An explicit construction of quantum codes from one-generator generalized quasi-cyclic codes

Yu Yao, *Yuena* Ma*, *Husheng* Li, and *Jingjie* Lv

Air Force Engineering University, Department of Basic Sciences, 710051Xi'an, P. R. China

Abstract. In this paper, we take advantage of a class of one-generator generalized quasi-cyclic (GQC) codes of index 2 to construct quantum error-correcting codes. By studying the form of Hermitian dual codes and their algebraic structure, we propose a sufficient condition for self-orthogonality of GQC codes with Hermitian inner product. By comparison, the quantum codes we constructed have better parameters than known codes.

1 Introduction

Quantum error-correcting codes (QECCs) have significant application value in quantum communication and quantum computing. Shor proposed the concept of QECCs in 1995 [1]. After the connection between classical error correction codes and QECCs was established, more and more researchers began to be interested in this aspect of work. With the development of research, the work has been extended to the q-ary QECCs. Many QECCs with good parameters have been constructed [2-5].

Generalized quasi-cyclic (GQC) codes are the remarkable generalization of cyclic codes and quasi-cyclic (QC) codes. Moreover, compared to QC codes, GQC codes have arbitrary length that made GQC codes are an important class of linear codes. The concept of GQC codes was proposed by Siap and Kulhan in 2005 [6]. Many high-performance LDPC codes are not QC codes but GQC codes [7-9]. Therefore, many researchers considered its structures and got many good results [10, 11].

Thus, we can use GQC codes to construct QECCs. Galindo et al. [12] first constructed QECCs via two-generator QC codes. Afterwards Lv et al. utilized the two-generator QC codes [13] and one-generator QC [14, 15] codes to construct QECCs, respectively, and gave many codes with good parameters. Inspired by these works, we consider one-generator GQC codes to construct QECCs. To our knowledge, few researches in this area involve.

The paper is organized as follows. Section 2 summarizes some preliminary concepts and results. In Section 3, we provide a construction of one-generator GQC codes which are Hermitian self-orthogonal. Section 4 utilizes the class of GQC codes to construct QECCs and gives examples of QECCs with good parameters. The paper is summarized with a discussion in Section 5.

* *Corresponding author: xakgd2020@163.com

2 Preliminaries

In this paper, let C be a code of length n, dimension k and minimum Hamming distance d over the finite field $\mathbb{F}_{q^2}^n$, where $\frac{k}{n}$ is called information rate. For any two vectors $u=(u_0,u_1,\cdots,u_{n-1})$, $v=(v_0,v_1,\cdots,v_{n-1})\in\mathbb{F}_{q^2}^n$, their Hermitian inner product is defined as $\langle u,v\rangle_H=\sum_{j=0}^{n-1}u_j^q v_j$, where $\alpha^q=\bar{\alpha}$ denote its conjugation. the Hermitian dual code of C is defined as $C^{\perp_H}=\left\{v\in\mathbb{F}_{q^2}^n \mid \langle u,v\rangle_H=0,\forall u\in C\right\}$.

Let C be a q^2-ary linear code of length n_1+n_2. For any codeword $c=(c_0,c_1,\cdots,c_{n_1-1},c_{n_1},c_{n_1+1},\cdots,c_{n_1+n_2-1})\in C$, if $\varphi(c)=(c_{n_1-1},c_0,\cdots,c_{n_1-2},c_{n_1+n_2-1},c_n,\cdots,c_{n_1+n_2-2})\in C$, then the code C is called a GQC code of length n_1+n_2 and index $l=2$ over $\mathbb{F}_{q^2}$. Note that, when $n_1=n_2$, C is a QC code. Furthermore if $l=1$, then C is a cyclic code.

According to the following theorem, we can know the dimension of a GQC code, which depends on its parity-check polynomial.

Theorem 1 [11] Let $h(x)$ be the parity-check polynomial of a 1-generator GQC code C of block lengths $(m_1,m_2,\cdots,m_l)$ with generator $(a_1(x),a_2(x),\cdots,a_l(x))$. Then,

$a-$ $h(x)=\mathrm{lcm}_{1\le i\le l}\{\frac{x^{m_i}-1}{g_i(x)}\}$, where $g_i(x)=\gcd(a_i(x),x^{m_i}-1)$.

$b-$ as a vector space over $\mathbb{F}_q$, dimension of C is $\deg(h(x))$.

