




Single-Shot Decoding of Good Quantum LDPC Codes

Shouzhen Gu¹ , Eugene Tang², Libor Caha³, Shin Ho Choe³,
Zhiyang He⁴, Aleksander Kubica⁵

¹ Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, CA, USA.
E-mail: sggu@caltech.edu

² Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA, USA

³ School of Computation, Information and Technology, Technical University of Munich and Munich Center for Quantum Science and Technology, Munich, Germany

⁴ Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, USA

⁵ AWS Center for Quantum Computing and California Institute of Technology, Pasadena, CA, USA

Received: 3 July 2023 / Accepted: 25 January 2024

Published online: 14 March 2024 – © The Author(s) 2024

Abstract: Quantum Tanner codes constitute a family of quantum low-density parity-check codes with good parameters, i.e., constant encoding rate and relative distance. In this article, we prove that quantum Tanner codes also facilitate single-shot quantum error correction (QEC) of adversarial noise, where one measurement round (consisting of constant-weight parity checks) suffices to perform reliable QEC even in the presence of measurement errors. We establish this result for both the sequential and parallel decoding algorithms introduced by Leverrier and Zémor. Furthermore, we show that in order to suppress errors over multiple repeated rounds of QEC, it suffices to run the parallel decoding algorithm for constant time in each round. Combined with good code parameters, the resulting constant-time overhead of QEC and robustness to (possibly time-correlated) adversarial noise make quantum Tanner codes alluring from the perspective of quantum fault-tolerant protocols.

1. Introduction

Quantum error correcting (QEC) codes [1, 2] are the backbone of quantum fault-tolerant protocols needed to reliably operate scalable quantum computers. Due to their simplicity, stabilizer codes [3], which can be realized by measuring a set of commuting Pauli operators known as parity checks, have received much attention. From the perspective of fault tolerance, it might be desirable to further require that qubits are placed on some lattice and to restrict parity checks to be constant-weight and geometrically local. However, such topological QEC codes, which include the toric code [4, 5] and the color code [6–8] as examples, have limited code parameters [9–11]. To avoid these limitations, one can drop the assumption about geometric locality of parity checks (while still maintaining the assumption about their constant weight) to obtain a more general family of QEC codes known as quantum low-density parity-check (QLDPC) codes; see Ref. [12] for a recent review. Importantly, QLDPC codes can have essentially optimal parameters, as shown by recent breakthrough results [13–16], culminating in the construction of

(asymptotically) good QLDPC codes whose encoding rates and relative distances are constant [17]. A key component of the construction of asymptotically good QLDPC codes is the presence of “product-expanding” local codes. Since then, a few alternative constructions of good QLDPC codes have been proposed [18, 19].

Good parameters alone are not enough for QEC codes to be interesting beyond the theoretical realm. In order to be practically relevant and useful, QEC codes need computationally efficient decoding algorithms which process the error syndrome and identify errors afflicting the encoded information. Importantly, decoding algorithms need to operate at least at the speed at which quantum fault-tolerant protocols are being implemented; otherwise, the error syndrome will keep accumulating and one will suffer from the so-called backlog problem [20]. Recently, a few computationally efficient (and provably correct) decoding algorithms have been developed for good QLDPC codes [19, 21, 22], assuming access to the noiseless error syndrome.

To extract the error syndrome, one usually implements appropriate quantum circuits composed of basic quantum operations, such as state preparation, entangling gates and measurements. Unfortunately, these basic operations are imperfect and, for that reason, the assumption about the noiseless error syndrome is unrealistic. In particular, practical QEC codes and decoding algorithms should exhibit robustness to measurement errors. Arguably, one of the simplest ways to achieve such robustness involves repeating measurements until a reliable account of the error syndrome is obtained [5, 23]. However, this approach incurs significant time overhead since the number of repetitions needed in general grows with the code distance.

An alternative to repeated measurement rounds of the error syndrome was introduced in the form of single-shot QEC by Bombín [24]. The basic idea behind single-shot QEC is to carefully select a code for which the decoding problem has sufficient structure to reliably infer qubit errors even with imperfect syndrome measurements. The strength of this approach is that significantly fewer measurements are necessary for codes that admit single-shot decoding compared to the simple strategy of repeated measurements.

Single-shot QEC can be considered either for stochastic or adversarial noise. In the stochastic case, one is interested in noise that afflicts a (randomly selected) constant fraction of qubits. Additional structure may be needed for both the noise and the code, since the expected weight of the errors can be far beyond the code distance. Examples of such structure include sufficiently high expansion in the associated factor graphs, e.g., quantum expander codes [25]; or the presence of geometrically local redundancies among constant-weight parity checks, e.g., the 3D subsystem toric code [26, 27] and the gauge color code [28]. In the adversarial case, as considered by Campbell [29], one can realize single-shot QEC for any code by measuring a carefully chosen set of parity checks; similar ideas of exploiting a redundant set of parity checks to simultaneously handle measurement and qubit errors were also explored in Refs. [30–32]. The limitation of this approach is that, even when starting with a QLDPC code, the parity checks needed for single-shot QEC may have weight growing with code length, which makes it less appealing from the perspective of quantum fault-tolerant protocols.

We remark that while stochastic noise and adversarial noise models are generally incomparable, the distinction fades for asymptotically good QEC codes. Since these codes, by definition, have constant relative distance, they have the ability to correct arbitrary errors of weight up to a constant fraction of the number of qubits. In particular, stochastic noise with sufficiently low rate is correctable with high probability. Since in the rest of the paper we focus on good QLDPC codes, it suffices to consider the case of adversarial noise.

1.1. Main results. In this article, we focus on a class of asymptotically good QLDPC codes called quantum Tanner codes [18]. They admit computationally efficient decoding algorithms, such as the sequential and parallel mismatch decomposition algorithms introduced in Ref. [33] and the potential-based decoder introduced in Ref. [22]. The problem of decoding quantum Tanner codes has so far been considered only in the scenario with noiseless error syndrome. Here, we study the performance of the aforementioned sequential and parallel mismatch decomposition decoders in the presence of measurement errors. We show that the decoders are *single-shot*, under the following definition. For a more detailed discussion of single-shot decoding, see Sect. 3.

Suppose a data error e occurs on the qubits. Let σ be the (ideal) syndrome corresponding to the data error. Suppose that the measured syndrome is corrupted by measurement error D . With access to the noisy syndrome $\tilde{\sigma} = \sigma + D$ as input, the decoder tries to output a correction \hat{f} close to the data error.

Definition 1.1 (*Informal Statement of Definition 3.3*). A decoder is said to be (α, β) -single-shot if, for sufficiently low-weight errors, the correction \hat{f} returned on input $\tilde{\sigma}$ satisfies $|e + \hat{f}|_R \leq \alpha|e|_R + \beta|D|$, where $|e|_R$ is the stabilizer-reduced weight of e , i.e., the weight of the smallest error equivalent to e up to the addition of stabilizers.

In other words, using a single round of noisy syndrome measurement, the decoder finds and applies the correction \hat{f} , resulting in the residual error $e + \hat{f}$ of weight below $\alpha|e|_R + \beta|D|$. Let n be the number of physical qubits of the quantum Tanner code. Our main theorems are as follows.

Theorem 1.2 (*Informal Statement of Theorem 4.17*). *There exists a constant β such that the sequential decoder (Algorithm 1) is $(\alpha = 0, \beta)$ -single-shot.*

Theorem 1.3 (*Informal Statement of Theorem 4.20*). *There exists a constant β such that for all $\alpha > 0$, the $O(\log(1/\alpha))$ -iteration parallel decoder (Algorithm 3) is (α, β) -single-shot. In particular, for $O(\log n)$ iterations of parallel decoding one obtains $\alpha = 0$.*

We further consider the situation where multiple rounds of qubit error, noisy syndrome measurement, and decoding occur. We show that under mild assumptions on the weights of qubit and measurement errors, repeated applications of an (α, β) -single-shot decoder will keep the residual error weight bounded. Specifically, consider the case where an initial error (e_1, D_1) is partially corrected by the decoder, leaving a residual error e'_1 . A new error (e_2, D_2) is then applied on top of the existing residual error, giving total error $(e'_1 + e_2, D_2)$. The decoder attempts to correct using a new round of syndrome measurements (without using the syndromes of previous rounds), leaving residue e'_2 . This process is repeated for multiple rounds. Then we have the following.

