An Efficient Decoder for a Linear Distance Quantum LDPC Code

An Efficient Decoder for a Linear Distance Quantum LDPC Code

Shouzhen Gu
California Institute of Technology
Institute for Quantum Information and Matter
Pasadena, CA, USA

Christopher A. Pattison
California Institute of Technology
Institute for Quantum Information and Matter
Pasadena, CA, USA

Eugene Tang
Massachusetts Institute of Technology
Center for Theoretical Physics
Cambridge, MA, USA

ABSTRACT

Recent developments have shown the existence of quantum low-density parity check (qLDPC) codes with constant rate and linear distance. A natural question concerns the efficient decodability of these codes. In this paper, we present a linear time decoder for the recent quantum Tanner codes construction of asymptotically good qLDPC codes, which can correct all errors of weight up to a constant fraction of the blocklength. Our decoder is an iterative algorithm which searches for corrections within constant-sized regions. At each step, the corrections are found by reducing a locally defined and efficiently computable cost function which serves as a proxy for the weight of the remaining error.

CCS CONCEPTS

• **Theory of computation** → **Error-correcting codes**; **Expander graphs and randomness extractors**; **Design and analysis of algorithms**.

KEYWORDS

Quantum error correction, quantum low-density parity-check codes, decoding algorithm, expander graphs, robust error-correcting codes

ACM Reference Format:
Shouzhen Gu, Christopher A. Pattison, and Eugene Tang. 2023. An Efficient Decoder for a Linear Distance Quantum LDPC Code. 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/10.1145/3564246.3585169

1 INTRODUCTION

Quantum error correcting codes with constant-sized check operators, known as quantum low-density parity check (qLDPC) codes, have myriad applications in computer science and quantum information. Indeed, almost all leading contenders [3, 6] for experimentally realizable fault-tolerant quantum memories are qLDPC codes. With more stringent requirements on their parameters, qLDPC codes can be used to achieve constant overhead fault-tolerant quantum computation as shown by Gottesman [12]. On the more theoretical side, qLDPC codes are believed to have connections to the quantum probabilistically checkable proofs (qPCP) conjecture [9].

A qLDPC code of blocklength n is said to be good when it encodes $\Theta(n)$ logical qubits and detects all errors up to weight $\Theta(n)$. For many years such codes have proven elusive, with an apparent distance "barrier" of around $\sqrt{n}$. It is natural to wonder if there is some fundamental limitation that prevents us from achieving the *a priori* best possible distance of $\Theta(n)$. However, a sequence of recent constructions of qLDPC codes with steadily improving code parameters [4, 14, 21] have culminated in the construction of asymptotically good qLDPC codes by Panteleev and Kalachev [20]. Alternative constructions of good qLDPC codes have since been given by Leverrier and Zémor [17] and conjectured by Lin and Hsieh [19].

An efficient decoder correcting all errors of weight up to $\Theta(n)$ is a useful primitive for both fault-tolerance purposes and complexity theory applications. To date, the best known efficient decoder corrects against all errors of weight up to $\Theta(\sqrt{n}\log n)$ [10]. In this paper, we demonstrate the first efficient decoder for a quantum error-correcting code that corrects all errors up to linear weight.

For our decoder, we focus on the quantum Tanner codes construction of Leverrier and Zémor [17]. Quantum Tanner codes were inspired by the original construction of good qLDPC codes of Panteleev and Kalachev [20], as well as by the classical locally testable codes of [7], serving as a intermediary between the two constructions. They can also be seen as a natural quantum generalization of classical Tanner codes [22]. A classical Tanner code is defined by placing bits on the edges of an expanding graph, with non-trivial checks defining local codes placed at the vertices. The codewords are the strings whose local views at each vertex belong to the codespace of the local code. A quantum Tanner code is a Calderbank-Shor-Steane (CSS) [5, 23] code defined by two classical Tanner codes stitched together using a two-dimensional expanding complex. For particular choices of the local checks and expanding complex, this construction has been shown to yield an asymptotically good family of qLDPC codes. We show that this construction can also yield an asymptotically good family of qLDPC codes which are efficiently decodable for errors of weight up to a constant fraction of the distance.

Our decoder is inspired by the small-set-flip [16] decoding algorithm for hypergraph product codes based on expanding graphs. Small-set-flip is an iterative algorithm, where at every step, small sets of qubits are flipped to decrease the syndrome weight. The candidate sets to flip are contained within the supports of individual stabilizer generators. A critical ingredient in the success of the small-set-flip decoder is the presence of expansion in the underlying geometric complex. Since the geometric complex defining quantum Tanner codes has a similar notion of expansion, one might expect that analogous ideas may work for decoding quantum Tanner codes.

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

ACM ISBN 978-1-4503-9913-5/23/06.
https://doi.org/10.1145/3564246.3585169

In our decoder, we define a "local potential function" on each local view which measures the distance of the error from the local codespace. The decoder reduces the sum of these potential functions by applying a constant-sized correction within some local view at each step. In the proof of correctness, we proceed by tracking the minimum weight correction according to each local view, and then use this data to show that a flip-set with the required properties must exist when the error is not too large. As a required step in the proof, we also strengthen the robustness parameters of the random classical codes used in the quantum Tanner code construction.

Our main result is stated below:

Theorem (Informal version of Theorems 12 and 13). *There exists a family of asymptotically good quantum Tanner codes such that our decoder successfully corrects all errors of weight up to $\Theta(n)$ and runs in time $O(n)$.*

We note that after the completion of this work, several other results on decoding good LDPC codes have since been shown [8, 18]. As a part of these developments, the existence of local codes with optimal robust parameter $w = \Theta(\Delta^2)$ have been shown to exist [8, 15]. The use of these codes will improve the parameters stated in Theorem 12.

The remainder of the paper is organized as follows. In Section 2 we provide a brief technical introduction to the quantum Tanner codes construction of asymptotically good qLDPC codes. There we present a terse, but self-contained, description of all the ingredients necessary to follow the rest of the paper. In Section 3 we formally define the decoding problem and present the overview of our decoder for the quantum Tanner codes. We also work out basic properties and consequences of our decoder in this section. In Section 4 we provide a summary of our results and present some relevant open problems. Finally, we defer the technical bulk of the paper to Section 5, which presents the main proof of the correctness of the decoder.

2 QUANTUM TANNER CODES

In this section, we review some coding theory background and summarize the construction of quantum Tanner codes by Leverrier and Zémor [17].

2.1 Classical Linear Codes

In this subsection we quickly review the necessary classical coding background. A classical linear code is a k-dimensional subspace $C \subseteq \mathbb{F}_2^n$, which is often specified by a parity check matrix $H \in \mathbb{F}_2^{(n-k)\times n}$ such that $C = \ker H$. Equivalently, the code can also be specified as the column space of a generator matrix $G \in \mathbb{F}_2^{n\times k}$, such that $C = \operatorname{col} G$. The parameter n is called the blocklength of the code. The number of encoded bits is k and $\rho = k/n$ is the rate of the code. The number of errors that the code can correct is determined by the distance of C, which is given by the minimum Hamming weight of a nonzero codeword: $d = \min_{x\in C\setminus\{0\}} |x|$. Sometimes, we consider the relative distance $\delta = d/n$. We say that such a code has parameters $[n, k, d]$.

Given a D-regular (multi)graph $\mathcal{G} = (V, E)$ and a code C_0 of blocklength D, we can define the classical Tanner code $C = T(\mathcal{G}, C_0)$ as follows. The bits of C are placed on the edges of $\mathcal{G}$, so it is a code of length $n = |E|$. For $x \in \mathbb{F}_2^E$, define the *local view* of x at a vertex $v \in V$ to be $x|_{E(v)}$, which is the restriction of x to $E(v)$, the set of edges incident to v. Then the codewords of C are those $x \in \mathbb{F}_2^E$ such that $x|_{E(v)} \in C_0$ for every $v \in V$, where we choose some way of identifying every edge-neighborhood of a vertex with the bits of the local code C_0. If H_0 is the parity check matrix of C_0, then the parity check matrix of C will have rows which are equal to a row of H_0 on an edge-neighborhood of a vertex and extended to be zero everywhere else. In the Tanner code construction, the code C_0 is often called the local, or base, code.

The dual of a classical linear code C, denoted $C^\perp$, is the subspace of all vectors orthogonal to the codewords of C; that is,

$$C^\perp = \{y \in \mathbb{F}_2^n : \forall x \in C,\ \langle x, y\rangle = 0\}, \tag{1}$$

where the inner product is taken modulo 2. If we have two classical codes $C_A = \ker H_A \subseteq \mathbb{F}_2^n$ and $C_B = \ker H_B \subseteq \mathbb{F}_2^n$, we can consider their tensor code and dual tensor code.

Definition 1 (Tensor and Dual Tensor Codes). *The tensor code of C_A and C_B is the usual tensor product $C_A \otimes C_B \subseteq \mathbb{F}_2^n \otimes \mathbb{F}_2^n$. We can naturally interpret $\mathbb{F}_2^n \otimes \mathbb{F}_2^n$ as the set of binary $n \times n$ matrices, and in this view, $C_A \otimes C_B$ is identified with the set of matrices X such that every column of X is a codeword of C_A and every row of X is a codeword of C_B.*

The dual tensor code of C_A and C_B is $(C_A^\perp \otimes C_B^\perp)^\perp \subseteq \mathbb{F}_2^n \otimes \mathbb{F}_2^n$, which can equivalently be expressed as $(C_A^\perp \otimes C_B^\perp)^\perp = C_A \otimes \mathbb{F}_2^n + \mathbb{F}_2^n \otimes C_B$. Codewords of the dual tensor code are precisely the set of matrices X such that $H_A X H_B^{\mathsf{T}} = 0$.

Note that if C_A is a $[n_A, k_A, d_A]$ code and C_B is a $[n_B, k_B, d_B]$ code, then their tensor code is a $[n_A n_B, k_A k_B, d_A d_B]$ code. Their dual tensor code is a $[n_A n_B, n_A k_B + n_B k_A - k_A k_B, \min(d_A, d_B)]$ code. Moreover, we have $C_A \otimes C_B \subseteq (C_A^\perp \otimes C_B^\perp)^\perp$.

2.2 Quantum CSS Codes

A quantum stabilizer code is a subspace $\mathcal{C} \subseteq \left(\mathbb{C}^2\right)^{\otimes n}$ that is the $+1$-eigenspace of an abelian subgroup S of the n-qubit Pauli group. If S can be generated by stabilizers that are products of X operators and stabilizers that are products of Z operators, we say that $\mathcal{C}$ is a CSS code. In this case, we can associate with $\mathcal{C}$ two classical codes $\mathcal{C}_X = \ker H_X$ and $\mathcal{C}_Z = \ker H_Z \subseteq \mathbb{F}_2^n$, where the rows of H_X (resp. H_Z) specify the X (resp. Z) type stabilizer generators. The property that X and Z generators commute translates to the condition $H_X H_Z^{\mathsf{T}} = 0$, or equivalently $\mathcal{C}_Z^\perp \subseteq \mathcal{C}_X$.

We can state the code parameters of a CSS code in terms of its underlying classical codes: if $\mathcal{C}_X$ (resp. $\mathcal{C}_Z$) has k_X (resp. k_Z) encoded bits, then the number of encoded qubits is $k = k_X + k_Z - n$. The distance of the CSS code is given by $d = \min\{d_X, d_Z\}$, where

$$d_X = \min_{x\in\mathcal{C}_Z\setminus\mathcal{C}_X^\perp} |x|, \quad d_Z = \min_{x\in\mathcal{C}_X\setminus\mathcal{C}_Z^\perp} |x|. \tag{2}$$

We say that such a quantum code has parameters $[[n, k, d]]$. A family of quantum codes is called *asymptotically good* (or simply *good*) if the rate $\rho = k/n$ and the relative distance $\delta = d/n$ are bounded below by a non-zero constant. The code family is said to be low-density parity check (LDPC) if it can be defined with stabilizer generators that have at most constant weight, with each qubit being in the support of at most a constant number of generators. This is the case if each row and column of H_X and H_Z have at most constant weight.

2.3 Left-Right Cayley Complexes

Let G be a finite group with a symmetric generating set A, i.e. $A = A^{-1}$. The left Cayley graph $\mathrm{Cay}(A, G)$ is the graph with vertex set G and edge set $\{(g, ag) : g \in G, a \in A\}$. There is also the notion of a right Cayley graph $\mathrm{Cay}(G, B)$ where the generator set acts on the right, with edges $\{(g, gb) : g \in G, b \in B\}$. Let A and B be two symmetric generating for G of size $|A| = |B| = \Delta$. The generating sets A and B are said to satisfy the *Total No-Conjugacy condition (TNC)* [7] if we have $ag \neq gb$ for all $a \in A$, $b \in B$, and $g \in G$.

