Some Quantum Error-Correcting Codes with $d = 5$

Husheng Li$^{1,a}$, Ruihu Li$^{2,b,*}$, Yu Yao$^{3,c}$, Qiang Fu$^{4,d}$

$^{1,2,3,4}$Department of Basic Sciences Air Force Engineering University Xi'an, Shaanxi, 710051, P. R. China

$^{b,*}$ldlv@xidian.edu.cn

$^{a}$E-mail: li1298670080@163.com, $^{b,*}$Corresponding author’s e-mail: llzsy2015@163.com, $^{c}$E-mail: njjbxqyy@163.com, $^{d}$E-mail: fuqiangkgd@163.com

Abstract—In this paper, we firstly give a computer-support method of searching for Hermitian self-orthogonal linear code. Then two linear codes with dual distance 5 over field $F_q$ for $q=2,3$, respectively, are chosen as ingredients. By use of this searching method, we totally find 88 Hermitian self-orthogonal linear codes and construct 88 related quantum error-correcting codes with $d=5$. Most of these results are best known quantum codes and a number of them have better parameters than that of previous quantum codes.

1. INTRODUCTION

Since 1980s, people have been developing the technologies of quantum computer fast and firmly. Due to the great characteristics of quantum bit (qubit), quantum computer has overwhelming superiority in operation and security than classical computers. In 1994, Shor [1] presented an algorithm that can factor an integer in polynomial time on a quantum computer, which cannot be finished in case of classical computers. However, in the implement of quantum computation [2], there exists several major sources of errors: dissipation, decoherence and measurement errors, etc. Thus, quantum error correction is quite essential.

In 1995, Shor [3] formulated the theory of quantum error-correcting codes (QEECs) and firstly constructed a quantum $[[9,1,3]]$-code, which could be used to encode a single qubit in nine qubits and concurrently correct one error.

After that, Calderbank, Rains, Shor and Bierbrauer etc [4]-[9] translated the problem of finding QEECs into the problem of determining classical codes with certain self-orthogonal (or dual-containing) properties, which offers some efficient methods of constructing $q$-ary QEECs. Especially, the construction theorem cited by this paper is given as follows:

**Lemma 1:** (Hermitian construction)[9] If $C$ is a $q^2$-ary linear code of length $n$, dimension $n-k$ and dual distance $d^\perp$, which is self-orthogonal with respect to the Hermitian inner product, then there exists a pure quantum error-correcting code with parameter $[[n, n-2k, d^\perp]]_q$.

Motivated by above works, in order to get more QEECs with different parameters through Hermitian construction, we give a method of searching for Hermitian self-orthogonal linear codes. For a certain $q^2$-ary linear code $C$, we can give all Hermitian self-orthogonal linear codes that exists by puncturing $C$ or the equivalents code of $C$. 
This paper is organized as follows. Basic concepts on linear code are recalled in Sect. 2. In Sect. 3, more details about that searching method are described. In Sect. 4, we choose two linear codes over field \( \mathbb{F}_q \) (\( q = 2, 3 \)) as ingredients and severally search for the Hermitian self-orthogonal linear codes they contain. Meanwhile, by Hermitian construction, these findings are used to construct QEECs with \( d = 5 \). Finally, the conclusions are given.

2. Fundamentals of linear codes

2.1. Some concepts of linear code

Let \( \mathbb{F}_q \) be the finite field of order \( q \). An \([n, k]_q\)-linear code \( C \) over finite field \( \mathbb{F}_q \) is simply a \( k \)-dimensional subspace of the vector space \( \mathbb{F}_q^n \). A generator matrix \( G \) for an \([n, k]_q\)-code \( C \) is any \( kn \times n \) matrix whose rows form a basis for \( C \).