Theorem 1.4 (*Informal Statement of Theorem 3.5*). *Consider an (α, β) -single-shot decoder and multiple rounds of errors (e_i, D_i) for $i = 1, \dots, M$. For any $c > 0$, there exists a constant $C_* > 0$ such that if $\max(|e_i|, |D_i|) \leq C_*n$ for all i , then the final residual error e'_M satisfies $|e'_M|_R \leq cn$.*

A direct implication of this result is that for the parallel decoder (Algorithm 3), a constant number of iterations suffices to keep the residual error weight bounded at each round. This process can be repeated essentially indefinitely until ideal error correction is required, at which point the $O(\log n)$ -iteration parallel decoder can be used. For more details, see the discussion at the end of Sect. 3.3.

The rest of this paper is organized as follows. In Sect. 2, we provide the necessary background on quantum Tanner codes. For more detailed explanations, see Refs. [18] and

[33]. In Sect. 3, we describe the decoding problem for quantum (CSS) codes under measurement noise, and discuss the notion of single-shot decoding. We then define (α, β) -single-shot decoding and derive general consequences of this definition under multiple rounds of error and decoding. The main result of this section is the proof of Theorem 3.5. Section 4 forms the bulk of the paper. There, we review the sequential and parallel decoders from Ref. [33] and prove that the decoders are single-shot in Theorems 4.17 and 4.20. Finally, we end with some discussions in Sect. 5.

2. Quantum Tanner Codes

2.1. Classical codes. A classical binary linear code is a subspace $C \subseteq \mathbb{F}_2^n$. We refer to n as the block length of the code. The number of encoded bits (also referred to as the code dimension) is given by $k = \dim C$ and the rate of the code is $R = k/n$. The distance of C is defined as $d = \min_{x \in C \setminus \{0\}} |x|$, where $|\cdot|$ is the Hamming weight of a vector and where 0 denotes the zero vector. A code with distance d can protect against any unknown error of weight less than $d/2$. Often, it is useful to specify a code C via a parity check matrix H . By definition, $C = \ker H$.

The dual code of a code C is defined as $C^\perp = \{x \in \mathbb{F}_2^n : \langle x, y \rangle = 0 \forall y \in C\}$. The tensor product code of two codes $C_A \subseteq \mathbb{F}_2^A, C_B \subseteq \mathbb{F}_2^B$ is $C_A \otimes C_B \subseteq \mathbb{F}_2^{A \times B}$, where the codewords can be thought of as matrices such that every column is a codeword of C_A and every row is a codeword of C_B . The dual tensor code of C_A and C_B , denoted by $C_A \boxplus C_B$, is defined as

$$C_A \boxplus C_B \equiv \left(C_A^\perp \otimes C_B^\perp \right)^\perp = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B \subseteq \mathbb{F}_2^{A \times B}.$$

A parity check matrix for $C_A \boxplus C_B$ is $H_A \otimes H_B$, where H_A and H_B are the parity check matrices of C_A and C_B , respectively.

The dual tensor codes we use are required to satisfy the following robustness condition.

Definition 2.1. The code $C_A \boxplus C_B$ is said to be κ -product-expanding if any $x \in C_A \boxplus C_B$ can be expressed as $c + r$, with $c \in C_A \otimes \mathbb{F}_2^B$ and $r \in \mathbb{F}_2^A \otimes C_B$ such that

$$\kappa \left(\frac{1}{|A|} \|c\|_A + \frac{1}{|B|} \|r\|_B \right) \leq \frac{1}{|A||B|} |x|.$$

Here, $\|c\|_A$ denotes the number of non-zero columns in c and $\|r\|_B$ denotes the number of non-zero rows in r . When it is clear from context, we will drop the subscripts on the norms. The notion of product-expansion was introduced by Panteleev and Kalachev [17]. It is equivalent to robust testability of tensor product codes [34] and agreement testability [35], and also implies another notion called w -robustness of dual tensor codes [18]. It has been proven that random codes are product-expanding with high probability [19,36].

Theorem 2.2 (Theorem 1 in Ref. [36]). *Let $\rho \in (0, 1)$. For any Δ , let C_A be a random code of dimension $\lceil \rho \Delta \rceil$ and C_B be a random code of dimension $\lceil (1 - \rho) \Delta \rceil$. There exists a constant κ such that both $C_A \boxplus C_B$ and $C_A^\perp \boxplus C_B^\perp$ are κ -product-expanding with probability approaching 1 as $\Delta \rightarrow \infty$.*

2.2. Quantum codes. An n -qubit quantum code is a subspace \mathcal{C} of an n -qubit Hilbert space, i.e., $\mathcal{C} \subseteq (\mathbb{C}^2)^{\otimes n}$. We are interested in stabilizer codes, which are codes that can be expressed as the simultaneous $+1$ -eigenspace of an abelian subgroup \mathcal{S} of the n -qubit Pauli group satisfying $-I \notin \mathcal{S}$. If \mathcal{S} can be generated by two sets \mathcal{S}_X and \mathcal{S}_Z comprising, respectively, Pauli X -type and Z -type operators, then we refer to the corresponding stabilizer code as a Calderbank-Shor-Steane (CSS) code [37,38]. By ignoring the phase factors for such X -type and Z -type operators, we can identify them with their supports as vectors in \mathbb{F}_2^n .

For any CSS code stabilized by $\mathcal{S} = \langle \mathcal{S}_X, \mathcal{S}_Z \rangle$, we can define two n -bit classical codes $C_X = \ker H_X$ and $C_Z = \ker H_Z$, where each row in H_X and H_Z is the support of a stabilizer generator in \mathcal{S}_X and \mathcal{S}_Z , respectively. The dimension of a CSS code is $k = k_X + k_Z - n$, where k_X and k_Z are the dimensions of C_X and C_Z , respectively. The distance is $d = \min(d_X, d_Z)$, where $d_X = \min_{x \in C_X \setminus C_X^\perp} |x|$ and $d_Z = \min_{x \in C_X \setminus C_Z^\perp} |x|$. A quantum code of distance d can protect against any unknown error of weight less than $d/2$. A quantum code $\mathcal{C} \subseteq (\mathbb{C}^2)^{\otimes n}$ of dimension k and distance d is said to be an $[[n, k, d]]$ code. A family of CSS codes is said to be low-density parity-check (LDPC) if H_X and H_Z are sparse, i.e., have at most a constant number of non-zero entries in every column and row.

2.3. Quantum Tanner code construction. We now describe the construction of quantum Tanner codes. The code is placed on a geometric object called the left-right Cayley complex. Let G be a finite group and $A = A^{-1}$, $B = B^{-1}$ be two symmetric generating sets of G . The left-right Cayley complex $\text{Cay}_2(A, G, B)$ is a two-dimensional object with vertices V , edges E , and faces Q defined as follows:

- $V = V_{00} \sqcup V_{01} \sqcup V_{10} \sqcup V_{11}$, where $V_{ij} = G \times \{(i, j)\}$ for $i, j \in \{0, 1\}$,
- $E = E_A \sqcup E_B$, where $E_A = \{(g, i0), (ag, i1) : g \in G, a \in A, i \in \{0, 1\}\}$ and $E_B = \{(g, 0j), (gb, 1j) : g \in G, b \in B, j \in \{0, 1\}\}$,
- $Q = \{(g, 00), (ag, 01), (gb, 10), (agb, 11) : g \in G, a \in A, b \in B\}$.

Let $Q(v)$ denote the set of faces incident to a given vertex v . Each face incident to v can be obtained by choosing an A -type edge and a B -type edge incident to v and completing them into a square. Therefore, $Q(v)$ is in bijection with the set $A \times B$, and can be thought of as a matrix with rows indexed by A and columns indexed by B (Fig. 1). Similarly, the set of faces incident to a given A -edge is in bijection with B and the set of faces incident to a given B -edge is in bijection with A .

Consider the usual Cayley graph $\text{Cay}(A, G)$ with the vertex set G and the edge set $\{(g, ag) : g \in G, a \in A\}$. Ignoring the B edges from the complex, we have that (V, E_A) is the disjoint union of two copies of the bipartite cover of $\text{Cay}(A, G)$. Similarly, (V, E_B) is the disjoint union of two copies of the bipartite cover of $\text{Cay}(G, B)$.¹ We say that a Δ -regular graph is Ramanujan if the second largest eigenvalue of its adjacency matrix is at most $2\sqrt{\Delta} - 1$, and we will consider left-right Cayley complexes with component Cayley graphs $\text{Cay}(A, G)$ and $\text{Cay}(G, B)$ that are Ramanujan. Explicitly, Ramanujan Cayley graphs can be obtained by taking $G = \text{PSL}_2(q^i)$, where q is an odd prime power and A, B are (appropriately chosen) symmetric generating sets of constant size $\Delta = |A| = |B| = q + 1$ [35].

