Applications of Graph Theory and Homological Algebra to Quantum LDPC Codes

Zoe Himwich

April, 2022

Contents

1 Introduction to the Problem

When communicating information over possibly unreliable communication channels, the parties on either end can use strategies to ensure that the message is relayed accurately. Sometimes this means including redundant information which allows the receiver to check the accuracy of the message and correct errors. An error correcting code is an algorithm which determines how the sender adds redundancy to increase the likelihood that the receiver is able to deduce the correct message. There are several genres of error correcting codes, but this article will focus on low-density parity check (LDPC) codes. We start by making a few preliminary definitions and setting up our notation.

For the duration of this article, we will use the following notation:

- We assume that the classical sender is transmitting a message, r, comprised of n bits, $r \in \{0,1\}^n$. Likewise, a quantum sender will transmit a message $|\psi\rangle \in \{|0\rangle, |1\rangle\}^{\otimes n}$.
- We assume that the transmission channel introduces errors independently at random anywhere in the message and that there is an equal probability, which we will denote by p, of changing $0 \to 1$ and $1 \to 0$.
- We will use length m for codewords.

1.1 Classical and Quantum LDPC Codes

There are several important definitions we must make before we can define an LDPC code (classical or quantum). This section is a quick review of those definitions.

Definition 1.1. *A **block code** for messages of n bits with block length m and distance d, (m, n, d), is a genre of error correcting code. The block code encodes the original message into a "codeword" called the block. In other words, a block code is an injective map*

$$C : \{0,1\}^n \to \{0,1\}^m,$$

where m is the block length of the code and $r = n/m$ is the rate. The distance d is the minimum Hamming distance between blocks for different messages,

$$d = \min_{m,m'} d(C(m), C(m')).$$

Remark 1.2. *The notation $(m, n, d)_q$ is often seen when working over a finite field of size q rather than only over bits. This article suppresses the q.*

Definition 1.3. *A **linear block code** is a block code which has the property that for any collection of messages $\{r_i\}_{i\in I}$, then any linear combination of elements in the collection $\{C(r_i)\}_{i\in I}$ will also be in the image of C. Typically we denote a linear code of length m by $\mathbb{F}_2^m$.*

Definition 1.4. *The **parity check matrix** H of a linear block code C is a matrix such that $c \in \{0,1\}^m$ is in the image of C if and only if $Hc = 0$. The parity matrix will have dimension $m \times k$ and there will be constraints that there are exactly a certain number, l, of 1's in each row and exactly a certain number, j, of 1's in each column, with the added constraint that $k > j$.*

The equations in the entries of c which arise through the condition $Hc = 0$ are called the parity equations of the code.

Finally, with all of these definitions in place, we are ready to introduce the notion of a low-density parity check code, which will be one of the two main focuses of this article.

Definition 1.5. *A low-density parity check, or LDPC, code is a linear error-correcting code specified by a parity-check matrix which contains mostly 0's and some 1's with low density.*

There are also quantum versions of each of the definitions above. We will quickly walk through each of these, for clarity.

Definition 1.6. *A quantum block code for messages of n qubits with block length m and distance d, (t, n, d), is a block code on qubits. Formally, a quantum block code is an injective map*

$$\mathcal{C} : (S^1)^{\otimes n} \to (S^1)^{\otimes m},$$

where, as before, m is the block length of the code and $r = n/m$ is the rate. The distance d is the minimum Hamming distance between blocks for different messages,

$$d = \min_{m,m'} d(\mathcal{C}(r), \mathcal{C}(r')).$$

Definition 1.7. *A quantum LDPC code is a linear quantum block code specified by a collection of local projection operators $\{\Pi_i\}_{i \in I}$. The local projectors act on a bounded (by a constant) number of qubits in the full state, and each qubit admits actions by a bounded (by a constant) number of local projectors. A state $|\psi\rangle \in (S^1)^{\otimes m}$ is a codeword when $\Pi_i|\psi\rangle = |\psi\rangle$ for each of the local projectors.*

Equivalently, we can say that the codewords are groundstates of a sparse local Hamiltonian, $H = -\sum_j \Pi_j$.