Denote by \( C^\perp \) the dual code of an \([n, k]_q\)-code \( C \), which is the orthogonal space of \( C \) with respect to an Euclidean inner product. The code’s parameters of \( C^\perp \) is \([n, n-k]\) and Euclidean inner product over \( \mathbb{F}_q \) is defined as

\[
\langle x, y \rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n = \sum_{i=1}^{n} x_iy_i, \quad x, y \in \mathbb{F}_q^n.
\]  

The (Hamming) weight \( \text{wt}(x) \) of a vector \( x \) is the number of nonzero coordinates in \( x \). For a linear code \( C \), its minimal distance \( d \) is defined as the smallest weight of all codewords. Especially, the minimal distance of \( C^\perp \) is called the dual distance of \( C \) and denoted by \( d^\perp \). The following lemma offers another way to determine dual distance of a linear code.

**Lemma 2**:[10] A linear code has dual distance \( d^\perp \) if and only if its generator matrix has a set of \( d^\perp \) linearly dependent columns but no set of \( d^\perp - 1 \) linearly dependent columns.

Next, the notion of punctured code and equivalent code is given.

**Definition 1**: Assume \( C \) is an \([n, k]_q\)-linear code with dual distance \( d^\perp \). If we puncture \( C \) by deleting \( t \) coordinates in each codeword, then the resulting code is called punctured code and denoted by \( \overset{*}{C} \). It’s easy to verify that \( \overset{*}{C} \) is still linear with parameters \([n-t, k-t]_q\) and dual distance \( d^\perp \).

**Definition 2**: Assume that \( F_q^* = F_q \setminus \{0\} \) and vector \( \overline{v} = (v_1, v_2, \cdots, v_n) \in F_q^* \). Consider the map \( \eta_c : C \to C^\perp \), where \( C^\perp = (v_1e_1 + v_2e_2 + \cdots + v_ne_n \mid (c_1, c_2, \cdots, c_n) \in C) \). Then we call \( C^\perp \) the equivalent code of \( C \) designed by varied vector \( \overline{v} \). Besides, both \( C \) and \( C^\perp \) have the same parameters.

2.2. Hermitian self-orthogonal code

Let \( F_q \) be the finite field with \( q^2 \) elements, where \( q \) is a prime power, then Hermitian inner product over \( F_q \) can be defined as

\[
\langle x, y \rangle_h = x_1y_1 + x_2y_2 + \cdots + x_ny_n = \sum_{i=1}^{n} x_iy_i, \quad x, y \in \mathbb{F}_q^n.
\]  

If \( C \) is a linear code of length \( n \) over \( F_q \), its Hermitian dual code can be defined as

\[
C^\perp_h = \{ \overline{x} \in F_q^n \mid \langle x, y \rangle_h = 0, \text{ for all } y \in C \}.
\]  

If \( C \) satisfies the condition that \( C \subseteq C^\perp_h \), then we call \( C \) self-orthogonal code with respect to the Hermitian inner product. For the judgement whether a linear code over \( F_q \) is Hermitian self-orthogonal or not, we have following lemma:
Lemma 3: [11] Let \( C \subseteq F_q^n \) be a linear code. Then \( C \) is self-orthogonal with respect to the Hermitian form if and only if \( \overline{\langle x, x \rangle} = 0 \) for all \( \overline{x} \in C \).

3. Method Of Searching For Hermitian Self-Orthogonal Linear Code

Assume \( \zeta \) is a primitive element of \( F_q \), then \( \omega = \zeta^{q+1} \) is a primitive element of \( F_q \). Therefore, we can define that \( F_q = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{q-2}\} \) and \( F_q = \{0, 1, \omega, \omega^2, \ldots, \omega^{q-2}\} \).

Definition 3: Let \( N: F_q^n \to F_q^n \) the norm \( (N(x) = x^{q+1}) \). It’s easy to check that \( N(\zeta^i) = \omega^i \), for \( 0 \leq i \leq q-2 \). Let \( C \) be an \( F_q^n \)-linear code of length \( n \). The norm code of \( C \) is the code \( N(C) \subseteq F_q^n \) spanned over \( F_q \) by the norms \( N(c) = (N(c_1), N(c_2), \ldots, N(c_n)) \), where \( c = (c_1, c_2, \ldots, c_n) \in C \). Denote by \( N(C)^\perp \) its dual with respect to the Euclidean inner product.

