Quantum QC-LDPC Codes with Large Girth

Daniel Panario
School of Mathematics and Statistics
Carleton University
daniel@math.carleton.ca

ALCOCRYPT – February 20-24, 2023

Joint work with F. Amirzade and M.-R. Sadeghi.

Outline

- Introduction to quantum codes, LDPC codes and QC-LDPC codes
- Quantum QC-LDPC codes
- Girth analysis of quantum QC-LDPC codes

Introduction

Calderbank, Shor and Steane (1996) introduce a class of quantum codes, now named CSS codes, that are obtained from a pair of classical linear codes. CSS codes allow storing and transmitting K qubits using $n > K$ qubits such that the transmitted qubit can be recovered if some subsets of n qubits contain arbitrary errors.

There are bit errors, phase errors or a combination of them.

An $[n, k_1 - k_2]$ CSS

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, and the dual of C_2, are equal, that is, $d = d_{\min}(C_1) = d_{\min}(C_2{}^{\perp})$.

Such $[n, k_1 - k_2]$ CSS code is capable of correcting $t = \lfloor \frac{d-1}{2} \rfloor$ bit errors and $t = \lfloor \frac{d-1}{2} \rfloor$ phase errors.

C_1 is used for bit errors and C_2 is used for phase errors.

The parity-check matrix of CSS codes

If H_1 and H_2 are the parity-check matrices of codes C_1 and $C_2^{\perp}$, respectively, then the parity-check matrix of the CSS code is

$$\begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix}.$$

Since $C_2 \subset C_1$ the parity-check matrices of C_1 and $C_2^{\perp}$ satisfy

$$H_1 \times H_2^T = 0.$$

Dual-containing

Given an $[n, k_1 - k_2]$ CSS code, if $C_2 = C_1{}^{\perp}$, then the CSS code is dual-containing.

In a dual-containing CSS code, the inner product of any pair of rows of the parity-check matrix H_1 is zero.

LDPC Codes

A low-density parity-check (LDPC) code is a linear code whose parity-check matrix is sparse.

Tanner graph

A Tanner graph is a bipartite graph with vertex sets formed by the set of variable nodes and the set of check nodes. The adjacency matrix of the Tanner graph is the parity-check matrix of the code.

If the degree of each variable node is m and the degree of each check node is n, then the code is a (m, n)-regular LDPC code. Otherwise, it is an irregular LDPC code.

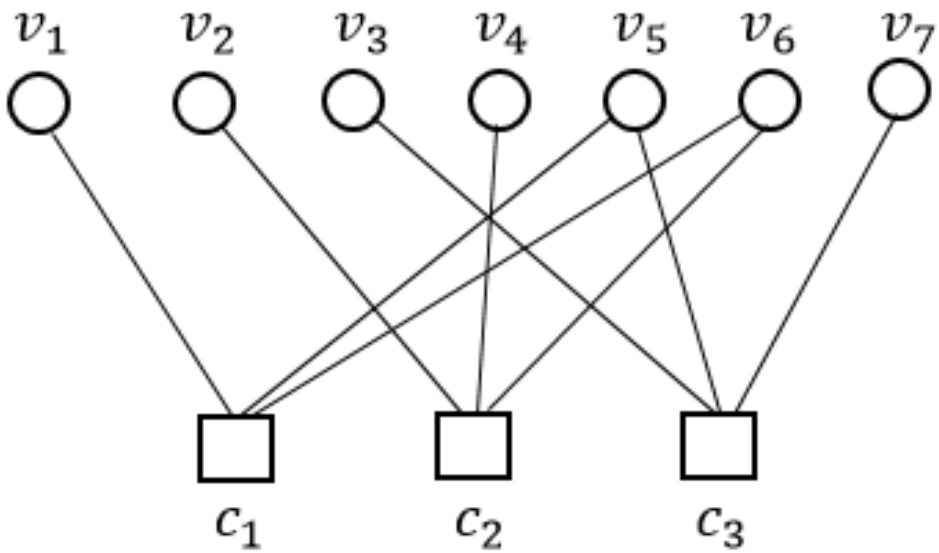
The length of the shortest cycles of the Tanner graph is the girth which has been known (experimentally) to influence the code performance.

