Quantum QC-LDPC Codes with large girth

Farzane Amirzade, Daniel Panario *Senior Member, IEEE and*
Mohammad-Reza Sadeghi

Abstract

In this paper, we show that all quantum quasi-cyclic LDPC (QQC-LDPC) codes with column weight at least 3 have girth at most 6. We also present an efficient method to construct QQC-LDPC codes with column weight 2 and girth 12.

Index Terms

Quantum QC-LDPC codes, Tanner graph, girth.

I. Introduction

In 1996, Calderbank, Shor and Steane proved that good quantum error-correcting codes exist [1], [2]. These codes which are denoted by CSS codes are known as a method of storing and transmitting K bits of quantum information using $n > K$ quantum bits such that the transmitted quantum information can be recoverd if some subsets of n quantum bits contain arbitrary errors, which are bit errors, phase errors or a combination of them. These codes, as a special class of stabilizer codes [6] are designed by a pair of classical linear codes. In fact, an $[n, k_1 - k_2]$ CSS code is constructed from two classical linear codes $C_1 = [n, k_1]$ and $C_2 = [n, k_2]$, where $C_2 \subset C_1$ and the minimum distance of C_1, $d_{\min}(C_1)$, and the dual of C_2, $d_{\min}({C_2}^{\perp})$, are equal to d. Such $[n, k_1 - k_2]$ CSS code is capable of correcting $t = \frac{d-1}{2}$ bit errors and $t = \frac{d-1}{2}$ phase errors. If $C_2 = {C_1}^{\perp}$, then the quantum code is *dual-containing*.

Low-density parity-check (LDPC) codes are known to be capacity-achieving with a low decoding complexity. There are different types of LDPC codes such as quasi-cyclic (QC) LDPC codes, algebraic-based LDPC codes as well as LDPC codes based on combinatorial designs. Good properties of LDPC codes motivate researchers to construct CSS codes consisting of two LDPC codes C_1 and C_2, which we call QLDPC codes [3]. If H_1 and H_2 are, respectively, the parity-check matrices of C_1 and the dual of C_2, then the parity-check matrix of the QLDPC code is $\begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix}$. According to [5], Tanner graph of dual-containing QLDPC codes have inevitable 4-cycles which deteriorate the performance of these codes when using

iterative decoding algorithms. Thus, all the QLDPC codes proposed in the literature are non-dual-containing codes whose Tanner graphs are free of 4-cycles. For example, in [4], [5] and [6], respectively, QC-LDPC codes, block designs and quadratic residue sets are used to obtain QLDPC codes whose Tanner graphs have girth 6.

In this paper, we focus on QLDPC codes consisting of QC-LDPC codes which we denote by *QQC-LDPC codes*. We first prove that the Tanner graph of these codes has girth at most 6 if the column weight of their parity-check matrix is at least 3. Then, we present a necessary and sufficient condition to obtain QQC-LDPC codes with column weight 2 and girth 12.

II. Preliminaries

Let $B = [b_{ij}]$ be an $m \times n$ exponent matrix of a QC-LDPC code with a lifting degree N, where $b_{ij} \in \{0, 1, \ldots, N-1\}$ or $b_{ij} = (\infty)$. If integer numbers, b_{ij}s, in the exponent matrix are replaced by $N \times N$ circulant permutation matrices (CPMs), whose first row has 1 in the b_{ij}-th column and zero in other columns, and (∞) is replaced by an $N \times N$ zero matrix (ZM), then we obtain a parity-check matrix whose null space forms a single-edge QC-LDPC code [8]. The number of 1s in a column (a row) of the parity-check matrix is the *column weight* (the *row weight*). If the parity-check matrix has a constant column weight m and a constant row weight n, then it is an (m, n)-regular QC-LDPC code. If all elements of the exponent matrix are integers, then the obtained parity-check matrix results in a *fully-connected QC-LDPC code*. To check $2k$-cycles in the Tanner graph of a QC-LDPC code, the exponent matrix B and the following Fossorier's equation [8] are used. If

