Good Quantum LDPC Codes with Linear Time Decoders*

Irit Dinur
The Weizmann Institute of Science
Rehovot, Israel
irit.dinur@weizmann.ac.il

Min-Hsiu Hsieh
Hon Hai Research Institute
Taipei, Taiwan
min-hsiu.hsieh@foxconn.com

Ting-Chun Lin
University of California San Diego
La Jolla, CA, USA
Hon Hai Research Institute
Taipei, Taiwan
til022@ucsd.edu

Thomas Vidick
The Weizmann Institute of Science
Rehovot, Israel
California Institute of Technology
Pasadena, CA, USA
thomas.vidick@weizmann.ac.il

ABSTRACT

We construct a new explicit family of good quantum low-density parity-check codes which additionally have linear time decoders. Our codes are based on a three-term chain $(\mathbb{F}_2^{m\times m})^V \xrightarrow{\delta^0} (\mathbb{F}_2^m)^E \xrightarrow{\delta^1} \mathbb{F}_2^F$ where V (X-checks) are the vertices, E (qubits) are the edges, and F (Z-checks) are the squares of a left-right Cayley complex, and where the maps are defined based on a pair of constant-size random codes $C_A, C_B : \mathbb{F}_2^m \to \mathbb{F}_2^\Delta$ where Δ is the regularity of the underlying Cayley graphs.

One of the main ingredients in the analysis is a proof of an essentially-optimal robustness property for the tensor product of two random codes.

CCS CONCEPTS

• **Theory of computation** → **Error-correcting codes**; Quantum complexity theory.

KEYWORDS

error-correcting codes, quantum low-density parity-check codes, locally testable codes

ACM Reference Format:
Irit Dinur, Min-Hsiu Hsieh, Ting-Chun Lin, and Thomas Vidick. 2023. Good Quantum LDPC Codes with Linear Time Decoders. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC '23), June 20–23, 2023, Orlando, FL, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3564246.3585101

1 INTRODUCTION

Quantum error correction is an essential ingredient to achieve fault-tolerant quantum computation. An important class of quantum codes relevant to fault-tolerance are quantum low-density parity-check (qLDPC) codes [26]. These are codes whose checks act only on a constant number of qubits, and further each qubit is acted on only by a constant number of checks. This low connectivity is desirable because it reduces the chance for errors to spread when checks are being measured for error correction.

Several families of qLDPC codes have been studied starting from Kitaev's toric code [39], with increasing rate and distance [10, 23, 24, 30, 38, 51, 55]. Recently Panteleev and Kalachev [50] gave the first construction of good qLDPC codes, i.e. qLDPC codes with constant rate and constant relative distance. A subsequent variation on their construction was given in [44]. The construction in [50] falls into the class of balanced product codes introduced in [10].

A natural question left open by the recent constructions of good qLDPC codes is the existence of efficient decoders for them. In this work, we give a new construction of qLDPC, which borrows many of the ingredients from [50] as well as ideas from the recent classical locally testable codes by [16], and show that our codes have linear time decoders. Our codes are balanced product codes, but (informally) place the qubits and checks on different cells of the underlying complex.

Theorem 1.1. *For every $r \in (0, 1/2)$, there exist constants $\delta > 0$, $w \in \mathbb{N}$ and an explicit infinite family of quantum LDPC codes with maximum weight w, rate r, and relative distance δ. Furthermore these codes are equipped with a linear time decoder that decodes up to linear distance.*

After the completion of this work, two independent papers obtained a similar result on qLDPC codes with efficient decoders [28, 42]. We first give an overview of our construction and proof techniques, compare our result with the related ones, and finally discuss further directions.

1.1 Overview of the Construction and Analysis

Our codes are based on a three-term chain complex

$$(\mathbb{F}_2^{m\times m})^V \xrightarrow{\delta^0} (\mathbb{F}_2^m)^E \xrightarrow{\delta^1} \mathbb{F}_2^F . \tag{1}$$

In contrast to other recent constructions of qLDPC this chain complex is ordered "geometrically" by dimension, so that V are the vertices, E are the edges, and F are the faces (squares) of a left-right Cayley complex. Informally, this complex has vertices labeled by

*The full version is available at [18]

STOC '23, June 20–23, 2023, Orlando, FL, USA

ACM ISBN 978-1-4503-9913-5/23/06.
https://doi.org/10.1145/3564246.3585101

elements g of a finite group G, edges labeled by two sets of generators A, B as (g, ag) and (g, gb) for $g \in G$, $a \in A$ and $b \in B$, and squares (g, ag, gb, agb) labeled by pairs $(a, b) \in A \times B$. The maps δ^0, δ^1 in (1) are defined via a pair of base codes $C_A, C_B : \mathbb{F}_2^m \to \mathbb{F}_2^\Delta$ where $\Delta = |A| = |B|$. [1] An advantage of the geometric ordering is that it may facilitate extending the chain to having more than three terms by going to higher dimensional geometric complexes. A drawback is that this kind of chain is asymmetric and therefore separate arguments are required for the analysis of the chain and co-chain (namely, X-distance and Z-distance).

Let us give an informal description of the chain map. Given a 0-chain $c^0 \in (\mathbb{F}_2^{m\times m})^V$, such that $c^0(v)$ is an $m \times m$ bit matrix for each $v \in V$, let us compute $\delta^0(c^0)$ assuming that c^0 is supported on a single vertex v (and this is extended linearly). We first apply the encoding C_A to each row of $c^0(v)$ separately to get a rectangular $m \times \Delta$ matrix, whose columns are now distributed among the A-edges neighboring v. Namely, each neighboring A-edge gets a single column from this matrix. Next, we apply the code C_B to each column of $c^0(v)$ separately to get a rectangular $\Delta \times m$ matrix whose rows we distribute among the B-edges neighboring v. The result is naturally interpreted as an element $c^1 = \delta^0(c^0) \in (\mathbb{F}_2^m)^E$.

Now given an arbitrary 1-chain $c^1 \in (\mathbb{F}_2^m)^E$, such that $c^1(e)$ is an m-bit vector for each edge $e \in E$, let us compute $\delta^1(c^1)$ assuming c^1 is supported on a single edge e (and this is extended linearly). If e is an A-edge then we compute the C_B encoding of $c^1(e)$, getting a vector of $|B| = \Delta$ bits, which we distribute one per square containing e. If e is a B-edge then we compute the C_A encoding of $c^1(e)$ and proceed similarly, adding the bits distributed to the same face modulo 2. This completes the description of our chain. The actual construction uses a 4-fold cover of a left-right complex, so we have four types of vertices and edges, see details in Section 3.1.

The linear time decoding algorithm is based on local bit-flips or small-set flips, which were first used in the quantum setting in [41]. The analysis of the distance of the code as well as of the decoding algorithm has two main components: expansion and robustness. The expansion arguments resemble previous works [16, 40, 50]. Technically, the key is analyzing the expansion of chains with a certain "local minimality" condition. The second ingredient is a *robustness* property for the pair of base codes (C_A, C_B) (and their duals $(C_A^\perp, C_B^\perp)$). Our second contribution in this work is a proof that two random codes are optimally robust. Interestingly, while our proof of linear distance and decoder construction are rather direct for the co-chain ordering (1), the analysis for the reverse ordering proceeds by a reduction to the co-chain. In this sense, the asymmetry induced by the geometric ordering we choose does not introduce substantial complications in the analysis.

We now discuss the robustness property. A pair (C_A, C_B) of codes, $C_A, C_B \subset \mathbb{F}_2^n$, is said to be d_2-robust if for every pair of $n \times n$ matrices M_A, M_B such that the rows of M_A are in C_A and the columns of M_B are in C_B, if the matrix $M = M_A + M_B$ has low weight, then it can be decomposed into a sum of only a few rows in C_A and a few columns in C_B, such that the number of rows and columns required is at most the weight of M divided by the robustness parameter d_2. (See Section 2.6 for formal definitions.) Whereas previous works [44, 50] showed that random codes have robustness that is $d_2 = n^{\frac{1}{2}-\epsilon}$, we show robustness with $d_2 = \Theta(n)$. This is clearly best possible (up to multiplicative constants) since the weight of M is quadratic in n and the number of rows/columns is linear in n.

Our second main result is the following.

Theorem 1.2 (Random Tensor Codes are Robust (Informal Theorem 2.10))**.** *For every $\rho_a, \rho_b \in (0, 1)$, there exist constants δ_1, δ_2 such that for C_A, C_B sampled from the uniform distribution of linear codes of length n and dimensions $\rho_a n, \rho_b n$, for large n, with high probability, C_A, C_B have distance $\delta_1 n$ and (C_A, C_B) is $\delta_2 n$ robust.*

Since the theorem is about random linear codes, it follows directly that robustness holds simultaneously for both (C_A, C_B) as well as $(C_A^\perp, C_B^\perp)$, with high probability. The same result on optimal robust codes is also obtained in [35].

The proof follows a counting argument similar to the proof of the Gilbert–Varshamov bound. One defines certain words as 'bad' and then shows that with high probability none of these 'bad' words is a codeword through a union bound. The main additional idea compared to the weaker result shown in [50] is that in the analysis we separate cases based on the rank of the matrix M. See Section 5 for details.

1.2 Related Work

Quantum LDPC Codes and LTCs. Our work fits into a line of recent works on quantum LDPC codes and LTCs [16, 44, 45, 50]. The constructions for qLDPC codes and LTCs turn out to be quite similar because both problems utilize 3-term chain complexes with expansion properties. We focus on the history of quantum LDPC codes. The historical development of LTCs can be found in [25] and a more recent development can be found in [16]. More discussion of qLDPC can be found in [11].

The earliest family of qLDPC codes are Kitaev's toric codes and surface codes [39] with dimension $k = \Theta(1)$ and distance $d = \Theta(\sqrt{n})$. Over time, better codes with increasing rate [55] $k = \Theta(n)$ and distance [23, 24, 38] $d = \Theta(\text{polylog}(n)\sqrt{n})$ have been discovered. Only recently did [30] and following works [10, 51] significantly break the square root barrier and achieve $d = \Theta(n/\log n)$. Finally, [50] showed the existence of good quantum LDPC codes with $k = \Theta(n)$ and $d = \Theta(n)$. More recently, [44] provide another construction of good quantum LDPC codes.

We now compare our qLDPC codes with two previous constructions [44, 50] in more detail. All of these qLDPC code constructions rely on Tanner codes which combine a 2-dimensional graph (left-right Cayley complex) with a 2-dimensional code (tensor code). The difference between the variants is on how one defines the 3-term chain complex from the 2-dimensional geometric complex.

Our construction has the advantage of being ordered by dimension (from vertices to edges to faces) which may be easier to generalize to higher dimensional complexes. Additionally, our proof uses tensor codes with better robustness which allows a simpler averaging argument, whereas earlier proofs required a more detailed study of the local structure and the resistance to *puncturing* for the tensor code. A similar simplification is also leveraged in [43].

[1] This over-simplification has 0 rate. To get positive rate, the base codes have different dimensions in the actual construction, $C_A : \mathbb{F}_2^{m_a} \to \mathbb{F}_2^\Delta$ and $C_B : \mathbb{F}_2^{m_b} \to \mathbb{F}_2^\Delta$ with $m_a \neq m_b$.

Decoders for Quantum LDPC Codes. Finding an efficient decoder is the natural next question after obtaining the qLDPC code. If one does not worry about the efficiency, in exponential time, it is known that one can decode up to $(d-1)/2$ errors by finding the closest codeword. Practically, it is more desirable to have a polynomial time or even a linear time decoder.

Existing decoders can be broadly separated into two families that focus on different type of qLDPC codes. The first family mainly decodes the surface codes, while the second family mainly decodes expander codes. Because the code structure is different, the corresponding decoding strategy is also very different. The first family includes minimum-weight perfect matching [13], union-find [12], and variants of belief propagation decoders [21, 49]. A more complete discussion can be found in [11].

We now focus on the second family, which the decoder of this paper belongs to. When the underlying graph has good expansion properties, often the greedy algorithm that flips the bits locally will work. This includes the classical expander codes [53] and the corresponding small set flip decoder in [41] for quantum codes. The same decoder was also applied to [23, 46]. In this work, we use the small set flip decoder to decode the direction of the co-chain complex (i.e. decode Z errors), and additionally use a "reconstruction" procedure to decode the direction of the chain complex (i.e. decode X errors).

Finally, we compare our result with the recent papers on the linear time sequential decoders [28, 42] and the parallel decoder [43]. In [28, 42], they show that the two previous qLDPC codes [44, 50] have linear time sequential decoders. Like our decoder, the decoder in [28] is a variant of the small-set-flip decoder. The decoder in [42] requires an additional *exceptional* mode. This difference is due to the fact that both [28] and our proof utilize tensor codes with better robustness, while [42] only uses the tensor code with weaker robustness. More recently, the better robust code is used in [43] to show the existence of a log time parallel decoder.

High Dimensional Expanders. Our work can be case as a study of notions of expansion in chain complexes. This relates to the study of high dimensional expanders (HDX), which is about notions of expansion for high-dimensional objects. The study of the HDX was introduced by Linial and Meshulam [47] to study random simplicial complexes and independently by Gromov [27] to study the topological overlapping principle. These natural questions have led to impressive results across areas including coding theory [16, 34, 45, 50], approximate sampling [3, 5, 6, 37], analysis of Boolean functions [8, 15, 29], agreement testing [14, 19], and sum-of-square lower bounds [17, 33].

The most studied type of HDX are called simplicial complexes. On the other hand, the recent development of qLDPC codes is more related to the cubical complexes. It would be interesting to see if one can translate the results from one to the other. One recent success is the application of qLDPC codes to sum-of-square lower bounds [33].

1.3 Further Directions

Towards Quantum LTCs. A notion that is related to qLDPC codes and LTCs is that of quantum locally testable codes (qLTCs) [2]. A natural way to go about this is to extend the 3-chain to a 5-chain. It seems that if each consecutive three terms are themselves sufficiently "expanding" then the entire chain would give a quantum LTC. Our proof technique may extend to the analysis of such higher-length chain complexes. Even if this were achieved, an important remaining challenge would be to find a higher dimensional robust code. Namely, there is a natural way to generalize the notion of robustness of a tensor product of three or more codes [35], however we do not currently know whether there are codes that are sufficiently robust. Indeed, even for two-dimensional tensors the current proofs only provide robustness via a probabilistic argument. It could be useful to have a direct, explicit construction as this may generalize more easily to higher dimensions than the probabilistic argument which seems inherently limited to two dimensions.