¹ We denote the Cayley graph with left group action by $\text{Cay}(A, G)$ and the Cayley graph with right group action by $\text{Cay}(G, B)$. Note that the right Cayley graph $\text{Cay}(G, B)$ with edges $\{g, gb\}$ is isomorphic to the left Cayley graph $\text{Cay}(B, G)$ by mapping every g to g^{-1} .

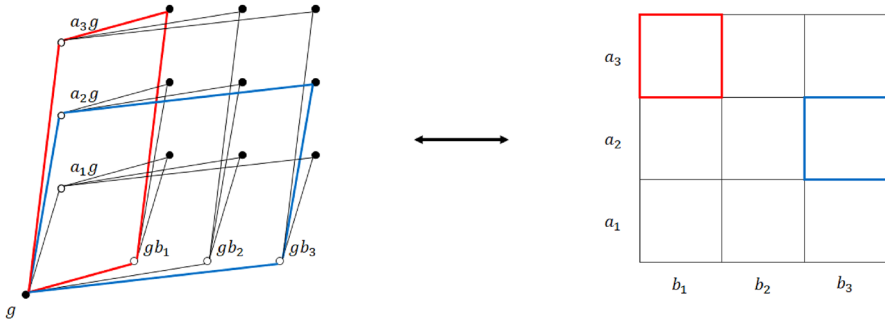


Fig. 1. The local structure of the left-right Cayley complex around a vertex labelled by $g \in G$. The incident faces $Q(v)$ has a natural bijection with $A \times B$. As examples, the red and blue faces in the complex are mapped to the squares of the same colors in the matrix given by $A \times B$

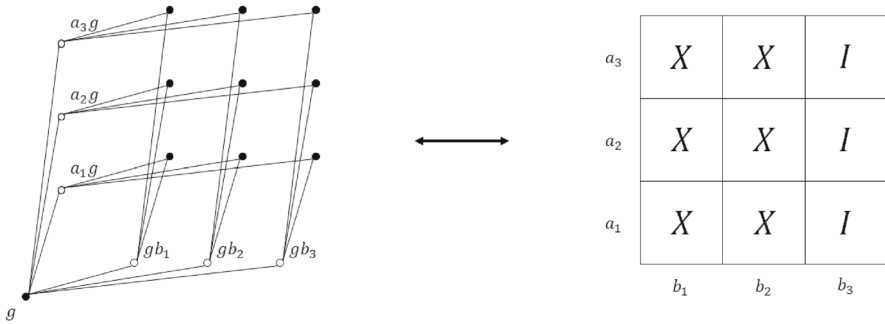


Fig. 2. An example of a stabilizer generator with local codes $C_A = \text{span}\{111\}$ and $C_B = \text{span}\{110, 011\}$. The codeword $x = 111 \otimes 110 \in C_A \otimes C_B$ has support as shown on the right. Identifying that matrix with the faces incident to a V_0 vertex gives an X -type stabilizer generator

Quantum Tanner codes are CSS codes defined by placing qubits on the faces of a left-right Cayley complex. We fix two classical codes, C_A of length $|A|$ and C_B of length $|B|$, which are used to define a pair of local codes providing the parity checks of the quantum code. An X -type stabilizer generator is defined as a codeword from a generating set of $C_0 = C_A \otimes C_B$, with support on the faces incident to a given vertex in $V_0 = V_{00} \cup V_{11}$. More precisely, there is an X -type stabilizer generator $s(x, v)$ for every generator $x \in C_A \otimes C_B$ and every vertex $v \in V_0$. Identifying $Q(v)$ with $A \times B$ using the bijection explained earlier, the support of $s(x, v)$ is the subset of $Q(v)$ defined by the support of x ; see Fig. 2 for an illustration. Similarly, the Z -type stabilizers are generated by codewords of $C_1 = C_A^\perp \otimes C_B^\perp$ on the faces incident to vertices of $V_1 = V_{01} \cup V_{10}$. The fact that X and Z parity checks commute is because X and Z generators are either disjoint or overlap on the faces incident to a single edge. On this set of faces, isomorphic to either B or A , the supports of the X and Z operators are codewords of either C_B and C_B^\perp , respectively, or C_A and C_A^\perp , respectively. It is clear that a family of quantum Tanner codes is QLDPC if the degrees of the component Cayley graphs are bounded.

Leverrier and Zémor showed that quantum Tanner codes defined on expanding left-right Cayley complexes using product-expanding local codes have good parameters [18,33].

Theorem 2.3 (Theorem 1 in Ref. [33]). *Let $\rho, d_r, \kappa \in (0, 1)$ and Δ be a sufficiently large constant. Let $C_A, C_B \subseteq \mathbb{F}_2^\Delta$ be classical codes of rates ρ and $(1 - \rho)$ respectively, such that the distances of $C_A, C_B, C_A^\perp, C_B^\perp$ are all at least $d_r \Delta$, and such that $C_A \boxplus C_B$ and $C_A^\perp \boxplus C_B^\perp$ are both κ -product-expanding. Using a family of Δ -regular Ramanujan Cayley graphs $\text{Cay}(A, G)$ and $\text{Cay}(G, B)$, define the left-right Cayley complex $\text{Cay}_2(A, G, B)$. Then the quantum Tanner codes defined using the components above have parameters*

$$\left[\left[n, k \geq (1 - 2\rho)^2 n, d \geq \frac{d_r^2 \kappa^2}{256 \Delta} n \right] \right].$$

3. Single-shot Decoding

3.1. Decoding CSS codes. Let us now formally define the decoding problem for quantum (CSS) codes. After we encode logical information in a quantum code, errors will occur on the physical system. We are interested in how to “undo” these errors and, subsequently, recover the original logical state. Specifically, consider a logical state $|\psi\rangle$ of a stabilizer code \mathcal{C} . A Pauli error E occurs, and we gain information about the error by measuring a set of stabilizer generators $\{S_i\}$. This gives a syndrome σ , a bit string whose values σ_i correspond to the eigenvalues $(-1)^{\sigma_i}$ of the stabilizers measured. Thus, $\sigma_i = 0$ whenever S_i commutes with E and $\sigma_i = 1$ when it anticommutes. The task of decoding is to use σ to determine a correction \hat{F} such that $\hat{F}E|\psi\rangle = |\psi\rangle$. In other words, $\hat{F}E$ should be a stabilizer of the code. When \mathcal{C} is a CSS code, we can express the problem as follows.

Definition 3.1. Let \mathcal{C} be a CSS code specified by two parity check matrices $H_X \in \mathbb{F}_2^{r_X \times n}$ and $H_Z \in \mathbb{F}_2^{r_Z \times n}$. Let $e = (e_X, e_Z) \in \mathbb{F}_2^{2n}$ be an error with corresponding syndrome $\sigma = (\sigma_X, \sigma_Z) \in \mathbb{F}_2^{r_X + r_Z}$, where $\sigma_Z = H_X e_Z$ and $\sigma_X = H_Z e_X$. Given input σ , the task of decoding is to find corrections $\hat{f} = (\hat{f}_X, \hat{f}_Z) \in \mathbb{F}_2^{2n}$ such that $e_X + \hat{f}_X \in C_X^\perp$ and $e_Z + \hat{f}_Z \in C_Z^\perp$.

In the definition above, we associate the bit string $e = (e_X, e_Z)$ with the Pauli errors $E = E_X E_Z$ where E_X and E_Z are Pauli X and Z operators with support e_X and e_Z , respectively (ignoring phase information). The correction \hat{f} is similarly associated with a Pauli operator \hat{F} .

We note that for CSS codes, the decoding problem can be split into two separate problems for the X and Z codes that can be solved independently. For quantum Tanner codes in particular, there is symmetry between the X and Z codes, as can be seen by switching V_0 and V_1 labels and switching C_A, C_B with C_A^\perp, C_B^\perp . Therefore, it suffices to give an algorithm for decoding one type of error. In the remainder of the paper, we will consider solely the case where X -errors occur, with Z -errors treated analogously. For convenience, we will often drop subscripts, for example writing e for e_X or H for H_Z .