$$\sum_{i=0}^{k-1} (b_{m_i n_i} - b_{m_i n_{i+1}}) \equiv 0 \pmod{N}, \tag{1}$$

where $n_k = n_0$, $m_i \neq m_{i+1}$, $n_i \neq n_{i+1}$ and $b_{m_i n_i}$ is the (m_i, n_i)-th entry of B, then the Tanner graph of the parity-check matrix has cycles of length $2k$. The smallest length of a cycle in the Tanner graph is the *girth* of the Tanner graph which is denoted by g.

Theorem 1: [4] Let $C = [c_{ij}]$ and $D = [d_{ij}]$ be the $m \times n$ exponent matrices of QC-LDPC codes. A pair (C, D) is a pair of exponent matrices of a QQC-LDPC code if and only if for row indices $i, i' \in \{1, \ldots, m\}$ each element of the set $R_{ii'} = \{(c_{ij} - d_{i'j}) \mid 1 \leq j \leq n\}$ appears an even number of times, where subtractions in $R_{ii'}$ are mod N.

III. Quantum QC-LDPC codes with column weight $m \geq 3$

In this section, we prove that the Tanner graphs of two exponent matrices of a QQC-LDPC code with column weight at least 3 have girth at most 6.

Lemma 1: Let $C = [c_{ij}]$ and $D = [d_{ij}]$ be the $m \times n$ exponent matrices of QQC-LDPC codes of girth at least 6. If for two row indices $i \neq i' \in \{1, 2, \ldots, m\}$ the set $R_{ii'}$ contains two elements $c_{ij} - d_{ij}$ and $c_{ij'} - d_{ij'}$, where $j \neq j' \in \{1, 2, \ldots, n\}$ and $c_{ij} - d_{ij} \equiv c_{ij'} - d_{ij'} \pmod N$, then we have (I) $c_{ij} - d_{i'j} \not\equiv c_{ij'} - d_{i'j'} \pmod N$, (II) $c_{i'j} - d_{ij} \not\equiv c_{i'j'} - d_{ij'} \pmod N$.

Proof: We prove condition (I). The proof of condition (II) is similar. We suppose that $c_{ij} - d_{i'j} \equiv c_{ij'} - d_{i'j'} \pmod N$. Thus, we have $c_{ij} \equiv d_{i'j} + c_{ij'} - d_{i'j'} \pmod N$. In $c_{ij} - d_{ij} \equiv c_{ij'} - d_{ij'} \pmod N$ we replace c_{ij} by $d_{i'j} + c_{ij'} - d_{i'j'} \pmod N$ which yields the following equality $d_{i'j} + c_{ij'} - d_{i'j'} - d_{ij} \equiv c_{ij'} - d_{ij'} \pmod N$ or $d_{i'j} - d_{i'j'} - d_{ij} \equiv -d_{ij'} \pmod N$. Thus, we have the equation $(d_{ij} - d_{ij'}) + (d_{i'j'} - d_{i'j}) \equiv 0 \pmod N$ which proves the existence of 4-cycles in the Tanner graph of the exponent matrix D, which is a contradiction. ■

Because of the space limit the proofs of Theorems 2 and 5 are omitted, and we only sketch the proof of Theorem 3.

Theorem 2: Any QQC-LDPC code with 3×4 exponent matrices has girth 4.

Theorem 3: QQC-LDPC codes with column weight at least 3 have girth at most 6.

