IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received January 20, 2019, accepted February 6, 2019, date of publication February 27, 2019, date of current version March 12, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2899383

New Non-Binary Quantum Codes Derived From a Class of Linear Codes

JIAN GAO AND YONGKANG WANG
School of Mathematics and Statistics, Shandong University of Technology, Zibo 255000, China
Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China

Corresponding author: Yongkang Wang (zcyongkang@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 11701336, Grant 11626144, and Grant 11671235, and in part by the Scientific Research Fund of Hubei Provincial Key Laboratory of Applied Mathematics (Hubei University) under Grant HBAM201804.

ABSTRACT In this short paper, we consider the non-binary quantum codes construction from a class of linear codes, which are not self-orthogonal over finite fields. As the computational results, new quantum codes $[[8, 0, \geq 4]]_3$, $[[8, 2, \geq 3]]_3$, $[[11, 1, \geq 5]]_3$, $[[10, 0, \geq 5]]_4$, and $[[16, 6, \geq 4]]_4$ are obtained.

INDEX TERMS Quantum codes, linear codes, Calderbank-Shor-Steane (CSS) construction.

I. INTRODUCTION

Quantum coherence plays an essential role in quantum information theory. Decoherence is a property of quantum, which can destroy quantum coherence. It makes quantum computation easy to make mistakes. Reducing the decoherence or controlling the decoherence to an acceptable level is a key problem that must be solved by scientists. From now on, quantum error-correcting codes is one of the most effective ways to overcome decoherence.

Shor [1] constructed the first quantum error-correcting code $[[9, 1, 3]]$, which can correct 1 bit quantum error with 9 quantum bits. This code space is a 2-dimensional complex space. In 1996, two independent research groups Calderbank and Shor [2] and Steane [3] adopted the idea of classical linear block error-correcting codes, and gave a method to construct quantum error-correcting codes using two classical binary error-correcting codes called Calderbank-Shor-Steane (CSS) construction method. In 1998, Calderbank *et al.* [4] gave the relationship between quantum codes and self-orthogonal codes on the quaternary field. Later, Ketkar *et al.* [5] gave a method to construct quantum codes by using the inclusion relationship of two linear codes over finite fields $\mathbb{F}_q$. This method is called the CSS quantum codes construction. Recently, with the development of quantum information theory, there have been a lot of applications of quantum codes in quantum environment, such as quantum network coding [6], [7], multiparty quantum key management (QKM) protocol [8], quantum cooperative multicast (QCM) [9], etc.

In recent years, a lot of good quantum codes are constructed by self-orthogonal codes over finite fields because the self-orthogonal codes satisfy the conditions of CSS quantum codes construction method, and the self-orthogonal codes can be constructed effectively by algebraic codes such as cyclic codes, constacyclic codes, AG codes and so on. For example, Thangaraj and McLaughlin [10] provided a construction for quantum codes from Hermitian self-orthogonal cyclic codes over $\mathbb{F}_{4^m}$, Guardia [11] constructed some new quantum codes from a class of special cyclic codes whose defining set consists of only one cyclotomic coset containing at least two consecutive integers; Xiaoyan [12] constructed quantum code from some classes of constacyclic codes, Koroglu [13] constructed eight new classes of entanglement-assisted quantum MDS codes by virtue of a decomposition of the defining set of constacyclic codes; Feng *et al.* [14] gave an asymptotic bounds on quantum codes from algebraic geometry codes, Chen [15] constructed asymptotically good family of quantum codes from algebraic geometric codes, Munuera *et al.* [16] studies quantum codes construction from algebraic geometric codes of Castle type.

One question is that if we can give a class of linear codes that are not self-orthogonal to construct quantum codes effectively. In 2018, Hivadi [17] presented a construction method for binary quantum codes from a class of non self-orthogonal binary linear codes. This construction method can be effectively extended to the case of non-binary quantum codes. In this short paper, we will do this issue.

The associate editor coordinating the review of this manuscript and approving it for publication was Xueqin Jiang.