A q-ary QECC of length n and dimension k is represented by $[\![n,k,d]\!]_q$, where d denotes the minimum distance and means that this code can detect $d-1$ errors and correct $\left\lfloor\frac{d-1}{2}\right\rfloor$ errors. From the following theorem, we can construct QECCs by classical Hermitian self-orthogonal linear codes.

Theorem 2 [2] If a Hermitian self-orthogonal $[n,k]_{q^2}$ linear code C exists, then a $[\![n,n-2k,d]\!]_q$ QECC yields, where no vectors of weight less than d in $C^{\perp_H}\setminus C$.

3 Hermitian self-orthogonal GQC codes

Next, a class of self-orthogonal one-generator GQC codes with the Hermitian inner product will be defined to construct QECCs.

Definition 1 If $\gcd(q,n_1)=\gcd(q,n_2)=1$, let C be a GQC code over $\mathbb{F}_{q^2}$ of length n_1+n_2 and index 2 generated by $(g_1(x),f(x)g_2(x))$, where $g_1(x)\mid x^{n_1}-1$, $g_2(x)\mid x^{n_2}-1$ and $\gcd(f(x),(x^{n_2}-1/g_2(x)))=1$.

Throughout this paper, we set $g(x)=g_0+g_1x+\cdots+g_{n-1}x^{n-1}$, and define the polynomials $g^q(x)=g_0^q+g_1^qx+\cdots+g_{n-1}^qx^{n-1}$. Moreover, when $g(x)h(x)=x^n-1$, then

$g^{\perp}(x) = x^{\deg h(x)} h(\frac{1}{x})$. Besides, $[g(x)]$ denotes the vector, which decided by the polynomial $g(x)$ coefficients over $\mathbb{F}_{q^2}^n$.

Next, the algebraic structure of the Hermitian dual code of C will be given and a sufficient condition for self-orthogonality with Hermitian inner product will be proposed.

Theorem 3 If a GQC code C satisfies $\gcd\left(\frac{g_2(x)}{g_1(x)}, x^{n_1}-1\right)=1$, $g_1^{\perp q}(x) \mid g_1(x) \mid g_2(x)$, $g_2^{\perp q}(x) \mid g_2(x)$ and $x^{n_1}-1 \mid x^{n_2}-1$, Then there exist

(1) $C^{\perp_H}$ is generated by $\left(g_1^{\perp q}(x), f(x) g_2^{\perp q}(x)\right)$, $\left(g_1(x), 0\right)$ and $\left(g_1^{\perp q}(x), 0\right)$, where $C^{\perp_H}$ is the Hermitian dual code of C over $\mathbb{F}_{q^2}$.

(2) C is Hermitian self-orthogonal.

Proof (1) we first prove that $C^{\perp_H}$ is generated by $\left(g_1^{\perp q}(x), f(x) g_2^{\perp q}(x)\right)$, $\left(g_1(x), 0\right)$ and $\left(g_1^{\perp q}(x), 0\right)$.

Ⅰ. Let $c_1 = \left([a(x)g_1(x)], [a(x)f(x)g_2(x)]\right)$ denote any codeword in C, and $c_2 = ([b(x)g_1^{\perp q}(x) + c(x)g_1(x) + d(x)g_1^{\perp q}(x)], [b(x)f(x)g_2^{\perp q}(x)])$ represent any codeword in the code D, which generated by $\left(g_1^{\perp q}(x), f(x) g_2^{\perp q}(x)\right)$, $\left(g_1(x), 0\right)$ and $\left(g_1^{\perp q}(x), 0\right)$, where $a(x)$, $b(x)$, $c(x)$ and $d(x)$ are arbitrary polynomials over $\mathbb{F}_{q^2}[x]$. Then $\langle c_1, c_2\rangle_H = \langle [a(x)g_1(x)], [(b(x)+d(x))g_1^{\perp q}(x)]\rangle_H + \langle [a(x)g_1(x)], [c(x)g_1]\rangle_H + \langle [a(x)f(x)g_2(x)], [b(x)f(x)g_2^{\perp q}(x)]\rangle_H$. Because $\langle g^{\perp q}(x)\rangle$ is Hermitian dual code of cyclic code $\langle g(x)\rangle$, and for arbitrary polynomials $k(x)$ over $\mathbb{F}_{q^2}[x]$, $\left\langle k(x)g(x)\right\rangle$ is the subcode of $\left\langle g(x)\right\rangle$. Obviously, $\left\langle c_1, c_2\right\rangle_H = \langle [a(x)g_1(x)], [c(x)g_1]\rangle_H = 0$ when $g_1^{\perp q}(x) \mid g_1(x)$. Thus, the Hermitian dual code $C^{\perp_H}$ includes the code D.