Lemma 4: [11] Let \( C \) be an \([n, k]\) code with dual distance \( d^\perp \). If \( N(C)^\perp \) has a codeword \( u \) of weight \( m \) and nonzero coordinates of \( u \) are all 1, then there is a Hermitian self-orthogonal code \( C^* \) with parameters \([m, \leq k]\) and dual distance \( d^\perp \) by puncturing \( C \). Particularly, if \( N(C)^\perp \) contains \( 1, (1,1, \ldots, 1) \), then \( C \) itself is Hermitian self-orthogonal.

Theorem 1: Let \( C \) be an \([n, k]\) code with dual distance \( d^\perp \). If \( N(C)^\perp \) has a codeword \( u \) of weight \( m \), then there is a \([m, \leq k]\) Hermitian self-orthogonal code with dual distance \( d^\perp \).

Proof: Assume the nonzero coordinates of \( u \) are in the positions \( \{i_1, i_2, \ldots, i_m\} \), so that \( u_i \neq 0 \), if \( i \in \{i_1, i_2, \ldots, i_m\} \).

Case 1: If \( u_i = 1 \), when \( i \in \{i_1, i_2, \ldots, i_m\} \). This case has been proofed by Lemma 4 in [11].

Case 2: If the nonzero coordinates of \( u \) consists of arbitrary elements in \( F_q^* \). According to the definition of dual code, \( \forall \overline{x} \in N(C) \), we have \( \overline{\langle x, u \rangle} = \sum_{i \in \{i_1, i_2, \ldots, i_m\}} x_i u_i = 0 \). Then consider code \( C^* \), which is the equivalent code of \( C \) and designed by varied vector \( \overline{v} = (v_1, v_2, \ldots, v_n) \in F_q^n \), where \( N(v_i) = u_i \). There must exist a codeword \( \overline{u}^* \) of \( N(C^*) \) that weight \( m \) and nonzero coordinates of \( \overline{u}^* \) are all 1. Thus, by Lemma 4, we can get a \([m, \leq k]\) Hermitian self-orthogonal code with dual distance \( d^\perp \) by puncturing \( C^* \).

Combining above theorem and Lemma 1, the following corollary can be obtained.

Corollary 1: Let \( C \) be an \([n, k]\) code with dual distance \( d^\perp \). If \( N(C)^\perp \) has a codeword of weight \( m \), then there is a pure quantum error-correcting code with parameter \([m, m-2k', d^\perp]\), where \( k' \leq k \).

In this paper, it’s easy to check that the dimensions of all the obtained Hermitian self-orthogonal codes and quantum error-correcting codes are unchanged.

4. QEECS With Minimal Distance \( d = 5 \)

In this section, two linear codes with parameters \([85, 8]\) and \([72, 6]\) are given. Both of them have dual distance \( d^\perp = 5 \). By the searching method, the Hermitian self-orthogonal codes they severally contain are listed and through Hermitian construction, their corresponding QEECs are also constructed.
4.1. 2-ary QEECs Constructed From \([85,8]\)_4-code

Assume \(F_4 = \{0,1,\omega,\omega^3\}\) is the finite field with 4 elements, where \(\omega\) is a primitive element of \(F_4\). For ease of presentation, we use the figures 2,3 to represent the elements \(\omega, \omega^3\), respectively. Hence, the generator matrix of code with parameters \([85,8]\)_4 and dual distance \(d^\perp = 5\) can be written as:

\[
G_{8,85} = (G_{8,43}, G_{8,42}) \,,
\]