II. CONSTRUCTION OF QUANTUM CODES

Let $\mathbb{F}_q$ be finite fields, where $q = p^t$, p is a prime, t is a positive integer. If C is a k-dimensional subspace of $\mathbb{F}_q^n$, then C will be called an $[n, k]$ linear code over $\mathbb{F}_q$. The linear code C has q^k codewords. For $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$, we define the weight as $\mathrm{wt}(\mathbf{c}) = \#\{i \mid c_i \neq 0,\ 0 \leq i \leq n-1\}$. The minimum distance is $d = \min\{wt(\mathbf{a} - \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in C\}$. Further, if the minimum distance d of C is known, it is also sometimes referred to as an $[n, k, d]$ linear code. In coding theory, two frequently-used ways to present a linear code are with either a generator matrix or a parity check matrix.

A $k \times n$ matrix G over $\mathbb{F}_q$ is called a generator matrix of C if the rows of G generates C and no proper subset of the rows of G generates C. Let $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$, $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_q^n$, the inner product of vectors $\mathbf{x}$ and $\mathbf{y}$ is $\mathbf{x} \cdot \mathbf{y} = \sum_{i=0}^{n} x_i y_i$. The dual code of C is defined by $C^{\perp} = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x} \cdot \mathbf{c} = 0, \forall\ \mathbf{c} \in C\}$. A parity check matrix H for a linear C is a generator matrix for the dual code $C^{\perp}$. A linear code C of length n is called self-orthogonal if $C \subseteq C^{\perp}$, and self-dual if $C^{\perp} = C$. Clearly, self-dual codes are subclass of self-orthogonal codes.

In the following, we will give the CSS quantum codes construction first.

Lemma 1 [5] (CSS Quantum Codes Construction): Let C_1 and C_2 be two linear codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, respectively. If $C_2^{\perp} \subseteq C_1$, then there is a quantum code with parameters $[[n, k_1 + k_2 - n, \geq d]]_q$, where $d = \min\{d_1, d_2\}$.

If $C_1 = C_2$, then we have the following Lemma 2. In fact, most of works on quantum codes construction from self-orthogonal linear codes over finite fields based on this fundamental result.

Lemma 2 [5]: Let C be a linear $[n, k, d]_q$ code satisfying $C^{\perp} \subseteq C$, then there is a quantum code with parameters $[[n, 2k - n, \geq d]]_q$.

In the following, we will introduce non-binary quantum codes construction from a class of linear codes, which are not self-orthogonal codes over finite fields.

At the beginning, we need some preparations. The permutation matrix P is a square matrix with exactly one 1 in each row and column and 0s elsewhere. The diagonal matrix D is a square matrix with only non-zero elements on the diagonal line. The monomial matrix is a square matrix with exactly one non-zero entry in each row and column. In other words, the monomial matrix M can be written either in the form DP or PD', where D and D' are diagonal matrices and P is a permutation matrix.

Lemma 3 [18]: Let C_1 and C_2 be linear codes of the same length over $\mathbb{F}_q$, and let G_1 be a generator matrix for C_1. Then

(i) C_1 and C_2 are permutation equivalent if there is a permutation matrix P such that $G_1 P$ is a generator matrix of C_2.

(ii) C_1 and C_2 are monomial equivalent if there is a monomial matrix M such that $G_1 M$ is a generator matrix of C_2.

(iii) C_1 and C_2 are equivalent if there is a monomial matrix M and an automorphism γ of the finite field $\mathbb{F}_q$ such that $G_1 M \gamma$ is a generator matrix of C_2.

Note that two equivalent codes have the same weight distribution.

Let $H(C_1)$ and $H(C_2)$ be parity check matrices of linear codes C_1 and C_2, respectively. If $H(C_2)H(C_1)^{\top} = 0$, then $C_2^{\perp} \subseteq C_1$ which implies that there is a quantum code associated to C_1 and C_2 by CSS quantum codes construction method. Let

$$H = \begin{bmatrix} H(C_2) & 0 \\ 0 & H(C_1) \end{bmatrix}$$

with $H(C_2)H(C_1)^{\top} = 0$. Then we call H is the parity check matrix of the associated quantum code. The problem of quantum codes construction from error-correcting codes over finite fields turns out to be a problem to construct the parity check matrix H.

Now, we will give the main construction results in the following.