An important point to note is that a quantum LDPC code can also be equivalently defined as a pair of classical LDPC codes which satisfy an orthogonality condition $H_1 H_2^* = 0$ on their parity check matrices H_1 and H_2.

1.2 Classical and Quantum Locally Testable Codes

Intuitively, we think about locally testable codes as error correcting codes in which it is possible to determine whether a string is a word in the code by looking at a small number of bits.

Definition 1.8. *[5] A classical code*

$$C : \{0,1\}^n \to \{0,1\}^l$$

is (w, s)-locally testable if it has a parity-check matrix $H \in \mathbb{F}_q^{m \times l}$ with rows of weight at most w such that for all $x \in \mathbb{F}_q^l$ we have

$$\frac{1}{m}|Hx| \geq \frac{s}{l} d(x, \mathcal{C})$$

Where $d(x, \mathcal{C}) := \min_{x \in \mathcal{C}} d(x, c)$ is the minimum of the Hamming distances.

The expression $\frac{1}{m}|Hx|$ can be interpreted as the probability of rejection, meaning the probability that the LTC determines that x is not a word in the code. The parameter w is called locality, and we can think of it as a parameter which governs the sparsity of H. The parameter s is called soundness, and it governs the linear rate of the probability of rejection relative to distance. The equation above tells us that a code is locally testable when it has a parity check matrix so that the probability of rejection grows linearly in $\frac{1}{m} d(x, \mathcal{C})$.

One of the main motivations for studying classical and quantum LDPC codes is for the purpose of creating locally testable codes. There are several practical and theoretical motivations for studying locally testable codes. In practice, they are a computational tool that provide an extremely fast probabilistic estimate of whether there are errors in a codeword. Quantum locally testable codes are the result of an effort to establish similar tools in the quantum code setting.

Definition 1.9. *[1] If $\mathcal{C}$ is a quantum code, defined as the groundspace of $H = \sum_i \Pi_i$ with $\{\Pi_i\}$ a collection of local projections, then $\mathcal{C}$ is quantum locally testable if, for all $\delta > 0$ and all $|\psi\rangle$,*

$$d(|\psi\rangle, \mathcal{C}) \geq \delta n \implies \frac{1}{m} \langle \psi | H | \psi \rangle \geq R(\delta)$$

Here $R(\delta)$ is a function $[0, 1] \to [0, 1]$ which is fixed for a fixed code and $d(|\psi\rangle, \mathcal{C}) = \min_{|\phi\rangle} d(|\psi\rangle, |\phi\rangle)$ is a quantum version of normalized minimum distance.

1.3 Open Problems and Recent Developments

The paper by Panteleev and Kalachev [5] focuses on the following longstanding problem about locally testable codes:

Question 1.10 (c^3-conjecture/qLTC conjecture)**.** *Do there exist families of locally testable codes of asymptotically constant locality, rate, and normalized minimum distance?*

With this question, we really ask whether there exist families of codes which are *asymptotically good.*

Definition 1.11. *A family of codes $\boldsymbol{C} = \{C_m\}$ of type $(m, n, d)_q$ is asymptotically good when $r(\boldsymbol{C}) = \lim_{m \to \infty}(n/m)$ and $\delta(\boldsymbol{C}) = \lim_{m \to \infty} d/m$ are both bounded below by constants strictly greater than 0.*

Their work establishes that there do exist such codes in the classical setting.

Theorem 1.1. *[5] For every $R \in (0, 1/2)$ it is possible to find universal constants s and w such that there exists a family of (w, s)-locally testable classical LDPC codes with the parameters $(m, n \geq Rm, d = \Theta(n))_q$ as $m \to \infty$*

While they do not solve the quantum version, they do provide a partial result, about qLDPC codes instead of qLTC codes:

Theorem 1.2. *[5] For every $R \in (0, 1/2)$ there exists an explicit family of qLDPC codes with parameters $(m, n \geq Rm, d = \Theta(m))_q$ as $m \to \infty$.*

The discussion in this paper will be an exposition of their results and methods. Their paper was interesting because of the importance of the questions they answered, but also because the methods were novel for the field. Hopefully resources which provide clear and thorough exposition of the methods will help future researchers adapt these methods for their own problems.