\[
G_{4,43} = \begin{pmatrix}
100000013033012111201232101031130332103313 \\
01000000203122220031211130120011210 \\
0010000301220132210232210133033313 \\
000100010232110201210111332001123202103 \\
0000100003102331102012101133200112320210 \\
0000010012031210323103133132021110112020 \\
000001023211022111200313320231003313001 \\
000000130330121112012321010311303321033132 \\
00000001000031023311020111203210332103313 \\
000000001000310233110201112032103321033132 \\
2031120321202132201201031321013231031130202 \\
02113221002122012322120031111330113123 \\
100222003131110113032210121013201301201 \\
2123312031203231001322110113030112230120 \\
3212312031203231010032211101330112230120 \\
3333001212202210132302012330210321002 \\
3211300131100312021111302333202303231203 \\
0311203221220321201103132103113022020
\end{pmatrix} \,.
\]

\[
G_{8,42} = \begin{pmatrix}
101113320010123203210 \\
1013103011223012 \\
3333001212202210132302012330210321002 \\
3211300131100312021111302333202303231203 \\
0311203221220321201103132103113022020
\end{pmatrix} \,.
\]

Denote the corresponding linear code of \(G_{8,85}\) by \(C_{8,85}\). After computation, the norm code \(N(C_{8,85})\) and its Euclidean dual code \(N(C_{8,85})^\perp\) can be obtained. Then we find that when \(t\) is even and \(16 \leq t \leq 72\), there exists codewords of weight \(t\) contained in \(N(C_{8,85})^\perp\), which implies the existence of Hermitian self-orthogonal code with parameters \([t,8]\)_4 and dual distance \(d^\perp = 5\). Thus, by Corollary 1, we have

**Theorem 2:** Assume \(s\) is even and \(16 \leq s \leq 72\), then there exists a pure \([s,s-16,5]\)_s quantum error-correcting code.

Compared to 2-ary QEECs in table made by Markus Grassl [12], most of these results are best known. Especially the \([72,56,5]\)_s quantum code has improved distance.

4.2. 3-ary QEECs Constructed From \([72,6]\)_6-code

Let \(F_3 = \{0,1,2\}\) be the finite field of order 3 and \(f(x) = x^2 + 2x + 2\) is a primitive element in \(F_3[x]\). We can define that \(F_9 = F_3 / \langle f(x) \rangle = \{0,1,w,w^2,2,w^2,w^6,w^7\}\), where \(w\) is a root of \(f(x)\). In the following part, the elements \(w,w^2,w^3,w^4,w^5,w^6,w^7\) are replaced by \(3,4,7,6,8,5\), respectively.

For \([72,6]\)_6-code with dual distance \(d^\perp = 5\), its generator matrix is given as follows:

\[
G_{7,72} = (G_{7,36}, G_{7,36}^2) \,.
\]
Denote the generated code of $G_{6,36}^r$ by $C_{6,36}$. We can get norm code $N(C_{6,36})$ and its Euclidean dual code $N(C_{6,36})^\perp$, where $N(C_{6,36})^\perp$ is a 3-ary linear code with parameters [72,36]. Then after a long-time calculation, we find $N(C_{6,36})^\perp$ contains the codeword of weight $t$, $t \in \{14,15,\ldots,72\}$. Therefore, when $14 \leq t \leq 72$, there exists Hermitian self-orthogonal code with parameters $[t,6]$, and dual distance $d^\perp = 5$. Similarly, through Corollary 1, we also have

**Theorem 3:** Assume $s \in \{14,15,\ldots,72\}$, then there exists a pure $[[s, s - 12, 5]]$ quantum error-correcting code.

By Comparing these results with quantum codes in [13]-[15], 56 constructed results are new and some have better parameters. Here we only list the QECCs which have better parameters than that of quantum codes in [13]-[15].