Theorem 1: Let C be an $[n, k, d]$ linear code over $\mathbb{F}_p$ with parity check matrix H, where p is an odd prime. If there is a monomial matrix M such that $H(HM)^{\top} = 0$, then there is a non-binary $[[n, 2k - n, \geq d]]_p$ quantum code with parity check matrix

$$\begin{bmatrix} H & 0 \\ 0 & HM \end{bmatrix}.$$

Proof: Let C be an $[n, k, d]$ linear code over $\mathbb{F}_p$ with parity check matrix H, M be an $(n-k) \times (n-k)$ monomial matrix over $\mathbb{F}_p$. Let C' be a linear code with parity check matrix HM. Then $C^{\perp}$ and $C'^{\perp}$ are monomial equivalent. Since $H(HM)^{\top} = 0$, it follows that $C^{\perp} \subseteq C'$. By Lemma 1, there is a quantum code associated to C and C'. Further, the matrix $\begin{bmatrix} H & 0 \\ 0 & HM \end{bmatrix}$ is the parity check matrix of the associated quantum code.

Now, we will show that the parameters of this quantum code are $[[n, 2k - n, \geq d]]_p$. The number of $\mathbb{F}_p$-linearity independent rows in the matrix $\begin{bmatrix} H & 0 \\ 0 & HM \end{bmatrix}$ is $2(n-k)$, so the quantum code has the dimension $n - 2(n-k) = 2k - n$. The linear code C has the minimum distance d. That is, the parity check matrix H of C has a set of d linear dependent columns but no set of $d-1$ linearly dependent columns. Clearly, H and HM have the same linearly correlation. Thus, the parameters of the quantum code are $[[n, 2k - n, \geq d]]_p$. ■

Theorem 2: Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$ with parity check matrix H, where $q = p^t$, p is an odd prime and $t \geq 2$ is a positive integer. If there is a monomial matrix M and an automorphism γ of the finite field $\mathbb{F}_q$ such that $H(HM\gamma)^{\top} = 0$, then there is a non-binary $[[n, 2k - n, \geq d]]_q$ quantum code with parity check matrix

$$\begin{bmatrix} H & 0 \\ 0 & HM\gamma \end{bmatrix}.$$

Proof: The proof process of this theorem is similar to Theorem 1. We omit it here. ■

III. SOME NEW NON-BINARY QUANTUM CODES

In this section, we will give some computational examples to illustrate that our construction method can produce good non-binary quantum codes. More importantly, some of these quantum codes can not be obtained by self-orthogonal codes.

Example 1: Let C be an $[8, 4, 4]$ linear code over $\mathbb{F}_3$. The parity check matrix H of this linear code is given as follows

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 \\ 0 & 1 & 0 & 0 & 1 & 2 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 \end{bmatrix}.$$

This linear code is not self-orthogonal. Consider the monomial matrix M on the matrix H as follows

$$HM = \begin{bmatrix} 2 & 2 & 0 & 0 & 2 & 0 & 1 & 2 \\ 2 & 1 & 0 & 0 & 0 & 2 & 2 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 2 & 2 \\ 2 & 2 & 0 & 1 & 0 & 0 & 2 & 1 \end{bmatrix}.$$

We have $H(HM)^{\top} = 0$. By Theorem 1, there is an $[[8, 0, \geq 4]]_3$ quantum code. This quantum code has the same length and dimension as the known quantum code $[[8, 0, 3]]_3$ appeared in [19], but our code has the larger minimum distance than that code. Further, since the highest minimum distance of the self-dual code of length 8 over $\mathbb{F}_3$ is 3, then we can not get the quantum code $[[8, 0, \geq 4]]_3$ by self-dual codes.

Example 2: Let C be an $[8, 5, 3]$ linear code over $\mathbb{F}_3$. The parity check matrix H of this linear code is given as follows

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 & 2 & 2 & 1 & 2 \\ 0 & 0 & 1 & 2 & 0 & 2 & 0 & 1 \end{bmatrix}.$$

This linear code is not self-orthogonal. Consider the monomial matrix M on the matrix H as follows

$$HM = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 2 & 1 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 1 & 2 & 0 & 0 \end{bmatrix}.$$

Then $H(HM)^{\top} = 0$. By Theorem 1, there is an $[[8, 2, \geq 3]]_3$ quantum code. This quantum code has the same length and minimum distance as the known quantum code $[[8, 0, 3]]_3$ appeared in [19], but our code has the larger dimension than that code.