Given a group G and two symmetric generating sets A and B satisfying TNC, we define their double-covered left-right Cayley complex $\mathrm{Cay}_2(A, G, B)$ as the 2-dimensional complex consisting of:

(1) Vertices $V = V_0 \sqcup V_1 = G \times \{0\} \sqcup G \times \{1\}$. There are a total of $|V| = 2|G|$ vertices, with $|V_0| = |V_1| = |G|$.
(2) Edges $E = E_A \sqcup E_B$, where

$$\begin{aligned} E_A &= \{((g, 0), (ag, 1)) : g \in G, a \in A\}, \quad \text{and} \\ E_B &= \{((g, 0), (gb, 1)) : g \in G, b \in B\}. \end{aligned} \tag{3}$$

Note that A-type edges are defined by a left-action of the generators, while that B-type edges are defined by a right-action of the generators. There are a total of $2\Delta|G|$ edges, with $|E_A| = |E_B| = \Delta|G|$.
(3) Squares Q defined by quadruplets of vertices:

$$Q = \{\{(g, 0), (ag, 1), (gb, 1), (agb, 0)\} : a \in A, b \in B, g \in G\}. \tag{4}$$

There are a total of $|Q| = \Delta^2|G|/2$ squares.

Note that the graph defined by (V, E_A) is precisely the double cover of the left Cayley graph $\mathrm{Cay}(A, G)$, and the graph defined by (V, E_B) is the double cover the right Cayley graph $\mathrm{Cay}(G, B)$. The full 1-skeleton of $\mathrm{Cay}_2(A, G, B)$ is a bipartite graph $\mathcal{G}^{\cup} = (V, E)$.

By TNC, each square is guaranteed to have 4 distinct vertices, so the graph $\mathcal{G}^{\cup}$ is a simple 2Δ-regular graph. There are Δ^2 squares incident to a given vertex, and the set of faces incident to a given vertex can be naturally identified with the set $A \times B$. Figure 1 illustrates the faces incident to a given vertex in the left-right Cayley complex.

Based on the structure of the graph $\mathcal{G}^{\cup}$, each face $q \in Q$ can be naturally identified with its diagonal connecting its corners in V_0. Through this identification, we can define a graph $\mathcal{G}_0^{\square}$ capturing the incidence structure of faces in the complex. The graph $\mathcal{G}_0^{\square} = (V_0, Q)$ is defined with vertex set $V_0 = G \times \{0\}$, where $q \in Q$ is present as an edge (v, v') in $\mathcal{G}_0^{\square}$ if and only if v and v' appear as opposite V_0-corners of the square q. Likewise, each face $q \in Q$ can be identified with its diagonal connecting its corners in V_1. This similarly defines a graph $\mathcal{G}_1^{\square} = (V_1, Q)$. Note that $\mathcal{G}_0^{\square}$ and $\mathcal{G}_1^{\square}$ are Δ^2-regular multigraphs.

2.4 Quantum Tanner Codes Construction

We now describe the construction of quantum Tanner codes [17]. The construction is dependent on the choice of a double-covered left-right Cayley complex $\mathrm{Cay}_2(A, G, B)$ with generating sets of size $|A| = |B| = \Delta$ satisfying TNC. It is also dependent on fixed classical codes C_A, C_B of blocklength Δ, which define local codes $C_0 = C_A \otimes C_B$ and $C_1 = C_A^{\perp} \otimes C_B^{\perp}$.

Given the data above, a quantum Tanner code C is then defined as the CSS code specified by the two classical Tanner codes $\mathcal{C}_Z = T(\mathcal{G}_0^{\square}, C_0^{\perp})$ and $\mathcal{C}_X = T(\mathcal{G}_1^{\square}, C_1^{\perp})$. More explicitly, qubits are placed on the squares of the left-right Cayley complex, and the Z (resp. X) type stabilizer generators are codewords of the local code $C_A \otimes C_B$ (resp. $C_A^{\perp} \otimes C_B^{\perp}$) on the Δ^2 squares incident to each vertex $v \in V_0$ (resp. $v \in V_1$). The incidence structure of the left-right Cayley complex ensures that the X and Z stabilizers commute.

Note that C is a qLDPC code: each stabilizer generator acts on a subset of the local view $Q(v)$ of Δ^2 qubits, and each qubit is acted on only by the stabilizers in the local views of its four corners. It is proven in [17] that for certain choices of the left-right Cayley complex and local codes, this construction yields a good family of quantum codes:

Theorem 2 (Theorem 16 of [17]). *Fix $\varepsilon \in (0, 1/2)$, $\rho \in (0, 1/2)$, and $\delta \in (0, 1/2)$ with $\delta < h^{-1}(\rho)$, where $h(x) = -x \log_2 x - (1 - x) \log_2(1 - x)$ is the binary entropy function. For some Δ sufficiently large, there exist classical codes C_A, C_B of blocklength Δ, rates ρ and $1 - \rho$ respectively, and relative distances at least δ, as well as an infinite family of left-right Cayley complexes $\mathrm{Cay}_2(A, G, B)$ with $|G| \to \infty$ and symmetric generating sets A, B of size $|A| = |B| = \Delta$ satisfying TNC, such that the quantum Tanner code defined above has parameters*

$$[[n = |Q|, k \geq (1 - 2\rho)^2 n, d \geq \frac{\delta}{4\Delta^{3/2+\varepsilon}} n]].$$

2.5 Expanding Cayley Complex and Robust Local Codes

In this subsection, we specify the technical properties of the Cayley complex and local codes that are used in the construction of good quantum Tanner codes described previously.

For a D-regular graph $\mathcal{G} = (V, E)$, the largest eigenvalue of its adjacency matrix is $\lambda_1 = D$, and we let $\lambda(\mathcal{G}) = \lambda_2$ denote its second largest eigenvalue. The value of $\lambda(\mathcal{G})$ is related to the expansion properties of the graph, as seen in the expander mixing lemma below. For subsets $S, T \subseteq V$, let $E(S, T)$ be the multiset of edges between S and T, where edges in $S \cap T$ are counted twice. We have the following:

Theorem 3 (Expander mixing lemma). *For a D-regular graph $\mathcal{G} = (V, E)$ and subsets $S, T \subseteq V$,*

$$|E(S, T)| \leq \frac{D}{|V|}|S||T| + \lambda(\mathcal{G})\sqrt{|S||T|}. \tag{5}$$

The groups G and generating sets A, B in Theorem 2 are chosen so that the resulting left-right Cayley complex has good expansion.

Lemma 4 (Claim 6.7 of [7]). *Let q be an odd prime power and $G = \mathrm{PSL}_2(q^i)$. There exist two symmetric generating sets A, B of size $|A| = |B| = \Delta = q + 1$ and satisfying TNC such that the resulting Cayley graphs $\mathrm{Cay}(A, G), \mathrm{Cay}(G, B)$ are Ramanujan, i.e. have second largest eigenvalue $\lambda_2 \leq 2\sqrt{\Delta}$.*

For G, A, B as above, it can be shown [17] that the relevant graphs in the quantum Tanner codes construction have the parameters specified in Table 1.

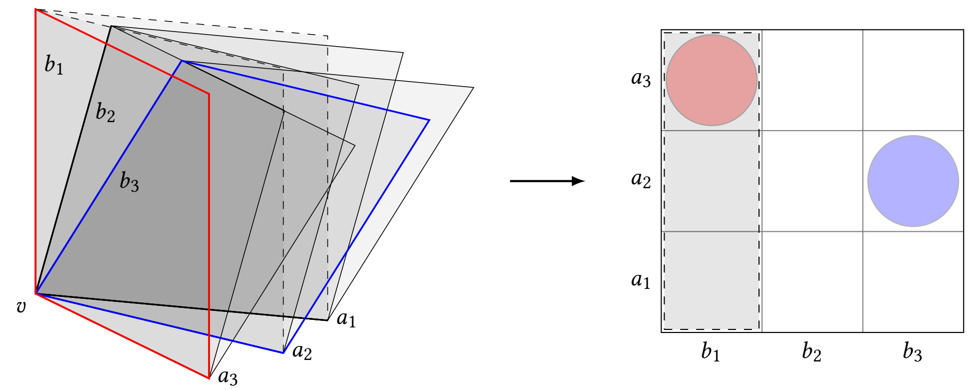

Figure 1: The local view of a vertex v and its identification with the set $A \times B$. Considering the "book" defined by the edge b_1 picks out a column, $A \times b_1$ (dashed). Specifying entries of $A \times B$ picks out specific faces (red, blue) of the local view, which can be regarded as entries of the corresponding matrix.

Table 1: Graph parameters

Graph	Degree	Number of vertices	Second eigenvalue
$\mathcal{G}^{\cup}$	2Δ	$2\lvert G\rvert = \lvert V_0\rvert + \lvert V_1\rvert$	$\leq 4\sqrt{\Delta}$
$\mathcal{G}_0^{\square}$	Δ^2	$\lvert G\rvert = \lvert V_0\rvert$	$\leq 4\Delta$
$\mathcal{G}_1^{\square}$	Δ^2	$\lvert G\rvert = \lvert V_1\rvert$	$\leq 4\Delta$

The classical codes used in the construction of quantum Tanner codes are required to satisfy a robustness property of their dual tensor code, introduced in [17].

Definition 5 (w-Robustness). *Let $C_A, C_B \subseteq \mathbb{F}_2^n$ be classical codes with distances d_A and d_B respectively. We say that the dual tensor code $C_{AB} = C_A \otimes \mathbb{F}_2^n + \mathbb{F}_2^n \otimes C_B$ is w-robust if every codeword $X \in C_{AB}$ with $|X| \leq w$ is supported on the union of at most $|X|/d_A$ non-zero columns and $|X|/d_B$ non-zero rows. That is, there exist rows A' with $|A'| \geq n - |X|/d_B$ and columns B' with $|B'| \geq n - |X|/d_A$ such that $X|_{A' \times B'} = 0$.*

When a codeword of a dual tensor code is supported on few columns and rows, it has a decomposition into column and row codewords respecting this support. The following lemma is proven in the full paper [13].

Lemma 45. *Let C_A and C_B be classical codes of distance at least d and $C = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ be the dual tensor code. Suppose $X \in C$ is supported on the union of α non-zero rows and β non-zero columns, with $\alpha, \beta < d$. Then X can be written as $X = \mathbf{r} + \mathbf{c}$ where $\mathbf{r} \in \mathbb{F}_2^A \otimes C_B$ is supported on at most α non-zero rows and $\mathbf{c} \in C_A \otimes \mathbb{F}_2^B$ is supported on at most β non-zero columns.*

If the dual tensor code of C_A and C_B is w-robust, then their tensor code satisfies a property similar to robust testability defined in [2].

Proposition 6 (Proposition 6 of [17]). *Let $C_A, C_B \subseteq \mathbb{F}_2^n$ be classical codes with distances d_A and d_B respectively such that their dual tensor code is w-robust for $w \leq d_A d_B/2$. Then*

$$d(x, C_A \otimes C_B) \leq \frac{3}{2}\left(d(x, C_A \otimes \mathbb{F}_2^n) + d(x, \mathbb{F}_2^n \otimes C_B)\right) \tag{6}$$

whenever $d(x, C_A \otimes \mathbb{F}_2^n) + d(x, \mathbb{F}_2^n \otimes C_B) \leq w$.

In the full paper [13], we prove Theorem 7 below, which shows that for sufficiently large blocklengths, there exist dual tensor codes of sufficiently large robustness.

Theorem 7. *Fix constants $\varepsilon \in (0, 1/28)$, $\rho \in (0, 1/2)$, and $\delta \in (0, 1/2)$ such that $\delta < h^{-1}(\rho)$, where $h(x)$ is the binary entropy function. For all sufficiently large Δ, there exist classical codes C_A, C_B of length Δ and rates $\rho_A = \rho$ and $\rho_B = 1 - \rho$ such that such that both the dual tensor code of C_A and C_B and the dual tensor code of $C_A^{\perp}$ and $C_B^{\perp}$ are $\Delta^{3/2+\varepsilon}$-robust and have distances at least $\delta\Delta$.*

With these ingredients, we can describe the construction in Theorem 2 in more detail. We first choose a prime power $q = \Delta - 1$ sufficiently large such that we can use Theorem 7 to find C_A, C_B with robustness parameter $\Delta^{3/2-\varepsilon}$. Then the infinite family of left-right Cayley complexes is defined using $G = \mathrm{PSL}_2(q^i)$ for increasing values of i and A, B as in Lemma 4. Note that the sizes of the groups satisfy $|G| = \frac{1}{2}q^i(q^{2i} - 1) \to \infty$.