Proof (Sketch): Suppose $C = [c_{ij}]$ and $D = [d_{ij}]$ are exponent matrices of a QQC-LDPC code. According to Theorem 1, each element of $R_{ii'}$ appears an even number of times. Thus, without loss of generality, we suppose that in the set $R_{11} = \{(c_{1j} - d_{1j}) \mid 1 \leq j \leq n\}$ we have $c_{11} - d_{11} = c_{12} - d_{12}$. Then, according to Lemma 1 for the set R_{12}, there exists an integer $j \neq 2$ which results in $c_{11} - d_{21} = c_{1j} - d_{2j}$ and similarly for the set R_{13} there is $j' \neq j$ and $j' \neq 2$ which gives $c_{11} - d_{31} = c_{1j'} - d_{3j'}$. Continuing with this process, we can show that there are column indices k, k', where $c_{12} - d_{22} = c_{1k} - d_{2k}$ and $c_{12} - d_{32} = c_{1k'} - d_{3k'}$. Thus, we obtain expressions $d_{11} = c_{11} - c_{12} + d_{12}$, $d_{21} = c_{11} - c_{1j} + d_{2j}$, $d_{31} = c_{11} - c_{1j'} + d_{3j'}$, $d_{22} = c_{12} - c_{1k} + d_{2k}$ and $d_{32} = c_{12} - c_{1k'} + d_{3k'}$ that we can substitute in the first three rows of the exponent matrix D which we denote by D'

$$D' = \begin{bmatrix} \mathbf{c_{11} - c_{12} + d_{12}} & \mathbf{d_{12}} & \cdots & d_{1j} & \cdots & d_{1j'} & \cdots \\ c_{11} - c_{1j} + d_{2j} & \mathbf{c_{12} - c_{1k} + d_{2k}} & \cdots & d_{12j} & \cdots & \mathbf{d_{2j'}} & \cdots \\ \mathbf{c_{11} - c_{1j'} + d_{3j'}} & c_{12} - c_{1k'} + d_{3k'} & \cdots & d_{3j} & \cdots & \mathbf{d_{3j'}} & \cdots \end{bmatrix}.$$

We check Equation (1) for 6-cycles from the highlighted elements in the above matrix D'

$$(c_{11} - c_{12} + d_{12} - d_{12}) + (c_{12} - c_{1k} + d_{2k} - d_{2j'}) + (d_{3j'} - c_{11} + c_{1j'} - d_{3j'}) \equiv 0 \pmod N$$

which shows the existence of 6-cycles. ■

IV. Quantum regular QC-LDPC codes with girth 12

We provide a necessary and sufficient condition to construct QQC-LDPC codes with large girth. As shown in Theorem 3, any quantum QC-LDPC code with column weight at least 3 has girth at most 6. Thus, to have a QQC-LDPC code with large girth we should focus on exponent matrices with column weight 2. Since any (m, n)-regular fully-connected QC-LDPC code has $g \leq 12$ [8] and the existence of a 2×3 submatrix of an exponent matrix with integer entries proves the existence of a 12-cycle in the Tanner graph of the code [9], we aim for a fully-connected QQC-LDPC code with column weight 2 and girth at most 12.

In order to construct the exponent matrix of a $(2, n)$-regular QC-LDPC code with girth 12 we should make sure the nonexistence of 4-cycles and 8-cycles. Because for the removal of 6-cycles (10-cycles), Equation (1) is checked for each 3×3 submatrix ($k \times \ell$ submatrix where $3 \leq k, l \leq 5$) of the exponent matrix with column weight at least 3 whereas our desired matrix has column weight 2. To have QQC-LDPC codes with the highest girth we should check 4-cycles using Equation (1) and Lemma 1 as well as 8-cycles using Theorem 4.

Theorem 4: [10] Given a $2 \times n$ exponent matrix C of the QC-LDPC code $\mathcal{C}$, the Tanner graph is free of 8-cycles if and only if the following set is free of repeated elements

$$\{(c_{1j} - c_{2j}) - (c_{1j'} - c_{2j'}) \pmod N;\ j \neq j' \in \{1, 2, \ldots, n\}\}.$$

The idea to construct a QQC-LDPC code with girth 12 is to find two exponent matrices $C = [c_{ij}]$ and $D = [d_{ij}]$ satisfying the following conditions:

C1. for $i, i' \in \{1, 2\}$, each element of the set $R_{ii'} = \{c_{ij} - d_{i'j} \ | 1 \leq j \leq n\}$ appears an even number of times;

C2. both matrices C and D are the exponent matrices of girth-12 QC-LDPC codes;

C3. the entries of D are linear functions of the entries of C.