The above discussion assumes that the ideal syndrome is accessible to the decoder. Let us now consider the case when the syndrome measurements are unreliable, motivated by the fact that the quantum circuits implementing the parity checks are necessarily imperfect. Suppose that the ideal syndrome σ_X of an error e_X is corrupted by measurement error D_X , so that the actual noisy syndrome readout is $\tilde{\sigma}_X = \sigma_X + D_X$. A naive decoding of the syndrome $\tilde{\sigma}_X$ may result in a correction \hat{f}_X which does not bring the state back to the code space, i.e., $e_X + \hat{f}_X \notin C_X^\perp$. Furthermore, there may be no guarantee that $e_X + \hat{f}_X$ is close to C_X^\perp .

One of the standard procedures to account for measurement errors is to repeatedly measure the stabilizer generators in order to gain enough confidence in their measurement outcomes [5, 23]. This will incur large time overhead. Alternatively, syndrome measurements can be performed fault-tolerantly by preparing special ancilla qubit states offline [39, 40]. This will incur large qubit overhead. It would be ideal if we could avoid both overheads at the same time.

3.2. Single-shot decoding. Bombín [24] introduced *single-shot* decoders as an alternative approach. These decoders take in a noisy syndrome as input and, even in the presence of syndrome noise, return a correction that can be used to reduce the data error. Most likely, there will be some resulting residual error, but its weight is bounded by some function of the syndrome noise. In more detail, the single-shot property posits that it suffices to perform $O(n)$ parity check measurements (in the context of QLDPC codes, one further requires constant weight of measured parity checks), and, using *only* these measurement outcomes, one can perform reliable QEC that keeps the residual noise at bay.

In our analysis, we need the following definition.

Definition 3.2. Let \mathcal{C} be an n -qubit CSS code and $e \in \mathbb{F}_2^n$ be a Pauli X error. The stabilizer-reduced weight $|e|_R$ of e is defined as the weight of the smallest error equivalent to e up to the addition of stabilizers of \mathcal{C} , i.e., $|e|_R = \min_{e' \in \mathcal{C}^\perp} |e + e'|$. The stabilizer-reduced weight of a Pauli Z error is defined analogously.

The stabilizer-reduced weight of an error is a convenient theoretical measure of how detrimental the error really is. Note that since stabilizers do not change the code state, errors are only well-defined up to the addition of stabilizers. As such, any bound on the performance of the decoder is unambiguously defined using the stabilizer-reduced weight, which can be significantly smaller than the original weight.

Since we focus on asymptotically good QLDPC codes, it is enough to consider single-shot decoding for adversarial noise. Campbell [29] captures adversarial single-shot decoding as follows. Let both the data error e and the syndrome noise D be sufficiently small. A decoder is single-shot if it outputs a correction such that the weight of the residual error is bounded by a polynomial of $|D|$. In this work, we would like to consider constant-time decoding using the parallel decoder (Algorithm 3) for quantum Tanner codes. This setting does not directly fit into the previous definition since the residual error could depend on $|e|$ in addition to $|D|$. To allow for nontrivial dependence on $|e|$, we give the following definition, which is relevant for asymptotically good codes where the residual error size is at most linear in $|e|$ and $|D|$.

Definition 3.3. Let \mathcal{C} be a CSS code specified by parity check matrices $H_X \in \mathbb{F}_2^{r_X \times n}$ and $H_Z \in \mathbb{F}_2^{r_Z \times n}$. Let $e = (e_X, e_Z) \in \mathbb{F}_2^{2n}$ be a data error, $D = (D_X, D_Z) \in \mathbb{F}_2^{r_Z + r_X}$ be a syndrome error, and $\tilde{\sigma} = (\tilde{\sigma}_X, \tilde{\sigma}_Z) \in \mathbb{F}_2^{r_Z + r_X}$ be the corresponding noisy syndrome, where $\tilde{\sigma}_X = H_Z e_X + D_X$ and $\tilde{\sigma}_Z = H_X e_Z + D_Z$. A decoder for \mathcal{C} is (α, β) -single-shot if there exist constants A, B, C such that, for $P \in \{X, Z\}$, whenever

$$A|e_P|_R + B|D_P| \leq Cn,$$

the decoder finds a correction $\hat{f}_P \in \mathbb{F}_2^n$ from given input $\tilde{\sigma}_P$ such that

$$|e_P + \hat{f}_P|_R \leq \alpha|e_P| + \beta|D_P|.$$

This definition, combined with Theorems 4.17 and 4.20 below, gives the following results for the sequential and parallel decoders of the quantum Tanner codes.

Theorem 3.4 (Summary). *There exist constants $A, B, C, \beta > 0$ (dependent on the parameters of the quantum Tanner code) such that if $A|e|_R + B|D| \leq Cn$, then the following conditions hold:*

1. *The sequential decoder (Algorithm 1) is $(\alpha = 0, \beta)$ -single-shot.*
2. *The parallel decoder (Algorithm 3) with k -iterations is $(\alpha = 2^{-\Omega(k)}, \beta)$ -single-shot.*

Note that the runtime of the sequential decoder is $O(n)$, and each iteration of the parallel decoder is constant time. For the parallel decoder, α decreases exponentially with the number of parallel decoding iterations k , and the results of this section will hold when k is a sufficiently large constant. It suffices to take $k = O(\log n)$ for $\alpha = 0$ in the parallel decoder.

Finally, we remark that we may increase the robustness to measurement errors and improve the overall performance of single-shot decoding by leveraging redundancies among parity checks, similar to the ideas explored in Refs. [30–32]. We can apply this approach to quantum Tanner codes without compromising their QLDPC structure, which is a crucial difference between our setting and the aforementioned works. Specifically, stabilizer generators of quantum Tanner codes are supported on local neighborhoods, defined by the local codes C_0 and C_1 . We may apply the technique of adding redundancy to each set of local checks separately. Since the local codes are of length Δ^2 , any redundant check in a fixed local neighborhood will not have weight more than Δ^2 , which is comparable to the weight of the original checks.

3.3. Multiple rounds of decoding. In this section, we discuss what happens after multiple rounds of errors, noisy measurements, and decoding. We show that under the assumptions of Definition 3.3, there exists a variety of noise models such that, as long as the overall noise level is sufficiently small, the encoded quantum information will persist for an exponential number of rounds.

The results proven in this section hold for any decoder that can solve the single-shot decoding problem under Definition 3.3. More precisely, we assume that if the decoder is given the noisy syndrome from data error $e \in \mathbb{F}_2^n$ and syndrome error $D \in \mathbb{F}_2^{r \times z}$ satisfying

$$A|e|_R + B|D| \leq Cn,$$

then it outputs a correction \hat{f} such that the residual error satisfies

$$|e + \hat{f}|_R \leq \alpha|e| + \beta|D|.$$

We will assume that β is constant and that α is a parameter in the decoder that can be made arbitrarily small. For our analysis, we let R, S be constants such that

$$R \leq \frac{(1 - \alpha)C}{2A} \quad \text{and} \quad S \leq \frac{(1 - \alpha)C}{2(\beta A + (1 - \alpha)B)}. \quad (1)$$

We prove that as long as the data and syndrome errors in each round are sufficiently small, the total error can be kept small indefinitely.

Theorem 3.5. Consider errors (e_i, D_i) that occur on rounds $i = 1, 2, \dots$, with decoding in between each round using new syndrome measurements (i.e., without using the previous syndromes). If the errors satisfy $|e_i| \leq Rn$ and $|D_i| \leq Sn$ for every round i , then the residual error e'_i after each round i satisfies

$$|e'_i|_R \leq \frac{\alpha R + \beta S}{1 - \alpha} n. \tag{2}$$

Proof. Initially, $e'_0 = 0$, which satisfies the bound. Suppose after round $i - 1$, the residual error e'_{i-1} satisfies (2). The new total error is $e'_{i-1} + e_i$, and we have

$$\begin{aligned} A|e'_{i-1} + e_i|_R + B|D_i| &\leq A|e'_{i-1}|_R + A|e_i| + B|D_i| \\ &\leq A \frac{\alpha R + \beta S}{1 - \alpha} n + ARn + BSn \\ &\leq Cn, \end{aligned}$$

where the last inequality follows since

$$A \frac{R + \beta S}{1 - \alpha} + BS \leq C$$

for R and S satisfying (1). Therefore, the decoder returns a correction \hat{f} with residual error

$$\begin{aligned} |e'_i|_R &\leq \alpha|e'_{i-1} + e_i|_R + \beta|D_i| \\ &\leq \alpha|e'_{i-1}|_R + \alpha|e_i| + \beta|D_i| \\ &\leq \alpha \frac{\alpha R + \beta S}{1 - \alpha} n + \alpha Rn + \beta Sn \\ &= \frac{\alpha R + \beta S}{1 - \alpha} n, \end{aligned}$$

where the third inequality uses the inductive hypothesis. □

From this result, we can immediately analyze the stochastic setting in which large errors are unlikely.