Example

The following matrix is the parity-check matrix of a code

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

The Tanner graph of this code is



QC-LDPC codes

Let N, the lifting degree, be a positive integer. Consider the following exponent matrix $B = [b_{ij}]$, where $b_{ij} \in \{0, 1, \ldots, N-1\}$ or $b_{ij} = \emptyset$:

$$B = \begin{bmatrix} b_{00} & b_{01} & \cdots & b_{0(n-1)} \\ b_{10} & b_{11} & \cdots & b_{1(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ b_{(m-1)0} & b_{(m-1)1} & \cdots & b_{(m-1)(n-1)} \end{bmatrix}.$$

If b_{ij} is an integer, then it is replaced by an $N \times N$ circulant permutation matrix (CPM) $I^{b_{ij}}$ with 1 on the position b_{ij} of the top row and 0 on the other entries of the first row.
If $b_{ij} = \emptyset$, then it is replaced by an $N \times N$ zero matrix.

The resulting matrix is the parity-check matrix of a quasi-cyclic LDPC (QC-LDPC) code. If all entries of the exponent matrix are integer numbers, then we have a fully-connected QC-LDPC code.

Example (An exponent matrix with $N = 5$ and its parity-check matrix)

$$B = \begin{bmatrix} 0 & 0 & 0 & \emptyset \\ 0 & \emptyset & 3 & 4 \\ 0 & 3 & \emptyset & 1 \end{bmatrix},$$

$$H = \left[\begin{array}{c|c|c|c} 1.... & 1.... & 1.... & ..... \\ .1... & .1... & .1... & ..... \\ ..1.. & ..1.. & ..1.. & ..... \\ ...1. & ...1. & ...1. & ..... \\ ....1 & ....1 & ....1 & ..... \\ \hline 1.... & ..... & ...1. & ....1 \\ .1... & ..... & ....1 & 1.... \\ ..1.. & ..... & 1.... & .1... \\ ...1. & ..... & .1... & ..1.. \\ ....1 & ..... & ..1.. & ...1. \\ \hline 1.... & ...1. & ..... & .1... \\ .1... & ....1 & ..... & ..1.. \\ ..1.. & 1.... & ..... & ...1. \\ ...1. & .1... & ..... & ....1 \\ ....1 & ..1.. & ..... & 1.... \end{array}\right].$$

Fossorier's Lemma for checking $2k$-Cycles

A necessary and sufficient condition for the existence of $2k$-cycles in the Tanner graph of simple QC-LDPC codes given by Fossorier is

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

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.

Example

$$B = \begin{bmatrix} 0 & 0 & 0 & \emptyset \\ 0 & \emptyset & 3 & 4 \\ 0 & 3 & \emptyset & 1 \end{bmatrix}, \; N = 5$$

The Tanner graph has 6-cycles since

$$(b_{00} - b_{02}) + (b_{12} - b_{13}) + (b_{23} - b_{20}) = (0-0) + (3-4) + (1-0) \equiv 0 \pmod{5}.$$

Quantum LDPC codes

The nice properties of LDPC codes motivated Postol (2001) to construct Quantum LDPC (QLDPC) codes consisting of two LDPC codes C_1 and C_2, where $C_2 \subset C_1$.

Remark

Tanner graphs of dual-containing LDPC codes inevitably have 4-cycles which deteriorate the performance of these codes when using iterative decoding algorithms.

All QLDPC codes in the literature are non-dual-containing.

Quantum QC-LDPC Codes

Definition

A CSS code with QC-LDPC codes C_1 and C_2, where $C_2 \subset C_1$, is a quantum QC-LDPC code, denoted by QQC-LDPC code.

Theorem (Hagiwara and Imai 2007)

Let $C = [c_{ij}]$ and $D = [d_{ij}]$ be $m \times n$ exponent matrices of fully-connected QC-LDPC codes. A pair (C, D) is a pair of exponent matrices of a QQC-LDPC code if and only if for any row indices $i, i' \in \{1, \ldots, m\}$ each element of the set

$$R_{i,i'} = \{(c_{ij} - d_{i'j}) \mid 1 \leq j \leq n\}$$

appears an even number of times.

