
-	$^*[[45, 26, 6]]_3$	0.578	$[[41, 23, 6]]_3$	0.561	$[[44, 24, 6]]_3$	-
$[44, 8]_9$	$^*[[44, 28, 5]]_3$	0.636	$[[40, 24, 5]]_3$	0.6	-	-
$[74, 10]_9$	$^*[[74, 54, 6]]_3$	0.730	$[[73, 37, 6]]_3$	0.507	-	-
-	$^*[[73, 54, 5]]_3$	-	$[[73, 49, 5]]_3$	-	-	-
-	$^*[[73, 55, 5]]_3$	-	$[[73, 49, 5]]_3$	-	-	-
-	$^*[[74, 53, 6]]_3$	-	$[[73, 37, 6]]_3$	-	-	-
-	$^*[[75, 54, 6]]_3$	-	$[[73, 37, 6]]_3$	-	-	-

[10] X. Kai, S. Zhu, New quantum MDS codes from negacyclic codes, IEEE Trans. Inf. Theory, vol. 59, no. 2, pp. 1193-1197, 2012.

[11] X. Kai, S. Zhu, P. Li, Constacyclic codes and some new quantum MDS codes, IEEE Trans. Inf. Theory, vol. 60, no. 4, pp. 2080-2086, 2014.

[12] Y. Edel, Table of quantum twisted codes, Online available at https://www.mathi.uni-heidelberg.de/~yves/Matritzen/QTBCH/QTBCHIndex.html Accessed on 2023-12-15.

[13] C. Galindo, F. Hernando, R. Matsumoto, Quasi-cyclic constructions of quantum codes, Finite Fields Th. App., vol. 52, pp. 261-280, 2018.

[14] J. Lv, R. Li, Q. Fu, Quantum codes derived from quasi-twisted codes of index 2 with Hermitian inner product, IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, vol. 102, no. 10, pp. 1411-1415, 2019.

[15] Y. Yao, Y. Ma, J. Lv, H. Song, Q. Fu, New binary quantum codes derived from quasi-twisted codes with Hermitian inner product, IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, vol. 104, no. 12, pp. 1718–1722, 2021.

[16] C. Guan, R. Li, L. Lu, Y. Yao, New binary quantum codes constructed from quasi-cyclic codes, Int J. Theor. Phys., vol. 61, no. 6, pp. 172, 2022.

[17] I. Siap, N. Aydin, D.K. Ray-Chaudhuri, New ternary quasi-cyclic codes with better minimum distances, IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1554-1558, 2000.

[18] R. Daskalov and P. Hristov, New binary one-generator quasi-cyclic codes, IEEE Trans. Inf. Theory, vol. 49, no. 11, pp. 3001-3005, 2003.

[19] E.Z. Chen, An explicit construction of 2-generator quasi-twisted codes, IEEE Trans. Inf. Theory, vol. 54, no. 12, pp. 5770-5773, 2008.

[20] R. Daskalov, P. Hristov, New quasi-twisted degenerate ternary linear codes, IEEE Trans. Inf. Theory, vol. 49, no. 9, pp. 2259-2263, 2003.

[21] Y. Yao, Y. Ma, J. Lv, Quantum codes and entanglement-assisted quantum codes derived from one-generator quasi-twisted codes, Int J. Theor. Phys., vol. 60, pp. 1077-1089, 2021.

[22] G.E. Séguin, A class of 1-generator quasi-cyclic codes, IEEE Trans. Inf. Theory, vol. 50, no. 8, pp. 1745-1753, 2004.

[23] J. Lv, R. Li, J. Wang, Quantum codes derived from one-generator quasi-cyclic codes with Hermitian inner product, Int J. Theor. Phys., vol. 59, no. 1, pp. 300-312, 2020.

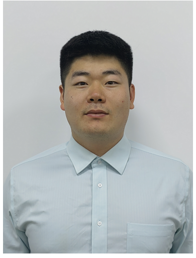
[24] K. Feng, Z. Ma, A finite Gilbert-Varshamov bound for pure stabilizer quantum codes, IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3323-3325, 2004.

[25] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symb. Comput., vol. 24, no. 3-4, pp. 235-265, 1997.

[26] M.F. Ezerman, S. Ling, B. Ozkaya, P. Solé, Good stabilizer codes from quasi-cyclic codes over F_4 and F_9, 2019 IEEE International Symposium on Information Theory (ISIT), pp. 2898–2902, 2019.

[27] C. Guan, R. Li, L. Lu, Y. Liu, H. Song, On construction of quantum codes with dual-containing quasi-cyclic codes, Quantum Inf. Process, vol. 21, no. 7, pp. 263, 2022.

[28] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, Online available at http://s208785153.online.de/codetables/ Accessed on 2023-12-20.



Zhihao Li received the B.E. degree from Air Force Engineering University in 2022. He is currently pursing the M.S. degree at quantum information laboratory, Air Force Engineering University. His research interests include coding theory and cryptography.

Ruihu Li received the Ph.D degree from northwestern polytechnical university University of Technology in 2004. He is currently a professor with the Department of Basic Sciences, Air Force Engineering University. His research interests include graph theory, group theory, coding theory and cryptography.

Chaofeng Guan is currently pursuing the Ph.D. degree with the Henan Key Laboratory of Network Cryptography in Zhengzhou, China. His research interests include coding theory, cryptography.

Liangdong Lu received the Ph.D. degree in Electronic Science and Technology from Air Force Engineering University, in 2015. He is currently an Associate Professor with Air Force Engineering University. His research interests include algebraic coding, quantum compution and quantum information.

Hao Song received the master degree in applied mathematics from Xi'an University of Architecture and Technology in 2011, the Ph.D degree from Air Force Engineering University in 2020. He is currently working in the Department of Basic Sciences, Air Force Engineering University. His research interests include coding theory and cryptography.

Qiang Fu received the B.E. degree in applied mathematics from Northwest University, Xi'an, China, in 2012, and the M.S. degree in applied mathematics and the Ph.D. degree in information and communication engineering from Air Force Engineering University, in 2015, and

2018, respectively. He is currently an Associate Professor with Air Force Engineering University. His research interests include algebraic coding, distribution storage coding and erasure coding.