2 Methods and Results

2.1 Overview

This section is a brief summary of the approach of Panteleev and Kalachev's argument. The main points are here, and the appropriate sections in the original paper are linked at each step.

1. **Constructing the families:**
   (a) LDPC codes can each be represented in a natural way as a two-term chain complex, with the parity check matrix as the boundary map:

$$A_2 \xrightarrow{\partial_A} A_1$$

$$B_2 \xrightarrow{\partial_B} B_1$$

   Say $\partial_A := H_A$, $\partial_B := H_B$ for parity check matrices H_A and H_B

   (b) Use a tensor product construction to make a new chain (three-term) chain complex:

$$A_2 \otimes B_2 \xrightarrow{\partial_2} A_1 \otimes B_2 \oplus A_2 \otimes B_1 \xrightarrow{\partial_1} A_1 \otimes B_1$$

   (c) Define the classical code as $ker(\partial_2)$, and the quantum code by the kernel of ∂_1 and ∂_2^*. This guarantees our quantum code will satisfy the orthogonality condition because $\partial_2 \circ \partial_1 = 0$.

   (d) The problem reduces to showing that H_A and H_B exist which allow our codes to meet the properties in each of the theorems

2. **Proof of the first theorem:**

(a) We consider an infinite family of Ramanujan graphs $X^{w-1,t}$ and show that every one of these graphs is edge-expanding with a fixed set of parameters $(n_0(t)/\sqrt{w}, 8\sqrt{w})$ for $n_0(t) = t(t^2-1) = |V(X^{w-1,t})|$.

(b) Construct two codes with respect to this Ramanujan graph and two, for now arbitrary, parity check matrices h and h'

(c) Represent these codes as chain complexes and take the tensor product chain complex to be $\mathcal{C}$. $\mathcal{C}$ is a three-term chain complex

$$\mathcal{C}_2 \xrightarrow{\partial_2} \mathcal{C}_1 \xrightarrow{\partial_1} \mathcal{C}_0$$

Our classical code is $ker(\partial_2) = Z_2(\mathcal{C})$.

(d) Show that there exist h and h' such that

$$d^{(1)}_{LM}(\mathcal{C}) \geq n_0(t)/2w\sqrt{w}$$

where c is *locally minimal* when $|c + \partial a x| \geq |c|$ for $x \in \mathcal{C}_{i+1}$ and a some coefficient

$$d^{(i)}_{LM} = \min\{|c||c \in Z_i(\mathcal{C}) - \{0\}, \text{c locally minimal}\}$$

(e) Show that the product chain complex satisfies the condition $d(H_i(\mathcal{C})) \geq d^i_{LM}(\mathcal{C})$ and then use the following homological algebra lemma to conclude that

$$|\partial c| \geq \min(d^{(1)}_{LM}(\mathcal{C}), |c + Z_2(\mathcal{C})|)$$

Lemma 2.1. *Let $\mathcal{C}$ be a chain complex over a local system then for every $i \in \mathbb{Z}$,*

$$d(H_i(\mathcal{C})) \geq d^i_{LM}(\mathcal{C})$$

then for every chain $c \in \mathcal{C}_{i+1}$ such that $|\partial c| < d^i_{LM}(\mathcal{C})$ we have

$$|\partial c| \geq d(c, Z_{i+1}(\mathcal{C})).$$

(f) Finally, show that the above implies that

$$\frac{1}{m}|\partial c| \geq \frac{w^{-7/2}}{2n}|c + Z_2(\mathcal{C})|$$

From this bound, we can show that the code is $(2w, \frac{1}{2}w^{-7/2})$-testable

(g) We show that the minimal distance of $Z_2(\mathcal{C})$ at least the minimal distance of one of our codes, which is an expander

(h) We show that since the code is an expander, and therefore we can fix a sufficiently large constant w such that $d(ker(h)) > \lambda_2(X^{w-1,t})$ and therefore the minimal distance of the associated code is $\Theta(n)$.