PCPs and Quantum PCPs. Probabilistically checkable proofs (PCPs) and locally testable codes are closely, though not formally, related. (See [25] for a survey.) In the quantum complexity literature there is a quantum version of PCPs [1], the existence of which remains open. It would be interesting to see if one can make progress on this question by leveraging the recent works on qLDPCs. A positive, though certainly not conclusive, indication that this is a viable path is provided by the recent resolution of the NLTS conjecture [7], which crucially relies not only on the existence of good LDPC but on specific properties of the existing constructions which were discovered in the construction of the linear time decoders for them.

2 PRELIMINARIES

2.1 Chain Complexes

Chain complexes provide a way to connect the study of quantum codes with high dimensional expanders.

Definition 2.1 (Chain complex)**.** *A chain complex X is a sequence of vector spaces $\mathbb{F}_2^{X(i)}$ generated by sets $X(i)$ together with linear maps $\partial_i : \mathbb{F}_2^{X(i)} \to \mathbb{F}_2^{X(i-1)}$ called the boundary operators. These boundary operators satisfy*

$$\partial_{i-1}\partial_i = 0 \ .$$

Because $\mathbb{F}_2^{X(i)}$ has a canonical choice of basis corresponding to the elements of $X(i)$, one can define the associated co-boundary operators $\delta^i := \partial_{i+1}^T : \mathbb{F}_2^{X(i)} \to \mathbb{F}_2^{X(i+1)}$, where $(\cdot)^T$ denotes the matrix transpose. The co-boundary operators automatically satisfy

$$\delta^{i+1}\delta^i = 0 \ .$$

We introduce some standard terminology. Elements of the kernel of the (co)-boundary operators are called (co)-cycles

$$Z_i := \ker \partial_i = \{c_i \in \mathbb{F}_2^{X(i)} : \partial_i c_i = 0\} \ ,$$
$$Z^i := \ker \delta^i = \{c^i \in \mathbb{F}_2^{X(i)} : \delta^i c^i = 0\} \ .$$

Elements of the image of the (co)-boundary operators are called (co)-boundaries

$$B_i := \operatorname{im} \partial_{i+1} = \{\partial_{i+1} c_{i+1} : c_{i+1} \in \mathbb{F}_2^{X(i+1)}\} \ ,$$
$$B^i := \operatorname{im} \delta^{i-1} = \{\delta^{i-1} c^{i-1} : c^{i-1} \in \mathbb{F}_2^{X(i-1)}\} \ .$$

Since $\partial_i \partial_{i+1} = 0$ it follows that $B_i \subset Z_i$. When $B_i = Z_i$ the chain complex is said to be *exact* at i.

2.2 Classical and Quantum Error Correcting Codes

A classical linear code is specified by a k-dimensional linear subspace $C \subset \mathbb{F}_2^n$. Here, n is called the length, k is called the dimension, and $d := \min_{c \in C} |c|$ is called the distance, where $|\cdot|$ is the Hamming weight, i.e. the number of non-zero entries. We call $r = k/n$ the rate and $\delta = d/n$ the relative distance of the code. A more explicit way of describing a classical linear code is by specifying a parity-check matrix $H : \mathbb{F}_2^n \to \mathbb{F}_2^m$ where $m = n - k$ and $C = \ker H$ is the kernel of the matrix.

A quantum CSS code is specified by two classical codes $C_z = \ker H_z \subset \mathbb{F}_2^n$ and $C_x = \ker H_x \subset \mathbb{F}_2^n$ such that $C_x^\perp \subset C_z$, i.e. $H_x H_z^T = 0$. This condition allows us to associate a 3-term chain complex to the quantum code,

$$X : \mathbb{F}_2^{m_z} \xrightarrow{H_z^T} \mathbb{F}_2^n \xrightarrow{H_x} \mathbb{F}_2^{m_x} .$$

Here are the relevant quantities associated with the quantum code. Elements of $C_x = Z^1$ (resp. $C_z = Z_1$) are called X (resp. Z)-logical operators. Elements of $C_x^\perp = B_1$ (resp. $C_z^\perp = B^1$) are called Z (resp. X)-stabilizers. The dimension of the code is $k = \dim Z_1 - \dim B_1$. The distance is $d = \min(d_x, d_z)$ where

$$d_x = \min_{c^1 \in Z^1 - B^1} |c^1| , \qquad d_z = \min_{c_1 \in Z_1 - B_1} |c_1|$$

and d_x, d_z are called the X-distance and Z-distance of the code respectively. The code is called a *quantum low-density parity-check code* (qLDPC) if H_x and H_z have a bounded number of nonzero entries in each column and row.

Having defined a quantum code, we now describe the task of decoding. The goal of the decoder is to recover the error pattern from the syndrome. Under the stabilizer formalism, one can express any error pattern as a pair (c^1, c_1) where $c^1 \in \mathbb{F}_2^n$ indicates coordinates with an X-error and $c_1 \in \mathbb{F}_2^n$ indicates coordinates with a Z-error. The decoder is given the syndrome $(\delta^1 c^1, \partial_1 c_1)$ and is required to return a correction $(\tilde{c}^1, \tilde{c}_1)$ such that the difference from the actual error is a stabilizer, i.e. $\tilde{c}^1 - c^1 \in B^1$ and $\tilde{c}_1 - c_1 \in B_1$. This task can be divided into two independent tasks where one recovers $\tilde{c}^1$ from $\delta^1 c^1$ (X-error decoding) and the other recovers $\tilde{c}_1$ from $\partial_1 c_1$ (Z-error decoding).

2.3 Expander Graphs

Expander graphs are used to obtain various important results in theoretical computer science. The most important one in our context is the expander codes [53]. We refer the reader to [32] for other applications of expander graphs.

Definition 2.2 (Spectral Expander Graphs and Ramanujan Graphs)**.** *Let $\mathcal{G} = (V, E)$ be an undirected, Δ-regular graph on n vertices, and define $\lambda(\mathcal{G}) := \max\{|\lambda_2|, |\lambda_n|\}$ where $\Delta = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ are the eigenvalues of the adjacency matrix of $\mathcal{G}$. We say that $\mathcal{G}$ is a λ-spectral expander if $\lambda(\mathcal{G}) \leq \lambda$.*

We use spectral expanders for two reasons. First, there are known explicit infinite families of spectral expanders [52]. Second, spectral expansion implies edge expansion which is a key ingredient to obtain our results. This property is captured in the following expander mixing lemma which first appeared in [4].

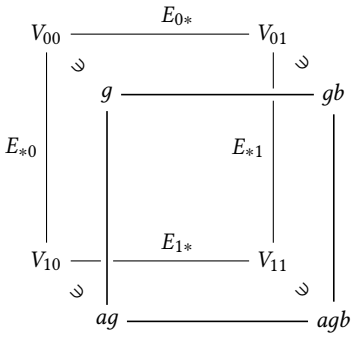

Figure 1: 4-fold left-right Cayley complex.

Lemma 2.3 (Expander Mixing Lemma)**.** *Let $\mathcal{G}$ be a Δ-regular graph with λ-spectral expansion. Then for any subset $S, T \subset V$, we have*

$$|E(S,T)| \leq \frac{\Delta}{|V|}|S||T| + \lambda\sqrt{|S||T|} .$$

Moreover, for any vectors $x, y \in \mathbb{R}^V$ we have

$$x^T M y \leq \frac{\Delta}{|V|}\|x\|_1\|y\|_1 + \lambda\|x\|_2\|y\|_2 ,$$

where M is the adjacency matrix of $\mathcal{G}$ and for $z \in \mathbb{R}^n$, $\|z\|_1 = \sum_i |z_i|$ and $\|z\|_2 = (\sum_i |z_i|^2)^{1/2}$ denote the L_1 and L_2 norm respectively.

2.4 Left-Right Cayley Complexes

Our code construction is based on the left-right Cayley complex introduced in [16]. A similar structure also appeared in [10, 50]. The *4-fold left-right Cayley complex* $\mathcal{G}_2(G, A, B)$ is specified by a finite group G and two sets of generators A and B which are closed under inverse. The complex is illustrated in Figure 1. It consists of vertices, edges, and faces as follows:

- The vertices are $V = V_{00} \cup V_{10} \cup V_{01} \cup V_{11}$ where $V_{00} \cong V_{10} \cong V_{01} \cong V_{11} \cong G$.
- The edges are $E = E^| \cup E^- = (E_{*0} \cup E_{*1}) \cup (E_{0*} \cup E_{1*})$ where
  $$E_{*0} = \{(g, ag) : g \in G, a \in A\} \subset V_{00} \times V_{10} ,$$
  $$E_{*1} = \{(gb, agb) : gb \in G, a \in A\} \subset V_{01} \times V_{11} ,$$
  $$E_{0*} = \{(g, gb) : g \in G, b \in B\} \subset V_{00} \times V_{01} ,$$
  $$E_{1*} = \{(ag, agb) : ag \in G, b \in B\} \subset V_{10} \times V_{11} .$$
- The faces are $F = \{(g, ag, gb, agb) : g \in G, a \in A, b \in B\} \subset V_{00} \times V_{10} \times V_{01} \times V_{11}$.

To clarify which vertex set, V_{00}, V_{01}, etc. a given vertex g belongs to, we sometimes write the vertex as $(g, 00)$ or $(g, 01)$, etc. The same convention applies to edges. For example, $((g, ag), *0)$ is an edge in E_{*0}. Note that the edges and faces are labeled by ordered tuples instead of sets. Elements of $E^|$ are referred to as *vertical edges*, and elements of E^- as *horizontal edges*. The appearance of faces crucially relies on the fact that the left action commutes with the right action, e.g. $a(gb) = (ag)b$.

We introduce the following important notation to describe the neighborhood relation between the vertices, edges and faces. For $v_{00} \in V_{00}$ we define $V_{10}(v_{00})$ as the set of vertices in V_{10} neighbor to v_{00} and $V_{11}(v_{00})$ as the set of vertices in V_{11} "neighbor" to v_{00}

by going through a horizontal edge and a vertical edge. Similarly we define $E_{*0}(v_{00})$ as the set of edges in E_{*0} incident to v_{00} and $E_{1*}(v_{00})$ as the set of edges accessible by v_{00} by first going through a vertical edge then choosing an adjacent horizontal edge.

More precisely, given $v_{00} = (g, 00)$ we define the following neighborhoods.

- $V_{10}(v_{00}) = \{(ag, 10) : a \in A\}$, $V_{01}(v_{00}) = \{(gb, 01) : b \in B\}$, $V_{11}(v_{00}) = \{(agb, 11) : a \in A, b \in B\}$,
- $E_{*0}(v_{00}) = \{((g, ag), *0) : a \in A\}$, $E_{0*}(v_{00}) = \{((g, gb), 0*) : b \in B\}$,
- $E_{*1}(v_{00}) = \{((gb, agb), *1) : a \in A, b \in B\}$, $E_{1*}(v_{00}) = \{((ag, agb), 1*) : a \in A, b \in B\}$,
- $E^{|}(v_{00}) = E_{*0}(v_{00})$, $E^{-}(v_{00}) = E_{0*}(v_{00})$, $E(v_{00}) = E^{|}(v_{00}) \cup E^{-}(v_{00})$,
- $F(v_{00}) = \{(g, ag, gb, agb) : a \in A, b \in B\}$.

Given $e_{*0} = ((g, ag), *0)$, we define the following neighborhoods.

- $E_{*1}(e_{*0}) = \{((gb, agb), *1) : b \in B\}$,
- $E_{0*}(e_{*0}) = \{((g, gb), 0*) : b \in B\}$, $E_{1*}(e_{*0}) = \{((ag, agb), 1*) : b \in B\}$,
- $F(e_{*0}) = \{(g, ag, gb, agb) : b \in B\}$.

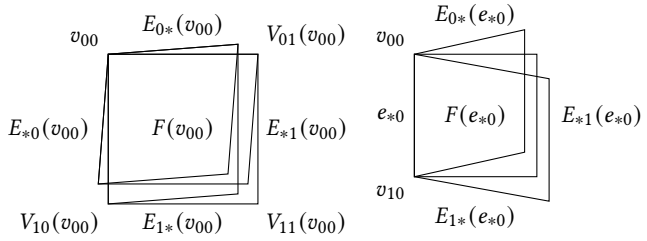

Figure 2: (Left) The neighboring sets of a vertex v_{00}. (Right) The neighboring sets of an edge e_{*0}.

Finally we introduce subgraphs of the complex that will be used to define Tanner codes in Section 2.6. $\mathcal{G}(E^{|}, F)$ is the bipartite graph that has $E^{|} = E_{*0} \cup E_{*1}$ as vertices and F as the edges between them. More precisely, the edges are $F \cong \{((g, ag), (gb, agb)) : g \in G, a \in A, b \in B\} \subset E_{*0} \times E_{*1}$. The bipartite graph $\mathcal{G}(E^{-}, F)$ is defined similarly. $\mathcal{G}(V, E^{|})$ is the bipartite graph that has $V = (V_{00} \cup V_{01}) \cup (V_{10} \cup V_{11})$ as vertices and $E^{|}$ as the edges between them. More precisely, the edges are $E^{|} = E_{*0} \cup E_{*1}$ where $E_{*0} \cong \{(g, ag) : g \in G, a \in A\} \subset V_{00} \times V_{10}$ and $E_{*1} \cong \{(g, ag) : g \in G, a \in A\} \subset V_{01} \times V_{11}$. One defines the bipartite graph $\mathcal{G}(V, E^{-})$ similarly.