We remark that in [17], a version of Theorem 7 was shown for robustness parameter $\Delta^{3/2-\varepsilon}$, but in the proof of correctness of our decoder, a larger parameter $\Delta^{3/2+\varepsilon}$ is needed. Because the proof of Theorem 2 given in [17] is valid even for negative values of ε, the existence of dual tensor codes with higher robustness implies a larger distance of the code itself, $d \geq \frac{\delta}{4\Delta^{3/2-\varepsilon}} n$. At the same time, the larger robustness parameter eliminates the need for resistance to puncturing required in [17], thus simplifying the overall description of the quantum Tanner code.

3 DECODING ALGORITHM

In this section, we give a description of our decoder for quantum Tanner codes. The quantum Tanner codes we consider are those described in the previous section with distance $d \geq \frac{\delta}{4\Delta^{3/2-\varepsilon}} n$, constructed using classical dual tensor codes of robustness $\Delta^{3/2+\varepsilon}$ as the local codes. In the decoding problem, an unknown (Pauli) error is applied to the code. We may only extract the syndrome of the error by measuring stabilizers, and based on the syndrome, apply corrections. We succeed in decoding if the correction we applied is equal to the error, up to a stabilizer (which has no effect on the codespace). Because quantum Tanner codes are CSS codes, it suffices to consider X and Z errors separately. If we have an algorithm to correct for errors that are purely a product of X operators and another one for a product of Z operators, a general error will be corrected after running both algorithms. Furthermore, since the code is symmetric between X and Z, we just consider the problem of correcting Z errors.

Definition 8 (Decoding Problem). *Let $e \in \mathbb{F}_2^Q$ be a Z error. Given the syndrome $\sigma = H_X e$ as input, the task of the decoding problem is to output a correction $f \in \mathbb{F}_2^Q$ such that $e - f \in \mathcal{C}_Z^\perp$.*

Our decoder is similar in flavor to the small-set-flip decoder used on certain hypergraph product codes [16]. Small-set-flip is an iterative decoder, where in each step the decoder tries to decrease the syndrome weight by looking for corrections within the support of a Z generator. If the initial error weight is less than the code distance, then such a correction can always be found, and this implies that the decoder can successfully errors of weight less than a constant fraction of the code distance [16].

In our case, the syndrome weight is not a very well-defined concept due to the presence of the local codes. Because the X stabilizers are generated by local tensor codes $C_1 = C_A^\perp \otimes C_B^\perp$, defining the Hamming weight of the syndrome involves choosing a basis for C_1. Unfortunately, there is no canonical choice of basis, and different choices will give different Hamming weights of a given error. We address this issue by introducing the concept of a potential function. Recall that an element $x \in \mathbb{F}_2^Q$ is a codeword of $\mathcal{C}_X = T(\mathcal{G}_1^\square, C_1^\perp)$ if and only if every local view $x|_{Q(v)}$, $v \in V_1$ is a codeword of $C_1^\perp$. We define the potential by the distance of the local view to the codespace, which can be inferred from the syndrome. More formally, we have the following definition:

Definition 9 (Local and Global Potential Functions). *Let $e \in \mathbb{F}_2^Q$ be an error. Define the* local potential *at a vertex $v \in V_1$ by the Hamming distance*

$$U_v(e) = d\left(e|_{Q(v)}, C_1^\perp\right). \tag{7}$$

The global potential *is defined as*

$$U(e) = \sum_{v \in V_1} U_v(e). \tag{8}$$

The local potential is the minimum weight of a correction that is needed to take the local view of the error (or corrupted codeword) back into the local codespace $C_1^\perp$. Thus, it is a quantity that can be computed just from the syndrome. We will abuse notation and also write $U_v(\sigma) = U_v(e)$ and $U(\sigma) = U(e)$. Note that in absence of a local code, in other words a local code where the codewords are the vectors of even Hamming weight, the local potential is simply either 0 or 1 depending on if the constraint is satisfied, so it coincides with the Hamming weight of the syndrome.

Our decoding algorithm (Algorithm 1) runs by looking for bits to flip in local views that will decrease the global potential.

We will show that Algorithm 1 succeeds in the decoding problem if the initial error has weight at most a constant fraction of code distance; that is, it can correct all errors up to some linear weight. The main difficulty of the proof is in showing that there always exists a vector z that decreases the global potential when flipped. This is captured in the following theorem, which we prove in the next section.

Algorithm 1 Decoder for quantum Tanner codes

Input: A syndrome $\sigma = H_X e \in \mathbb{F}_2^{|V_1| \dim C_1}$ of an error $e \in \mathbb{F}_2^Q$.
Output: A correction $f \in \mathbb{F}_2^Q$ for e.

```
f ← 0
U ← U(σ)
while U > 0 do
    Look for a vector z ∈ F_2^Q supported on a local view Q(v),
v ∈ V_0 ∪ V_1 such that U(σ + H_X z) < U
    f ← f + z
    σ ← σ + H_X z
    U ← U(σ)
end while
return f
```

Theorem 10. *Let $e \in \mathbb{F}_2^Q$ be an error of weight $|e| \leq \delta n / 6\Delta^{3/2-\varepsilon}$ with syndrome $\sigma = H_X e$. Then there exists $v \in V_0 \cup V_1$ and some $z \in \mathbb{F}_2^Q$ supported on the local view $Q(v)$, such that $U(\sigma + H_X z) < U(\sigma)$.*

From this property, we can show that the algorithm will output a valid correction. We do this by proving a statement that applies to a more general class of small-set-flip type decoders based on a potential function. The proof follows the same idea as that of Lemma 10 in [16].

Lemma 11. *Let $\alpha < 1, s, c$ be constants. Let C be an $[[n, k, d]]$ quantum CSS code defined by the classical codes $\mathcal{C}_X, \mathcal{C}_Z \subseteq \mathbb{F}_2^n$. Let $U : \mathbb{F}_2^n \to \mathbb{Z}_{\geq 0}$ be a (global) potential function that is constant on cosets of $\mathcal{C}_X$, satisfies $U(e) = 0$ if and only if $e \in \mathcal{C}_X$, and $U(e) \leq s|e|$ for all $e \in \mathbb{F}_2^n$. Suppose we have an iterative decoder that, given the syndrome of a non-zero Z error of weight less than αd, can decrease the potential by applying an X operator of weight at most c. Then the decoder can successfully correct errors of weight less than $\alpha d/(1 + sc)$.*

Proof. Let $x' = x + e \in \mathbb{F}_2^n$ be a corrupted codeword with $x \in \mathcal{C}_X$ and error e of weight $|e| < \frac{\alpha d}{1+sc}$. The decoder outputs a sequence of corrections $0 = f_0, f_1, f_2, \dots$ such that the resulting errors $e_i = e + f_i$ satisfy $|e_{i+1} - e_i| \leq c$ and $U(e_i) - U(e_{i+1}) \geq 1$ for all i. Suppose we have decoded up to step j. Then

$$\begin{aligned}
|e_j| &\leq |e_0| + |e_1 - e_0| + \cdots + |e_j - e_{j-1}| && (9)\\
&\leq |e| + c + \cdots + c && (10)\\
&\leq |e| + c(U(e_0) - U(e_1)) + \cdots + c(U(e_{j-1}) - U(e_j)) && (11)\\
&= |e| + c(U(e_0) - U(e_j)) && (12)\\
&\leq (1 + sc)|e| && (13)\\
&< \alpha d. && (14)
\end{aligned}$$

So either $U(e_j) = 0$, or the decoder can find the next correction f_{j+1} to produce e_{j+1}. Eventually, the decoder will output e_J such that $U(e_J) = 0$. In other words, $e_J \in \mathcal{C}_X$. But since $|e_J| < \alpha d < d$, it must be in $\mathcal{C}_Z^\perp$, and we have decoded to the correct codeword. □

We can now state our main theorems.

Theorem 12. *Fix $\varepsilon \in (0, 1/28)$, $\rho \in (0, 1/2)$, and $\delta \in (0, 1/2)$ with $\delta < h^{-1}(\rho)$, where $h(x)$ is the binary entropy function. For some Δ sufficiently large, there is an infinite family of quantum Tanner codes with parameters*

$$[[n, k \geq (1-2\rho)^2 n, d \geq \frac{\delta}{4\Delta^{3/2-\varepsilon}} n]]$$

with $n \to \infty$, such that for each n, Algorithm 1 can correct all errors of weight

$$|e| \leq \frac{\delta n}{6\Delta^{3/2-\varepsilon}(1+2\Delta^2)}\,. \tag{15}$$

Proof. The infinite family of quantum Tanner codes is as described in Section 2 (with distance parameter from the improved robustness of the classical local codes). To prove the decodable distance, consider the parameters in Lemma 11. Every bit in an error can at most increase the local potentials of the two incident V_1 vertices by one each. This implies the bound $U(e) \leq 2|e|$, so we can take $s = 2$. Since at each step, the algorithm flips sets within a local view, we set $c = \Delta^2$. From Theorem 10, the decoder can reduce the global potential when the error has weight up to $\alpha d = \delta n / 6\Delta^{3/2-\varepsilon}$. The theorem then follows from Lemma 11. □

Theorem 13. *Algorithm 1 runs in time $O(n)$.*

Proof. To compute the global potential U, we must compute $O(n)$ local potentials. Each local potential is a function of the constant-sized local view and can be computed in $O(1)$ time by enumerating vectors supported in the local view. At the same time, we can store the best candidate correction for the local view. Thus, the initialization runs in time $O(n)$.

In each iteration, we apply corrections in a constant-sized region, so only a constant number of local views and candidate corrections need to be updated for the syndrome and local potentials by the LDPC property. Each iteration of the algorithm runs in a constant amount of time, and there can be at most $O(n)$ iterations. Hence, the total runtime of Algorithm 1 is $O(n)$. □

The correctness of the decoding algorithm implies a form of soundness for the quantum code. This notion is a related to local testability but weaker because it only applies to errors of sufficiently small weight.

Corollary 14 (Soundness). *If e is an error that is correctable using Algorithm 1, then $U(e) \geq \Delta^{-2} d(e, \mathcal{C}_Z^{\perp})$.*

Proof. Using Algorithm 1, e can be corrected to a codeword of $\mathcal{C}_Z^{\perp}$ in at most $U(e)$ steps. In each step, at most Δ^2 bits are flipped. Therefore, we have $d(e, \mathcal{C}_Z^{\perp}) \leq \Delta^2 U(e)$. □

This soundness results yields an interesting consequence related to the No Low-Energy Trivial States (NLTS) conjecture [11]. After the completion of this work, a proof of the NLTS conjecture was established by Anshu *et al.* [1]. The main result of [1] showed that good quantum LDPC codes with soundness (called *clustering of approximate codewords* in [1]) satisfy the NLTS property. We note that Corollary 14 provides an independent proof of the main clustering property used in [1] and provides a close connection between efficiently decodable quantum LDPC codes and NLTS.

Corollary 15 (Threshold). *Let $e \in \mathbb{F}_2^n$ be a random error with each entry independently and identically distributed such that $e_i = 1$ with probability p and $e_i = 0$ with probability $1-p$. Under this model, the probability that Algorithm 1 fails to return a correction f such that $e + f \in \mathcal{C}_Z^{\perp}$ is $O(e^{-an})$, with $a > 0$, so long as $p < p^*$, where*

$$p^* \equiv \frac{\delta}{6\Delta^{3/2-\varepsilon}(1+2\Delta^2)} \tag{16}$$

is a lower bound for the accuracy threshold under independent bit and phase flip noise.