3. **Proof of the Second Theorem:**

   (a) Again construct an infinite family of graphs $X^{w-1,t}$ which are $(n_0(t)/\sqrt{w}, 8\sqrt{w})$-edge-expanding, with $n_0(t) = t(t^2-1) = |V(X^{w-1,t})|$.

   (b) As before, construct two codes associated to each Ramanujan graph, with parity check matrices h and h'. Take their tensor product chain complex.

   (c) Show that there exist h and h' such that

   $$d^{(1)}_{LM}(\mathcal{C}) \geq n_0(t)/2w\sqrt{w} \qquad\qquad d^{(1)}_{LM}(\mathcal{C}^*) \geq n_0(t)/2w\sqrt{w}$$

   Where $\mathcal{C}^*$ is the dual chain complex

   (d) We consider the quantum code given by the pair of parity check matrices ∂_1 and ∂_2^*.

   (e) By defining $n = dim\mathcal{C}_1$, we show that

   $$d(H_1(\mathcal{C})) \geq d^{(1)}_{LM}(\mathcal{C}) > \frac{n}{2w^{7/2}}$$

   and

   $$d(H_1(\mathcal{C}^*)) \geq d^{(1)}_{LM}(\mathcal{C}^*) > \frac{n}{2w^{7/2}}$$

   and therefore $d(\mathcal{Q}) \geq \frac{n}{2w^{7/2}}$ for our quantum code $\mathcal{Q}$.

   (f) For a suitable choice of R, we show that

   $$dim(\mathcal{C}_0) < n(1-R)/2 \qquad\qquad dim(\mathcal{C}_2) < n(1-R)/2$$

   and therefore $dim(H_1(\mathcal{C})) \geq nR$.

In the sections below, some of the key conceptual steps get a longer explanation.

2.2 Product Chain Complex Construction

A problem in constructing quantum LDPC codes from classical LDPC codes has been dealing with the orthogonality condition. Phrasing the problem in terms of chain complexes provides a natural way of understanding this condition.

We can phrase a classical code with parity-check H_1 as a 2-term chain complex by setting the boundary map $\partial_1 = H_1$. The parity check matrix can be considered a map from strings in the block where the message is encoded $\mathbb{F}_q^n$ to the space of checks, which has some dimension m_1, $\mathbb{F}_q^{m_1}$.

$$\mathbb{F}_q^n \xrightarrow{\partial_1} \mathbb{F}_q^{m_1}$$

By adding another term, we can encode another set of checks which correspond to another parity check matrix

$$\mathbb{F}_q^{m_2} \xrightarrow{\partial_2} \mathbb{F}_q^n \xrightarrow{\partial_1} \mathbb{F}_q^{m_1}$$

In this case $\partial_2^* = H_2$ for a second parity check matrix H_2. In that case, the fact that this sequence is exact implies that $H_1 H_2^* x = 0$.

Definition 2.2. *We consider two two-term chain complexes $\mathcal{A}$ and $\mathcal{B}$ with boundary maps ∂_A and ∂_B, respectively. We assume that $\mathcal{A}$ is a right, free R-module and $\mathcal{B}$ is a left, free R-module. The lifted product of $\mathcal{A}$ and $\mathcal{B}$ over R is the tensor product chain complex, defined by taking the tensor product over R.*

To clarify the notation a bit, we provide a bit more discussion of this tensor product construction.

Definition 2.3. *For a ring R, a right R-module A and a left R-module B, the tensor product $A \otimes_R B$ (read as "the tensor product over R") is an abelian group which associates to elements $a \in A$, $b \in B$ an element $a \otimes b \in A \otimes_R B$ which satisfies the relations*

- $a \otimes (b + b') = a \otimes b + a \otimes b'$
- $(a + a') \otimes b = a \otimes b + a' \otimes b$
- $(ar) \otimes b = a \otimes (rb)$

Here r is an element of R.

Similarly, we formally define the tensor product chain complex.