We conclude by discussing an explicit instance that is used in our construction. We use the Ramanujan graph constructed in [52]. Let p and q be unequal primes $\equiv 1 \mod 4$ and $\left(\frac{q}{p}\right) = 1$ where $\left(\frac{q}{p}\right)$ is the Legendre symbol. Let $G = \mathrm{PSL}(2, \mathbb{Z}/q\mathbb{Z})$ and $S = S^{-1}$ be the set of size $\Delta = p + 1$ as defined in the paper. The paper above shows that the Cayley graph $Cay(G, S)$ with vertex set G and edge set $\{\{g, ag\} : g \in G, a \in S\}$ is a Ramanujan graph. Finally, the 4-fold left-right Cayley complex we consider is $\mathcal{G}_2(G, A = S, B = S)$.

2.5 Expansion Properties of Left-Right Cayley Complexes

We give three lemma that state expansion properties of operators defined on graphs obtained from the left-right Cayley complex. The first two lemma show expansion properties of two different random walks on the edges of $\mathcal{G}_2(G, A, B)$.

Lemma 2.4. *Let $M_1 \in \mathbb{R}^{E \times E}$ be the adjacency matrix between opposing edges of the same face in $\mathcal{G}_2(G, A, B)$, i.e. the adjacency matrix of the graph*

$$((g, ag), *0) \sim ((gb, agb), *1), \quad ((g, gb), 0*) \sim ((ag, agb), 1*).$$

Suppose that $\mathrm{Cay}(G, A)$ *and* $\mathrm{Cay}(G, B)$ *are λ-spectral expanders. Then for any subset $S \subset E$ it holds that*

$$1_S^T M_1 1_S \leq \lambda |S| + \frac{\Delta}{2|G|} |S|^2 . \tag{2}$$

Proof. M_1 is the disjoint union of $|G|$ copies of $\mathrm{Cay}^b(G, A)$ and $|G|$ copies of $\mathrm{Cay}^b(G, B)$ where $\mathrm{Cay}^b(G, A)$ and $\mathrm{Cay}^b(G, B)$ are the double covers of the λ-spectral expander graphs $\mathrm{Cay}(G, A)$ and $\mathrm{Cay}(G, B)$. Let $S = \cup_i (S_i^0 \cup S_i^1)$ be a partition of S according to each disjoint graph and their two vertex sets. Each disjoint graph satisfies,

$$1_{S_i^0}^T M_1 1_{S_i^1} \leq \lambda \sqrt{|S_i^0||S_i^1|} + \frac{\Delta}{|G|} |S_i^0||S_i^1|.$$

So

$$\begin{aligned} 1_S^T M_1 1_S &= 2 \sum_i 1_{S_i^0}^T M_1 1_{S_i^1} \\ &\leq \lambda |S| + \frac{\Delta}{2|G|} |S|^2 . \end{aligned}$$

□

Lemma 2.5. *Let $M_0 \in \mathbb{R}^{E \times E}$ be the adjacency matrix where two edges of $\mathcal{G}_2(G, A, B)$ are connected if one of their endpoints are connected through an edge, i.e. $M_0 = U M_0' D$ where $D \in \mathbb{R}^{V \times E}$ and $U \in \mathbb{R}^{E \times V}$ are the incidence matrices between the edges and the vertices and M_0' is the adjacency matrix of the graph*

$$(g, 00) \sim (ag, 10), \ (g, 00) \sim (gb, 01),$$
$$(ag, 10) \sim (agb, 11), \ (gb, 01) \sim (agb, 11).$$

Suppose that $\mathrm{Cay}(G, A)$ *and* $\mathrm{Cay}(G, B)$ *are λ-spectral expanders. Then for any subset $S \subset E$ it holds that*

$$1_S^T M_0 1_S \leq 8\lambda\Delta |S| + \frac{2\Delta}{|G|} |S|^2 . \tag{3}$$

Note that we allow multi-edges, so some entries of M_0 could be greater than 1 when there are degeneracies.

Proof. M_0' is the union of two copies of $\mathrm{Cay}^b(G, A)$ and two copies of $\mathrm{Cay}^b(G, B)$. Let $\mathcal{V}_{00} \subset V_{00}$, $\mathcal{V}_{10} \subset V_{10}$, $\mathcal{V}_{10} \subset V_{10}$ and $\mathcal{V}_{11} \subset V_{11}$ be the vertices incident on $\mathcal{E}$. Because each edge is connected to two vertices,

$$\|\mathcal{V}_{00}\|_1 + \|\mathcal{V}_{10}\|_1 + \|\mathcal{V}_{01}\|_1 + \|\mathcal{V}_{11}\|_1 \leq 2|\mathcal{E}|.$$

Because each vertex is connected by at most 2Δ edges, $\|\mathcal{V}_{00}\|_\infty \leq 2\Delta$, so

$$\|\mathcal{V}_{00}\|_2^2 + \|\mathcal{V}_{10}\|_2^2 + \|\mathcal{V}_{01}\|_2^2 + \|\mathcal{V}_{11}\|_2^2 \leq 2|\mathcal{E}| \cdot 2\Delta.$$

The expander subgraph $\mathrm{Cay}^b(G,A)$ between $\mathcal{V}_{00}$ and $\mathcal{V}_{10}$ gives

$$\begin{aligned}1_{\mathcal{V}_{00}}^T M_0' 1_{\mathcal{V}_{10}} &\le \lambda\|\mathcal{V}_{00}\|_2\|\mathcal{V}_{10}\|_2 + \frac{\Delta}{|G|}\|\mathcal{V}_{00}\|_1\|\mathcal{V}_{10}\|_1 \\ &\le \lambda\frac{\|\mathcal{V}_{00}\|_2^2 + \|\mathcal{V}_{10}\|_2^2}{2} + \frac{\Delta}{|G|}\|\mathcal{V}_{00}\|_1\|\mathcal{V}_{10}\|_1.\end{aligned}$$

By combining with other expander subgraphs, we have

$$\begin{aligned}1_{\mathcal{E}}^T M_0 1_{\mathcal{E}} &= 2(1_{\mathcal{V}_{00}}^T M_0' 1_{\mathcal{V}_{10}} + 1_{\mathcal{V}_{00}}^T M_0' 1_{\mathcal{V}_{01}} \\ &\quad + 1_{\mathcal{V}_{10}}^T M_0' 1_{\mathcal{V}_{11}} + 1_{\mathcal{V}_{01}}^T M_0' 1_{\mathcal{V}_{11}}) \\ &\le 2\lambda(\|\mathcal{V}_{00}\|_2^2 + \|\mathcal{V}_{10}\|_2^2 + \|\mathcal{V}_{01}\|_2^2 + \|\mathcal{V}_{11}\|_2^2) \\ &\quad + \frac{2\Delta}{|G|}(\|\mathcal{V}_{00}\|_1\|\mathcal{V}_{10}\|_1 + \|\mathcal{V}_{00}\|_1\|\mathcal{V}_{01}\|_1 \\ &\qquad + \|\mathcal{V}_{10}\|_1\|\mathcal{V}_{11}\|_1 + \|\mathcal{V}_{01}\|_1\|\mathcal{V}_{11}\|_1) \\ &\le 8\lambda\Delta|\mathcal{E}| + \frac{2\Delta}{|G|}|\mathcal{E}|^2 .\end{aligned}$$

□

The third lemma shows co-expansion of an associated graph.

Lemma 2.6 (Co-Expansion $\mathbb{F}_2^{X(1)} \leftarrow \mathbb{F}_2^{X(0)}$)**.** *Given Δ-regular λ-spectral expander graphs $\mathrm{Cay}(G,A)$, $\mathrm{Cay}(G,B)$ and linear codes $C_A^\perp, C_B^\perp$ of length Δ with distance d_1.*

Then the map

$$(\mathbb{F}_2^{m_a})^{E^-} \times (\mathbb{F}_2^{m_b})^{E^|} \xleftarrow{\delta^0} (\mathbb{F}_2^{m_a\times m_b})^V$$

satisfies

$$\|\delta^0 c^0\|_E \ge 2(d_1-\lambda)\|c^0\|_V - \frac{\Delta}{2}\frac{\|c^0\|_V^2}{|G|} .$$

Proof. To show the expansion, one consider each component $c^1(E_{*0}) = \delta^0 c^0(V_{00}) + \delta^0 c^0(V_{10})$ separately. Because of code distance, each non-zero vertices in V_{00} contribute to at least d_1 distinct non-zero edges in $\delta^0 c^0(V_{00})$. Same for $\delta^0 c^0(V_{10})$. What is left is to bound the number of cancellations in $\delta^0 c^0(V_{00}) + \delta^0 c^0(V_{10})$. Because (V_{00}, V_{10}, E_{*0}) is the double cover of the λ-spectral expander $\mathrm{Cay}(G,A)$, the number of cancellation is at most $\lambda\sqrt{\|c^0(V_{00})\|_V\|c^0(V_{10})\|_V} + \frac{\Delta}{|G|}\|c^0(V_{00})\|_V\|c^0(V_{10})\|_V$. So

$$\begin{aligned}\|c^1(E_{*0})\|_E &\ge d_1(\|c^0(V_{00})\|_V + \|c^0(V_{10})\|_V) \\ &\quad - 2(\lambda\sqrt{\|c^0(V_{00})\|_V\|c^0(V_{10})\|_V} \\ &\quad + \frac{\Delta}{|G|}\|c^0(V_{00})\|_V\|c^0(V_{10})\|_V) \\ &\ge (d_1-\lambda)(\|c^0(V_{00})\|_V + \|c^0(V_{10})\|_V) \\ &\quad - \frac{2\Delta}{|G|}\|c^0(V_{00})\|_V\|c^0(V_{10})\|_V.\end{aligned}$$

Now we combine the four contributions and use AM-GM inequality to obtain

$$\begin{aligned}\|\delta^0 c^0\|_E &= \|c^1(E_{*0})\|_E + \|c^1(E_{*0})\|_E + \|c^1(E_{*0})\|_E + \|c^1(E_{*0})\|_E \\ &\ge 2(d_1-\lambda)\|c^0\|_V - \frac{\Delta}{2}\frac{\|c^0\|_V^2}{|G|}.\end{aligned}$$

□

2.6 Tensor Codes and Robustness

Robust codes were first studied in [9] and [20] in the context of locally testable codes (LTC). Similar variants are applied to the construction LTC and qLDPC in [16, 44, 50]. In this paper, the definition of robustness is identical to agreement testability up to a normalization constant. We first give the definition, then discuss its equivalence to agreement testability, and finally state our result stating robustness of the tensor product of random tensor codes.

Given 2 linear codes C_A, C_B of length n_a, n_b let $C_A \otimes C_B$ be the set of $n_a \times n_b$ matrices where each column vector belongs to C_A and each row vector belongs to C_B. Let $\Sigma(C_A,C_B) \coloneqq C_A \otimes \mathbb{F}_2^{n_b} + \mathbb{F}_2^{n_a} \otimes C_B$ be the set of matrices that can be expressed as a sum of two $n_a \times n_b$ matrices, where the first has each column in C_A and the second has each row in C_B. We introduce convenient notation for measuring different variations on the Hamming weight of a matrix: by entries, by rows, or by columns.

Definition 2.7. *Given a matrix $f \in \mathbb{F}_2^{n_a\times n_b}$, we let*

$$\begin{aligned}\|f\|_{[n_a\times n_b]} &= |\{(i,j) : f_{i,j} \neq 0\}| , \\ \|f\|_{[n_b]} &= |\{j : f_{\cdot,j} \neq 0\}| , \\ \|f\|_{[n_a]} &= |\{i : f_{i,\cdot} \neq 0\}| ,\end{aligned}$$

This definition allows us to introduce the notion of robustness we make use of.

Definition 2.8 (Robustness of Tensor Codes)**.** *Let C_A, C_B be linear codes of length n_a, n_b respectively and $d_2 \in \mathbb{R}_+$. We say that (C_A, C_B) is d_2-robust if for all $c \in \Sigma(C_A,C_B) \subset \mathbb{F}_2^{n_a\times n_b}$, there exists $c_a \in C_A \otimes \mathbb{F}_2^{n_b}$ and $c_b \in \mathbb{F}_2^{n_a} \otimes C_B$ such that $c = c_a + c_b$ and*

$$\|c\|_{[n_a]\times[n_b]} \ge d_2(\|c_a\|_{[n_b]} + \|c_b\|_{[n_a]}) .$$

The notion of robustness can be understood as boundary expansion for a chain complex naturally associated with the pair of codes (C_A, C_B). To see this define a 3-term chain complex

$$Y(H_A,H_B)\colon \mathbb{F}_2^{n_a\times n_b} \xrightarrow{\partial_2} \mathbb{F}_2^{n_a\times m_b + m_a\times n_b} \xrightarrow{\partial_1} \mathbb{F}_2^{m_a\times m_b} \tag{4}$$

through the maps

$$\partial_2(c_2) = ((I_{[n_a]}\otimes H_B)c_2, (H_A \otimes I_{[n_b]})c_2)$$

and

$$\partial_1(c_1 = (c_a, c_b)) = (H_A \otimes I_{[m_b]})c_a + (I_{[m_a]} \otimes H_B)c_b ,$$

where for an integer $k \ge 1$, $I_{[k]}$ denotes the identity map of $\mathbb{F}_2^k$. Then it follows easily from the Künneth formula (see e.g. [31, Section 3.B]) that $Y(H_A,H_B)$ is *exact*, i.e. any element in the kernel of ∂_1 is in the image of ∂_2.

Now consider the co-chain

$$Y(H_A^\perp, H_B^\perp)\colon \mathbb{F}_2^{n_a\times n_b} \xleftarrow{\delta^1} \mathbb{F}_2^{n_a\times k_b + k_a\times n_b} \xleftarrow{\delta^0} \mathbb{F}_2^{k_a\times k_b} ,$$

where $H_A^\perp\colon \mathbb{F}_2^{n_a} \to \mathbb{F}_2^{k_a}$ is the parity check matrix of the dual code $C_A^\perp$. Using this complex, Definition 2.8 can be reformulated as saying that for all $c^2 \in \Sigma(C_A,C_B) = \mathrm{im}\,\delta^1$, there exists $c^1 \in \mathbb{F}_2^{n_a\times m_b + m_a\times n_b}$ such that $c^2 = \delta^1 c^1$ and

$$\|c^2\|_{[n_a]\times[n_b]} \ge d_2\|c^1\|_{[n_a]\cup[n_b]}$$

where the variables c, c_a, c_b from Definition 2.8 correspond to the new variables c^2, $((H_A^\perp)^T \otimes I_{[n_b]})c_a^1$, $(I_{[n_b]} \otimes (H_B^\perp)^T)c_b^1$ where $c^1 =$

$(c_a^1, c_b^1) \in \mathbb{F}_2^{m_a \times n_b} \oplus \mathbb{F}_2^{n_a \times m_b}$. Here we used the fact that $\|c_a^1\|_{[n_b]} = \|((H_A^\perp)^T \otimes I_{[n_b]})c_a^1\|_{[n_b]}$ because $(H_A^\perp)^T$ is injective.