Proof. By Theorem 12, the decoder is guaranteed to succeed as long as $|e| \leq np^*$. The Hamming weight of e is distributed as a Binomial random variable which concentrates around the mean np. For $p^* > p$, we can use Hoeffding's inequality to bound the probability that $|e| > np^*$ as

$$\Pr\left(|e| > np^*\right) < e^{-2n(p^*-p)^2}, \tag{17}$$

which completes the proof. □

4 DISCUSSION AND OPEN PROBLEMS

In this paper, we show the existence of a provably correct decoder for the recent quantum Tanner codes construction of asymptotically good qLDPC codes. Our decoder has runtime linear in the code blocklength, and provably corrects all errors with weight up to a constant fraction of the distance (and hence the blocklength). A key idea behind the decoder is the introduction of a global potential function which measures the stability of the error against locally defined corrections. Our decoder proceeds operationally in a manner similar to the small-set-flip decoder for quantum expander codes [16], checking candidate subsets defined within the local views of the code to see if the global potential function can be reduced at each step. We prove that such a reduction is always possible for sufficiently low weight errors, which we use to show that the decoder successfully corrects all errors of weight $|e| \lesssim \delta n / \Delta^{7/2-\varepsilon}$. The existence of our decoder implies a notion of soundness for the quantum Tanner codes construction (see Corollary 14). It also implies an accuracy threshold against stochastic noise (see Corollary 15).

An important part of our proof for the correctness of the decoder involves showing the existence of dual tensor codes of larger robustness ($\Delta^{3/2+\varepsilon}$) than was established in [17]. This result also gives a constant factor improvement in the distance of the code. In addition, it leads to a simplification in the construction of quantum Tanner codes in that the dual tensor codes are no longer required to be resistant to puncturing.

A number of open problems remain at this point. One major problem is the time complexity of the decoder. While the runtime of the decoder is linear in the blocklength, there are constant prefactors on the order of 2^{Δ^2} arising from the need to check all subsets of the Δ^2-sized local views. This renders the decoder impractical in reality. Part of the problem stems from the inherently large check weights (Δ^2) of the quantum Tanner codes construction. A natural follow-up problem therefore is to look for ways to reduce the absolute runtime of the decoder, for example by reducing the check weights of the underlying code construction.

Another problem is related to the decoding of the asymptotically good qLDPC codes by Panteleev and Kalachev [20]. This question has been resolved in [18] by reducing the decoding problem of the Panteleev-Kalachev code to that of decoding quantum Tanner codes. A related – and more generic – problem is the existence of efficient decoders for good qLDPC codes constructed by the balanced product construction [4] in general, especially with the presence of non-trivial local codes.

Our current decoder requires the checking of local views belonging to vertices of both V_0 and V_1. This is in contrast to the small-set-flip decoder, which only requires checking the supports of generators of a single type. It may be possible that a tighter analysis (for example, using a stronger version of the low-overlap property, or more robust local codes) may allow us to eliminate the need to check both vertex types. A better understanding of the candidate flip-sets in general may be useful, especially towards the problem of lowering the runtime mentioned earlier.

5 PROOF OF THEOREM 10

Before beginning the proof of Theorem 10, we first elaborate on some conventions and notation. In the remainder of the paper we will adopt the convention that a vector $x \in \mathbb{F}_2^Q$ is treated equivalently as the subset of Q indicated by the vector. This allows us to write expressions such as $x \cup y \in \mathbb{F}_2^Q$ to denote the vector defined by the union of $x, y \subseteq Q$.

We will often need to consider the restriction of a vector $x \in \mathbb{F}_2^Q$ to the set of faces $Q(v)$ incident to some vertex $v \in V$. This is called the *local view* of x at v. In a convenient abuse of notation, we will equivalently consider local views as elements of $\mathbb{F}_2^{Q(v)}$, or as elements of $\mathbb{F}_2^Q$ with support on $Q(v)$. For simplicity of notation, we write local views at $v \in V$ with a subscript v, for example $x_v = x|_{Q(v)}$.

By the TNC condition, $Q(v)$ is in bijection with $A \times B$ so that each local view naturally defines a $\Delta \times \Delta$ matrix, i.e., $x_v \in \mathbb{F}_2^{\Delta\times\Delta}$. We will label the faces of $Q(v)$ by pairs of vertices v_1, v_2, where v_1 is connected to v by an edge in A, and v_2 to v by an edge in B. In this case, we denote the unique face defined by these vertices by $[v_1, v_2] \in Q(v)$ and we say that v_1 is a row vertex for v, and that v_2 is a column vertex. We will use the notation $x_v[v_1, v_2]$ to denote the entry of x_v specified by the face $[v_1, v_2]$. Likewise, we will adopt the notation $x_v[v_1, \cdot]$ to denote the row of x_v indexed by the row vertex v_1, and similarly $x_v[\cdot, v_2]$ to denote the column of x_v indexed by v_2. Given neighboring vertices $v \in V_0$ and $v' \in V_1$, the shared row (resp. column) of the local views x_v and $x_{v'}$ can be equivalently denoted by either $x_v[v', \cdot]$ or $x_{v'}[v, \cdot]$ (resp. $x_v[\cdot, v']$ or $x_{v'}[\cdot, v]$).

Let us now define the notion of a local minimum weight correction and other associated objects.

Definition 16. *Let $e \in \mathbb{F}_2^Q$ be a Z error. For each vertex $v \in V_1$, we define $c_v(e)$ as a closest codeword in $C_1^\perp$ to the local view e_v. If there are multiple closest codewords, then we may fix an arbitrary one.*

For each vertex $v \in V_1$, let $R_v^+(e) = e_v - c_v(e) \subseteq Q(v)$. Then we call $R_v^+(e)$ the local minimum weight correction *at the vertex v. We will denote the collection of all local minimum weight corrections by $\mathcal{R}(e) = \{R_v^+(e)\}_{v\in V_1}$. We will also define the total correction*

$$R(e) = \bigcup \mathcal{R}(e) = \bigcup_{v\in V_1} R_v^+(e)\,. \tag{18}$$

Note that the local potential at v is given by

$$U_v(e) = d\left(e_v, C_1^\perp\right) = |e_v - c_v(e)| = |R_v^+(e)|\,, \tag{19}$$

and our goal is to reduce the global potential $U(e) = \sum_{v\in V_1} U_v(e)$ at every step of the decoding. When the error e is understood, we will often simply write c_v, R_v^+, and R for short.

We can now proceed with the proof of Theorem 10, which we split into three cases:

(1) In the first case, we consider whether flipping single qubits can decrease the total potential. If this is not the case, it will introduce extra structure in the set R.
(2) In the second case, we ask if R has high overlap with a codeword of $C_1^\perp$ in a V_1 local view. If so, it will allow us to flip a set of qubits that together can decrease the total potential.
(3) The third and most complicated case is the one complementary to the first two, where no single qubit flip can decrease the total potential, and where R has low overlap with all local codewords. The intuition here is that R cannot be a very large set, so every V_1 local view of the error is close to the local code. Because the error "looks like" a codeword, we are able to apply reasoning similar to the local minimality argument in the proof of the distance of the code. In essence, the expansion of the graph allows us to find a special V_0 vertex whose local view contains a flip-set to decrease the total potential.

5.1 Proof of Cases 1 and 2

In this subsection, we prove Theorem 10 for the first two cases listed above. The terminology and definitions established in this subsection will also be crucial to the proof of case 3. To consider the first case, we define the concept of a metastable configuration.

Definition 17. *Let $e \in \mathbb{F}_2^Q$ be an error. We say that e is* metastable *if flipping any one qubit $q \in Q$ does not decrease the global potential. We also say that $\mathcal{R}(e)$ and $R(e)$ are metastable if they are obtained from a metastable error e. Note that while we only define and use metastability for an error e and its configuration of local minimum weight corrections, the property of metastability is really a property intrinsic to the underlying syndrome σ.*

Note that case 1 pertains precisely to the case when the error e is not metastable. If e is not metastable then there exists some $q \in Q$ which decreases the global potential and Theorem 10 follows. Therefore, in the remainder of this section we consider the case that e (and hence R) is metastable.

Definition 18. *Let $e \in \mathbb{F}_2^Q$ be an error, and let $\mathcal{R} = \{R_v^+(e)\}_{v\in V_1}$ be a set of local minimum weight corrections for e. We say that $\mathcal{R}$ is* disjoint *if $R_v^+(e) \cap R_{v'}^+(e) = \emptyset$ for all $v \neq v'$.*

When $\mathcal{R}$ is a disjoint set of corrections we can think of it as a directed subgraph of $\mathcal{G}_1^\square$ by viewing each R_v^+ as the set of outgoing edges from v (see Figure 2). The local view R_v is then the set of all edges, incoming or outgoing, incident to v in this directed graph.

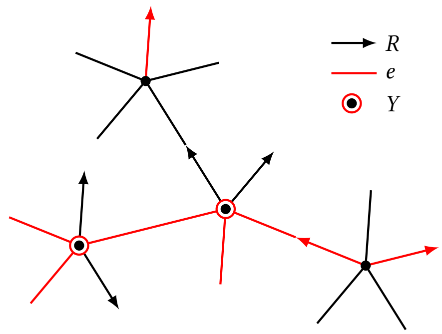

Figure 2: Subsets of $\mathcal{G}_1^\square$ indicating e, R, and elements of Y. In the diagram $C_1^\perp$ is the repetition code (codewords 00000 and 11111). Note that the red edges without an arrow are in y, the red edges with an arrow are in $R \cap e$, and the undecorated black edges are just the remaining edges in $\mathcal{G}_1^\square$.

Note that in this case, the set $\mathcal{R}$ completely defines the underlying directed graph. Conversely, given the directed subgraph, we may uniquely recover $\mathcal{R}$ by taking $R_v^+(e)$ as the set of outgoing edges at each vertex. Therefore we will identify a disjoint $\mathcal{R}$ with the directed subgraph it defines in the following. We can likewise identify the set of total corrections R with the undirected graph underlying $\mathcal{R}$.

Note that $\mathcal{R}$ will always be disjoint when e is a metastable error (otherwise flipping a shared qubit will lower the global potential by 2). For a metastable error, flipping a qubit $q = (v, v') \in R_v^+$, which is a directed edge from v to v', decreases U_v by one and increases $U_{v'}$ by one. We first prove a lemma which shows that metastable errors are somewhat rigid under additional bit-flips.

Lemma 19 (R-flipping). *Let $\mathcal{R}(e)$ be a directed subgraph of $\mathcal{G}_1^\square$ corresponding to a set of local minimum weight corrections for a metastable error e. Suppose furthermore that for some subset $\hat{R} \subseteq R(e)$, flipping all qubits of $\hat{R}$ does not decrease the global potential. Consider the error $e+\hat{R}$. Then a valid configuration $\mathcal{R}(e+\hat{R})$ of locally minimum weight corrections for $e + \hat{R}$ is obtained from $\mathcal{R}(e)$ by reversing the directions of all edges in $\hat{R}$. Moreover, the nearest codewords c_v at each vertex remains unchanged, i.e.,*

$$c_v(e) = e_v + R_v^+(e) = (e + \hat{R})_v + R_v^+(e + \hat{R}) = c_v(e + \hat{R}) \,. \tag{20}$$

Proof. Consider any $v \in V_1$. By definition, each $R_v^+(e)$ is a minimum weight correction to the local code at v, so $c_v(e) = e_v + R_v^+(e)$ and $U_v(e) = |R_v^+(e)|$. Now suppose we flip all qubits in $\hat{R}$. In the local view of v, we have

$$\begin{aligned} c_v(e) &= e_v + \hat{R} \cap Q(v) + R_v^+(e) + \hat{R} \cap Q(v) & (21)\\ &= (e + \hat{R})_v + R_v^+(e) + \hat{R} \cap R_v^+(e) + \hat{R} \cap R_v^-(e) \,, & (22)\end{aligned}$$

where we define $R_v^-(e) = R_v(e) \backslash R_v^+(e)$. Note that $R_v^-(e)$ can be thought of as the set of incoming edges at v in the directed graph defined by $\mathcal{R}(e)$. Therefore, we can bound the weight of the new minimal weight correction for vertex v by

$$\begin{aligned} U_v(e + \hat{R}) &\le |R_v^+(e) + \hat{R} \cap R_v^+(e) + \hat{R} \cap R_v^-(e)| & (23)\\ &= |R_v^+(e) + \hat{R} \cap R_v^+(e)| + |\hat{R} \cap R_v^-(e)| & (24)\\ &= U_v(e) - |\hat{R} \cap R_v^+(e)| + |\hat{R} \cap R_v^-(e)| \,, & (25)\end{aligned}$$

where the first line follows from equation (22) and the second from the disjointness of the sets $R_v^+(e)$ and $R_v^-(e)$. Note that if equality holds in equation (23), then a valid minimum weight correction for $(e + \hat{R})_v$ is given by

$$R_v^+(e + \hat{R}) = R_v^+(e) + \hat{R} \cap R_v^+(e) + \hat{R} \cap R_v^-(e) \,. \tag{26}$$

The set $R_v^+(e + \hat{R})$ above is obtained from $R_v^+(e)$ by removing all outgoing edges in $\hat{R}$ and changing all incoming edges in $\hat{R}$ to outgoing edges. Also note that in this case the nearest codeword remains $c_v(e)$.