Example 3: Let C be an $[11, 6, 5]$ linear code over $\mathbb{F}_3$. The parity check matrix H of this linear code is given as follows

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 2 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 0 & 1 \end{bmatrix}.$$

This linear code is not self-orthogonal. Consider the monomial matrix M on the matrix H as follows

$$HM = \begin{bmatrix} 1 & 0 & 0 & 2 & 2 & 1 & 2 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 & 1 & 0 & 2 & 1 & 0 & 0 & 2 \\ 0 & 0 & 2 & 2 & 1 & 2 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 & 2 & 2 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Then $H(HM)^{\top} = 0$. By Theorem 1, there is an $[[11, 1, \geq 5]]_3$ quantum code. This quantum code has the same length and dimension as the known quantum code $[[11, 1, 4]]_3$ appeared in [19], but our code has the larger minimum distance than that code.

Example 4: Let C be an $[10, 5, 5]$ linear code over $\mathbb{F}_4$. The parity check matrix H of this linear code is given as follows

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & w^2 & w^2 & 0 & w \\ 0 & 1 & 0 & 0 & 0 & w & 0 & w & w^2 & w^2 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & w^2 & w & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & w & w & w^2 & 0 \\ 0 & 0 & 0 & 0 & 1 & w^2 & w^2 & 0 & w & w \end{bmatrix},$$

where w is a primitive element of $\mathbb{F}_4$. This linear code is not self-orthogonal. Consider the monomial matrix M and the automorphism γ over $\mathbb{F}_4$ on the matrix H as follows

$$HM\gamma = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & w & w & 0 & w^2 \\ 0 & w^2 & 0 & 0 & w & 1 & w^2 & 0 & 0 & w \\ 0 & 1 & 0 & 1 & w^2 & 0 & w & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & w & 0 & w^2 & w^2 & 0 & 0 \\ 0 & w & 0 & 0 & w^2 & 0 & 0 & w & 1 & w^2 \end{bmatrix}.$$

Then $H(HM\gamma)^{\top} = 0$. By Theorem 2, there is an $[[10, 0, \geq 5]]_4$ quantum code. Since the highest minimum distance of the self-dual code of length 10 over $\mathbb{F}_4$ is 4, then we can not get the quantum code $[[10, 0, \geq 5]]_4$ by self-dual codes.

Example 5: Let C be an $[14, 10, 4]$ linear code over $\mathbb{F}_4$. The parity check matrix H of this linear code is given as follows

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & w & w & w^2 & 1 & 0 & w & w & 0 & 1 \\ 0 & 1 & 0 & 0 & w & w & 1 & w^2 & 1 & 1 & w^2 & 1 & w & w \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & w & w & 1 & w^2 & 1 & 1 & w^2 \\ 0 & 0 & 0 & 1 & w & w & w^2 & 1 & 0 & w & w & 0 & 1 & w^2 \end{bmatrix},$$

where w is a primitive element over $\mathbb{F}_4$. This linear code is not self-orthogonal. Consider the monomial matrix M and the automorphism γ over $\mathbb{F}_4$ on the matrix H as follows

$$HM\gamma = \begin{bmatrix} w & 0 & 0 & 1 & 0 & w^2 & 1 & 1 & 0 & 1 & w^2 & 0 & w^2 & w^2 \\ w & 0 & 1 & 1 & 1 & w & w^2 & 0 & 0 & w^2 & w^2 & w^2 & 1 & 1 \\ w^2 & 1 & 0 & w^2 & 1 & w & w & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & w^2 & w^2 & w & 0 & 1 & w^2 & w^2 & 1 & 0 & w \end{bmatrix}.$$

Then $H(HM\gamma)^{\top} = 0$. By Theorem 2, there is an $[[14, 6, \geq 4]]_4$ quantum code. This quantum code has the same length and minimum distance as the known quantum code $[[14, 0, 4]]_4$ appeared in [19], but our code has the larger dimension than that code. □

IV. CONCLUSION

In this paper, we studied the non-binary quantum codes construction from a class of linear codes, which are not self-orthogonal over finite fields. We can construct some quantum codes with special parameters $[[n, 0, \geq d]]$, which can not be constructed by self-orthogonal codes over finite fields.