The perspective through chain complexes allows us to make the connection with agreement testability. Note that the definition below differs from [16, Definition 2.8] by a normalization factor.

Definition 2.9 (Agreement Testability)**.** *Let C_A, C_B be linear codes of length n_a, n_b respectively and $d_2' \in \mathbb{R}_+$. We say that $C_A \otimes C_B$ is d_2'-agreement testable if for all $c_a \in C_A \otimes \mathbb{F}_2^{n_b}$, $c_b \in \mathbb{F}_2^{n_a} \otimes C_B$, there exists $c \in C_A \otimes C_B$ such that*

$$\|c_a + c_b\|_{[n_a]\times[n_b]} \geq d_2'(\|c + c_a\|_{[n_b]} + \|c + c_b\|_{[n_a]}) \ .$$

Using the same notation as above, Definition 2.9 is saying that for all $c^1 \in \mathbb{F}_2^{n_a \times m_b + m_a \times n_b}$ there exists $c^0 \in \mathbb{F}_2^{m_a \times m_b}$ such that

$$\|\delta^1 c^1\|_{[n_a]\times[n_b]} \geq d_2' \|c^1 + \delta^0 c^0\|_{[n_a]\cup[n_b]} \ ,$$

where now c in Definition 2.9 corresponds to $((H_A^\perp)^T \otimes (H_B^\perp)^T)c^0$ and c_a, c_b are as before. Because the chain complex Y is exact, the two definitions are identical with $d_2 = d_2'$.

Finally, we state our result on the robustness of random tensor codes. We consider the case when n_a and n_b are equal, $n_a = n_b = \Delta$. In [44] it is shown that for for arbitrary $\epsilon > 0$ and C_A and C_B chosen uniformly at random, the pair (C_A, C_B) is $\Omega(\Delta^{1/2-\epsilon})$-robust with high probability. Using a different counting argument we show that a uniformly random pair of codes is $\Theta(\Delta)$-robust with high probability.

Theorem 2.10 (Random codes are robust)**.** *Fix $\rho_a, \rho_b \in (0,1)$, let $\delta_1 \in (0, 1/2), \delta_2 \in (0, \delta_1(1-\delta_1/2)/8)$ satisfy*

$$2h(\delta_1/2) + 2(1-\delta_1/2)h\left(\frac{4\delta_2}{\delta_1(1-\delta_1/2)}\right) < \frac{3}{4}\frac{(1-\delta_1/2-\rho_a)(1-\delta_1/2-\rho_b)}{1-\delta_1/2} \quad (5)$$

where $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$.[2] Let C_A, C_B be random codes sampled from the uniform distribution with length Δ and dimensions $\rho_a\Delta, \rho_b\Delta$. Then as Δ goes to infinity, with probability tending to 1, C_A, C_B have distance $d_1 = \delta_1\Delta$ and (C_A, C_B) is $d_2 = \delta_2\Delta$-robust.

The theorem is shown in Section 5. When C_A is sampled uniformly among codes of dimension $\rho_a\Delta$, $C_A^\perp$ is sampled uniformly among codes of dimension $(1-\rho_a)\Delta$. So the same theorem applies to $C_A^\perp$ and $C_B^\perp$ and through a union bound we obtain the following corollary.

Corollary 2.11. *Fix $\rho_a, \rho_b \in (0,1)$. There exist constants δ_1 and δ_2 such that for large enough Δ there exist codes C_A and C_B of length Δ where*

(1) $\dim C_A = \rho_a\Delta$ and $\dim C_B = \rho_b\Delta$,
(2) $C_A, C_B, C_A^\perp, C_B^\perp$ have distance $d_1 = \delta_1\Delta$,
(3) (C_A, C_B) and $(C_A^\perp, C_B^\perp)$ are both $d_2 = \delta_2\Delta$-robust.

[2]The allowed range for δ_2 is chosen such that the argument in $h(\cdot)$ is valued between $(0, 1/2)$.

2.7 Tanner Codes

The Tanner construction [54] is a method to obtain 'large' code by combining a 'large' graph and a 'small' local code. This allows one to find an infinite family of codes by combining an infinite family of graphs with a fixed local code. As long as the graphs are explicit, the Tanner codes are also explicit, even if finding the desired local code requires brute force search. When the underlying graph is an expander, the Tanner code often inherits desireable properties from the small code. Later, we will not only be interested in the code but also in the parity-check matrix that generates the code, since the LDPC property is defined on the parity-check matrix. Therefore, we sometimes abuse language and refer to the code and the linear map (parity-check matrix) interchangeably.

We consider a Δ-regular bipartite graph $\mathcal{G} = (V_0, V_1, E)$ with the $1-1$ identification $E \times [2] \cong V \times [\Delta]$, where the additional index on the edge indicates whether it is asking for the vertex on the side of V_0 or V_1, and the additional index on the vertex gives an ordering to the edges incident to the vertex. For example, for the double cover of the Cayley graph with $V_0 \cong V_1 \cong G$ and $E = \{(g, ag) : g \in G, a \in A\}$, a choice of the identification is $(e = (g, ag), 0) \leftrightarrow (v_0 = (g, 0), a)$ and $(e = (g, ag), 1) \leftrightarrow (v_1 = (ag, 1), a)$.

Given a Δ-regular bipartite graph $\mathcal{G}$ and a local code C with parity-check matrix $H \colon \mathbb{F}_2^\Delta \to \mathbb{F}_2^m$, the Tanner code $\mathcal{T}(\mathcal{G}, H) \colon \mathbb{F}_2^E \to (\mathbb{F}_2^m)^V$ is defined through the composition

$$\mathbb{F}_2^E \to (\mathbb{F}_2^\Delta)^V \to (\mathbb{F}_2^m)^V$$

where the first map copies the value on the edge to the vertices incident to the edge and the second map applies H to $\mathbb{F}_2^\Delta \cong \mathbb{F}_2^{\{(v,a):a\in[\Delta]\}}$ for each vertex v.

Another way to think about the map is though its submatrices. This description will be helpful to prove that the construction in Section 3 is a chain complex. Given an edge $e \in E$ and a vertex $v \in V$, consider the submatrix $\mathcal{T}(\mathcal{G}, H)_e^v \colon \mathbb{F}_2 \to \mathbb{F}_2^m$ which is the restriction where the input vector is supported on e and the output vector is restricted to v. Describing $\mathcal{T}(\mathcal{G}, H)$ is the same as describing $\mathcal{T}(\mathcal{G}, H)_e^v$ for each $e \in E$ and $v \in V$. When v and e are not incident, $\mathcal{T}(\mathcal{G}, H)_e^v$ is simply 0. When v and e are incident, and suppose $(e, i) \leftrightarrow (v, a)$, then $\mathcal{T}(\mathcal{G}, H)_e^v = H(\bar{a}) \colon \mathbb{F}_2 \to \mathbb{F}_2^m$, where $\bar{a}$ is the basis vector of $\mathbb{F}_2^\Delta$ corresponding to the element $a \in [\Delta]$.

2.8 Expansion Properties of Chain Complexes

The distance of a quantum code falls into a broader category of expansion properties of chain complexes. This includes (co)-systolic distance (the one equivalent to quantum code distance), small set (co)-boundary expansion [33], and (co)-locally minimal expansion [22, 36]. We discuss them together because heuristically they are of similar difficulty, that is a proof that works for one often implies the other. On the other hand, in certain scenario they can be distinguished. For example, locally testable code does not follow directly from systolic distance, but does follow from small set boundary expansion. This is one of the motivations for considering small set boundary expansion. See [48] for the history and more discussions on the study of these expansion properties.

We first define the different notions of expansion, then we discuss relations between them and with code properties. As we will discuss more precisely in Section 3, we consider a weight on elements of

a complex that is different from the Hamming weight, and which counts the number of non-zero geometric objects instead of non-zero bits. This weight is denoted as $\|\cdot\|$ and differs from the usual Hamming weight by a constant factor, i.e. $\|\cdot\| = \Theta(|\cdot|)$ (because the chain complex we consider has bounded degree). Note that $\|\cdot\|$ is similar to the block weight defined in [50].

Definition 2.12 ((Co)-Systolic Distance). *We say that* $X : \mathbb{F}_2^{X(2)} \xrightarrow{\partial_2} \mathbb{F}_2^{X(1)} \xrightarrow{\partial_1} \mathbb{F}_2^{X(0)}$ *has systolic distance* α *if*

$$\forall c_1 \in Z_1 - B_1 : \|c_1\| \geq \alpha |X(1)|.$$

Similarly, X *has co-systolic distance* α *if*

$$\forall c^1 \in Z^1 - B^1 : \|c^1\| \geq \alpha |X(1)|.$$

It is not hard to see and well-known that constant (co)-systolic distance of a chain complex is equivalent to linear X-distance and Z-distance of the corresponding quantum CSS code.

Definition 2.13 (Small-Set (Co)-Boundary Expansion). *We say that* $X : \mathbb{F}_2^{X(2)} \xrightarrow{\partial_2} \mathbb{F}_2^{X(1)} \xrightarrow{\partial_1} \mathbb{F}_2^{X(0)}$ *is a* (α, β, γ)*-small-set boundary expander if*

$$\forall c_1 \in \mathbb{F}_2^{X(1)}, \|c_1\| < \alpha |X(1)| : \\ \exists c_2 \in \mathbb{F}_2^{X(2)}, \|\partial_1 c_1\| \geq \beta \|c_1 + \partial_2 c_2\|, \|c_2\| \leq \gamma \|c_1\|.$$

Similarly, X *is a* (α, β, γ)*-small-set co-boundary expander if*

$$\forall c^1 \in \mathbb{F}_2^{X(1)}, \|c^1\| < \alpha |X(1)| : \\ \exists c^0 \in \mathbb{F}_2^{X(0)}, \|\delta^1 c^1\| \geq \beta \|c^1 + \delta^0 c^0\|, \|c^0\| \leq \gamma \|c^1\|.$$

We made a modification from [33] by including a bound on $\|c_2\|$ and $\|c^0\|$. This additional bound is needed to show local testability.

Definition 2.14 ((Co)-Locally Minimal). *We say that* $c_1 \in \mathbb{F}_2^{X(1)}$ *is locally minimal if*

$$\forall e_2 \in \mathbb{F}_2^{X(2)}, \|e_2\| = 1 : \|c_1\| \leq \|c_1 + \partial_2 e_2\|.$$

Similarly, we say $c^1 \in \mathbb{F}_2^{X(1)}$ *is co-locally minimal if*

$$\forall e^0 \in \mathbb{F}_2^{X(0)}, \|e^0\| = 1 : \|c^1\| \leq \|c^1 + \delta^0 e^0\|.$$

Definition 2.15 (Small-Set (Co)-Locally-Minimal Expansion). *We say that* $X : \mathbb{F}_2^{X(2)} \xrightarrow{\partial_2} \mathbb{F}_2^{X(1)} \xrightarrow{\partial_1} \mathbb{F}_2^{X(0)}$ *is a* (α, β)*-small-set locally-minimal expander if*

$$\forall c_1 \in \mathbb{F}_2^{X(1)} \text{ s.t. } c_1 \text{ is locally minimal and } \|c_1\| < \alpha |X(1)| : \\ \|\partial_1 c_1\| \geq \beta \|c_1\|.$$

Similarly, X *is an* (α, β)*-small-set co-locally-minimal expander if*

$$\forall c^1 \in \mathbb{F}_2^{X(1)} \text{ s.t. } c^1 \text{ is locally minimal and } \|c^1\| < \alpha |X(1)| : \\ \|\delta^1 c^1\| \geq \beta \|c^1\| .$$

For our construction in Section 3 we will show that the chain complex has small-set co-locally-minimal expansion but not small-set locally-minimal expansion. This is roughly because in our construction $X(2), X(1)$, and $X(0)$ correspond to the faces, edges, and vertices. So e_2 corresponds to a face and e^0 corresponds to a vertex. Flipping $\partial_2 e_2$ only affects the four edges incident to the face, whereas $\delta^0 e^0$ affects the 2Δ edges incident to the vertex. Roughly, this means there are more freedom when flipping using $\delta^0 e^0$ than $\partial_2 e_2$. This is the rationale for why the chain complex does not (seem to) have small-set locally-minimal expansion.

Given the definitions, we now discuss their relations. The first lemma is between the expanders. The second and third lemma show that small-set boundary expansion implies systolic distance and local testability.

Lemma 2.16 (Small-Set (Co)-Locally-Minimal Expansion → Small-Set (Co)-Boundary Expansion). *Let* $c_2 \in \mathbb{F}_2^{X(2)}$ *be such that* $\|\partial_2 c_2\| \leq \mu \|c_2\|$. *Assume the gap between the possible values that* $\|c_1\|$ *can take, for* $c_1 \in \mathbb{F}_2^{X(1)}$, *is at least* ν *(i.e.* $|\|c_1\| - \|c_1'\|| \geq \nu$ *for any* c_1, c_1' *such that* $\|c_1\| \neq \|c_1'\|$.*)*

If X *has* (α, β)*-small-set locally-minimal expansion, then* X *has* $(\alpha/(1+\mu/\nu), \beta, 1/\nu)$*-small-set boundary expansion.*

The assumptions in the lemma often hold when the chain complex has bounded degree.

Proof. Given c_1, consider the local flipping process of the decoder of the expander code [53] which outputs c_2.