Summing inequality (23) for all $v \in V_1$ gives a bound on the global potential as

$$\begin{aligned} U(e + \hat{R}) &\le \sum_{v \in V_1} U_v(e) - \sum_{v \in V_1} |\hat{R} \cap R_v^+(e)| + \sum_{v \in V_1} |\hat{R} \cap R_v^-(e)| & (27)\\ &= U(e) - |\hat{R} \cap R(e)| + |\hat{R} \cap R(e)| & (28)\\ &= U(e) \,, & (29)\end{aligned}$$

where in the second line we've used the fact that $R(e) = \bigsqcup_{v \in V_1} R_v^+(e) = \bigsqcup_{v \in V_1} R_v^-(e)$ by metastability. By the assumption of the lemma, $U(e + \hat{R}) \ge U(e)$. This means inequality (23) must hold with equality for all $v \in V_1$. Hence, we have proven that $\mathcal{R}(e + \hat{R})$ can be taken as $\mathcal{R}(e)$, but with the directions of edges in $\hat{R}$ reversed. □

Remark 20. *In the scenario of the R-flipping lemma, while the error $e + \hat{R}$ may not be metastable itself, the set $\mathcal{R}(e + \hat{R})$ as defined as in the lemma is still disjoint. This new set is a valid correction in the sense that each $R_v^+(e + \hat{R})$ gives a minimum weight correction to the local code — correcting the error $(e + \hat{R})_v$ to $c_v(e + \hat{R}) = c_v(e)$ — at every $v \in V_1$. Note that the set of total corrections remains invariant in this case, i.e., $R(e) = R(e + \hat{R})$.*

In the second case, we assume that R has high overlap with a codeword of $C_1^\perp$. We formalize this property below.

Definition 21 (Low Overlap). *The set R is said to have the* low-overlap *property at $v \in V_1$ if for all codewords $c \in C_1^\perp$, we have $|R_v \cap c| \le |c|/2$. We will say that the set R has the low-overlap property if it has the low-overlap property at every $v \in V_1$.*

Before formally proving case 2, let us first provide some rough intuition. When the low-overlap property is not satisfied, there exists some codeword $c \in C_1^\perp$ at some vertex $v \in V_1$ which has large agreement with R_v. Using the R-flipping Lemma 19, we may assume without loss of generality that $R_v^+ = 0$. Now imagine flipping the set $R_v \cap c$. Since $R_v^+ = 0$, every edge in R_v belongs to a local correction neighboring v. Flipping $R_v \cap c$ will therefore lower the local potential at each of these neighbors by 1. It will also raise the local potential at v, which was zero before. However, since R_v has large overlap with c it is actually more efficient to apply the correction $c \backslash R_v$ instead of $R_v \cap c$. In this case, the local error is pushed out of the neighborhood of its original nearest codeword $c_v(e)$ and into the neighborhood of $c_v(e) + c$ instead. The local potential at v is therefore raised by an amount less than $R_v \cap c$, which results in an overall lowering of the global potential.

Lemma 22. *Let R be metastable. If R does not have the low-overlap property, then there exists $v \in V_1$ and a subset $f \subseteq Q(v)$ such that flipping the qubits of f decreases the total potential.*

Proof. Suppose that R is metastable and does not have the low-overlap property. Then there exists some $v \in V_1$ and some $c \in C_1^\perp \setminus \{0\}$ such that $|R_v(e) \cap c| > |c|/2$. Let $e' = e + R_v^+(e)$. If $U(e') < U(e)$ then we are done. Otherwise $U(e') = U(e)$, and by the R-flipping Lemma 19, we may take $R(e') = R(e)$ with $R_v^+(e') = 0$.

Consider now flipping the additional set of qubits $f' = R_v(e') \cap c$ to obtain the error $e'' = e' + f'$. For each $q = (v', v) \in f'$, we have $q \in R_{v'}^+(e')$, so that $|R_{v'}^+(e'')| = |R_{v'}^+(e')| - 1$. This is the new value of the local potential at v'. Since we had $U_v(e') \equiv |R_v^+(e')| = 0$, the change in the global potential is given by $U(e'') - U(e') = U_v(e'') - |f'|$.

Since $e'_v \in C_1^\perp$, a valid correction for e''_v is given by $f' + c$, where c is the high-overlap codeword from earlier. This correction has weight $|f' + c| = |R_v(e) \cap c + c| < |c|/2 < |R_v(e) \cap c| = |f'|$. Therefore $U_v(e'') - |f'| < 0$, and we have $U(e'') < U(e') = U(e)$. Our desired flip-set is therefore $f = R_v^+(e) + R_v(e) \cap c$. ◻

5.2 Proof of Case 3

The preceding subsection proves Theorem 10 in the cases when R is not metastable, or when R is metastable but does not have the low-overlap property. In what follows, we consider the remaining case where R is both metastable and has the low-overlap property. We summarize our key list of assumptions for this case below for convenience.

Assumption 23. *Let $e \in \mathbb{F}_2^Q$ be a Z error of weight $|e| \le \delta n/6\Delta^{3/2-\varepsilon}$. We assume that e is a reduced error, i.e., it is the minimum weight element of the coset $e + \mathcal{C}_Z^\perp$. We assume that e is a metastable error, and that its set of local minimum weight corrections $R(e)$ satisfies the low-overlap property 21. Finally, we also require that the underlying quantum Tanner code be defined using dual tensor codes of sufficiently large robustness, i.e., with robustness parameter $\Delta^{3/2+\varepsilon'}$ for some $\varepsilon' > 0$. Throughout the rest of the proof, we fix any $\varepsilon < \varepsilon'$.*

The proof of case 3 proceeds in two general steps. In the first step, we show using the expansion of the underlying graphs that, given an error e of sufficiently low weight, there always exists a special vertex $v_0 \in V_0$ with the property that v_0 "sees" many non-trivial codewords of C_A and C_B amongst its shared local views with the minimum weight corrections on neighboring vertices.

The second step of the proof proceeds to analyze the local view at the vertex v_0 described above. We show that due to the pattern of its many shared codewords, it is either the case that $R_{v_0} \subset Q(v_0)$ is sufficiently large to contain a flip-set which reduces the potential, or else it is small enough that e_{v_0} has many columns and rows which are close to non-trivial codewords of C_A and C_B. In the latter case, the robustness of the underlying dual tensor code then implies that e_{v_0} must have sufficient overlap with a Z-stabilizer that the addition of this stabilizer will reduce the weight of e. Since we began without loss of generality with a reduced error e, this leads to a contradiction.

5.2.1 *Existence of $v_0 \in V_0$.*

In the first part of the analysis of the third case, we proceed in a manner parallel to the proof of Theorem 1 in [17]. The goal is to show that for an error e with weight $|e| \le \delta n/6\Delta^{3/2-\varepsilon}$, there always exists a vertex $v_0 \in V_0$ whose local view contains many columns and rows which are close to non-trivial codewords of C_A and C_B. Aside from some differences in definitions, the proofs and results of this subsection are equivalent to their counterparts in [17]. Please see the full paper [13] for the omitted proofs.

Since our goal is to find a vertex $v_0 \in V_0$ whose local view has many rows and columns close non-trivial codewords, we first parametrize the vertices of V_1 with non-trivial nearest codewords. This is captured by the set Y below.

Definition 24. *Let $e \in \mathbb{F}_2^Q$ be an error and let $\mathcal{R} = \{R_v^+(e)\}_{v \in V_1}$ be a set of local minimum weight corrections. We define the set of non-trivially corrected vertices $Y \subseteq V_1$ as*

$$Y = \{v \in V_1 \mid R_v^+ \ne e_v\}. \tag{30}$$

That is, a vertex v is in Y if and only if the result of applying the locally minimum weight correction at v results in a non-trivial codeword i.e. $c_v = e_v + R_v^+ \ne 0$.

To work with the vertex set Y, it will also be convenient to define an edgewise version of the condition $R_v^+ \ne e_v$. To that end, we introduce the set y of "residual errors". Given an error $e \in \mathbb{F}_2^Q$, the elements of y are all of the elements of e which have no overlap with the set of minimum weight corrections $R(e)$ (see Figure 2).

Definition 25. *Let $e \in \mathbb{F}_2^Q$ be an error and let $\mathcal{R} = \{R_v^+(e)\}_{v \in V_1}$ be a set of local minimum weight corrections. The set of "residual" errors is defined by $y = e \backslash R \in \mathbb{F}_2^Q$, i.e., y labels the set of errors which are not in any of the local minimum weight corrections.*

The edges of $\mathcal{G}_1^\square$ indexed by y define a subgraph of $\mathcal{G}_1^\square$ which we will call $G_{1,y}^\square$. This subgraph is closely related to the set Y. It is straightforward to see that every vertex of $\mathcal{G}_{1,y}^\square$ must belong to Y. Conversely, the low-overlap property implies that each vertex of Y must be incident to many edges in $\mathcal{G}_{1,y}^\square$. This means that Y is precisely the vertex set of $\mathcal{G}_{1,y}^\square$ and moreover $\mathcal{G}_{1,y}^\square$ must have large minimum degree. This discussion is formalized below by Lemmas 26 and 27.

Lemma 26. *Let $(v, v') \in y$ be an edge in $\mathcal{G}_{1,y}^\square$. Then both v and v' are elements of Y.*

Proof. By definition, the edge $(v, v') \in y$ is an element of e but not of R. Therefore (v, v') is an element of e_v (and likewise, of $e_{v'}$) but not an element of R_v^+ (and likewise, $R_{v'}^+$). It follows that $e_v \ne R_v^+$ and $e_{v'} \ne R_{v'}^+$. ◻

Lemma 27. *Every vertex $v \in Y$ is incident to at least $\delta\Delta/2$ edges in y. In particular, the subgraph $\mathcal{G}_{1,y}^\square$ has vertex set equal to Y and minimum degree at least $\delta\Delta/2$.*

Each vertex v of $\mathcal{G}_{1,y}^\square$ has a non-trivial nearest codeword $c_v \in C_1^\perp$. To ensure that the individual columns and rows of c_v are themselves close to non-trivial codewords of C_A and C_B, we appeal to the robustness of the dual tensor code $C_1^\perp$. Since robustness only applies to codewords of weight at most $\Delta^{3/2+\varepsilon}$, we first define the concept of a *normal* vertex. Roughly speaking, a vertex is considered *normal* precisely when robustness can be applied to its nearest codeword.

Definition 28. *Let us define a* normal *vertex of Y as a vertex with degree at most $\frac{1}{2}\Delta^{3/2+\varepsilon}$ in $\mathcal{G}_{1,y}^\square$. A vertex of Y which is not normal is* *called* exceptional. *We denote the subsets of normal and exceptional vertices as Y_n and Y_e, respectively.*

Since $\mathcal{G}^{\square}_{1,y}$ has large minimum degree, the expansion of $\mathcal{G}^{\square}_1$ now ensures that as long as $\mathcal{G}^{\square}_{1,y}$ has sufficiently few edges, it must contain many normal vertices. Note that Lemma 29 is the only place where the assumption on the weight of $|e|$ (and hence $|y|$) is explicitly used.

Lemma 29. *Suppose that $|y| \le \delta n/6\Delta^{3/2-\varepsilon} = \delta\Delta^{1/2+\varepsilon}|V_1|/12$. Then the fraction of exceptional vertices in $Y_e \subseteq Y$ is bounded above as*

$$\frac{|Y_e|}{|Y|} \le \frac{576}{\Delta^{1+2\varepsilon}}\,. \tag{31}$$

Using the robustness of $C_1^{\perp}$ and the low-overlap property, we can now show that each column and row of c_v for $v \in Y_n$ is indeed close to a codeword of C_A and C_B.