Corollary 3.6. Let $\{(e_i, D_i)\}_{i=1}^M$ be randomly distributed data and syndrome errors (with possible correlations) such that

$$\Pr(|e_i| > Rn) \leq e^{-an}, \quad \text{and} \quad \Pr(|D_i| > Sn) \leq e^{-bn},$$

for constants $a, b > 0$. Suppose the decoder is run after each round of errors using new syndrome measurements (i.e., without using the syndromes of previous rounds). Then the final residual error e'_M satisfies

$$\Pr\left(|e'_M|_R > \frac{\alpha R + \beta S}{1 - \alpha} n\right) \leq M(e^{-an} + e^{-bn}).$$

Proof. This follows immediately from Theorem 3.5 after using a union bound on the probability of a large data or syndrome error at every round. □

As a sample application of Corollary 3.6, we analyze the case of p -bounded noise [25, 41], although any model of errors with sufficiently suppressed tails will give the same conclusions.

Definition 3.7 (p -bounded noise). Let $p \in [0, 1)$. Let A be a set and let 2^A be its power set. We say that a probability distribution $E : 2^A \rightarrow [0, 1]$ is p -bounded if for any $B \subseteq A$ we have

$$\sum_{B' \supseteq B} E(B') \leq p^{|B|}.$$

Corollary 3.8. Let $\{(e_i, D_i)\}_{i=1}^M$ be data and syndrome errors where each of the marginal distributions of e_i and D_i are p - and q -bounded, respectively. Suppose the decoder is run after each round of errors using a new round of syndrome measurements (without using the syndromes of previous rounds). Then, the final residual error e'_M satisfies

$$\Pr\left(|e'_M|_R > \frac{\alpha R + \beta S}{1 - \alpha} n\right) \leq M \left(e^{-n \ln(2^{-H(R)} p^{-R})} + e^{-n \ln(2^{-eH(S/q)} q^{-S})} \right),$$

where $H(\tau) = -\tau \log_2 \tau - (1 - \tau) \log_2(1 - \tau)$ is the binary entropy function, and $Q = r_Z/n$.

Proof. Let us first upper bound $\Pr(|e_i| > Rn)$. We have

$$\Pr(|e_i| > Rn) = \sum_{|e| > Rn} \Pr(e_i = e) \leq \sum_{|e|=Rn} \Pr(e_i \supset e) \leq \sum_{|e|=Rn} p^{|e|} \leq \binom{n}{Rn} p^{Rn},$$

where the last inequality follows by p -boundedness. Using the binary entropy bound for the binomial coefficient, we then have

$$\Pr(|e_i| > Rn) \leq \binom{n}{Rn} p^{Rn} \leq 2^{nH(R)} p^{Rn} = e^{-n \ln(2^{-H(R)} p^{-R})}.$$

Similarly, we have

$$\Pr(|D_i| > Sn) \leq e^{-n \ln(2^{-eH(S/q)} q^{-S})}.$$

Applying Corollary 3.6 gives the result. \square

In particular, there exist thresholds $(p_*, q_*) = (2^{-H(R)/R}, 2^{-eH(S/q)/S})$ below which errors are kept under control for an exponential number of rounds of single-shot QEC with high probability.

Finally, we comment on the last round of QEC. In a typical setting of fault tolerance, we choose to measure logical qubits in the computational basis, which for a CSS code can be accomplished by measuring each physical qubit (also in the computational basis). We then apply one final round of QEC, where the Z -stabilizer eigenvalues are inferred by multiplying the Z -measurement outcomes from those qubits in the stabilizer supports. Note that in this final round, any measurement error can be treated as an X data error immediately before the measurement. We run the decoder with α sufficiently small so that by the guarantee on the decoder, $|e + \hat{f}|_R = 0$, i.e., we completely correct the error. We can then infer the logical information by combining the corrected single-qubit Z -measurement outcomes making up the Z -logical operators. Therefore, fault tolerance may be achieved by using a faster (e.g., constant-time) decoder with larger α value in the middle of the computation, and only applying the full decoder (e.g., logarithmic-time) with $\alpha = 0$ at the end of the computation.

4. Proofs of Single-shot Decoding of Quantum Tanner Codes

4.1. Decoding algorithms. We consider the decoding problem for quantum Tanner codes with parameters as in Theorem 2.3. We first provide an overview of how the decoder works. As before, we will work exclusively with X -type errors, with Z -errors being analogous. Suppose that the code state experiences data error e , and the measurements experience syndrome error D . The decoder is consequently given as input the noisy syndrome $\tilde{\sigma} = \sigma + D = H_Z e + D$. Due to the structure of the code, the global syndrome $\tilde{\sigma}$ can equivalently be viewed as a set of noisy local syndromes $\{\tilde{\sigma}_v\}_{v \in V_1}$, where $\tilde{\sigma}_v$ denotes the restriction of $\tilde{\sigma}$ to the checks associated with the local code C_1^\perp at vertex v . At each V_1 vertex, the decoder computes a minimal weight correction $\tilde{\varepsilon}_v \subseteq Q(v)$ based on the local syndrome $\tilde{\sigma}_v$, i.e.,

$$\tilde{\varepsilon}_v = \operatorname{argmin}\{|y| : y \subseteq Q(v), \sigma_v(y) = \tilde{\sigma}_v\}.$$

Note that this is a completely local operation which can be done without consideration of the syndrome state of the other vertices. Each square $q \in Q$ contains two V_1 vertices, say $v \in V_{01}$ and $v' \in V_{10}$. These two vertices are each associated with their own local corrections, $\tilde{\varepsilon}_v$ and $\tilde{\varepsilon}_{v'}$, which may disagree on whether there is an error on q . If there is no disagreement on any square $q \in Q$, then a global correction $\hat{f} \in \mathbb{F}_2^Q$ can be unambiguously defined by

$$\hat{f} = \bigsqcup_{v \in V_{01}} \tilde{\varepsilon}_v = \bigsqcup_{v' \in V_{10}} \tilde{\varepsilon}_{v'}.$$

However, this will usually not be the case. The disagreement between the different candidate local corrections is captured by a “noisy mismatch vector” defined as

$$\tilde{Z} = \sum_{v \in V_1} \tilde{\varepsilon}_v. \tag{3}$$

The goal of the main part of the algorithm is to reduce the size of \tilde{Z} by successively updating the best local corrections on the V_1 vertices. For example, it is possible that for a given $v \in V_1$, replacing $\tilde{\varepsilon}_v$ with $\tilde{\varepsilon}_v + x$ for some $x \in C_1^\perp$ in (3) would significantly decrease $|\tilde{Z}|$. In general, we attempt to decompose \tilde{Z} by adding codewords $x \in C_1^\perp$ on local views $Q(v)$ of vertices $v \in V$.² We keep track of the decomposition process through quantities $\hat{C}_0, \hat{C}_1, \hat{R}_0, \hat{R}_1 \subseteq \mathbb{F}_2^Q$, which are initially 0 and updated as follows. Suppose $x = c + r$ is supported on a V_{ij} local view ($i, j \in \{0, 1\}$), where $c \in C_A \otimes \mathbb{F}_2^B$ and $r \in \mathbb{F}_2^A \otimes C_B$. Then we add c to \hat{C}_j and r to \hat{R}_i . The interpretation is that $\hat{C}_1 + \hat{R}_0$ is the total change made to the local corrections $\tilde{\varepsilon}_v$ from the V_{01} vertices, and $\hat{C}_0 + \hat{R}_1$ is the total change made to those from the V_{10} vertices. Therefore, at the end of the procedure, we output a guess for the error, which from the perspective of the V_{01} vertices is

$$\hat{f} = \sum_{v \in V_{01}} \tilde{\varepsilon}_v + \hat{C}_1 + \hat{R}_0.$$

² In the presence of measurement errors, a full decomposition of \tilde{Z} into local codewords may not be possible. See Definition 4.4 and related comments before and after.