Our results

- We derive a necessary and sufficient condition for 4-cycles in the Tanner graph of a QQC-LDPC code. The occurrence of 4-cycles has to be avoided when constructing the exponent matrices.
- We prove that the Tanner graph of QQC-LDPC codes has girth at most 6 if the column weight is at least 3.
- We present a necessary and sufficient condition to obtain QQC-LDPC codes with column weight 2 and large girth.
- We provide a method to construct QQC-LDPC codes with girths 8 and 12.

Necessary and sufficient condition of 4-cycles

Lemma

Let $C = [c_{ij}]$ and $D = [d_{ij}]$ be $m \times n$ exponent matrices of QC-LDPC codes C_1 and C_2, respectively, and such that the Tanner graph of C_1 has girth at least 6. The codes C_1 and C_2 yield a QQC-LDPC code with girth at least 6 if and only if for any two equal elements $c_{ij} - d_{i'j}$ and $c_{ij'} - d_{i'j'}$ in the set $R_{i,i'}$ with two row indices $i \neq i' \in \{1, 2, \ldots, m\}$, where $j \neq j' \in \{1, 2, \ldots, n\}$, the sets $R_{i,i''}$ and $R_{i'',i'}$ satisfy the following

(I) $c_{ij} - d_{i''j} \not\equiv c_{ij'} - d_{i''j'} \pmod{N}$;

(II) $c_{i''j} - d_{i'j} \not\equiv c_{i''j'} - d_{i'j'} \pmod{N}$.

Theorem

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

Theorem

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

Proof. Consider a QQC-LDPC code with exponent matrices $C = [c_{ij}]$ and $D = [d_{ij}]$. We suppose in the set $R_{1,1} = \{(c_{1j} - d_{1j}) \mid 1 \leq j \leq n\}$ we have

$$c_{11} - d_{11} \equiv c_{12} - d_{12} \pmod{N}$$

from which we have $d_{11} \equiv c_{11} - c_{12} + d_{12} \pmod{N}$.

Due to the lemma and because of even multiplicity in the sets $R_{1,i'}$, for $i' \in \{1, 2, \ldots, m\}$, $i' \neq 1$, we have

- in the set $R_{1,2}$, there exist integers $j \neq 2$, $k \neq 2$, which results in

  $$c_{11} - d_{21} \equiv c_{1j} - d_{2j} \pmod{N} \text{ and } c_{12} - d_{22} \equiv c_{1k} - d_{2k} \pmod{N}$$

  from which we obtain $d_{22} \equiv c_{12} - c_{1k} + d_{2k} \pmod{N}$;

Cont.

- in the set $R_{1,3}$ there is $j' \neq 2$ which gives

$$c_{11} - d_{31} = c_{1j'} - d_{3j'}.$$

and therefore $d_{31} \equiv c_{11} - c_{1j'} + d_{3j'} \pmod{N}$.

We use the equivalences of d_{11}, d_{22} and d_{31} in the first three rows of the exponent matrix D

$$\begin{bmatrix} c_{11} - c_{12} + d_{12} & d_{12} & \cdots & d_{1j'} & \cdots \\ d_{21} & c_{12} - c_{1k} + d_{2k} & \cdots & d_{2j'} & \cdots \\ c_{11} - c_{1j'} + d_{3j'} & d_{32} & \cdots & d_{3j'} & \cdots \end{bmatrix}.$$

We check 6-cycles in the above submatrix of D and conclude that

$$\begin{aligned} & (D_{11} - D_{12}) + (D_{22} - D_{2j'}) + (D_{3j'} - D_{31}) \\ &= (c_{11} - c_{12} + d_{12} - d_{12}) + (c_{12} - c_{1k} + d_{2k} - d_{2j'}) + (d_{3j'} - (c_{11} - c_{1j'} + d_{3j'})) \\ &= -c_{1k} + d_{2k} - d_{2j'} + c_{1j'}. \end{aligned}$$

Cont.