Lemma 30. *Let $v \in Y_n$ be a normal vertex. Then every column (resp. row) of c_v is distance at most $\Delta^{1/2+\varepsilon}/\delta$ from a codeword in C_A (resp. C_B). Moreover, c_v contains at least one row or column which is close to a non-zero codeword of C_A or C_B.*

Proof. By assumption of v being a normal vertex, we know that $|y_v| = |e_v \backslash R_v| \le \frac{1}{2}\Delta^{3/2+\varepsilon}$. From the low-overlap property, we see that

$$\frac{1}{2}|c_v| \le |(e_v\backslash R_v) \cap c_v| \le |e_v\backslash R_v| \le \frac{1}{2}\Delta^{3/2+\varepsilon}\,. \tag{32}$$

By the robustness of the dual tensor code $C_1^{\perp}$, it follows that the support of c_v is concentrated on the union of at most $|c_v|/\delta\Delta \le \Delta^{1/2+\varepsilon}/\delta$ non-zero columns and rows. Using Lemma 45, we conclude that there exists a decomposition $c_v = \mathbf{c}+\mathbf{r}$, where $\mathbf{c} \in C_A \otimes \mathbb{F}_2^B$ is supported on at most $\Delta^{1/2+\varepsilon}/\delta$ non-zero columns, and where $\mathbf{r} \in \mathbb{F}_2^A \otimes C_B$ is supported on at most $\Delta^{1/2+\varepsilon}/\delta$ non-zero rows. In particular, this implies that each column (resp. row) of c_v is distance at most $\Delta^{1/2+\varepsilon}/\delta$ from a codeword of C_A (resp. C_B). Since c_v is non-zero by definition of Y, it follows at least one of $\mathbf{c}$ or $\mathbf{r}$ is non-zero, so that at least one column or row is close to a non-zero codeword. ◻

Now we are in a position to start the search for our special vertex $v_0 \in V_0$. To that end, we define our analog of "heavy" edges in [17], which we call "dense" edges.

Definition 31 (Dense Edges). *Let $E_y \subseteq E(\mathcal{G}^{\cup})$ be the edges in $\mathcal{G}^{\cup}$ which are incident to some square in y. We say that an edge $(v, v') \in E_y$, where $v \in V_1$ and $v' \in V_0$, is* dense *if it is incident to at least $\delta\Delta - \Delta^{1/2+\varepsilon}/\delta$ squares of c_v.*

We then define the vertex set $W \subseteq V_0$ to be the set of all vertices incident to a normal vertex $v \in Y_n$ through a dense edge.

From the perspective of a vertex $v' \in V_0$, only individual columns and rows of its neighboring nearest codewords c_v are visible. Dense edges are precisely the edges through which v' expects to see non-trivial codewords of C_A or C_B. The set $W \subseteq V_1$ defined above can therefore be thought of as the set of "candidate" v_0's. We will identify a vertex of W with a linear number of dense edges but a sublinear number of exceptional neighbors in Y_e. Such a vertex will allows us to utilize the robustness properties of the local codes.

We first show that each $v' \in W$ must have many neighbors in Y.

Lemma 32. *The degree in E_y of any $v' \in W$ is at least $\frac{1}{2}\delta\Delta - \Delta^{1/2+\varepsilon}/\delta$. In particular, every $v' \in W$ is adjacent to at least $\frac{1}{2}\delta\Delta - \Delta^{1/2+\varepsilon}/\delta$ vertices in Y.*

Proof. Let $v' \in W$. By assumption, there exists a dense edge (v, v') connecting v' to a normal vertex $v \in Y_n$. Let us assume without loss of generality that (v, v') is a B-edge so that $c_v[\cdot, v']$ defines a column of c_v.

Note that the degree of v' in E_y is lower bounded by the weight of the corresponding column in y_v, i.e., $\deg_{E_y}(v') \ge |y_v[\cdot, v']|$.

Let $c_A \in C_A$ denote the codeword closest to $c_v[\cdot, v']$. Since (v, v') is dense, it follows from Lemma 30 that c_A is non-zero. We can form the matrix which is zero everywhere except on the v'-column, where it is equal to c_A. Note that this matrix will be a codeword of $C_1^{\perp}$, and that the low-overlap property applied to this codeword implies that $|R_v[\cdot, v'] \cap c_A| \le |c_A|/2$.

Then we have

$$\begin{aligned}
|c_A| &= |c_v[\cdot, v'] \cap c_A| + |c_A \backslash c_v[\cdot, v']| && (33)\\
&\le |c_v[\cdot, v'] \cap c_A| + \Delta^{1/2+\varepsilon}/\delta && (34)\\
&\le |y_v[\cdot, v'] \cap c_A| + |R_v[\cdot, v'] \cap c_A| + \Delta^{1/2+\varepsilon}/\delta && (35)\\
&\le |y_v[\cdot, v']| + |c_A|/2 + \Delta^{1/2+\varepsilon}/\delta\,, && (36)
\end{aligned}$$

where the second line follows from Lemma 30, the third line from the fact that $c_v \subseteq y_v \cup R_v$, and the last line from the low-overlap property. This gives us

$$\delta\Delta/2 \le |c_A|/2 \le |y_v[\cdot, v']| + \Delta^{1/2+\varepsilon}/\delta\,. \tag{37}$$

Therefore we have

$$\deg_{E_y}(v') \ge |y_v[\cdot, v']| \ge \frac{1}{2}\delta\Delta - \Delta^{1/2+\varepsilon}/\delta\,. \tag{38}$$

Lemma 26 now ensures that each $v' \in W$ is adjacent to at least $\frac{1}{2}\delta\Delta - \Delta^{1/2+\varepsilon}/\delta$ elements of Y. ◻

Knowing that each $v' \in W$ has many neighbors in Y, the expansion of $\mathcal{G}^{\cup}$ implies that the number of vertices in W must be small compared to Y.

Lemma 33. *For Δ large enough, the set W satisfies the bound*

$$|W| \le \frac{81}{\delta^2\Delta}|Y|\,. \tag{39}$$

We expect each $v \in Y_n$ to be incident to at least one dense edge by virtue of having a column or row close to a non-trivial codeword. This means that the total number of dense edges is at least on the order of $|Y_n|$. Lemma 33 in turn suggests that the number of dense edges is large relative to $|W|$. This implies that the average vertex in W should be incident to a large number of dense edges. This is formalized by Lemma 34 and Corollary 35 below.

Lemma 34. *Let $\mathcal{D}$ denote the set of dense edges incident to W. Then the average degree of W in $\mathcal{D}$ is bounded by*

$$\frac{|\mathcal{D}|}{|W|} \ge 2\alpha\Delta \tag{40}$$

for some constant $\alpha > 0$ (which we may choose to be anything smaller than $\delta^2/192$ by taking Δ sufficiently large).

Corollary 35. *At least an $\alpha/2$ fraction of the vertices in W are incident to at least $\alpha\Delta$ dense edges.*

Proof. Let η be the fraction of vertices in W with dense degree greater than $\alpha\Delta$. The maximum degree of any vertex in $\mathcal{G}^{\cup}$ is 2Δ, so it follows that

$$2\alpha\Delta \leq \frac{|\mathcal{D}|}{|W|} \leq 2\Delta\eta + (1-\eta)\alpha\Delta\,. \tag{41}$$

Therefore we have $\eta \geq \alpha/(2-\alpha) \geq \alpha/2$. □

We have now shown that there exists a subset of vertices in W incident to many dense edges. We must now show that within this subset, there exists vertices which are *not* adjacent to many exceptional vertices in Y_e. We expect this to be the case since the number of exceptional vertices is small relative to the number of normal vertices. To proceed, we bound the number of edges shared between W and Y_e in Lemma 36 below.

Lemma 36. *The total number of edges in $\mathcal{G}^{\cup}$ between W and Y_e is bounded above by*

$$|E_{\mathcal{G}^{\cup}}(W, Y_e)| \leq 193\Delta^{1/2-\varepsilon}|W|\,. \tag{42}$$

Putting everything together, we can finally show the existence of the special vertex v_0, as formalized by Corollary 37.

Corollary 37. *At least an $\alpha/4$ fraction of the vertices of W:*

(1) *are incident to at least $\alpha\Delta$ dense edges, and*
(2) *are adjacent to at most $(772/\alpha)\Delta^{1/2-\varepsilon} \equiv \beta\Delta^{1/2-\varepsilon}$ vertices of Y_e.*

In particular, at least one such vertex exists since $\alpha > 0$.

Proof. Let W_1 be the subset of vertices in W satisfying condition 1, and let $\overline{W_2}$ be the subset of vertices in W *not* satisfying condition 2. Since each vertex of $\overline{W_2}$ is adjacent to more than $(772/\alpha)\Delta^{1/2-\varepsilon}$ vertices of Y_e, we get

$$|\overline{W_2}| \cdot (772/\alpha)\Delta^{1/2-\varepsilon} \leq |E_{\mathcal{G}^{\cup}}(W, Y_e)| \leq 193\Delta^{1/2-\varepsilon}|W|\,, \tag{43}$$

which implies that $|\overline{W_2}| \leq (\alpha/4)|W|$. Therefore the set of vertices satisfying both condition 1 and 2 is bounded below by

$$|W_1\backslash\overline{W_2}| \geq |W_1| - |\overline{W_2}| \geq \alpha|W|/2 - \alpha|W|/4 = \alpha|W|/4\,. \tag{44}$$

□

5.2.2 The Local View at v_0. Let $v_0 \in W$ be a vertex satisfying the conditions of Corollary 37. In this subsection, we analyze the structure of y and R *from the perspective of* $v_0 \in V_0$. Let y_0, e_0, and R_0 denote the local views of y, e, and R at the vertex v_0.

We will write $[v, v'] \in Q(v_0)$ to denote the face anchored at v_0 with neighboring V_1 vertices v and v', with the implicit convention that unprimed vertices v denote row vertices, and primed vertices v' denote column vertices. We will also write $N(v_0) \subseteq V_1$ to denote the set of all neighbors of v_0 in $\mathcal{G}^{\cup}$, and $N_r(v_0)$ and $N_c(v_0)$ to denote the set of row and column vertex neighbors, respectively.

We first show a key result regarding the structure of y_0 and R_0. As a consequence of metastability, the edges of R_0 must complement the edges of y_0 to complete codewords on either columns or rows shared with neighboring local views (see equation 45). This allows us to split R_0 into disjoint parts depending on whether columns or rows are corrected.

Lemma 38. *We can write $R_0 = R_{\text{col}} \sqcup R_{\text{row}}$, where we have*

$$\begin{aligned} y_0[v,\cdot] \sqcup R_{\text{row}}[v,\cdot] &= c_v[v_0,\cdot]\,, \qquad \textit{and} \\ y_0[\cdot,v'] \sqcup R_{\text{col}}[\cdot,v'] &= c_{v'}[\cdot,v_0]\,, \end{aligned} \tag{45}$$

for all $v \in N_r(v_0)$ and $v' \in N_c(v_0)$.

Proof. Let $q = [v, v'] \in R_0$. Since R is metastable, it follows that q belongs to exactly one of R_v^+ or $R_{v'}^+$. Suppose without loss of generality that $q \in R_v^+$. Since $e_v + R_v^+ = c_v$, it follows that $q \in c_v$ if and only if $q \notin e$. Likewise, since $q \notin R_{v'}^+$, it follows that $q \in c_{v'}$ if and only if $q \in e$. It follows that q must be an element of exactly one of c_v or $c_{v'}$.