The algorithm can run either sequentially (Algorithm 1) or in parallel (Algorithm 3), with the corresponding \tilde{Z} decomposition subroutines presented in Algorithm 2 and Algorithm 4 respectively.

Algorithm 1 Sequential decoder for quantum Tanner codes with parameter ε

Input: A noisy syndrome $\tilde{\sigma}$ arising from data error e and syndrome error D .

Output: A correction \hat{f} that approximates e .

- 1: $\tilde{\varepsilon}_v \leftarrow \operatorname{argmin}\{|y| : y \subseteq Q(v), \sigma_v(y) = \tilde{\sigma}_v\}$ (or $\tilde{\varepsilon}_v \leftarrow 0$ if no such y exists) for all $v \in V_1$
 - 2: $\tilde{Z} \leftarrow \sum_{v \in V_1} \tilde{\varepsilon}_v$
 - 3: $(\hat{C}_0, \hat{C}_1, \hat{R}_0, \hat{R}_1) \leftarrow \text{MISMATCH}_\varepsilon(\tilde{Z})$
 - 4: $\hat{f} \leftarrow \sum_{v \in V_{01}} \tilde{\varepsilon}_v + \hat{C}_1 + \hat{R}_0$
 - 5: **return** \hat{f}
-

Algorithm 2 Sequential mismatch decomposition with parameter ε

Input: A vector $Z \in \mathbb{F}_2^Q$.

Output: A collection $(\hat{C}_0, \hat{C}_1, \hat{R}_0, \hat{R}_1) \equiv \text{MISMATCH}_\varepsilon(Z)$.

- 1: Set $\hat{C}_0 = \hat{C}_1 = \hat{R}_0 = \hat{R}_1 = 0$ and $\hat{Z} = Z$.
 - 2: **while** $\hat{Z} \neq 0$ **do**
 - 3: **if** $\exists v \in V_{ij}$ and $0 \neq x_v \in C_1^\perp$ in $Q(v)$ such that $|\hat{Z}| - |\hat{Z} + x_v| \geq (1 - \varepsilon)|x_v|$ **then**
 - 4: Find $r_v \in \mathbb{F}_2^A \otimes C_B$ and $c_v \in C_A \otimes \mathbb{F}_2^B$ such that $\|c_v\| + \|r_v\|$ is minimal among all c_v, r_v such that $r_v + c_v = x_v$
 - 5: $\hat{C}_j \leftarrow \hat{C}_j + c_v$
 - 6: $\hat{R}_i \leftarrow \hat{R}_i + r_v$
 - 7: $\hat{Z} \leftarrow \hat{Z} + c_v + r_v$
 - 8: **else**
 - 9: **return** $(\hat{C}_0, \hat{C}_1, \hat{R}_0, \hat{R}_1)$
 - 10: **end if**
 - 11: **end while**
 - 12: **return** $(\hat{C}_0, \hat{C}_1, \hat{R}_0, \hat{R}_1)$
-

Algorithm 3 Parallel decoder for quantum Tanner codes with k iterations

Input: A noisy syndrome $\tilde{\sigma}$ from a data error e and syndrome error D , and an integer $k > 0$.

Output: A correction \hat{f} that approximates e .

- 1: **parallel for each** $v \in V_1$ **do**
 - 2: $\tilde{\varepsilon}_v \leftarrow \operatorname{argmin}\{|y| : y \subseteq Q(v), \sigma_v(y) = \tilde{\sigma}_v\}$ (or $\tilde{\varepsilon}_v \leftarrow 0$ if no such y exists)
 - 3: $\tilde{Z} \leftarrow \sum_{v \in V_1} \tilde{\varepsilon}_v$
 - 4: $\hat{f} \leftarrow \sum_{v \in V_{01}} \tilde{\varepsilon}_v$
 - 5: **end parallel for each**
 - 6: $(\hat{C}_0, \hat{C}_1, \hat{R}_0, \hat{R}_1) \leftarrow \text{PARMISMATCH}^{(k)}(\tilde{Z})$
 - 7: $\hat{f} \leftarrow \hat{f} + \hat{C}_1 + \hat{R}_0$ // update \hat{f} in parallel for each vertex $v \in V_{01}$
 - 8: **return** \hat{f}
-

Algorithm 4 Parallel mismatch decomposition procedure with k iterations

Input: A vector $Z \in \mathbb{F}_2^Q$ and integer $k > 0$.
Output: A collection $(\hat{C}_0, \hat{C}_1, \hat{R}_0, \hat{R}_1) \equiv \text{PARMISMATCH}^{(k)}(Z)$.

- 1: Set $\hat{C}_0 = \hat{C}_1 = \hat{R}_0 = \hat{R}_1 = 0$ and $\hat{Z} = Z$.
- 2: **repeat** k **times**
- 3: **for** $(i, j) \in \{0, 1\}^2$ **do**
- 4: **parallel for each** $v \in V_{ij}$ **do**
- 5: **if** there exists $0 \neq x_v \in C_1^\perp$ in $Q(v)$ such that $|\hat{Z}| - |\hat{Z} + x_v| \geq |x_v|/2$ **then**
- 6: Choose x_v such that $|x_v|$ maximal among all possible choices
- 7: Find $r_v \in \mathbb{F}_2^A \otimes C_B$ and $c_v \in C_A \otimes \mathbb{F}_2^B$ such that $\|c_v\| + \|r_v\|$ is minimal among all c_v, r_v such that $r_v + c_v = x_v$
- 8: $\hat{C}_j \leftarrow \hat{C}_j + c_v$
- 9: $\hat{R}_i \leftarrow \hat{R}_i + r_v$
- 10: $\hat{Z} \leftarrow \hat{Z} + c_v + r_v$
- 11: **end if**
- 12: **end parallel for each**
- 13: **end for**
- 14: **end repeat**
- 15: **return** $(\hat{C}_0, \hat{C}_1, \hat{R}_0, \hat{R}_1)$

These algorithms were analyzed in the scenario with perfect measurement outcomes in Ref. [33], giving the following results:

Theorem 4.1 (Theorem 13 in Ref. [33]). *Let $\varepsilon \in (0, 1)$. Suppose Algorithm 1 with parameter ε is given as input the noiseless syndrome $\sigma = Hze$ of an error $e \in \mathbb{F}_2^Q$ of weight*

$$|e| \leq \frac{1}{2^{11}} \min\left(\frac{\varepsilon^3}{16}, \kappa\right) (1 - \varepsilon) d_r^2 \kappa^2 \frac{n}{\Delta}.$$

Then it will output a correction \hat{f} such that $e + \hat{f} \in C_X^\perp$ in time $O(n)$.

Theorem 4.2 (Theorem 20 in Ref. [33]). *Let $\varepsilon \in (0, 1/6)$. Suppose Algorithm 3 is given as input the noiseless syndrome $\sigma = Hze$ of an error $e \in \mathbb{F}_2^Q$ of weight*

$$|e| \leq \frac{1}{2^{12}} \min\left(\frac{\varepsilon^3}{16}, \kappa\right) d_r^2 \kappa^2 \frac{n}{\Delta}.$$

Then it will output a correction \hat{f} such that $e + \hat{f} \in C_X^\perp$ in time $O(\log n)$.

In the next sections, we will consider what happens when the decoders are given a syndrome with possible errors.

4.2. Proof preliminaries. We first give a summary of the main ideas of the proof. The key idea of the proof is to bound the reduction in the weight of the noisy mismatch vector \tilde{Z} through each step of the algorithm, and to show that when the weight of \tilde{Z} is reduced, the weight of the residual error is also subsequently reduced. There is a technical challenge to this idea however: there is no direct relation between the weight of \tilde{Z} and the error weight.

To bridge these two objects, we define the notion of an ideal mismatch vector Z (see Eq. (4) below), which is equal to \tilde{Z} when there is no measurement noise. Since the mismatch Z only captures the portion of the error which cannot be removed using independent local corrections, we must first “pre-process” the error by making any possible local corrections (see Eq. (5) below). This establishes a direct connection between Z and the “pre-processed” error e_0 (see Lemma 4.7) and our analysis will be built upon this connection.

We show that if Z is decomposable into local corrections by Algorithm 2, then most of these correction sets will also reduce the weight of \tilde{Z} (Lemma 4.13). This in turn allows us to relate the weights of Z and \tilde{Z} . Finally, we show that if the qubit and measurement error weights are bounded, the ideal mismatch vector Z always admits the desired decomposition into local correction sets (Lemma 4.15). These lemmas allow us to prove our main result (Theorem 4.17): as the weight of \tilde{Z} decreases throughout the steps of the algorithm, the residual error weight must also decrease. The analysis of the parallel decoder then builds upon this bound, with the additional requirement of showing that the decomposition of Z into local corrections must be essentially disjoint (Lemma 4.18).