Ⅱ. Moreover, according to Theorem 1, the dimension of C is $\dim(C) = \deg\left(\operatorname{lcm}\left\{\frac{x^{n_1}-1}{g_1(x)}, \frac{x^{n_2}-1}{g_2(x)}\right\}\right)$. $x^{n_1}-1 \mid x^{n_2}-1$, $g_1(x) \mid g_2(x)$ and $\gcd(\frac{g_2(x)}{g_1(x)}, x^{n_1}-1) = 1$, thus $\frac{x^{n_1}-1}{g_1(x)} \mid \frac{x^{n_2}-1}{g_2(x)}$. and then $\dim(C) = n_2 - \deg g_2(x)$. On the other hand, due to $g_1^{\perp q}(x) \mid g_1(x)$ and $g_2^{\perp q}(x) \mid g_2(x)$, $\deg\left(\operatorname{lcm}\left\{\frac{x^{n_1}-1}{g_1^{\perp q}(x)}, \frac{x^{n_2}-1}{g_2^{\perp q}(x)}\right\}\right) = \deg\frac{x^{n_2}-1}{g_2^{\perp q}(x)} = \deg g_2(x)$. It is easy to know that $\dim(D) = \deg g_2(x) + (n_1 - \deg g_1(x)) + \deg g_1(x) = n_1 + \deg g_2(x)$, which is exactly equal to the dimension of $C^{\perp_H}$. So $C^{\perp_H}$ is generated by $(g_1^{\perp q}(x), f(x)g_2^{\perp q}(x))$, $(g_1(x), 0)$ and $(g_1^{\perp q}(x), 0)$.

(2) Next we prove that C is Hermitian self-orthogonal. It is directly derived from the following equation:

$$(g_1(x), f(x)g_2(x)) = \frac{g_2(x)}{g_2^{\perp q}(x)}(g_1^{\perp q}(x), f(x)g_2^{\perp q}(x)) + (g_1(x), 0) - \frac{g_2(x)}{g_2^{\perp q}(x)}(g_1^{\perp q}(x), 0).$$

So, when $g_2^{\perp_q}(x) \mid g_2(x)$, $C \subseteq C^{\perp_H}$.

In summary, our conclusion is proved.

4 Construction of QECCs

We can straightforward draw the following theorem via Theorem 2 and 3.

Theorem 4 Let $\gcd\left(\frac{g_2(x)}{g_1(x)}, x^{n_1}-1\right)=1$, $g_1^{\perp_q}(x) \mid g_1(x) \mid g_2(x)$, $g_2^{\perp_q}(x) \mid g_2(x)$ and $x^{n_1}-1 \mid x^{n_2}-1$. Then there exist Hermitian self-orthogonal code C and QECC with parameters $\left[\!\left[n_1+n_2, n_1+2\deg g_2(x)-n_2, d_{\min}(C^{\perp_H})\right]\!\right]_q$, where $d_{\min}\left(C^{\perp_H}\right)$ denotes the distance of Hermitian dual code $C^{\perp_H}$.

Next, we compare the new QECCs with existing ones to illustrate that many QECCs with good parameters can be constructed from Hermitian self-orthogonal GQC codes.

Example 1. Assume that $q=4$, $n_1=7$ and $n_2=21$. Let ω be a primitive element of $\mathbb{F}_{16}$. Let $g_1(x)=x^4+x^3+x^2+1$ and $g_2(x)=x^{15}+x^{14}+\omega^5x^{13}+\omega^5x^{12}+x^{11}+\omega^{10}x^{10}+x^9$ $+\omega^5x^8+x^7+x^6+x^5+\omega^{10}x^4+\omega^5x^3+\omega^{10}x^2+\omega^{10}x+1$. Set $f(x)=\omega x^2+x+1$ then a GQC code C with parameters $[28,6,12]_{16}$ obtained, which satisfies Theorem 4. Naturally, we obtain a $[\![28,16,3]\!]_4$ quantum code with information rate 0.571. Furthermore, it has better parameters than $[\![26,14,3]\!]_4$ with information rate 0.538 in [16].