For n even, we suppose that we have the following exponent matrix

$$C = \begin{bmatrix} x_1 & \cdots & x_n \\ y_1 & \cdots & y_n \end{bmatrix}.$$

Then, we find all permutations π written as transpositions (cycles of length 2) from n objects $(1\ 2\ \ldots\ n)$. For example, one of these permutations is $(1\ \frac{n}{2}+1)\ (2\ \frac{n}{2}+2)\cdots(\frac{n}{2}\ n)$. The

number of permutations of order 2 from n objects is $\prod_{k=0}^{\frac{n}{2}-1}(n-(2k+1))$. Using any of these permutations of order 2 we can define the other exponent matrix D as follows,

$$D = \begin{bmatrix} -x_{\pi(1)} & \cdots & -x_{\pi(n)} \\ -y_{\pi(1)} & \cdots & -y_{\pi(n)} \end{bmatrix}.$$

Theorem 5: Let a be an integer number with $1-a$ coprime to N. Two matrices C and D assuming $y_i \equiv ax_i \pmod N$ result in a QQC-LDPC code with girth 12 if and only if (i) each element of the set $\{x_i + ax_{\pi(i)};\ 1 \leq i \leq n\}$ appears an even number of times, (ii) the set $\{(x_i - x_j) \mid i \neq j \in \{1, \ldots n\}\}$ is free of repeated elements, and each element of the set is nonzero. All computations in conditions (i) and (ii) are modulo N.

Example 1: An exponent matrix C with the first row [0 1 5 45 27 73 34 37], the coefficient $a = 7$ and lifting degree $N = 57$ has girth 12. Now considering permutation (1 2)(3 6)(4 7)(5 8) we obtain the exponent matrix D which satisfies Theorem 5.

V. Conclusion

We show that the Tanner graph of any QQC-LDPC code with column wight at least 3 has 6-cycles. Moreover, we provide a necessary and sufficient condition to construct $(2, n)$-regular QQC-LDPC codes with girth 12.

References

[1] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist", *Phys. Rev. A* vol. 54, pp. 1098–1105, 1996.

[2] A. M Steane, "Simple quantum error-correcting codes", *Phys. Rev. A* vol. 54, pp. 4741–4751, 1996.

[3] M. S Postol, "A proposed quantum low density parity check code", *arXiv:quant-ph/0108131*, 2001.

[4] M. Hagiwara and H. Imai, "Quantum quasi-cyclic LDPC codes", *IEEE Int. Symp. Inf. Theory*, pp. 806–810, 2007.

[5] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Construction of Quantum LDPC Codes From Classical Row-Circulant QC-LDPCs", *IEEE Commun. Letters*, vol. 20, no. 1, pp. 9–12, 2016.

[6] X. Xie, J. Yang and Q. T. Sun, "Design of Quantum LDPC Codes From Quadratic Residue Sets", *IEEE Trans. Commun.* vol. 66, no. 9, pp. 3721–3735, 2018.

[7] R. M. Tanner, "A recursive approach to low complexity codes", *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, 1981.

[8] M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices", *IEEE Trans. Inf. Theory*, vol. **50**, no. 8, pp. 1788–1793, 2004.

[9] H. Park, S. Hong, J. Seon and D. J. Shin, "Design of multiple-edge protographs for QC-LDPC codes avoiding short inevitable cycles", *IEEE Trans. Inf. Theory*, vol. **59**, no. 7, pp. 4598–4614, 2013.

[10] F. Amirzade and M.-R Sadeghi, "Lower bounds on the lifting degree of QC-LDPC codes by difference matrices", *IEEE Access*, vol. **6**, pp. 23688–23700, 2018.