In the remainder of this section, we set up notation and provide some preliminary results used in the proofs of Theorems 4.17 and 4.20. We first define quantities relating to the states of the decoders. Given the local structure of the quantum Tanner codes, it will be more convenient to bound the size of the syndrome noise in terms of its vertex support.

Definition 4.3. Given a quantum Tanner code and a syndrome noise D , let us define D_v to be the restriction of D to the set of stabilizer generators associated with vertex v . We define the vertex support of D to be the set of all vertices such that $D_v \neq 0$. We denote the size of the vertex support by $|D|_V$. Note that we have $\Delta^{-2}|D| \leq r^{-1}|D| \leq |D|_V \leq |D|$, where r is the number of stabilizer generators associated with the local code.

Given the noisy syndrome $\tilde{\sigma} = H_Z e + D$, let $\tilde{\sigma}_v$ denote the restriction of $\tilde{\sigma}$ to the checks associated with the vertex v . For each vertex $v \in V_1$, the decoder finds a locally minimal correction $\tilde{\varepsilon}_v$ such that $\sigma_v(\tilde{\varepsilon}_v) = \tilde{\sigma}_v$. In the event that no local correction $\tilde{\varepsilon}_v$ exists for $\tilde{\sigma}_v$, we may define $\tilde{\varepsilon}_v$ arbitrarily. In our case, we will simply define $\tilde{\varepsilon}_v = 0$ by convention. If ε_v is the locally minimal correction associated with the noiseless syndrome σ_v , then we can decompose $\tilde{\varepsilon}_v$ into “noiseless” and “noisy” parts as

$$\tilde{\varepsilon}_v = \varepsilon_v + \varepsilon_v(D),$$

where $\varepsilon_v(D)$ is defined by $\varepsilon_v(D) = \tilde{\varepsilon}_v - \varepsilon_v$. Note that $\varepsilon_v(D)$ will be non-zero only when D has non-zero support on v .

The full noisy mismatch vector initialized by the decoder is given by

$$\tilde{Z} = \sum_{v \in V_1} \tilde{\varepsilon}_v = \sum_{v \in V_1} (\varepsilon_v + \varepsilon_v(D)).$$

It will likewise be convenient to split the mismatch into a noiseless and a noisy part, defined by

$$Z = \sum_{v \in V_1} \varepsilon_v \quad \text{and} \quad Z_N = \sum_{v \in V_1} \varepsilon_v(D), \quad (4)$$

so that $\tilde{Z} = Z + Z_N$. We will also need the restrictions of these vectors onto the vertices of V_{01} , which we define as

$$\tilde{Z}^{01} = \sum_{v \in V_{01}} \tilde{\varepsilon}_v, \quad Z^{01} = \sum_{v \in V_{01}} \varepsilon_v, \quad \text{and} \quad Z_N^{01} = \sum_{v \in V_{01}} \varepsilon_v(D).$$

The key idea of the proof is to pre-process the error using \tilde{Z}^{01} , and apply the local corrections x_v step by step. Specifically, we define the initial pre-processed error \tilde{e}_0 , and the “noiseless” pre-processed error e_0 , by

$$\begin{aligned} \tilde{e}_0 &= e + \tilde{Z}^{01} = e + \sum_{v \in V_{01}} \tilde{\varepsilon}_v, \\ e_0 &= e + Z^{01} = \tilde{e}_0 + Z_N^{01}. \end{aligned} \tag{5}$$

For the purpose of our proof, we consider the vector \tilde{e}_0 as the initial error state of the algorithm, and $\tilde{Z}_0 = \tilde{Z}$ as the initial mismatch. Note that in practice it does not matter at what point in the decoding procedure the set \tilde{Z}^{01} is flipped. The pre-processing is only introduced as a convenience in our proof in order to relate the weight of e to the weight of Z . The original algorithms considered in Ref. [33] involve a “post-processing” step instead, where \tilde{Z}^{01} is applied at the very end rather than the beginning. Since the sets of qubits flipped are ultimately the same in either case, the results here hold without modification.

The core loop of the decoding algorithm finds, at each step i , some local codeword $x_i = r_i + c_i \subseteq Q(v_i)$ such that

$$|\tilde{Z}_{i-1}| - |\tilde{Z}_{i-1} + x_i| \geq (1 - \varepsilon)|x_i|. \tag{6}$$

Having found a codeword which satisfies (6), we update the error and the mismatch vectors by

$$\tilde{e}_i = \tilde{e}_{i-1} + f_i, \quad \text{and} \quad \tilde{Z}_i = \tilde{Z}_{i-1} + x_i,$$

where the flip-set $f_i \subseteq Q(v_i)$ is defined by

$$f_i = \begin{cases} 0 & v_i \in V_{10}, \\ x_i & v_i \in V_{01}, \\ c_i & v_i \in V_{11}, \\ r_i & v_i \in V_{00}. \end{cases}$$

Likewise, we can define the associated “noiseless” error and mismatch at each step by

$$e_i = e_{i-1} + f_i = \tilde{e}_i + Z_N^{01}, \quad \text{and} \quad Z_i = Z_{i-1} + x_i = \tilde{Z}_i + Z_N.$$

Note that Z_N and Z_N^{01} are determined entirely by the syndrome noise D and initial error e , and are constant through the decoding process.

In the presence of measurement errors, it is no longer true that the noisy mismatch \tilde{Z} can be decomposed into a sum of local codewords.³ As such, some care must be taken in

³ In the case of perfect syndrome measurements, we have

$$Z = \sum_{v \in V_1} \varepsilon_v = \sum_{v \in V_1} (e_v + r_v + c_v) = \sum_{v \in V_1} (r_v + c_v),$$

where $r_v + c_v$ is the codeword that the local error is corrected to: $e_v + \varepsilon_v = r_v + c_v$. This decomposition no longer holds in the presence of imperfect measurements.

characterizing what exactly we mean by a “mismatch”. This is captured by the definition below.

Definition 4.4. A mismatch vector is any $Z \in \mathbb{F}_2^Q$ that can be decomposed as $Z = C_0 + C_1 + R_0 + R_1$, where

$$C_j = \sum_{v \in V_{\bar{j}j}} c_v \quad \text{and} \quad R_i = \sum_{v \in V_{i\bar{i}}} r_v$$

are the sum of local column codewords $c_v \in C_A \otimes \mathbb{F}_2^B$ and row codewords $r_v \in \mathbb{F}_2^A \otimes C_B$ on $Q(v)$, i.e., a mismatch vector is an element in the span of local codewords C_1^\perp . Here, we define $\bar{i} = 1 - i$ for convenience.

The division of Z into local codewords of the form (C_0, C_1, R_0, R_1) is called a *decomposition* of Z . Any given mismatch vector Z may have many distinct decompositions. Given any decomposition, we define its *weight* by

$$\text{wt}(C_0, C_1, R_0, R_1) = \|C_0\| + \|C_1\| + \|R_0\| + \|R_1\|,$$

where $\|C_i\|$ and $\|R_i\|$ denote the number of non-zero columns and rows, respectively, present in C_i and R_i . Note that the weight is well-defined since distinct local codewords $c_v \subseteq C_i$ and $r_v \subseteq R_i$ are disjoint. We then define the *norm* of a mismatch to be

$$\|Z\| = \min_{\substack{(C_0, C_1, R_0, R_1) \\ Z=C_0+C_1+R_0+R_1}} \text{wt}(C_0, C_1, R_0, R_1).$$

Decompositions such that $\text{wt}(C_0, C_1, R_0, R_1) = \|Z\|$ are called *minimal weight decompositions* for Z .

Note that technically the vector \tilde{Z} which we call the noisy mismatch vector is *not* a mismatch vector at all as defined by Definition 4.4. Nevertheless, we will continue to call \tilde{Z} the noisy mismatch since there is little chance of confusion. The noiseless part Z is a genuine mismatch vector by definition. The properties of the noiseless mismatch Z are characterized by the following lemma from Ref. [33].