Algorithm 1: Local flip decoder. (Input: $c_1 \in \mathbb{F}_2^{X(1)}$)

(1) (Initialization) $c_1^0 := c_1$.
(2) (Main loop) In the i-th iteration, if there is e_2^i with $\|e_2^i\| = 1$ such that $\|c_1^i + \partial_2 e_2^i\| < \|c_1^i\|$, set $c_1^{i+1} := c_1^i + \partial_2 e_2^i$ and repeat.
(3) (End) Output $c_2 := \sum e_2^i$.

We show that c_2 satisfies the desired properties: $\|\partial_1 c_1\| \geq \beta \|c_1 + \partial_2 c_2\|$ and $\|c_2\| \leq \gamma \|c_1\|$.

We first show $\|c_2\| \leq \gamma \|c_1\|$. Because $\|c_2\| \leq \sum \|e_2^i\|$ is bounded by the number of iterations, and each iteration reduces $\|c_1^i\|$ by at least ν, we have $\|c_2\| \leq 1/\nu \|c_1\|$.

We now show $\|\partial_1 c_1\| \geq \beta \|c_1 + \partial_2 c_2\|$ Because the decoder cannot find e_2 and stops at $c_1 + \partial_2 c_2$, that means $c_1 + \partial_2 c_2$ is locally minimal. To apply small set locally minimal expansion, we suffice to show $c_1 + \partial_2 c_2$ has small size. Because $\|c_1 + \partial_2 c_2\| \leq \|c_1\| + \|\partial_2 c_2\| \leq \|c_1\| + \mu \|c_2\| \leq (1 + \mu/\nu)\|c_1\|$, when $\|c_1\| < \frac{\alpha}{1+\mu/\nu} |X(1)|$, $\|c_1 + \partial_2 c_2\|$ satisfies the small set condition. Therefore, $\|\partial_1 c_1\| \geq \beta \|c_1 + \partial_2 c_2\|$. □

Lemma 2.17 (Small-Set (Co)-Boundary Expansion → (Co)-Systolic Distance). *If* X *has* (α, β, γ)*-small-set boundary expansion, then* X *has systolic distance* α.

When the chain complex has bounded degree, this is equivalent to linear distance.

Proof. Suppose $c_1 \in Z_1$ and $\|c_1\| < \alpha |X(1)|$. Then by small set boundary expansion, there exists c_2, such that $0 = \|\partial_1 c_1\| \geq \beta \|c_1 + \partial_2 c_2\|$. This means $c_1 = \partial_2 c_2 \in B_1$. Therefore, for $c_1 \in Z_1 - B_1$ we have $\|c_1\| \geq \alpha |X(1)|$. □

Lemma 2.18 (Small-Set (Co)-Boundary Expansion → (Co)-Locally Testable Code). *If* X *has* (α, β, γ)*-small-set boundary expansion, then*

the classical code C with parity check matrix $H = \partial_2 : \mathbb{F}_2^{X(2)} \to \mathbb{F}_2^{X(1)}$ satisfies

$$\|Hv\| \geq \min\left(\frac{1}{\gamma}, \frac{\alpha|X(1)|}{|X(2)|}\right) \min_{c \in C} \|v - c\|.$$

When the chain complex has bounded degree, this is equivalent to the condition for local testability.

Proof. Denote $c_2 = v$. Let $c_1 = \partial_2 c_2 \in Z_1$. When $\|c_1\| < \alpha|X(1)|$, by small set boundary expansion, there exists c_2', such that $0 = \|\partial_1 c_1\| \geq \beta\|c_1 + \partial_2 c_2'\|$ and $\|c_2'\| \leq \gamma\|c_1\|$. This means $\partial_2 c_2' = c_1$ and $\partial_2(c_2 + c_2') = 0$. That is $c := c_2 + c_2' \in C$ and $\gamma\|c_1\| \geq \|c_2 - c\|$.

When $\|c_1\| \geq \alpha|X(1)|$, we set $c = 0$, and we have $\|c_1\| \geq (\alpha|X(1)|/|X(2)|)\|c_2\|$. Overall, we have $\|c_1\| \geq \min(1/\gamma, \alpha|X(1)|/|X(2)|) \min_{c \in C}\|c_2 - c\|$. □

3 LINEAR DIMENSION AND LINEAR DISTANCE

We give our construction of a quantum code and show that it leads to a family of quantum LDPC codes with linear dimension and distance. Additionally, we show that the associated chain complexes have various kinds of good expansion properties.

3.1 Construction

Let G be a finite group and A and B sets of generators for G that are closed under inverse and have cardinality $|A| = n_a$, $|B| = n_B$. Throughout we assume that $n_A = n_B$ and write $\Delta = n_A = n_B$. The construction uses Tanner codes over the 4-fold left-right Cayley complex $\mathcal{G}_2(G, A, B)$ with $|A| = |B| = \Delta$ and local tensor codes C_A, C_B with parity-check matrices $H_A : \mathbb{F}_2^\Delta \to \mathbb{F}_2^{m_a}$, $H_B : \mathbb{F}_2^\Delta \to \mathbb{F}_2^{m_b}$. The idea is to construct four Tanner codes and then combine them into a chain complex. We use the graphs $\mathcal{G}(E^-, F)$, $\mathcal{G}(E^|, F)$, $\mathcal{G}(V, E^-)$, $\mathcal{G}(V, E^|)$ induced from the left-right Cayley complex defined in Section 2.4 and the Tanner code construction in Section 2.7. The four Tanner codes we make use of are

$$\mathcal{T}(\mathcal{G}(E^-, F), H_A) : \mathbb{F}_2^F \to (\mathbb{F}_2^{m_a})^{E^-},$$

$$\mathcal{T}(\mathcal{G}(E^|, F), H_B) : \mathbb{F}_2^F \to (\mathbb{F}_2^{m_b})^{E^|},$$

$$\mathcal{T}(\mathcal{G}(V, E^-), H_B) : (\mathbb{F}_2^{m_a})^{E^-} \to (\mathbb{F}_2^{m_a \times m_b})^V,$$

$$\mathcal{T}(\mathcal{G}(V, E^|), H_A) : (\mathbb{F}_2^{m_b})^{E^|} \to (\mathbb{F}_2^{m_a \times m_b})^V.$$

To clarify the notation we explicitly spell out the map $\mathcal{T}(\mathcal{G}(E^-, F), H_A)$. By the definition of the Tanner construction, this map is the composition

$$\mathbb{F}_2^F \to (\mathbb{F}_2^\Delta)^{E^-} \to (\mathbb{F}_2^{m_a})^{E^-}$$

where the first map copies the value on the face to the horizontal edges incident to the face (each horizontal edge is incident to $|A| = \Delta$ faces, so each horizontal edge is valued in $\mathbb{F}_2^\Delta$) and the second map applies H_A to $\mathbb{F}_2^\Delta$ for each horizontal edge.

The resulting chain complex is

$$X : \mathbb{F}_2^F \xrightarrow{\partial_2} (\mathbb{F}_2^{m_a})^{E^-} \oplus (\mathbb{F}_2^{m_b})^{E^|} \xrightarrow{\partial_1} (\mathbb{F}_2^{m_a \times m_b})^V, \tag{6}$$

where

$$\partial_2(c_2) = (\mathcal{T}(\mathcal{G}(E^-, F), H_A)(c_2), \mathcal{T}(\mathcal{G}(E^|, F), H_B)(c_2))$$

$$\begin{array}{ccc} \mathbb{F}_2^F & \xrightarrow{\mathcal{T}(\mathcal{G}(E^|, F), H_B)} & (\mathbb{F}_2^{m_b})^{E^|} \\ \Big\downarrow{\scriptstyle \mathcal{T}(\mathcal{G}(E^-, F), H_A)} & & \Big\downarrow{\scriptstyle \mathcal{T}(\mathcal{G}(V, E^|), H_A)} \\ (\mathbb{F}_2^{m_a})^{E^-} & \xrightarrow[\mathcal{T}(\mathcal{G}(V, E^-), H_B)]{} & (\mathbb{F}_2^{m_a \times m_b})^V \end{array}$$

Figure 3: The chain complex as a composition of the Tanner codes.

and

$$\partial_1(c_1^-, c_1^|) = \mathcal{T}(\mathcal{G}(V, E^-), H_B)(c_1^-) + \mathcal{T}(\mathcal{G}(V, E^|), H_A)(c_1^|)$$

where $c_2 \in \mathbb{F}_2^F, c_1^- \in \mathbb{F}_2^{E^-}, c_1^| \in \mathbb{F}_2^{E^|}$.

We denote this chain complex as $X(\mathcal{G}_2, C_A, C_B)$, where $\mathcal{G}_2$ is a shorthand for $\mathcal{G}_2(G, A, B)$. (Later in the analysis we also consider the chain complex $X(\mathcal{G}_2, C_A^\perp, C_B^\perp)$ with the same graph but a different local code.) We use $C(\mathcal{G}_2, C_A, C_B)$ to denote the associated quantum CSS code (see Section 2.2), and often write only C for simplicity.

We end this section by commenting on the way to obtain an explicit family of groups and generating sets that satisfy all the expansion properties required for the quantum code C to have linear distance and linear-time decoding, as shown in the following sections. This relies on having an explicit construction of large Ramanujan graphs [52] and the existence of (at least) one good local code pair Corollary 2.11. First, we discuss the graph. The graphs depend on the group G and generators A, B. The group G belongs to an infinite family of groups with generators A, B of fixed size Δ such that $\mathrm{Cay}(G, A)$, $\mathrm{Cay}(G, B)$ are $\lambda = 2\sqrt{\Delta - 1}$-spectral expanders. Second, we discuss the base codes. As shown in Section 3.4, to show constant systolic and co-systolic distance we need (C_A, C_B) and its dual code $(C_A^\perp, C_B^\perp)$ to have distance d_1 and robustness d_2 satisfying $d_1 d_2 - \lambda d_2 - 8\lambda\Delta > 0$. From Corollary 2.11 we know that for fixed ρ_a, ρ_b there exist constants δ_1, δ_2 such that for large enough Δ, $C_A, C_B, C_A^\perp, C_B^\perp$ have distance $\delta_1\Delta$ and (C_A, C_B), $(C_A^\perp, C_B^\perp)$ have robustness $\delta_2\Delta$. Because of the scaling $\lambda = \Theta(\Delta^{1/2}), d_1 = \Theta(\Delta), d_2 = \Theta(\Delta)$, for some large but fixed Δ, there exists a good local code pair (C_A, C_B). This good code pair can be found by brute forcing all the possible code pairs. Because Δ is fixed, the family of chain complexes remains explicit.

3.2 Notation

The following important notations are used for the analysis. First, we describe the notation that extracts the local structure. Given $c_2 \in \mathbb{F}_2^F$, we denote $c_2(f) \in \mathbb{F}_2$ as the value of c_2 at $f \in F$. Similarly, for $c_1 \in (\mathbb{F}_2^{m_a})^{E^-} \oplus (\mathbb{F}_2^{m_b})^{E^|}$ and $c_0 \in (\mathbb{F}_2^{m_a \times m_b})^V$, one has $c_1(e^-) \in \mathbb{F}_2^{m_a}$ for $e^- \in E^-$, $c_1(e^|) \in \mathbb{F}_2^{m_b}$ for $e^| \in E^|$, and $c_0(v) \in \mathbb{F}_2^{m_a \times m_b}$ for $v \in V$. We also write $c^1(E_{*0}(V_{00})) \in \mathbb{F}_2^{m_a \times n_a}$ to denote the entries on $E_{*0}(V_{00})$, where recall that this set is defined in Section 2.4. Notice that $E_{*0}(V_{00})$ contains n_a edges and each edge gives a vector of size m_a.

Second, we describe notation for measuring the size, or norm, of elements of the complex X. The norm is defined as the number

of non-zero geometric objects, i.e. $\|c_2\|_F = |\{f \in F : c_2(f) \neq 0\}|$, $\|c_1\|_E = |\{e \in E : c_1(e) \neq 0\}|$, $\|c_0\|_V = |\{v \in V : c_0(v) \neq 0\}|$. We also write $\|c_1(E_{*0}(v_{00}))\|_E = |\{e \in E_{*0}(v_{00}) : c_1(e) \neq 0\}|$.

An element $c_2 \in \mathbb{F}_2^F$ is usually indexed by F, leading to the norm $\|c_2\|_F$ as defined above, it can also naturally be indexed by E_{*0} through $c_2(e_{*0}) = c_2(F(e_{*0}))$. This allows us to define $\|c_2\|_{E_{*0}}$. The difference between the two norms is analogous to the difference between the different variants of the Hamming norm introduced in Definition 2.7. Similarly, an element $s^2 \in (\mathbb{F}_2^{n_a})^{E^-} \times (\mathbb{F}_2^{n_b})^{E^|}$ is indexed by E, but notice that for any $e_{*0} \in E_{*0}$, $s^2(e_{*0})$ can be indexed by $F(e_{*0})$. This allows us to write $s^2(e_{*0}, f) \in \mathbb{F}_2$ for $f \in F(e_{*0})$. This leads to the definition $EF = E^-F \cup E^|F = \{(e, f) \in E \times F : f \in F(e)\}$, where E^-F and $E^|F$ specialize to horizontal and vertical edges. So s^2 can be indexed by EF and this leads to the norm $\|s^2\|_{EF} = |\{(e, f) \in EF : s^2(e, f) \neq 0\}|$. We will also write $\|s^2(E^{*0})\|_F$ for $\|s^2(E^{*0})\|_{EF}$; this is because when the edges are restricted to E^{*0} we have $E^{*0}F \cong F$. One can similarly define VE, VF and their corresponding norms.

Finally, the last notation we discuss is with regard to H_A and H_B. By thinking of F as being indexed by E_{0*}, we have $H_A^{\uparrow} : \mathbb{F}_2^F \cong (\mathbb{F}_2^{n_a})^{E_{0*}} \to (\mathbb{F}_2^{m_a})^{E_{0*}}$. Similarly, by thinking of F as being indexed by E_{1*}, we have $H_A^{\downarrow} : \mathbb{F}_2^F \cong (\mathbb{F}_2^{n_a})^{E_{1*}} \to (\mathbb{F}_2^{m_a})^{E_{1*}}$. We can also define $H_B^{\leftarrow}$ and $H_B^{\rightarrow}$. When the context is clear, we sometime hide the arrows.