Let $R_{\text{row}} \subseteq R_0$ denote the collection of all $q \in R_0$ which belong to c_v for some row vertex v. Likewise, let $R_{\text{col}} \subseteq R_0$ denote the collection of all $q \in R_0$ which belong to $c_{v'}$ for some column vertex v'. Then by the preceding discussion we have

$$R_0 = R_{\text{row}} \sqcup R_{\text{col}}\,. \tag{46}$$

Next, we show equation (45). We focus on the row case, with the column case being analogous. Note that we have

$$\begin{aligned} y_0[v,\cdot] &= e_v[v_0,\cdot]\backslash R_v[v_0,\cdot] \subseteq e_v[v_0,\cdot]\backslash R_v^+[v_0,\cdot] \\ &\subseteq e_v[v_0,\cdot] + R_v^+[v_0,\cdot] = c_v[v_0,\cdot]\,. \end{aligned} \tag{47}$$

Also, we have $R_{\text{row}}[v,\cdot] \subseteq c_v[v_0,\cdot]$ by definition. This implies that

$$y_0[v,\cdot] \sqcup R_{\text{row}}[v,\cdot] \subseteq c_v[v_0,\cdot]\,. \tag{48}$$

Conversely, we have

$$\begin{aligned} c_v[v_0,\cdot] &= e_v[v_0,\cdot] + R_v^+[v_0,\cdot] \subseteq e_v[v_0,\cdot] \cup R_v[v_0,\cdot] \\ &= y_v[v_0,\cdot] \sqcup R_v[v_0,\cdot] = y_0[v,\cdot] \sqcup R_0[v,\cdot]\,. \end{aligned} \tag{49}$$

Since all elements of R_0 belonging to c_v are by definition in R_{row}, it follows that we have

$$c_v[v_0,\cdot] \subseteq y_0[v,\cdot] \sqcup R_{\text{row}}[v,\cdot]\,. \tag{50}$$

It therefore follows that

$$\begin{aligned} y_0[v,\cdot] \sqcup R_{\text{row}}[v,\cdot] &= c_v[v_0,\cdot]\,, \qquad \text{and} \\ y_0[\cdot,v'] \sqcup R_{\text{col}}[\cdot,v'] &= c_{v'}[\cdot,v_0]\,, \end{aligned} \tag{51}$$

which hold for all $v \in N_r(v_0)$ and $v' \in N_c(v_0)$. □

Corollary 39. *Let $[v, v'] \in Q(v_0)$. If $v \notin Y$ then $R_{\text{row}}[v,\cdot] = 0$. Likewise, if $v' \notin Y$ then $R_{\text{col}}[\cdot,v'] = 0$.*

Proof. We work with the row vertex v, with the column case being identical. Suppose that $v \notin Y$. Then by definition, the closest codeword to e_v at v is the trivial codeword $c_v = 0$. Evaluating equation (45) at the row defined by edge (v_0, v), we have

$$y_0[v,\cdot] \sqcup R_{\text{row}}[v,\cdot] = c_v[v_0,\cdot] = 0\,, \tag{52}$$

which implies that $R_{\text{row}}[v,\cdot] = 0$. □

Let us now provide some intuition for the remainder of the proof. The decomposition shown in Lemma 38 allows us to consider two separate scenarios:

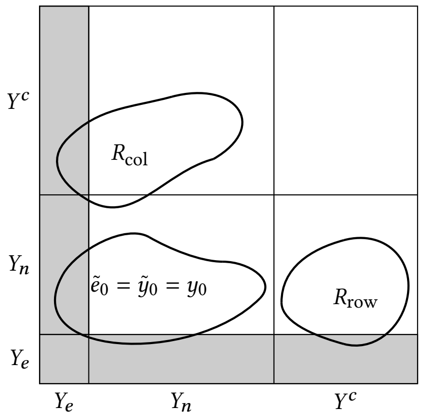

Figure 3: The v_0 local view after flipping $R_0 \cap e$. The various regions indicate the possible supports of the labeled quantities.

(1) First, imagine that R_0 has high weight relative to y_0. Then Lemma 38 suggests that the columns and rows of R_0 are close to codewords of C_A and C_B. An argument similar to the one used in the proof of case 2 would seem to suggest that there exists some subset of R_0 which would decrease the global potential when flipped.
(2) Alternatively, consider the scenario where R_0 has low weight relative to y_0. In this case, y_0 is close to e_0, and Lemma 38 now implies that the columns and rows of e_0 are close to codewords of C_A and C_B. The robustness of the dual tensor code $C_1^{\perp}$ suggests that we can find a codeword $c_0 \in C_A \otimes C_B$, i.e., a Z-stabilizer, which has high overlap with e_0. But this is in contradiction with the fact that e was assumed to be a reduced error.

Given the discussion above, we will finish the proof as follows: Suppose that no subset of $Q(v_0)$ decreases the global potential when flipped. We will show that this necessarily implies that R_0 has sufficiently low weight (as formalized by Lemma 41) that the argument outlined in scenario 2 can be carried out. Specifically, we will show that there exists some $c_0 \in C_A \otimes C_B$ such that $|e + c_0| < |e|$, contradicting the fact that e is reduced.

To proceed, we will need to analyze the value of the potential on a new configuration of errors, one obtained from e by flipping all the qubits of $e \cap R_0$. The utility of this new error configuration $\tilde{e}$ comes from the fact that the rows of R_{row} and columns of R_{col} are exactly equal to the local minimum weight corrections for $\tilde{e}$ (see equation 53), giving us better control over the potential.

Let $\tilde{e} = e + e \cap R_0 = e \backslash R_0$. We first show that some key quantities remain unchanged in this new error configuration. Since $\tilde{e}$ is obtained from e by flipping a subset of R without decreasing the global potential, the R-flipping Lemma 19 implies that the new total correction $\tilde{R} \equiv R(\tilde{e})$ will be equal to the old one, i.e., $\tilde{R} = R(\tilde{e}) = R(e)$. This implies that the vector of residual errors y likewise stays invariant, i.e., $\tilde{y} = y(\tilde{e}) = \tilde{e} \backslash \tilde{R} = e \backslash R(e) = y(e)$. The situation after flipping $R_0 \cap e$ is illustrated in Figure 3 and summarized by Lemma 40.

Lemma 40. *Suppose that no subset of $Q(v_0)$ decreases the global potential when flipped. Let $\tilde{e} = e \backslash R_0$ denote the configuration of errors obtained after flipping all the elements of $R_0 \cap e$. In this new error configuration, we may take the local minimum weight corrections to be as given by the R-flipping Lemma 19. Specifically, we have $\tilde{R} = R$ and $\tilde{y} \equiv \tilde{e} \backslash \tilde{R} = e \backslash R = y$. Moreover, we have $\tilde{e}_0 = y_0$, and*

$$R_{\mathrm{row}}[v, \cdot] = \tilde{R}_v^{+}[v_0, \cdot], \quad \text{and} \quad R_{\mathrm{col}}[\cdot, v'] = \tilde{R}_{v'}^{+}[\cdot, v_0], \tag{53}$$

for all $[v, v'] \in Q(v_0)$.

Proof. The fact that we may take $\tilde{R} = R$ follows directly from the R-flipping Lemma 19, which ensures that the original and updated local minimum weight correction sets differ only by the orientations of edges. It follows that we also have

$$y = e \backslash R = (e \backslash R_0) \backslash R = \tilde{e} \backslash \tilde{R} = \tilde{y}. \tag{54}$$

Note that since $\tilde{e} \cap R_0 = \emptyset$, it also follows that $\tilde{y}_0 = \tilde{e}_0$.

Now, let v be a neighbor of v_0, and suppose without loss of generality that it is a row vertex. By the R-flipping Lemma 19, the nearest codeword c_v remains unchanged after flipping $R_0 \cap e$. In particular, we must have

$$\begin{aligned} y_0[v, \cdot] \sqcup R_{\mathrm{row}}[v, \cdot] = c_v[v_0, \cdot] &= \tilde{e}_0[v, \cdot] + \tilde{R}_v^{+}[v_0, \cdot] \\ &= y_0[v, \cdot] \sqcup \tilde{R}_v^{+}[v_0, \cdot], \end{aligned} \tag{55}$$

where the first equality follows from Lemma 38, the second from the invariance of the codeword c_v, and the last from the facts that $\tilde{e}_0 = \tilde{y}_0 = y_0$ and $\tilde{e}_0[v, \cdot] \cap \tilde{R}_v^{+}[v_0, \cdot] \subseteq \tilde{e}_0[v, \cdot] \cap \tilde{R}_0[v, \cdot] = \emptyset$. It follows that we must have $R_{\mathrm{row}}[v, \cdot] = \tilde{R}_v^{+}[v_0, \cdot]$. □

Since the rows (resp. columns) of R_{row} (resp. R_{col}) are equal to the local minimum weight corrections (for $\tilde{e}$) on neighboring vertices, we expect that R_0 cannot be too large. Otherwise, R_0 would have enough overlap with the neighboring local minimum weight corrections that subsets of it can start lowering the potential. Therefore the fact that no subset of R_0 can lower the potential implicitly places a bound on its size. This is formalized by Lemma 41 below.

Lemma 41. *Suppose that no subset of $Q(v_0)$ decreases the global potential U when flipped. Then we have*

$$|R_0| \le \frac{3\Delta^{3/2+\varepsilon}}{\delta} \tag{56}$$

for sufficiently large Δ.

Proof. Consider the error configuration $\tilde{e} = e \backslash R_0$. By assumption we have $U(\tilde{e}) = U(e)$. Using Lemma 40, we have $\tilde{e}_0 = \tilde{y}_0 = y_0$ and $\tilde{R}_0 = R_0$.

Let v be, without loss of generality, a row vertex. Since we have $R_{\mathrm{row}}[v, \cdot] = \tilde{R}_v^{+}[v_0, \cdot]$, it follows that flipping $R_{\mathrm{row}}[v, \cdot]$ decreases the local potential $U_v(\tilde{e})$ by $|R_{\mathrm{row}}[v, \cdot]|$, i.e.,

$$U_v(\tilde{e} + R_{\mathrm{row}}[v, \cdot]) = U_v(\tilde{e}) - |R_{\mathrm{row}}[v, \cdot]|. \tag{57}$$

Now, suppose that $v \in Y_n$. Let c_B be the closest codeword of C_B to $c_v[v_0, \cdot]$. Then

$$\begin{aligned} U_v(\tilde{e} + y_0[v, \cdot]) &= U_v(\tilde{e} + R_{\text{row}}[v, \cdot] + c_v[v_0, \cdot]) && (58)\\ &\le U_v(\tilde{e} + R_{\text{row}}[v, \cdot] + c_B) + \frac{\Delta^{1/2+\varepsilon}}{\delta} && (59)\\ &= U_v(\tilde{e} + R_{\text{row}}[v, \cdot]) + \frac{\Delta^{1/2+\varepsilon}}{\delta} && (60)\\ &= U_v(\tilde{e}) - |R_{\text{row}}[v, \cdot]| + \frac{\Delta^{1/2+\varepsilon}}{\delta}, && (61) \end{aligned}$$

where the first equality follows from the fact that

$$y_0[v, \cdot] \sqcup R_{\text{row}}[v, \cdot] = y_0[v, \cdot] + R_{\text{row}}[v, \cdot] = c_v[v_0, \cdot]. \quad (62)$$

The second line follows from Lemma 30, and the third line follows from the fact that $U_v(e + c) = U_v(e)$ for any $c \in C_1^{\perp}$. The last line is just equation (57). Note that an analogous version of inequality (61) also holds for column vertices.

Consider now the global potential $U(\tilde{e} + y_0)$. Note that it follows from Lemma 26 that y_0 will have empty intersection with the local view of any v not in Y, so that only the local potentials associated with vertices of Y can be affected by flipping y_0. We will bound the potential by explicitly separating out the contributions of the exceptional vertices in Y_e over which we have little control. Let us write $\beta \equiv 772/\alpha$ for the constant appearing in Corollary 37. Then we can bound the change in the potential by

$$\begin{aligned} 0 &\le U(\tilde{e} + y_0) - U(\tilde{e}) && (63)\\ &= \sum_{v \in N(v_0) \cap Y} (U_v(\tilde{e} + y_0) - U_v(\tilde{e})) && (64)\\ &\le \sum_{v \in N(v_0) \cap Y_n} (U_v(\tilde{e} + y_0) - U_v(\tilde{e})) + \beta \Delta^{3/2-\varepsilon}, && (65) \end{aligned}$$

where the first inequality follows from the assumption that no subset of $Q(v_0)$ decreases the global potential when flipped, the second line from the fact that only the local views associated with vertices of $N(v_0) \cap Y$ are affected by flipping y_0, and the last line removes the contributions resulting from the vertices in Y_e. The $\beta \Delta^{3/2-\varepsilon}$ term in the last line comes from the fact that there are at most $\beta \Delta^{1/2-\varepsilon}$ vertices of $N(v_0) \cap Y_e$ as a result of Corollary 37, each of which can increase the weight of the potential by at most Δ.