Definition 2.4. *For two two-term chain complexes $\mathcal{A}$ and $\mathcal{B}$ as above, $\mathcal{A} \otimes_R \mathcal{B}$ is the three-term chain complex*

$$A_1 \otimes_R B_1 \xrightarrow{\partial_2} A_1 \otimes_R B_2 \oplus A_2 \otimes_R B_1 \xrightarrow{\partial_1} B_1 \otimes_R B_2.$$

Where A_i, B_i are, respectively, the ith terms of $\mathcal{A}$ and $\mathcal{B}$. The boundary maps are given by

$$\partial_2 = \begin{bmatrix} -\mathbf{1} \otimes \partial_B \\ \partial_A \otimes \mathbf{1} \end{bmatrix}$$

and

$$\partial_1 = \begin{bmatrix} \mathbf{1} \otimes \partial_B, \partial_A \otimes \mathbf{1} \end{bmatrix}$$

such that $\partial_2 \circ \partial_1 = 0$.

We can also define this notion with respect to a group G. In order to produce this construction, we require the classical linear codes represented by our two chain complexes are G-invariant. We will not discuss this extensively, but curious readers can look at [6] for the full condition. A lifted product is a G-lifted product when $R = \mathbb{F}_q G$ a group algebra over G.

Definition 2.5. *The group algebra $\mathbb{F}_q G$ is an algebra on the set of all linear combinations of elements of G with coefficients in $\mathbb{F}_q$. It is a group ring in the specialized case where multiplication is abelian. There is a multiplication and addition on this underlying set, which the reader can find described at*

A natural question, faced with this construction, could be the following:

Question 2.6. *What motivated the G-lifted product construction?*

One basic point is that the G-lifted product construction allows us to define a tensor product construction for two chain complexes. Since we need a two term chain complex to define a quantum code, and we want to define the chain complex in terms of two classical codes, this is an important step towards using the homological algebra construction to show anything about quantum codes. However, up to this point, the fact that G is a group has not been necessary at all. This component of the construction is a necessary when we begin to construct a family of codes of varying sizes. The manner which this paper takes to construct families of acceptable codes is to take *lifts* of a smaller code (see the next section). This construction needs extra structure to define the new parity checks of the larger code, and that structure comes from a group G. With the addition of the group G to the construction, we need the G-lifted product construction to produce a valid chain complex at each level.

2.3 Expander graphs, lifts, shifts

Up to this point, we have not formally defined the Tanner graph of an LDPC code.

Definition 2.7. *A Tanner graph associated to an LDPC code with parity check matrix H is a pair of collections of vertices, $\{v_i\}_{i=1}^n$ and $\{c_j\}_{j=1}^m$ which correspond respectively to the columns and rows of H, or, in other words, the codewords and the checks. There is an edge between v_i and c_j whenever the h_{ij} entry in H is 1. There are no edges between v_i's or c_j's.*

A Tanner graph can be used equivalently in exchange for the parity check matrix H to specify the LDPC code. We can also use it to construct new LDPC codes by expanding it by a certain factor. This principle arises from a much studied general graph-theoretic construction called graph expansion.

Definition 2.8. *Given a graph $\Gamma = (V, E)$, we denote by n the size of the vertex set V, and label the vertices $1, ..., n$. We write the adjacency matrix of G as $A(\Gamma) = \{a_{ij}\}_{i,j=1}^n$ where $a_{ij} = 1$ if $(v_i, v_j) \in E$ and $a_{ij} = 0$ otherwise. $A(\Gamma)$ has real eignevalues which we label as $\lambda_1 \geq \ldots \geq \lambda_n$. We refer to an n-vertex d-regular graph with parameter λ as an (n, d, λ)-expander graph when $\max_{i \neq 1} |\lambda_i| \leq \lambda$.*

We call Γ an *expander graph* because it is high connected. When $\lambda_2 \leq 2\sqrt{d-1} + \epsilon$ we say the graph is Ramanujan. These graphs will be crucial to the construction in the proof. They are widely used in graph theory because of the special property that their spectral gap is extremely large. In fact, Ramanujan graphs are also very good expanders, because the Alon-Boppana bound [4] tells us that for all $d, \epsilon > 0$ there exists n such that all d regular graphs on n vertices have $\lambda(G) = \max_{i \neq 1} |\lambda_i| > 2\sqrt{d-1} - \epsilon$. The following collection of graphs will be important to the argument.