3.3 Dimension and Low Density

Before measuring the dimension of the quantum code based on X, we verify that X is a well-defined chain complex. For this it suffices to show that for each $f \in F$ and $v \in V$, the restriction $(\partial_1\partial_2)_f^v : \mathbb{F}_2 \to \mathbb{F}_2^{m_a \times m_b}$ is 0. To do so, we first recall the submatrices of the Tanner code described in Section 2.7.

Given elements $e^- \in E^-$ and $f \in F$, the submatrix $\mathcal{T}(\mathcal{G}(E^-, F), H_A)_f^{e^-} : \mathbb{F}_2 \to \mathbb{F}_2^{m_a}$ is 0 when e^- and f are not incident. When e^- and f are incident, say $e^- = ((g, gb), 0*)$, $f = (g, ag, gb, agb)$, we have

$$\mathcal{T}(\mathcal{G}(E^-, F), H_A)_f^{e^-} = H_A(\bar{a}) : \mathbb{F}_2 \to \mathbb{F}_2^{m_a}$$

where $\bar{a}$ is the basis vector of $\mathbb{F}_2^A \cong \mathbb{F}_2^\Delta$ corresponding to the element $a \in A$.

Similarly, given elements $v \in V$ and $e^- \in E^-$, the submatrix $\mathcal{T}(\mathcal{G}(V, E^-), H_B)_{e^-}^v : \mathbb{F}_2^{m_a} \to \mathbb{F}_2^{m_a \times m_b}$ is 0 when v and e^- are not incident. When v and e^- are incident, say $v = (g, 00)$, $e^- = ((g, gb), 0*)$, we have

$$\mathcal{T}(\mathcal{G}(V, E^-), H_B)_{e^-}^v = - \otimes H_B(\bar{b}) : \mathbb{F}_2^{m_a} \to \mathbb{F}_2^{m_a \times m_b}$$

where $\bar{b}$ is the basis vector of $\mathbb{F}_2^B \cong \mathbb{F}_2^\Delta$ and $-$ is the placeholder where $- \otimes H_B(\bar{b}) : v \mapsto v \otimes H_B(\bar{b})$.

Lemma 3.1. *X is a well-defined chain complex, i.e.*

$$(\partial_1\partial_2)_f^v : \mathbb{F}_2 \to \mathbb{F}_2^{m_a \times m_b} = 0 .$$

Proof. Because $\partial_1\partial_2 = \mathcal{T}(\mathcal{G}(V, E^-), H_B)\mathcal{T}(\mathcal{G}(E^-, F), H_A) + \mathcal{T}(\mathcal{G}(V, E^|), H_A)\mathcal{T}(\mathcal{G}(E^|, F), H_B)$ it suffices to compute $(\mathcal{T}(\mathcal{G}(V, E^-), H_B)\mathcal{T}(\mathcal{G}(E^-, F), H_A))_f^v$ and $(\mathcal{T}(\mathcal{G}(V, E^|), H_A)\mathcal{T}(\mathcal{G}(E^|, F), H_B))_f^v$. Now, by matrix multiplication, $(\mathcal{T}(\mathcal{G}(V, E^-), H_B)\mathcal{T}(\mathcal{G}(E^-, F), H_A))_f^v = \sum_{e^- \in E^-} \mathcal{T}(\mathcal{G}(V, E^-), H_B)_f^{e^-} \mathcal{T}(\mathcal{G}(E^-, F), H_A)_{e^-}^v$. We consider the following two cases.

When v and f are not incident, there is no e^- for both $\mathcal{T}(\mathcal{G}(V, E^-), H_B)_f^{e^-}$ and $\mathcal{T}(\mathcal{G}(E^-, F), H_A)_{e^-}^v$ to be non-zero, so $(\mathcal{T}(\mathcal{G}(V, E^-), H_B)\mathcal{T}(\mathcal{G}(E^-, F), H_A))_f^v = 0$. Similarly, $(\mathcal{T}(\mathcal{G}(V, E^|), H_A)\mathcal{T}(\mathcal{G}(E^|, F), H_B))_f^v = 0$. So $(\partial_1\partial_2)_f^v = 0$ in the case when v and f are not incident.

When v and f are incident, suppose $v = (g, 00)$ and $f = (g, ag, gb, agb)$. We define $e^- = ((g, gb), 0*)$ and $e^| = ((g, ag), *0)$. Because e^- is the only edge in E^- that is incident to both v and f, we have

$$\begin{aligned}
&(\mathcal{T}(\mathcal{G}(V, E^-), H_B)\mathcal{T}(\mathcal{G}(E^-, F), H_A))_f^v \\
&= \mathcal{T}(\mathcal{G}(V, E^-), H_B)_{e^-}^v \mathcal{T}(\mathcal{G}(E^-, F), H_A)_f^{e^-} \\
&= H_A(\bar{a}) \otimes H_B(\bar{b}).
\end{aligned}$$

Similarly,

$$\begin{aligned}
&(\mathcal{T}(\mathcal{G}(V, E^|), H_A)\mathcal{T}(\mathcal{G}(E^|, F), H_B))_f^v \\
&= \mathcal{T}(\mathcal{G}(V, E^|), H_A)_{e^|}^v \mathcal{T}(\mathcal{G}(E^|, F), H_B)_f^{e^|} \\
&= H_A(\bar{a}) \otimes H_B(\bar{b}).
\end{aligned}$$

This implies $(\partial_1\partial_2)_f^v = 0$ and implies X is a chain complex. □

We now check that the boundary maps ∂_2 and ∂_1 have bounded number of non-zero entries in each column and row.

Lemma 3.2. *The code C is low density, i.e. the maps ∂_2 and ∂_1 have at most 4Δ nonzero entries in each row and column.*

Proof. The result follows because the left-right Cayley graph has bounded degree and the non-zero entry appears only when there is an incident relation. We call $F, E^- \times [m_a] \cup E^| \times [m_b]$, and $V \times [m_a] \times [m_b]$ the face bits, the edge bits, and the vertex bits. And we say that a face bit is incident to an edge bit if the corresponding entry in the boundary map is non-zero.

We first consider ∂_2. Each face is incident to 4 edges and each edge is incident to Δ faces. Now $\mathcal{T}(\mathcal{G}(E^-, F), H_A)_f^{e^-} : \mathbb{F}_2 \to \mathbb{F}_2^{m_a}$ and $\mathcal{T}(\mathcal{G}(E^|, F), H_B)_f^{e^|} : \mathbb{F}_2 \to \mathbb{F}_2^{m_b}$ have ≤ 1 non-zero entry in each row and $\leq \max(m_a, m_b)$ non-zero entries in each column. So each face bit is incident to $\leq 4\max(m_a, m_b)$ edge bits and each edge bit is incident to $\leq \Delta$ face bits.

We now consider ∂_1. Each edge is incident to 2 vertices and each vertex is incident to 2Δ edges. Now $\mathcal{T}(\mathcal{G}(V, E^-), H_B)_{e^-}^v : \mathbb{F}_2^{m_a} \to \mathbb{F}_2^{m_a \times m_b}$ and $\mathcal{T}(\mathcal{G}(V, E^|), H_A)_{e^|}^v : \mathbb{F}_2^{m_b} \to \mathbb{F}_2^{m_a \times m_b}$ have ≤ 1 non-zero entry in each row and $\leq \max(m_a, m_b)$ non-zero entries in each column. So each edge bit is incident to $\leq 2\max(m_a, m_b)$ vertex bits and each vertex bit is incident to $\leq 2\Delta$ edge bits. □

It is easy to check that the quantum code has linear dimension.

Lemma 3.3. *The code C has rate at least*

$$\frac{-(2\rho_a - 1)(2\rho_b - 1)}{2(2 - \rho_a - \rho_b)} .$$

Proof. The rate is at least

$$\frac{|X(1)|-|X(2)|-|X(0)|}{|X(1)|} = \frac{-(\Delta-2m_a)(\Delta-2m_a)|G|}{2(m_a+m_b)\Delta|G|} = \frac{-(2\rho_a-1)(2\rho_b-1)}{2(2-\rho_a-\rho_b)} .$$

□

Note that one can achieve any rate in $(0, 1/2)$ by choosing corresponding ρ_a and ρ_b.

3.4 Distance

A quantum CSS code has linear distance if and only if the chain complex X has constant systolic and co-systolic distance. We start with a general theorem, Theorem 3.4 that shows a certain co-expansion property of the complex $X(\mathcal{G}_2, C_A, C_B)$ defined in (6). The property of having linear X-distance for C, i.e. linear co-systolic distance of X, follows almost immediately and is shown in Corollary 3.5. The argument for showing linear Z-distance for C, i.e. linear systolic distance for X, is more involved and proceeds by reduction to the co-systolic distance. This is shown in Theorem 3.8. After having shown the distance properties, we show that the co-expansion property shown in Theorem 3.4 also implies small-set expansion properties for X.

3.4.1 *Co-expansion and co-systolic distance.*

We start with the main theorem on co-expansion.

Theorem 3.4 (Co-Expansion). *Given Δ-regular λ-spectral expander graphs $\mathrm{Cay}(G, A)$, $\mathrm{Cay}(G, B)$ and linear codes $C_A^\perp, C_B^\perp$ of length Δ with distance d_1 and $(C_A^\perp, C_B^\perp)$ with robustness d_2. If $c^1 \in \mathbb{F}_2^{X(1)}$ is co-locally minimal, then*

$$\|\delta^1 c^1\|_F \geq \frac{d_1d_2-\lambda d_2-8\lambda\Delta}{4d_2+8\Delta}\|c^1\|_E - \frac{\Delta d_2/2+2\Delta}{4d_2+8\Delta}\frac{\|c^1\|_E^2}{|G|} . \quad (7)$$

Corollary 3.5. *Under the same assumptions as Theorem 3.4, suppose further that $d_1d_2-\lambda d_2-8\lambda\Delta > 0$. Then the co-chain complex (6) has co-systolic distance at least $\frac{\eta}{2\Delta(m_a+m_b)}$, where $\eta := \frac{d_1d_2-\lambda d_2-8\lambda\Delta}{\Delta d_2/2+2\Delta}$.*

Proof. When c^1 is a non-zero co-cycle $c^1 \in Z^1 - 0$, (7) implies

$$\frac{\Delta d_2/2+2\Delta}{4d_2+8\Delta}\frac{\|c^1\|_E^2}{|G|} \geq \frac{d_1d_2-\lambda d_2-8\lambda\Delta}{4d_2+8\Delta}\|c^1\|_E ,$$

which gives

$$\|c^1\|_E \geq \frac{d_1d_2-\lambda d_2-8\lambda\Delta}{\Delta d_2/2+2\Delta}|G| := \eta|G| = \frac{\eta}{2\Delta(m_a+m_b)}|X(1)| .$$

□

We now move on to prove the theorem.

Proof of Theorem 3.4. Let c^1 be co-locally minimal and $c^2 = \delta^1 c^1$. Let $\mathcal{E} \subset E$ be the support of c^1, i.e. $\mathcal{E} = \{e \in E : c^1(e) \neq 0\}$. (Recall that $c^1(e_{*0}), c^1(e_{*1}) \in \mathbb{F}_2^{m_b}$ and $c^1(e_{0*}), c^1(e_{1*}) \in \mathbb{F}_2^{m_a}$.) The proof strategy is to count the number of "neighbors" between $\mathcal{E}$, for some appropriate neighborhood structure. The expansion of the graph gives an upper bound on the number of "neighbors" and the distance and the robustness of the local code give a lower bound. Comparing the two bounds gives Equation (7).

Step 1: Define "neighbors" M. Recall the adjacency matrices M_0 and M_1 defined in Lemma 2.5 and Lemma 2.4 respectively. We describe the neighborhood structure through the matrix

$$M = d_2M_1 + M_0 \in \mathbb{R}^{E\times E} .$$

Let $1_{\mathcal{E}} \in \mathbb{F}_2^E$ be the indicator vector for $\mathcal{E}$.

Step 2: Upper bound from expansion. Combining Lemma 2.5 and Lemma 2.4,

$$1_{\mathcal{E}}^T M 1_{\mathcal{E}} \leq \lambda(d_2+8\Delta)|\mathcal{E}| + \frac{\Delta}{|G|}\left(\frac{d_2}{2}+2\right)|\mathcal{E}|^2 . \quad (8)$$

Step 3: Lower bound from distance and robustness. We show a lower bound on $1_{\mathcal{E}}^T M 1_{\mathcal{E}}$ using the distance and the robustness of the local tensor code. We start with two claims. The first claim uses the distance property of $C_B^\perp$.

Claim 3.6. *For any edge $e_{*0} \in E_{*0}$ it holds that*

$$\|c^2(F(e_{*0}))\|_F + \|c^1(E_{*1}(e_{*0}))\|_E + \|c^1(E_{0*}(e_{*0}))\|_E + \|c^1(E_{1*}(e_{*0}))\|_E \geq d_1\|c^1(e_{*0})\|_E . \quad (9)$$

Proof. The distance property of $C_B^\perp$ immediately implies that

$$\|s^2(e_{*0})\|_F \geq d_1\|c^1(e_{*0})\|_E . \quad (10)$$

Recall that

$$c^2 = s^2(E_{*0}) + s^2(E_{*1}) + s^2(E_{0*}) + s^2(E_{1*}) . \quad (11)$$

Thus each non-zero entry $f = (g, ag, gb, agb)$ of $s^2(e_{*0})$, where $e_{*0} = (g, ag)$, is either a non-zero entry in c^2 or is canceled by a term in $s^2(E_{*1})$, $s^2(E_{0*})$, or $s^2(E_{1*})$ that contributes to the entry at f. Such a term, say $s^2(e_{*1}) \neq 0$, must have its edge e_{*1} incident to the face f which is incident to e_{*0}, i.e. $e_{*1} \in E_{*1}(e_{*0})$. Therefore, each cancellation contributes to $\|s^2(E_{*1}(e_{*0}))\|_E$, $\|s^2(E_{0*}(e_{*0}))\|_E$, or $\|s^2(E_{1*}(e_{*0}))\|_E$. Notice that $s^2(e_{*1}) \neq 0 \iff c^1(e_{*1}) \neq 0$. Thus from (11) we get that

$$\|c^2(F(e_{*0}))\|_F + \|c^1(E_{*1}(e_{*0}))\|_E + \|c^1(E_{0*}(e_{*0}))\|_E + \|c^1(E_{1*}(e_{*0}))\|_E \geq \|c^1(E_{*0}(e_{*0}))\|_E .$$

Combined with (10), this shows the claim. □

The second claim uses the robustness property of $\Sigma(C_A^T, C_B^T)$.