Splitting the sum above into row and column parts and applying inequality (61), we get

$$\sum_{v \in N(v_0) \cap Y_n} (U_v(\tilde{e} + y_0) - U_v(\tilde{e})) \quad (66)$$

$$\le \sum_{v \in N_r(v_0) \cap Y_n} \left(-|R_{\text{row}}[v, \cdot]| + \frac{\Delta^{1/2+\varepsilon}}{\delta} \right) + \sum_{v' \in N_c(v_0) \cap Y_n} \left(-|R_{\text{col}}[\cdot, v']| + \frac{\Delta^{1/2+\varepsilon}}{\delta} \right) \quad (67)$$

$$\le - \sum_{v \in N_r(v_0) \cap Y_n} |R_{\text{row}}[v, \cdot]| - \sum_{v' \in N_c(v_0) \cap Y_n} |R_{\text{col}}[\cdot, v']| + \frac{2\Delta^{3/2+\varepsilon}}{\delta}. \quad (68)$$

By Corollary 39, it follows that the rows of R_{row} (and columns of R_{col}, respectively) are zero if the indexing vertex is not in Y. It follows that we have

$$\sum_{v \in N_r(v_0) \cap Y_n} |R_{\text{row}}[v, \cdot]| = \sum_{\substack{v \in N_r(v_0) \\ v \notin Y_e}} |R_{\text{row}}[v, \cdot]| \ge |R_{\text{row}}| - \beta \Delta^{3/2-\varepsilon}, \quad (69)$$

and likewise

$$\sum_{v' \in N_c(v_0) \cap Y_n} |R_{\text{col}}[\cdot, v']| = \sum_{\substack{v' \in N_c(v_0) \\ v' \notin Y_e}} |R_{\text{col}}[\cdot, v']| \ge |R_{\text{col}}| - \beta \Delta^{3/2-\varepsilon}, \quad (70)$$

where the $\beta \Delta^{3/2-\varepsilon}$ correction term again comes from the vertices in Y_e over which we have no control. Altogether, we have

$$0 \le -|R_{\text{row}}| - |R_{\text{col}}| + \frac{2\Delta^{3/2+\varepsilon}}{\delta} + 3\beta \Delta^{3/2-\varepsilon}. \quad (71)$$

Taking Δ sufficiently large so that $\Delta^{2\varepsilon} \ge 3\delta\beta$, we finally get

$$|R_0| \le \frac{3\Delta^{3/2+\varepsilon}}{\delta}. \quad (72)$$

□

Lemma 41 shows that R_0 is small. This now allows us to follow the remaining steps outlined in scenario 2 above to complete the proof of Theorem 10.

Corollary 42. *Suppose that no subset of $Q(v_0)$ decreases the global potential U when flipped. Then we have*

$$d(y_0, C_A \otimes \mathbb{F}_2^{\Delta}) + d(y_0, \mathbb{F}_2^{\Delta} \otimes C_B) \le \frac{10\Delta^{3/2+\varepsilon}}{\delta} \quad (73)$$

for sufficiently large Δ.

Proof. Consider the distance of y_0 to the row codespace $\mathbb{F}_2^A \otimes C_B$ (with the column case being identical). From equation (45), we have

$$y_0[v, \cdot] + R_{\text{row}}[v, \cdot] = y_0[v, \cdot] \sqcup R_{\text{row}}[v, \cdot] = c_v[v_0, \cdot]. \quad (74)$$

If $v \notin Y$ then Corollary 39 implies that each of the terms above is zero. If $v \in Y_n$, then Lemma 30 implies that

$$d(y_0[v, \cdot] + R_{\text{row}}[v, \cdot], C_B) = d(c_v[v_0, \cdot], C_B) \le \frac{\Delta^{1/2+\varepsilon}}{\delta}. \quad (75)$$

Summing over all rows, and accounting for the exceptional vertices $v \in Y_e$, we get

$$d(y_0 + R_{\text{row}}, \mathbb{F}_2^A \otimes C_B) \le \frac{\Delta^{3/2+\varepsilon}}{\delta} + \beta \Delta^{3/2-\varepsilon}, \quad (76)$$

where the $\Delta^{3/2+\varepsilon}$ term comes from the non-exceptional vertices and the $\Delta^{3/2-\varepsilon}$ term from the exceptional vertices. Since

$$|R_{\text{row}}| \le |R_0| \le \frac{3\Delta^{3/2+\varepsilon}}{\delta} \quad (77)$$

by Lemma 41, it follows that we have

$$d(y_0, \mathbb{F}_2^A \otimes C_B) \le \frac{4\Delta^{3/2+\varepsilon}}{\delta} + \beta \Delta^{3/2-\varepsilon} \le \frac{5\Delta^{3/2+\varepsilon}}{\delta}, \quad (78)$$

where the last inequality follows from the fact that we took Δ large enough so that $\Delta^{2\varepsilon} \ge 3\beta\delta$ in Lemma 41. □

Corollary 43. *Suppose no subset of $Q(v_0)$ decreases the global potential U when flipped. Then the local view y_0 has weight*

$$|y_0| \geq \frac{1}{4}\alpha\delta\Delta^2 \tag{79}$$

for sufficiently large Δ.

Proof. From Corollary 37 it follows that v_0 is adjacent to either $\geq (\alpha\Delta - \beta\Delta^{1/2-\varepsilon})/2$ normal row vertices $v \in N_r(v_0) \cap Y_n$ or $\geq (\alpha\Delta - \beta\Delta^{1/2-\varepsilon})/2$ normal column vertices $v' \in N_c(v_0) \cap Y_n$ through dense edges. Suppose without loss of generality that it is the former. Then by definition of dense edges, it follows that $|c_v[v_0, \cdot]| \geq \delta\Delta - \Delta^{1/2+\varepsilon}/\delta$ for each of these vertices.

Summing the first equation in (45) over all row vertices v, we get

$$\begin{aligned} |y_0| + |R_{\text{row}}| &= \sum_{v \in N_r(v_0)} |y_0[v, \cdot] \sqcup R_{\text{row}}[v, \cdot]| && (80) \\ &= \sum_{v \in N_r(v_0)} |c_v[v_0, \cdot]| && (81) \\ &\geq (\alpha\Delta - \beta\Delta^{1/2-\varepsilon})(\delta\Delta - \Delta^{1/2+\varepsilon}/\delta)/2\,, && (82) \end{aligned}$$

where the last inequality follows from the preceding discussion. Choosing Δ sufficiently large so that

$$(\alpha\Delta - \beta\Delta^{1/2-\varepsilon})(\delta\Delta - \Delta^{1/2+\varepsilon}\delta) \geq \frac{2}{3}\alpha\delta\Delta^2 \tag{83}$$

and applying Lemma 41, we get

$$|y_0| \geq \frac{1}{3}\alpha\delta\Delta^2 - \frac{3\Delta^{3/2+\varepsilon}}{\delta}\,. \tag{84}$$

This implies that $|y_0| \geq \frac{1}{4}\alpha\delta\Delta^2$, for sufficiently large Δ. □

Finally, we are now in a position to complete the proof of Theorem 10.

Proof of Theorem 10. Since the code $C_1^\perp$ is chosen to be $\Delta^{3/2+\varepsilon'}$ robust for $\varepsilon' > \varepsilon$, it follows from Corollary 42 and Proposition 6 that there exists some $c_0 \in C_A \otimes C_B$ such that $|y_0 - c_0| \leq 15\Delta^{3/2+\varepsilon}/\delta$, which holds so long as Δ is chosen large enough so that $\delta\Delta^{\varepsilon'} \geq 10\Delta^{\varepsilon}$. Applying Lemma 41, this implies that

$$|e_0 + c_0| = |y_0 + e_0 \cap R_0 + c_0| \leq |y_0 + c_0| + |R_0 \cap e_0| \leq \frac{18\Delta^{3/2+\varepsilon}}{\delta}\,. \tag{85}$$

Since we have $|e_0| \geq |y_0| \geq (\alpha\delta/4)\Delta^2$, it follows that we have $|e_0 + c_0| < |e_0|$ whenever

$$\frac{72}{\alpha\delta^2} < \Delta^{1/2-\varepsilon}\,. \tag{86}$$

This contradicts the fact that e was chosen to be a reduced error. □

ACKNOWLEDGEMENTS

The authors would like to thank Zhiyang He for his valuable suggestions and his careful reading of an earlier draft of this work. We also thank Anand Natarajan, John Preskill, and Michael Beverland for helpful comments and discussions. S.G. acknowledges funding from the U.S. Department of Energy (DE-AC02-07CH11359), and the National Science Foundation (PHY-1733907). C.A.P. acknowledges funding from the Air Force Office of Scientific Research (AFOSR), FA9550-19-1-0360. The Institute for Quantum Information and Matter is an NSF Physics Frontiers Center. E.T. acknowledges funding received from DARPA 134371-5113608, DOD grant award KK2014.

REFERENCES

[1] Anurag Anshu, Nikolas P. Breuckmann, and Chinmay Nirkhe. 2022. NLTS Hamiltonians from good quantum codes. https://doi.org/10.48550/ARXIV.2206.13228

[2] Eli Ben-Sasson and Madhu Sudan. 2006. Robust Locally Testable Codes and Products of Codes. *Random Struct. Algorithms* 28, 4 (2006), 387–402. https://doi.org/10.1007/978-3-540-27821-4_26

[3] H. Bombin and M. A. Martin-Delgado. 2006. Topological Quantum Distillation. *Phys. Rev. Lett.* 97 (2006), 180501. Issue 18. https://doi.org/10.1103/PhysRevLett.97.180501

[4] 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

[5] A. R. Calderbank and Peter W. Shor. 1996. Good quantum error-correcting codes exist. *Phys. Rev. A* 54 (1996), 1098–1105. Issue 2. https://doi.org/10.1103/PhysRevA.54.1098

[6] 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

[7] Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes. 2022. Locally Testable Codes with Constant Rate, Distance, and Locality. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing* (Rome, Italy) *(STOC 2022)*. Association for Computing Machinery, New York, NY, USA, 357–374. https://doi.org/10.1145/3519935.3520024

[8] Irit Dinur, Min-Hsiu Hsieh, Ting-Chun Lin, and Thomas Vidick. 2022. Good Quantum LDPC Codes with Linear Time Decoders. https://doi.org/10.48550/ARXIV.2206.07750

[9] Lior Eldar and Aram W Harrow. 2017. Local Hamiltonians whose ground states are hard to approximate. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 427–438. https://doi.org/10.1109/FOCS.2017.46

[10] Shai Evra, Tali Kaufman, and Gilles Zémor. 2022. Decodable Quantum LDPC Codes beyond the $\sqrt{n}$ Distance Barrier Using High-Dimensional Expanders. *SIAM J. Comput.* 0, 0 (2022), FOCS20–276–FOCS20–316. https://doi.org/10.1137/20M1383689 arXiv:https://doi.org/10.1137/20M1383689

[11] M. H. Freedman and M. B. Hastings. 2013. Quantum Systems on Non-k-Hyperfinite Complexes: A Generalization of Classical Statistical Mechanics on Expander Graphs. (2013). https://doi.org/10.48550/ARXIV.1301.1363

[12] Daniel Gottesman. 2014. Fault-Tolerant Quantum Computation with Constant Overhead. *Quantum Info. Comput.* 14, 15–16 (2014), 1338–1372.

[13] Shouzhen Gu, Christopher A. Pattison, and Eugene Tang. 2022. An efficient decoder for a linear distance quantum LDPC code. https://doi.org/10.48550/ARXIV.2206.06557

[14] 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.* Association for Computing Machinery, New York, NY, USA, 1276–1288. https://doi.org/10.1145/3406325.3451005

[15] Gleb Kalachev and Pavel Panteleev. 2022. Two-sided Robustly Testable Codes. https://doi.org/10.48550/ARXIV.2206.09973

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

[17] Anthony Leverrier and Gilles Zémor. 2022. Quantum Tanner codes. https://doi.org/10.48550/ARXIV.2202.13641

[18] Anthony Leverrier and Gilles Zémor. 2023. *Efficient decoding up to a constant fraction of the code length for asymptotically good quantum codes.* Society for Industrial and Applied Mathematics, 1216–1244. https://doi.org/10.1137/1.9781611977554.ch45 arXiv:https://epubs.siam.org/doi/pdf/10.1137/1.9781611977554.ch45

[19] Ting-Chun Lin and Min-Hsiu Hsieh. 2022. Good quantum LDPC codes with linear time decoder from lossless expanders. *arXiv:2203.03581 [quant-ph]* (2022). https://doi.org/10.48550/ARXIV.2203.03581 arXiv: 2203.03581.

[20] Pavel Panteleev and Gleb Kalachev. 2022. Asymptotically Good Quantum and Locally Testable Classical LDPC Codes. *arXiv:2111.03654 [quant-ph]* (2022). https://doi.org/10.48550/ARXIV.2111.03654 arXiv: 2111.03654.

[21] 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

[22] M. Sipser and D.A. Spielman. 1996. Expander codes. *IEEE Transactions on Information Theory* 42, 6 (1996), 1710–1722. https://doi.org/10.1109/18.556667

[23] A. M. Steane. 1996. Error Correcting Codes in Quantum Theory. *Phys. Rev. Lett.* 77 (1996), 793–797. Issue 5. https://doi.org/10.1103/PhysRevLett.77.793

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