Thus, if the Tanner graph of the exponent matrix D is free of 6-cycles, then

$$(D_{11} - D_{12}) + (D_{22} - D_{2j'}) + (D_{3j'} - D_{31}) \not\equiv 0 \pmod{N}.$$

This means that for each j' and k we have

$$(-c_{1k} + d_{2k}) + (c_{1j'} - d_{2j'}) \not\equiv 0 \pmod{N}.$$

Hence, for each j' and k we have $c_{1j'} - d_{2j'} \not\equiv c_{1k} - d_{2k}$ which proves that in the set $R_{1,2}$, there is an element like $c_{1k} - d_{2k}$ which appears once. This is in contradiction with the condition of even multiplicity in the sets $R_{i,i'}$. ■

QQC-LDPC codes with large girth

Since any QQC-LDPC code with column weight at least 3 has girth at most 6, to have a QQC-LDPC code with large girth we should focus on exponent matrices with column weight 2.

Theorem (Fossorier 2004)

For any (m, n)-regular QC-LDPC code with column weight at least 2 and row weight at least 3 we have girth $g \leq 12$.

To have a 6-cycle or a 10-cycle in the Tanner graph of a QC-LDPC code the exponent matrix must be of at least three rows (Fossorier).

Thus, an exponent matrix with column weight 2 is free of 6-cycles and 10-cycles.

A method to construct QQC-LDPC code with girth $g \geq 8$

We find $C = [c_{ij}]$ and $D = [d_{ij}]$ satisfying the following:

- Condition 1: for $i, i' \in \{1, 2\}$, each element of the set $R_{i,i'} = \{c_{ij} - d_{i'j} \,|1 \leq j \leq n\}$ appears an even number of times;
- Condition 2: C and D are the exponent matrices of QC-LDPC codes with the same girth;
- Condition 3: the entries of D are linear functions of the entries of C.

Two matrices C and D satisfying Conditions 2 and 3

Let C be the exponent matrix of a QC-LDPC code

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

where $x_i \neq x_j$ for $i \neq j$ and $y_i \equiv a x_i \pmod{N}$ for $2 \leq a \leq N-2$ integer. For n even, we find a permutation π written as transpositions (cycles of length 2) from n objects $(1\ 2\ \ldots\ n)$. For example, one of these permutations is $(1\ \frac{n}{2}+1)\ (2\ \frac{n}{2}+2)\cdots(\frac{n}{2}\ n)$.

Using any permutation π, we define

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

- C and D have the same girth (Condition 2).
- The entries of D are linear functions of the entries of C (Condition 3).

Constructing a QQC-LDPC code with girth at least 8

Theorem

Let a be an integer number with $2 \leq a \leq N-2$. Two matrices C and D as above, with $y_i \equiv ax_i \pmod{N}$, result in a QQC-LDPC code with girth at least 8 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, and

(ii) $x_i \neq x_j$ for $i \neq j \in \{1, \ldots, n\}$.

All computations in Conditions (i) and (ii) are modulo N.

Note: If two exponent matrices C and D satisfy condition (ii), then there are no cycles of length 4 since modulo N

$$(C_{1i} - C_{1j}) + (C_{2j} - C_{2i}) = (x_i - x_j) + (ax_j - ax_i) = (1-a)(x_i - x_j) \not\equiv 0.$$

Example

An exponent matrix C with the first row [0 1 5 45 27 43 34 37], the coefficient $a = 7$ and lifting degree $N = 57$ has girth 8

$$C = \begin{bmatrix} 0 & 1 & 5 & 45 & 27 & 43 & 34 & 37 \\ 0 & 7 & 35 & 30 & 18 & 16 & 10 & 31 \end{bmatrix}.$$

Now considering permutation (1 2)(3 6)(4 7)(5 8) we obtain

$$D = \begin{bmatrix} -1 & 0 & -43 & -34 & -37 & -5 & -45 & -27 \\ -7 & 0 & -16 & -10 & -31 & -35 & -30 & -18 \end{bmatrix}.$$