Claim 3.7. *For any vertex $v_{00} \in V_{00}$ it holds that*

$$\|c^2(F(v_{00}))\|_F + \|c^1(E_{*1}(v_{00}))\|_E + \|c^1(E_{1*}(v_{00}))\|_E \geq d_2(\|c^1(E_{*0}(v_{00}))\|_E + \|c^1(E_{0*}(v_{00}))\|_E) . \quad (12)$$

Similarly, for any vertex $v_{10} \in V_{10}$ it holds that

$$\|c^2(F(v_{10}))\|_F + \|c^1(E_{*1}(v_{10}))\|_E + \|c^1(E_{0*}(v_{10}))\|_E \geq d_2(\|c^1(E_{*0}(v_{10}))\|_E + \|c^1(E_{1*}(v_{10}))\|_E) . \quad (13)$$

Proof. The proof is similar to the previous claim, using the robustness property of $(C_A^\perp, C_B^\perp)$ instead of the distance property of C_B. □

Let $e_{*0} \in E_{*0}$ have endpoints $v_{00} \in V_{00}$ and $v_{10} \in V_{10}$. Using the definition of $M = d_2 M_1 + M_0$,

$$\begin{aligned}
&1_{\mathcal{E}}^T M 1_{e_{*0}} \\
&= 1_{\mathcal{E}}^T \big(d_2 M_1 + M_0\big) 1_{e_{*0}} \\
&= d_2 \|c^1(E_{*1}(e_{*0}))\|_E + \|c^1(E_{*1}(v_{00}))\|_E + \|c^1(E_{1*}(v_{00}))\|_E \\
&\quad + \|c^1(E_{*1}(v_{10}))\|_E + \|c^1(E_{0*}(v_{10}))\|_E \\
&\geq d_2 \|c^1(E_{*1}(e_{*0}))\|_E + d_2 \|c^1(E_{*0}(v_{00}))\|_E + d_2 \|c^1(E_{0*}(v_{00}))\|_E \\
&\quad + d_2 \|c^1(E_{*0}(v_{10}))\|_E + d_2 \|c^1(E_{1*}(v_{10}))\|_E \\
&\quad - |c^2(F(v_{00}))| - |c^2(F(v_{10}))| \\
&\geq d_2 \|c^1(E_{*1}(e_{*0}))\|_E + d_2 \|c^1(E_{0*}(v_{00}))\|_E + d_2 \|c^1(E_{1*}(v_{10}))\|_E \\
&\quad - \|c^2(F(v_{00}))\|_F - \|c^2(F(v_{10}))\|_F \\
&= d_2 \|c^1(E_{*1}(e_{*0}))\|_E + d_2 \|c^1(E_{0*}(e_{*0}))\|_E + d_2 \|c^1(E_{1*}(e_{*0}))\|_E \\
&\quad - \|c^2(F(v_{00}))\|_F - \|c^2(F(v_{10}))\|_F \\
&\geq d_1 d_2 \|c^1(e_{*0})\|_E - d_2 \|c^2(F(e_{*0}))\|_F \\
&\quad - \|c^2(F(v_{00}))\|_F - \|c^2(F(v_{10}))\|_F \,.
\end{aligned}$$

Here, the first inequality uses (12) and (13), the second inequality drops non-negative terms, and the last inequality follows from (9). Summing over all edges e_{*0} and analogous inequalities shown for edges e_{*1}, e_{0*} and e_{1*} we obtain

$$1_{\mathcal{E}}^T M 1_{\mathcal{E}} \geq d_1 d_2 \|c^1\|_E - 4 d_2 \|c^2\|_F - 8\Delta \|c^2\|_F \,, \tag{14}$$

where the factor of 4 is because each face is counted 4 times by the 4 edges incident to the face, and the factor of 8Δ because each vertex is summed over 2Δ times by the 2Δ edges incident to the vertex and each face is incident to 4 vertices.

Step 4: Combine the upper and lower bounds. Combining (8) and (14),

$$\begin{aligned}
d_1 d_2 \|c^1\|_E - (4d_2 + 8\Delta)\|c^2\|_F &\leq 1_{\mathcal{E}}^T M 1_{\mathcal{E}} \\
&\leq \lambda(d_2 + 8\Delta)\|c^1\|_E + \frac{\Delta}{|G|}\left(\frac{d_2}{2} + 2\right)\|c^1\|_E^2 \,,
\end{aligned}$$

which implies

$$\|c^2\|_F \geq \frac{d_1 d_2 - \lambda d_2 - 8\lambda\Delta}{4d_2 + 8\Delta}\|c^1\|_E - \frac{\Delta d_2/2 + 2\Delta}{4d_2 + 8\Delta}\frac{\|c^1\|_E^2}{|G|} \,.$$

This concludes the proof of (7). □

3.4.2 Expansion and systolic distance. The second main theorem for this section shows that systolic distance follows from cp-systolic distance. In fact, we will prove a stronger statement which also shows that expansion follows from co-expansion.

Theorem 3.8 (Co-Expansion → Expansion)**.** *If $X(\mathcal{G}_2, C_A^\perp, C_B^\perp)$ has co-systolic distance $\frac{\eta}{2\Delta(k_a+k_b)}$, then $X(\mathcal{G}_2, C_A, C_B)$ has systolic distance $\frac{\eta}{2\Delta(m_a+m_b)}$.*

Furthermore, if $X(\mathcal{G}_2, C_A^\perp, C_B^\perp)$ is a $(\frac{\eta}{4\Delta(k_a+k_b)}, \beta, \gamma)$-small-set co-boundary expander, then $X(\mathcal{G}_2, C_A, C_B)$ is a $(\frac{\eta}{4\Delta(m_a+m_b)}, \frac{1}{\Delta^2+\Delta+\frac{\Delta^3}{\beta}}, \Delta + \Delta^2\gamma)$-small-set boundary expander.

We now have all the ingredients to state the property of linear distance for our quantum code.

Corollary 3.9. *Assume that $\mathrm{Cay}(G, A), \mathrm{Cay}(G, B)$ are $\lambda = \Theta(\sqrt{\Delta})$-spectral expanders and that C_A, C_B have distance $d_1, d_2 = \Theta(\Delta)$. Then the quantum code C has linear distance.*

Proof. The assumptions made in the corollary imply that for large enough Δ, $d_1 d_2 - \lambda d_2 - 8\lambda\Delta > 0$. By Theorem 3.4, $X(\mathcal{G}_2, C_A, C_B)$ and $X(\mathcal{G}_2, C_A^\perp, C_B^\perp)$ have linear co-systolic distance. By Theorem 3.8, $X(\mathcal{G}_2, C_A, C_B)$ has linear systolic distance. Therefore, C has distance $\frac{d_1 d_2 - \lambda d_2 - 8\lambda\Delta}{\Delta^2(m_a+m_b)(d_2+4)} n$. □

The proof of Theorem 3.8 can be found in [18].

4 LINEAR TIME DECODER

In this section we construct a linear time decoder for the quantum code C introduced in Section 3.1. As discussed in the introduction, one can separate the task of decoding into two. We call one of them the decoder and the other the co-decoder: the decoder recovers $\tilde{c}_1$ given the syndrome $\partial_1 c_1$ such that $\tilde{c}_1 \in c_1 + B_1$; the co-decoder recovers $\tilde{c}^1$ given the syndrome $\delta^1 c^1$ such that $\tilde{c}^1 \in c^1 + B^1$.

This section parallels the section on distance with similar proof techniques. We first show the existence of a linear time co-decoder. Then we use the linear time co-decoder to obtain a linear time decoder.

Theorem 4.1 (Co-Decoder)**.** *$X(\mathcal{G}_2, C_A, C_B)$ has a linear time co-decoder up to distance $\frac{\kappa}{2\Delta(m_a+m_b)}|X(1)|$ where $\kappa = \frac{\Delta d_2/2+2\Delta}{8\Delta d_2+16\Delta^2}\eta'\eta$, $\eta = \frac{d_1 d_2 - \lambda d_2 - 8\lambda\Delta}{\Delta d_2/2+2\Delta}$, $\eta' = \frac{d_1 d_2/4 - \lambda d_2/2 - 8\lambda\Delta}{\Delta d_2/4+2\Delta}$.*

Theorem 4.2 (Co-Decoder → Decoder)**.** *If $X(\mathcal{G}_2, C_A^\perp, C_B^\perp)$ has a linear time co-decoder up to distance $\eta''|G|$, then $X(\mathcal{G}_2, C_A, C_B)$ has a linear time decoder up to distance $\frac{\eta''}{6+4\Delta/d_2}|G|$.*

Together we obtain a linear time decoder for $C(\mathcal{G}_2, C_A, C_B)$ up to distance $\frac{\kappa}{4\Delta(m_a+m_b)(6+4\Delta/d_2)}|X(1)|$. The full proof can be found in [18].

4.1 Co-Decoder

Theorem 4.1 is the main theorem we will show in this subsection. We discuss the construction, the correctness, and the running time of the decoder which together proves the theorem.

Construction: The co-decoder in the direction of the co-chain complex $\mathbb{F}_2^{X(2)} \leftarrow \mathbb{F}_2^{X(1)} \leftarrow \mathbb{F}_2^{X(0)}$ is the small-set-flip decoder introduced in [41]. The small-set-flip decoder is a generalization of the local-flip decoder for the expander codes [53] where the decoder observes a local region and make local changes that reduce the weight of the syndrome.

Algorithm 2: Simple small-set-flip decoder. (Input: $c^2 \in \mathbb{F}_2^{X(2)}$)

(1) (Initialization) $c_0^2 := c^2$.
(2) (Main loop) In the i-th iteration, if there is a vertex v_i with e_i^1 supported on $E(v_i)$ such that $|c_i^2 + \delta^1 e_i^1| < |c_i^2|$, set $c_{i+1}^2 := c_i^2 + \delta^1 e_i^1$ and repeat.
(3) (End) Output $\tilde{c}^1 := \sum e_i^1$.

Besides these variables, we define other variables not directly known by the decoder. Let c_0^1 be the minimal chain in $c^1 + B^1$ and c_{i+1}^1 be the minimal chain in $c_i^1 + e_i^1 + B^1$. One can interpret c_i^1 as the error at the i-th iteration and c_i^2 as corresponding syndrome. Note that the decoder knows the syndrome c_i^2 but not the error c_i^1.

Recall that the final syndrome of a local-flip decoder is locally minimal. Similarly, the final syndrome of a small-set-flip decoder satisfies a similar property which we call extended local minimality.

Definition 4.3 (Extended Co-Locally Minimal)**.** *We say $c^2 \in \mathbb{F}_2^{X(2)}$ is co-locally minimal from $X(0)$ if*

$$\forall v \in V, c^1 \in \mathbb{F}_2^{X(1)}, \mathrm{supp}(c^1) \subset E(v) : \|c^2\|_F \leq \|c^2 + \delta^1 c^1\|_F,$$

where $E(v) \subset E$ are the edges incident to v.

The analysis for correctness and time complexity of the co-decoder can be found in [18].

5 OPTIMAL ROBUST TENSOR CODES

This section shows that random codes have linear robustness with high probability. We improve on the result in [44, 50] by using the idea of puncturing and a new counting argument.

Recall that C_A and C_B are linear codes of length n_a and n_b with rate ρ_a and ρ_b. For simplicity we assume that $n_a = n_b = \Delta$. An s-punctured code of C_A is obtained by first choosing s coordinates $I_a \subset [n_a]$ then consider the codewords of C_A restricted to $[n_a] - I_a$. Notice that $\|c\|_{[n_a]\times[n_b]} = |c|$ is identical to the Hamming weight, so we will mostly use $|c|$ in this section to simplify the notation.

We now recall Theorem 2.10, which is the main theorem to prove in this section.

Theorem 2.10 (Random codes are robust)**.** *Fix $\rho_a, \rho_b \in (0,1)$, let $\delta_1 \in (0, 1/2), \delta_2 \in (0, \delta_1(1-\delta_1/2)/8)$ satisfy*

$$2h(\delta_1/2) + 2(1-\delta_1/2)h\left(\frac{4\delta_2}{\delta_1(1-\delta_1/2)}\right) < \frac{3}{4}\frac{(1-\delta_1/2-\rho_a)(1-\delta_1/2-\rho_b)}{1-\delta_1/2} \quad (5)$$

where $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$.[3] Let C_A, C_B be random codes sampled from the uniform distribution with length Δ and dimensions $\rho_a\Delta, \rho_b\Delta$. Then as Δ goes to infinity, with probability tending to 1, C_A, C_B have distance $d_1 = \delta_1\Delta$ and (C_A, C_B) is $d_2 = \delta_2\Delta$-robust.

The proof follows a similar strategy in [44, 50], where the key is to show that a codeword with a small weight $|c| < w = \Theta(\Delta^2)$ is "structured", i.e. c is only supported on a few columns and a few rows, with high probability.

To show codewords with small weights are "structured", we show all non-zero codewords in a random code have some column or row with large weight with high probability. Because the punctured code of a random code is still roughly a random code, the same property also applies to its punctured codes. Now, since we assumed the codeword $c \in \Sigma(C_A, C_B)$ has small weight, we can remove a few columns and rows with large weights, such that the rest have small weight in all columns and rows. We then apply the property of the punctured code above which implies the rest is 0, so c is only supported on those removed columns and rows, i.e. c is "structured".

When c is "structured", one can then find c_a supported on the few columns and c_b supported on the few rows. This means the cancellation in c_a+c_b could only happen in the intersection of those columns and rows which is small. Since each column of c_a is a codeword, when the distance is large, $|c_a| \geq d_1\|c_a\|_{[n_b]} = \Theta(\Delta)\|c_a\|_{[n_b]}$. This implies codewords with small weight satisfy the inequality for robustness $|c| = |c_a| + |c_b| -$ small number of cancellations $\geq \Theta(\Delta)(\|c_a\|_{[n_b]} + \|c_b\|_{[n_a]})$.