Example 2. Now suppose that $q=4$, $n_1=15$ and $n_2=45$. Set ω be a primitive element of $\mathbb{F}_{16}$. Take the $g_1(x)=x^{13}+\omega^2x^{12}+\omega^6x^{11}+\omega^6x^{10}+\omega^{13}x^9+\omega^{14}x^8+\omega^8x^7+$ $\omega^{14}x^6+\omega^2x^5+\omega^{13}x^4+\omega^3x^3+x^2+\omega^8x+\omega^3$, $g_2(x)=x^{40}+\omega^2x^{39}+\omega^6x^{38}+x^{37}+\omega^6x^{36}$ $+\omega^9x^{35}+\omega^3x^{34}+\omega^9x^{33}+\omega^{12}x^{32}+\omega^{12}x^{31}+\omega^4x^{30}+\omega^5x^{29}+\omega x^{28}+\omega^6x^{27}+\omega^3x^{26}+\omega^3x^{25}$ $+\omega^{10}x^{24}+\omega^{11}x^{23}+\omega^{11}x^{22}+\omega^3x^{21}+\omega^4x^{20}+\omega^{12}x^{19}+\omega^7x^{18}+\omega^9x^{16}+\omega^{11}x^{15}+x^{14}+\omega^{11}x^{13}$ $+\omega x^{12}+\omega^{13}x^{11}+\omega^7x^{10}+\omega^{13}x^9+\omega x^8+\omega^9x^7+\omega^4x^6+\omega^{11}x^4+\omega^{13}x^3+\omega^2x^2+\omega^{10}x+\omega^5$. And select $f(x)=\omega^3x^4+x^3+x^2+x+1$. We know C is a GQC code with parameters $[60,5,15]_{16}$. By Theorem 4, a $[\![60,50,3]\!]_4$ quantum code with information rate 0.833 is obtained. In comparison with the $[\![65,53,3]\!]_4$ quantum code with information rate 0.815 in [16], it has better parameters.

5 Conclusion

In this paper, we consider a class of one-generator GQC codes with index 2 and study the form of its Hermitian dual code. Moreover, a sufficient condition to decide the Hermitian self-orthogonality of GQC codes is provided, so that many QECCs with good parameters can be constructed by these GQC codes effectively. Therefore, our method achieves both feasible and practical values.

This work is supported by National Natural Science Foundation of China (Nos.11801564, 11901579).

References

1. P. W. Shor, Phys. Rev. A, Gen. Phys. **52(4)**, 2493-2496 (1995)
2. A. Ashikhmin, E. Knill, IEEE Trans. Inf. Theory **47(7)**, 3065-3072 (2001)
3. D. Gottesman, Ph.D. Thesis, California Institute of Technology (1977)
4. A. Ketkar, A. Klappenecker, S. Kumar, IEEE Trans. Inf. Theory **52**, 4892-4914 (2006)
5. S. Ling, J.Luo, C. Xing, IEEE Trans. Inf. Theory **56**, 4080-4084 (2008)
6. I. Siap, N. Kulhan, Appl. Math. **5**, 24-30 (2005)
7. Y. Kou, S. Lin, M. P. C. Fossorier, IEEE Trans. Inf. Theory **47(7)**, 2711-2736 (2001)
8. H. Tang, J. Xu, S. Lin, K. A. S. Abdel-Ghaffar, IEEE Trans. Inf. Theory **51(2)**, 572-596 (2005)
9. V.Y. Van, H. Matsui, S. Mita,: IEEE Global Telecommunications Conference GLOBECOM, Miami, FL, USA 1-6 (2010)
10. Y. Cao, Codes Cryptogr. **60**, 67-79 (2011)
11. M. Esmaeili, S. Yari, AAECC. **20**, 159-173 (2009)
12. C. Galindo, F. Hernando, R. Mastsumoto, Finite Fields Appl. **52**, 261-280 (2018)
13. J. Lv, R. Li, J. Wang, IEEE Communications Letters, 1-1 (2020)
14. J. Lv, R. Li, J.Wang, International Journal of Theoretical Physics. **59**, 300-312 (2020)
15. J. Lv, R. Li, J.Wang, IEEE Access **7**, 85782-85785 (2019)
16. Y. Edel, Table of quantum twisted codes. electronic address: www.mathi.uniheidelberg.de/yves/matritzen/QTBCH/QTBCHIndex.html