| QEECs in this paper | QEECs in [12] | QEECs in [14] |
|---------------------|---------------|---------------|
| $[[56,44,5]]_i$     | $[[56,40,5]]_i$ | -             |
| $[[56,44,5]]_i$     | $[[56,44,4]]_i$ | -             |
| $[[70,58,5]]_i$     | -             | $[[70,54,5]]_i$ |

| Table II. Comparison of the QECCs in this paper and in [15] |
|-------------------------------------------------------------|
| QEECs in this paper | QEECs in [15] |
| $[[21,9,5]]_i$   | $[[21,7,5]]_i$ |
| $[[40,28,5]]_i$  | $[[40,26,5]]_i$ |
| $[[41,29,5]]_i$  | $[[41,27,5]]_i$ |
| $[[52,40,5]]_i$  | $[[52,34,5]]_i$ |
| $[[53,41,5]]_i$  | $[[53,36,5]]_i$ |
| $[[57,45,5]]_i$  | $[[57,37,5]]_i$ |
| $[[57,45,5]]_i$  | $[[57,43,4]]_i$ |
| $[[65,53,5]]_i$  | $[[65,47,4]]_i$ |
| $[[65,53,5]]_i$  | $[[65,43,5]]_i$ |
| $[[70,58,5]]_i$  | $[[70,52,4]]_i$ |
| $[[71,59,5]]_i$  | $[[71,57,3]]_i$ |
5. CONCLUSION
By searching method, we have totally found 88 Hermitian self-orthogonal codes from two linear codes with dual distance 5. Then through Hermitian construction, 88 related QEECs with $d = 5$ are also constructed. Most of obtained QEECs are new or best known, and some even have improved parameters.

ACKNOWLEDGMENT
This work is supported by the National Natural Science Foundation of China under Grant No. 11801564, 11901579.

REFERENCES
[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th annual symposium on foundations of computer science, pp. 124-134, 1994.
[2] D. Bartoli, G. Faina, S. Marcugini, et al. "New quantum caps in PG(4,4)," Journal of Combinatorial Designs, vol. 20, no. 10, pp. 448-466, Jan. 2012.
[3] P. W. Shor. "Scheme for reducing decoherence in quantum computer memory," Phys. Rev. A., vol. 52, no. 4, pp. 2493-2496, Oct. 1995. K. Elissa, “Title of paper if known,” unpublished.
[4] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," IEEE Trans. Inf. Theory, vol.44, no. 4, pp. 1369-1387, Jul. 1998.
[5] A. M. Steane. "Enlargement of Calderbank-Shor-Steane quantum codes," IEEE Trans. Inf. Theory, vol. 45, no. 7, pp. 2492-2495, Nov. 1999.
[6] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A., vol. 54, no. 2, pp. 1098-1105, Aug. 1996.
[7] J. Bierbrauer and Y. Edel. "Quantum twisted codes," J. Comb. Designs, vol. 8, no. 3, pp. 174-188, Apr. 2000.
[8] M. Grassl, T. Beth and M. Rotteler. "On optimal quantum codes," Int. J. Quantum Inform., vol. 2, no. 1, pp. 55-64, 2004.
[9] A. Ketkar, A. Klappenecker and S. Kumar, "Nonbinary stablizer codes over finite fields," IEEE Trans. Inf. Theory, vol. 52, pp. 4892-4914, 2006.
[10] Huffman, W and Pless, V. (2003). "Fundamentals of Error-Correcting Codes," Cambridge: Cambridge University Press. doi:10.1017/CBO9780511807077
[11] J. Bierbrauer, D. Bartoli, G. Faina, et al. "The structure of quaternary quantum caps," Designs, Codes and Cryptography, vol. 72, no. 3, pp.733-747, Sep. 2014.
[12] GRASSL M. Bounds on the minimum distance of QEECs. [EB/OL]. Available: http://www.codetables.de/ Accessed 7 Aug. 2019.
[13] J. Lv, R. Li, J. Wang. "Constructions of quasi-twisted quantum codes, " Quantum Inf. Processing, 19, 274 Jul. 2020.
[14] Lv, Jingjie, Li, Ruihu and Wang, Junli. (2019). "Quantum Codes Derived from One-Generator Quasi-Cyclic Codes with Hermitian Inner Product." International Journal of Theoretical Physics. 59. 10.1007/s10773-019-04324-z.
[15] Y. Edel’s homepage: www.mathi.uni-heidelberg.de/~yves/ Matritzen/QTBC/QTBCIndex.html