When c has large weight $|c| \geq w = \Theta(\Delta^2)$, because $\|c_a\|_{[n_b]} + \|c_b\|_{[n_a]} \leq 2\Delta$, the inequality for robustness $|c| \geq d_2(\|c_a\|_{[n_b]} + \|c_b\|_{[n_a]})$ is easily satisfied by setting $d_2 = w/(2\Delta) = \Theta(\Delta)$.

We state the two lemmas. The proof of the theorem and the two lemmas can be found in [18]. The first lemma says each non-zero codeword has at least one row or column with large weight (which implies codewords with small weight are "structured"). The second lemma says "structured" codewords satisfy robustness.

Lemma 5.1. *Fix $\rho_a, \rho_b \in (0,1)$, let $\sigma \in (0,1), \tau \in (0, (1-\sigma)/2)$ satisfy*

$$2h(\sigma) + 2(1-\sigma)h\left(\frac{\tau}{1-\sigma}\right) < \frac{3}{4}\frac{(1-\sigma-\rho_a)(1-\sigma-\rho_b)}{1-\sigma}.$$

Let C_A, C_B be random codes sampled from the uniform distribution with length Δ and dimensions $k_a = \rho_a\Delta, k_b = \rho_b\Delta$. Then as Δ goes to infinity, with probability tending to 1, the following holds: for any $s = \sigma\Delta$-punctured code C_A', C_B', all non-zero codewords in $\Sigma(C_A', C_B')$ have at least one row or one column with weight $\geq t = \tau\Delta$. In other words, if a codeword in $\Sigma(C_A', C_B')$ has all its rows and columns with weight $< t$, then the codeword is 0.

Lemma 5.2 (Modification of [50, Lemma 8] or [44, Lemma 30])**.** *Suppose C_A and C_B have distance d_1. If $c \in \Sigma(C_A, C_B)$ is supported on $I_a \times [n_b] \cup [n_a] \times I_b$ and $|I_a|, |I_b| < d_1$, then there exists $c_a \in C_A \otimes \mathbb{F}_2^{n_b}$ supported on $[n_a] \times I_b$ and $c_b \in \mathbb{F}_2^{n_a} \otimes C_B$ supported on $I_a \times [n_b]$ such that $c = c_a + c_b$.*

Furthermore, if $|I_a|, |I_b| < d_1/2$, we have

$$|c| \geq \frac{d_1}{2}(\|c_a\|_{[n_b]} + \|c_b\|_{[n_a]}).$$

[3] The allowed range for δ_2 is chosen such that the argument in $h(\cdot)$ is valued between $(0, 1/2)$.

REFERENCES

[1] Dorit Aharonov, Itai Arad, and Thomas Vidick. 2013. Guest column: the quantum PCP conjecture. *Acm sigact news* 44, 2 (2013), 47–79. https://doi.org/10.1145/2491533.2491549

[2] Dorit Aharonov and Lior Eldar. 2015. Quantum locally testable codes. *SIAM J. Comput.* 44, 5 (2015), 1230–1262. https://doi.org/10.1137/140975498

[3] Vedat Levi Alev and Lap Chi Lau. 2020. Improved Analysis of Higher Order Random Walks and Applications. *arXiv preprint arXiv:2001.02827* (2020).

[4] Noga Alon and Fan RK Chung. 1988. Explicit construction of linear sized tolerant networks. *Discrete Mathematics* 72, 1-3 (1988), 15–19. https://doi.org/10.1016/0012-365X(88)90189-6

[5] Nima Anari, Kuikui Liu, and Shayan Oveis Gharan. 2020. Spectral Independence in High-Dimensional Expanders and Applications to the Hardcore Model. *arXiv preprint arXiv:2001.00303* (2020).

[6] Nima Anari, Kuikui Liu, Shayan Oveis Gharan, and Cynthia Vinzant. 2019. Log-concave polynomials II: high-dimensional walks and an FPRAS for counting bases of a matroid. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*. 1–12. https://doi.org/10.1145/3313276.3316385

[7] Anurag Anshu, Nikolas Breuckmann, and Chinmay Nirkhe. 2022. NLTS Hamiltonians from good quantum codes. *arXiv preprint arXiv:2206.13228* (2022).

[8] Mitali Bafna, Max Hopkins, Tali Kaufman, and Shachar Lovett. 2021. Hypercontractivity on High Dimensional Expanders. *arXiv preprint arXiv:2111.09444* (2021).

[9] Eli Ben-Sasson and Madhu Sudan. 2004. Robust locally testable codes and products of codes. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*. Springer, 286–297. https://doi.org/10.1007/978-3-540-27821-4_26

[10] Nikolas P Breuckmann and Jens N Eberhardt. 2021. Balanced product quantum codes. *IEEE Transactions on Information Theory* 67, 10 (2021), 6653–6674. https://doi.org/10.1109/TIT.2021.3097347

[11] Nikolas P Breuckmann and Jens Niklas Eberhardt. 2021. Quantum low-density parity-check codes. *PRX Quantum* 2, 4 (2021), 040101. https://doi.org/10.1103/PRXQuantum.2.040101

[12] Nicolas Delfosse and Naomi H Nickerson. 2021. Almost-linear time decoding algorithm for topological codes. *Quantum* 5 (2021), 595. https://doi.org/10.22331/q-2021-12-02-595

[13] Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill. 2002. Topological quantum memory. *J. Math. Phys.* 43, 9 (2002), 4452–4505. https://doi.org/10.1063/1.1499754

[14] Yotam Dikstein and Irit Dinur. 2019. Agreement testing theorems on layered set systems. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 1495–1524. https://doi.org/10.1109/FOCS.2019.00088

[15] Yotam Dikstein, Irit Dinur, Yuval Filmus, and Prahladh Harsha. 2018. Boolean function analysis on high-dimensional expanders. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

[16] Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes. 2021. Locally Testable Codes with constant rate, distance, and locality. *arXiv preprint arXiv:2111.04808* (2021).

[17] Irit Dinur, Yuval Filmus, Prahladh Harsha, and Madhur Tulsiani. 2020. Explicit SoS lower bounds from high-dimensional expanders. *arXiv preprint arXiv:2009.05218* (2020).

[18] Irit Dinur, Min-Hsiu Hsieh, Ting-Chun Lin, and Thomas Vidick. 2022. Good quantum LDPC codes with linear time decoders. *arXiv preprint arXiv:2206.07750* (2022).

[19] Irit Dinur and Tali Kaufman. 2017. High dimensional expanders imply agreement expanders. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 974–985. https://doi.org/10.1109/FOCS.2017.94

[20] Irit Dinur, Madhu Sudan, and Avi Wigderson. 2006. Robust local testability of tensor products of LDPC codes. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*. Springer, 304–315. https://doi.org/10.1007/11830924_29

[21] Guillaume Duclos-Cianci and David Poulin. 2010. Fast Decoders for Topological Quantum Codes. *Phys. Rev. Lett.* 104 (Feb 2010), 050504. Issue 5. https://doi.org/10.1103/PhysRevLett.104.050504

[22] Shai Evra and Tali Kaufman. 2016. Bounded degree cosystolic expanders of every dimension. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*. 36–48. https://doi.org/10.1145/2897518.2897543

[23] Shai Evra, Tali Kaufman, and Gilles Zémor. 2020. Decodable quantum LDPC codes beyond the square root distance barrier using high dimensional expanders. *arXiv preprint arXiv:2004.07935* (2020).

[24] Michael H Freedman, David A Meyer, and Feng Luo. 2002. Z2-systolic freedom and quantum codes. In *Mathematics of quantum computation*. Chapman and Hall/CRC, 303–338.

[25] Oded Goldreich. 2010. Short locally testable codes and proofs: A survey in two parts. In *Property testing*. Springer, 65–104. https://doi.org/10.1007/978-3-642-16367-8_6

[26] Daniel Gottesman. 2013. Fault-tolerant quantum computation with constant overhead. *arXiv preprint arXiv:1310.2984* (2013).

[27] Mikhail Gromov. 2010. Singularities, expanders and topology of maps. Part 2: From combinatorics to topology via algebraic isoperimetry. *Geometric and Functional Analysis* 20, 2 (2010), 416–526. https://doi.org/10.1007/s00039-010-0073-8

[28] Shouzhen Gu, Christopher A Pattison, and Eugene Tang. 2022. An efficient decoder for a linear distance quantum LDPC code. *arXiv preprint arXiv:2206.06557* (2022).

[29] Tom Gur, Noam Lifshitz, and Siqi Liu. 2021. Hypercontractivity on high dimensional expanders. *arXiv preprint arXiv:2111.09375* (2021).

[30] Matthew B Hastings, Jeongwan Haah, and Ryan O'Donnell. 2021. Fiber bundle codes: breaking the n 1/2 polylog (n) barrier for Quantum LDPC codes. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. 1276–1288. https://doi.org/10.1145/3406325.3451005

[31] Allen Hatcher. 2002. *Algebraic Topology*. Cambridge University Press.

[32] Shlomo Hoory, Nathan Linial, and Avi Wigderson. 2006. Expander graphs and their applications. *Bull. Amer. Math. Soc.* 43, 4 (2006), 439–561.

[33] Max Hopkins and Ting-Chun Lin. 2022. Explicit Lower Bounds Against $\Omega(n)$-Rounds of Sum-of-Squares. *arXiv preprint arXiv:2204.11469* (2022).

[34] Fernando Granha Jeronimo, Shashank Srivastava, and Madhur Tulsiani. 2021. Near-linear time decoding of Ta-Shma's codes via splittable regularity. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. 1527–1536. https://doi.org/10.1145/3406325.3451126

[35] Gleb Kalachev and Pavel Panteleev. 2022. Two-sided Robustly Testable Codes. *arXiv preprint arXiv:2206.09973* (2022).

[36] Tali Kaufman, David Kazhdan, and Alexander Lubotzky. 2014. Ramanujan complexes and bounded degree topological expanders. In *2014 IEEE 55th Annual Symposium on Foundations of Computer Science*. IEEE, 484–493. https://doi.org/10.1109/FOCS.2014.58

[37] Tali Kaufman and Izhar Oppenheim. 2020. High order random walks: Beyond spectral gap. *Combinatorica* (2020), 1–37. https://doi.org/10.1007/s00493-019-3847-0

[38] Tali Kaufman and Ran J Tessler. 2020. New Cosystolic Expanders from Tensors Imply Explicit Quantum LDPC Codes with $\Omega(\sqrt{n}\log^k n)$ Distance. *arXiv preprint arXiv:2008.09495* (2020).

[39] A Yu Kitaev. 2003. Fault-tolerant quantum computation by anyons. *Annals of Physics* 303, 1 (2003), 2–30. https://doi.org/10.1016/S0003-4916(02)00018-0

[40] Anthony Leverrier, Vivien Londe, and Gilles Zémor. 2022. Towards local testability for quantum coding. *Quantum* 6 (2022), 661. https://doi.org/10.22331/q-2022-02-24-661

[41] Anthony Leverrier, Jean-Pierre Tillich, and Gilles Zémor. 2015. Quantum expander codes. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*. IEEE, 810–824. https://doi.org/10.1109/FOCS.2015.55

[42] Anthony Leverrier and Gilles Zémor. 2022. Efficient decoding up to a constant fraction of the code length for asymptotically good quantum codes. *arXiv preprint arXiv:2206.07571* (2022).

[43] Anthony Leverrier and Gilles Zémor. 2022. A parallel decoder for good quantum LDPC codes. *arXiv preprint arXiv:2208.05537* (2022).

[44] Anthony Leverrier and Gilles Zémor. 2022. Quantum Tanner codes. *arXiv preprint arXiv:2202.13641* (2022).

[45] Ting-Chun Lin and Min-Hsiu Hsieh. 2022. c^3-Local Testable Codes from Lossless Expanders. *arXiv preprint arXiv:2201.11369* (2022).

[46] Ting-Chun Lin and Min-Hsiu Hsieh. 2022. Good quantum LDPC codes with linear time decoder from lossless expanders. *arXiv preprint arXiv:2203.03581* (2022).

[47] Nathan Linial* and Roy Meshulam*. 2006. Homological connectivity of random 2-complexes. *Combinatorica* 26, 4 (2006), 475–487. https://doi.org/10.1007/s00493-006-0027-9

[48] Alexander Lubotzky. 2014. Ramanujan complexes and high dimensional expanders. *Japanese Journal of Mathematics* 9, 2 (2014), 137–169. https://doi.org/10.1007/s11537-014-1265-z

[49] Pavel Panteleev and Gleb Kalachev. 2019. Degenerate Quantum LDPC Codes With Good Finite Length Performance. arXiv:1904.02703 [quant-ph]

[50] Pavel Panteleev and Gleb Kalachev. 2021. Asymptotically Good Quantum and Locally Testable Classical LDPC Codes. *arXiv preprint arXiv:2111.03654* (2021).

[51] Pavel Panteleev and Gleb Kalachev. 2022. Quantum LDPC codes with almost linear minimum distance. *IEEE Transactions on Information Theory* 68, 1 (2022), 213–229. https://doi.org/10.1109/TIT.2021.3119384

[52] A Philips, R Lubotsky, and P Sarnak. 1988. Ramanujan graphs. *Combinatorica* 8, 3 (1988), 261–277. https://doi.org/10.1007/BF02126799

[53] Michael Sipser and Daniel A Spielman. 1996. Expander codes. *IEEE transactions on Information Theory* 42, 6 (1996), 1710–1722. https://doi.org/10.1109/18.556667

[54] R Tanner. 1981. A recursive approach to low complexity codes. *IEEE Transactions on information theory* 27, 5 (1981), 533–547. https://doi.org/10.1109/TIT.1981.1056404

[55] Jean-Pierre Tillich and Gilles Zémor. 2013. Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength. *IEEE Transactions on Information Theory* 60, 2 (2013), 1193–1202. https://doi.org/10.1109/TIT.2013.2292061

Received 2022-11-07; accepted 2023-02-06