Example 2.9. *(Note, this is slightly different from Panteleev and Kalachev's notation — they use $X^{p,q}$ for the non-bipartite version of this construction and $\overline{X}^{p,q}$ for the bipartite version)*

We construct a family of Ramanujan graphs $X^{p,q}$ as follows: Here p and q are primes with $q > 2\sqrt{p}$ and both primes congruent to 1 mod 4, and with $p^{(q-1)/2}$ congruent to 1 mod q. For more detail on where these constraints come from, see [3]. $X^{p,q}$ will be the $(p+1)$-regular and bipartite graph with $n = 2|G|$ vertices from a fixed graph G such that $|G| = q(q^2-1)/2$ (for example, $G = PSL(\mathbb{F}_q^2)$). Specifically we construct this graph as the double cover of the Cayley graph of G. This graph is constructed in more detail in [3]. In particular, they show that $\lambda = \min_{i \neq 1} |\lambda_i| \leq 2\sqrt{p}$ and $\lambda_2 \leq 2\sqrt{p}$. Furthermore, this graph admits a free action of G.

We can also define a lift of a graph.

Definition 2.10. *An l-lift or an l-cover of a base graph Γ is a new graph Γ' obtained by replacing each vertex v in the original graph by l copies of that vertex $v_1, \ldots, v_l$ and each edge (v, v') between that vertex v and another vertex v' by l copies of that edge $(v_i, v'_{\pi(i)})$ where $v'_{\pi(i)}$ is a corresponding copy of v' under a permutation of the indices. This permutation will be specified by some element in G, such that $v'_i \cdot g = v'_{\pi(i)}$ and there may be a different permutation associated to each i. We assume that G is abelian for convenience.*

Definition 2.11. *When the group G in an l-lift is a cyclic group, we refer to the lift as a shift l-lift.*

This concept was used earlier on to show the existence of a family of qLDPC codes with almost linear distance [6]. There is a similar construction called the *balanced product* which was used to obtain qLDPC codes with very large distances [2].

References

[1] Dorit Aharonov and Lior Eldar. "Quantum locally testable codes". In: *SIAM Journal on Computing* 44.5 (2015), pp. 1230–1262.

[2] Nikolas P. Breuckmann and Jens N. Eberhardt. "Balanced Product Quantum Codes". In: *IEEE Transactions on Information Theory* 67.10 (Oct. 2021), pp. 6653–6674. DOI: 10.1109/tit.2021.3097347. URL: https://doi.org/10.1109%2Ftit.2021.3097347.

[3] Alexander Lubotzky, R. Phillips, and P. Sarnak. "Ramanujan Graphs". In: *Combinatorica* 8 (Sept. 1988), pp. 261–277. DOI: 10.1007/BF02126799.

[4] A. Nilli. "On the second eigenvalue of a graph". In: *Discrete Mathematics* 91.2 (1991), pp. 207–210. ISSN: 0012-365X. DOI: https://doi.org/10.1016/0012-365X(91)90112-F. URL: https://www.sciencedirect.com/science/article/pii/0012365X9190112F.

[5] Pavel Panteleev and Gleb Kalachev. *Asymptotically Good Quantum and Locally Testable Classical LDPC Codes*. 2021. DOI: 10.48550/ARXIV.2111.03654. URL: https://arxiv.org/abs/2111.03654.

[6] Pavel Panteleev and Gleb Kalachev. "Quantum LDPC Codes With Almost Linear Minimum Distance". In: *IEEE Transactions on Information Theory* 68.1 (Jan. 2022), pp. 213–229. DOI: 10.1109/tit.2021.3119384. URL: https://doi.org/10.1109%2Ftit.2021.3119384.