REFERENCES

[1] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, no. 4, pp. R2493–R2496, Oct. 1995.

[2] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996.

[3] A. Steane, "Multiple-particle interference and quantum error correction," *Proc. Roy. Soc. A, Math. Phys. Eng. Sci.*, vol. 452, no. 1954, pp. 2551–2577, Nov. 1996.

[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. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4892–4914, Nov. 2006.

[6] J. Li, X. Chen, X. Sun, Z. Li, and Y. Yang, "Quantum network coding for multi-unicast problem based on 2D and 3D cluster states," *Sci. China Inf. Sci.*, vol. 59, Apr. 2016, Art. no. 042301.

[7] J. Li, X. B. Chen, G. Xu, Y. X. Yang, and Z. P. Li, "Perfect quantum network coding independent of classical network solutions," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 115–118, Feb. 2015.

[8] G. Xu, X.-B. Chen, Z. Duo, Y.-X. Yang, and Z. Li, "A novel protocol for multiparty quantum key management," *Quantum Inf. Process.*, vol. 14, no. 8, pp. 2959–2980, Aug. 2015.

[9] G. Xu, X.-B. Chen, J. Li, C. Wang, Y.-X. Yang, and Z. Li, "Network coding for quantum cooperative multicast," *Quantum Inf. Process.*, vol. 14, no. 11, pp. 4297–4322, Nov. 2015.

[10] A. Thangaraj and S. W. McLaughlin, "Quantum codes from cyclic codes over GF(4^m)," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 1176–1178, Mar. 2001.

[11] G. G. L. Guardia, "Quantum codes derived from cyclic codes," *Int. J. Theor. Phys.*, vol. 56, no. 8, pp. 2479–2484, Aug. 2017.

[12] L. Xiaoyan, "Quantum cyclic and constacyclic codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 547–549, Mar. 2004.

[13] M. E. Koroglu, "New entanglement-assisted MDS quantum codes from constacyclic codes," *Quantum Inf. Process.*, vol. 18, no. 1, p. 44, Feb. 2019.

[14] K. Feng, S. Ling, and C. Xing, "Asymptotic bounds on quantum codes from algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 986–991, Mar. 2006.

[15] H. Chen, "Some good quantum error-correcting codes from algebraic-geometric codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 2059–2061, Jul. 2001.

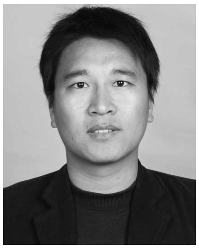
[16] C. Munuera, W. Tenório, and F. Torres, "Quantum error-correcting codes from algebraic geometry codes of castle type," *Quantum Inf. Process.*, vol. 15, no. 10, pp. 4071–4088, Oct. 2016.

[17] M. Hivadi, "On quantum SPC product codes," *Quantum Inf. Process.*, vol. 17, p. 324, Dec. 2018.

[18] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003, pp. 19–28.

[19] Y. Edel. *Some Good Quantum Twisted Codes*. Accessed: Jan. 12, 2019. [Online]. Available: https://www.mathi.uni-heidelberg.de/ yves/Matritzen/QTBCH/QTBCHIndex.html

[20] P. Gaborit. *Tables of Self-Dual Codes*. Accessed: Jan. 12, 2019. [Online]. Available: http://www.unilim.fr/pages_perso/philip- pe.gaborit/SD/SelfDualCodes.htm



JIAN GAO received the Ph.D. degree from the Chern Institute of Mathematics, Nankai University, in 2015. He is currently a Lecturer with the School of Mathematics and Statistics, Shandong University of Technology, and also with the Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University. His research interest includes coding theory and cryptography.

YONGKANG WANG received the B.E. degree from the Shandong University of Technology, in 2016, where he is currently pursuing the master's degree with the School of Mathematics and Statistics. He is also with the Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University. His research interest includes coding theory and cryptography.