We should check $R_{i,i'}$. Since in these sets each element appears twice, C and D yield a QQC-LDPC code with column weight 2 and girth 8:

$$R_{1,1} = \{0+1, 1+0, 5+43, 45+34, 27+37, 43+5, 34+45, 37+27\}$$
$$R_{1,2} = \{7, 1, 21, 55, 1, 21, 7, 55\}$$
$$R_{2,1} = \{1, 7, 21, 7, 55, 21, 55, 1\}$$
$$R_{2,2} = \{7, 7, 51, 40, 49, 51, 40, 49\}$$

QQC-LDPC code with girth 12

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.

Theorem (Amirzade and Sadeghi 2018)

Given a $2 \times n$ exponent matrix C of the QC-LDPC code, the Tanner graph is free of 8-cycles if and only if the following set is free of repeated elements

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

Example

The following exponent matrix C with lifting degree $N = 31$ satisfies the condition of the theorem and hence yields a girth-12 QC-LDPC code

$$C = \begin{bmatrix} 0 & 1 & 3 & 10 & 14 & 26 \\ 0 & 5 & 15 & 19 & 8 & 6 \end{bmatrix}.$$

Constructing a QQC-LDPC code with girth 12

Theorem

Let a be an integer number with $\gcd(1-a, N) = 1$. Two matrices C and D with $y_i \equiv ax_i \pmod{N}$ 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

An exponent matrix C with the first row [0 1 3 10 14 26], the coefficient $a = 5$ and lifting degree $N = 31$ has girth 12

$$C = \begin{bmatrix} 0 & 1 & 3 & 10 & 14 & 26 \\ 0 & 5 & 15 & 19 & 8 & 6 \end{bmatrix}.$$

Now considering permutation (1 4)(2 5)(3 6) we obtain

$$D = \begin{bmatrix} -10 & -14 & -26 & 0 & -1 & -3 \\ -19 & -8 & -6 & 0 & -5 & -15 \end{bmatrix}.$$

We should check $R_{i,i'}$. Since in these sets each element appears twice, C and D yield a QQC-LDPC code with column weight 2 and girth 12

$$\begin{aligned} R_{1,1} &= \{0+10,\ 1+14,\ 3+26,\ 10+0,\ 14+1,\ 26+3\} \\ R_{1,2} &= \{0+19,\ 1+8,\ 3+6,\ 10+0,\ 14+5,\ 26+15\} \\ R_{2,1} &= \{0+10,\ 5+14,\ 15+26,\ 19+0,\ 8+1,\ 6+3\} \\ R_{2,2} &= \{0+19,\ 5+8,\ 15+6,\ 19+0,\ 8+5,\ 6+15\} \end{aligned}$$

Conclusion

- Any QQC-LDPC code with exponent matrices of size 3×4 has girth 4.
- Any QQC-LDPC code with column weight at least 3 has girth at most 6.
- In order to have QQC-LDPC codes with high girth we should focus on exponent matrices with two rows.
- A general method is given to obtain QQC-LDPC codes with girth 8 and 12 from $(2, n)$-regular QC-LDPC codes.

Future work

- We plan to use the proposed general method to provide more numerical results for QQC-LDPC codes girths 8 and 12.
- We plan to consider graphical structures such as trapping sets in the Tanner graphs of QQC-LDPC codes given by Hagiwara and Imai.

Conclusion

- Any QQC-LDPC code with exponent matrices of size 3×4 has girth 4.
- Any QQC-LDPC code with column weight at least 3 has girth at most 6.
- In order to have QQC-LDPC codes with high girth we should focus on exponent matrices with two rows.
- A general method is given to obtain QQC-LDPC codes with girth 8 and 12 from $(2, n)$-regular QC-LDPC codes.

Future work

- We plan to use the proposed general method to provide more numerical results for QQC-LDPC codes girths 8 and 12.
- We plan to consider graphical structures such as trapping sets in the Tanner graphs of QQC-LDPC codes given by Hagiwara and Imai.

Thank you very much for your attention!


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


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


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


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


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.


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.