Lemma 4.5 (Lemma 17 in Ref. [33]). *Let $e \in \mathbb{F}_2^Q$ be an error and let ε_v be a local minimal correction for e_v at every vertex $v \in V_1$. Let*

$$Z = \sum_{v \in V_1} \varepsilon_v.$$

Then Z is a mismatch vector which satisfies

$$|Z| \leq 4|e|_R, \quad \text{and} \quad \|Z\| \leq \frac{4}{\kappa \Delta} |e|_R.$$

The main purpose of pre-processing in our proof is that the noiseless pre-processed error e_0 and the noiseless mismatch Z_0 can be easily related through the following property.

Definition 4.6. Let $e \in \mathbb{F}_2^Q$ be an error. We say that the error is V_{ij} -weighted if $\sigma_v(e) = 0$ for all $v \in V_{\bar{i}\bar{j}}$. Given a V_{ij} -weighted error e , we say that a mismatch vector Z is *associated* with e if $\sigma_v(Z) = \sigma_v(e)$ for all $v \in V_{ij}$.

Lemma 4.7. *The quantity e_0 is a V_{10} -weighted error and $Z_0 = Z$ is a mismatch vector associated with e_0 .*

Proof. First, we show that Z is a mismatch vector. Note that Z is the sum of local minimal corrections ε_v to the error e , i.e.,

$$Z = \sum_{v \in V_1} \varepsilon_v,$$

where for each vertex $v \in V_1$ we have $e_v = \varepsilon_v + x_v$ for some $x_v \in C_1^\perp$. Therefore

$$Z = \sum_{v \in V_1} (e_v + x_v) = \sum_{v \in V_1} x_v,$$

where the e_v terms cancel since each face occurs exactly twice in the sum above. Next, we show that e_0 is V_{10} -weighted. We have

$$e_0 = e + Z^{01} = e + \sum_{v \in V_{01}} \varepsilon_v.$$

Note that the terms in the latter sum are disjoint for distinct vertices $v, v' \in V_{01}$. It follows that the restriction of e_0 to a vertex $v \in V_{01}$ is given by

$$(e_0)_v = e_v + \varepsilon_v = x_v,$$

which has zero syndrome. Finally we show that Z is associated with e_0 . The restriction of e_0 to a vertex $v \in V_{10}$ is given by

$$(e_0)_v = e_v + Q(v) \cap \sum_{u \in V_{01}} \varepsilon_u.$$

Likewise, the restriction of Z to $v \in V_{10}$ is given by

$$Z_v = \varepsilon_v + Q(v) \cap \sum_{u \in V_{01}} \varepsilon_u.$$

It follows that

$$\sigma_v(Z) = \sigma_v(\varepsilon_v) + \sigma_v \left(Q(v) \cap \sum_{u \in V_{01}} \varepsilon_u \right) = \sigma_v(e_v) + \sigma_v \left(Q(v) \cap \sum_{u \in V_{01}} \varepsilon_u \right) = \sigma_v(e_0),$$

which shows that Z is associated with e_0 . □

The notion of e_i being a V_{10} -weighted error is invariant as the decoder proceeds, i.e., if e_i is initially V_{10} -weighted then it remains so. Moreover, if Z was initially a mismatch associated with e_0 then Z_i remains associated with e_i throughout all steps i of the decoder.

Lemma 4.8. *Let Z be a weighted mismatch vector associated with a V_{10} -weighted error e . Let $x = c + r \subseteq Q(v)$ be a codeword of C_1^\perp , with $v \in V_{ij}$. Define*

$$f = \begin{cases} 0, & v \in V_{10}, \\ x, & v \in V_{01}, \\ c, & v \in V_{11}, \\ r, & v \in V_{00}, \end{cases}$$

to be the associated flip set. Then $e + f$ is again a V_{10} -weighted error and $Z + x$ is an associated mismatch vector.

Proof. It is clear that $Z + x$ is a mismatch vector since Z was one and we add a single C_1^\perp codeword.

We first show that $e + f$ remains V_{10} -weighted. Clearly $e + f$ is V_{10} -weighted if $v \in V_{10}$ or $v \in V_{01}$ since we either add nothing, or a local codeword to a V_{01} vertex. Now suppose that $v \in V_{00}$ so that $f = r$. We can decompose r into $r = r_1 + \dots + r_k$, where each r_i is a local codeword supported on a single row, which we can assume to be indexed by the edge (v, u_i) for some $u_i \in V_{01}$. The syndrome of $e + r$ on a vertex $u \in V_{01}$ is therefore given by

$$\sigma_u(e + f) = \begin{cases} \sigma_u(e) & u \neq u_i \text{ for all } i, \\ \sigma_u(e + r_i) & u = u_i \text{ for some } i. \end{cases}$$

In either case, we have $\sigma_u(e + f) = 0$ so that $e + f$ is V_{10} -weighted. The case where $v \in V_{11}$ is analogous, taking $f = c$ and making a similar decomposition.

Finally, we show that $Z + x$ is associated with $e + f$. Let us write

$$Z = \sum_{u \in V_{10}} \varepsilon_u,$$

where $\sigma_u(Z) = \sigma_u(e)$ for all $u \in V_{10}$. If $v \in V_{10}$ then there is nothing to show since all syndromes are unchanged. If $v \in V_{01}$ then define

$$\varepsilon'_u = \varepsilon_u + Q(u) \cap x$$

so that

$$Z + x = \sum_{u \in V_{10}} \varepsilon'_u.$$

Since $(e + x)_u = e_u + Q(u) \cap x$, we see that ε'_u has the same syndrome as $(e + f)_u$.

Lastly, suppose $v \in V_{00}$, with the V_{11} case being analogous. Let $f = r$. Note that $\varepsilon'_u = \varepsilon_u$ and $(e + r)_u = e_u$ for all $u \in V_{10}$ not adjacent to v . Therefore it suffices to consider $u \in N(v)$. In this case, $Q(u) \cap c$ is just the column of c labeled by the edge (u, v) and so $Q(u) \cap c$ is a local codeword. Therefore $\sigma_u(c) = 0$. It follows that

$$\sigma_u(\varepsilon'_u) = \sigma_u(\varepsilon_u) + \sigma_u(x) = \sigma_u(e) + \sigma_u(r) + \sigma_u(c) = \sigma_u(e) + \sigma_u(r) = \sigma_u(e + r)$$

for all $u \in N(v)$. Therefore $\sigma_u(Z + x) = \sigma_u(e + f)$ for all $u \in V_{10}$ and so $Z + x$ is associated with $e + f$. \square

Lemma 4.7 and Lemma 4.8 show that Z_i is a mismatch vector associated with the V_{10} -weighted error e_i for all i . We further cite the following lemma from Ref. [33], which gives a sufficient condition for the existence of good local corrections. This is the key to proving that in the noiseless case, the sequential and parallel decoders converge.

Definition 4.9. Let Z be a mismatch vector and let $Z = C_0 + C_1 + R_0 + R_1$ be a minimal decomposition for Z . We say that a vertex $v \in V_{ij}$ is *active* with respect this decomposition if $Q(v) \cap (R_i + C_j) \neq \emptyset$.

Theorem 4.10 (Theorem 12 in Ref. [33]). *Fix $\delta \in (0, 1)$. Let Z be a non-zero mismatch vector. If for all $i, j \in \{0, 1\}$, the set of active vertices $S_{ij} \subseteq V_{ij}$ for a minimal decomposition of Z satisfies*

$$|S_{ij}| \leq \frac{1}{2^{12}} d_r^2 \delta^3 \kappa |V_{00}|,$$

where d_r denotes the relative distance of the local code, then there exists a non-zero $x \subseteq Q(v)$ for some $v \in V_{ij}$ that is a C_1^\perp codeword such that

$$|Z| - |Z + x| \geq (1 - \delta)|x|.$$

4.3. Sequential decoder. To begin analyzing the sequential decoder with noisy input, the natural question to ask is that if the ideal mismatch Z can be decomposed by Algorithm 2 into $\mathcal{F} = \{x_i\}_{i=1}^t$, how well do these local corrections x_i decompose the noisy mismatch $\tilde{Z} = Z + Z_N$? The following two lemmas address this question.

Definition 4.11. Let Z be a mismatch vector. We say that Z is δ -decomposable if Algorithm 2 successfully returns a decomposition of Z when run with parameter δ , i.e., if Algorithm 2 halts with state $\hat{Z} = 0$.

Lemma 4.12. *Let Z be an δ -decomposable mismatch and let $\mathcal{F} = \{x_i\}_{i=1}^t$ denote the codewords returned by Algorithm 2 run with input Z and parameter δ . Then*

$$(1 - \delta) \sum_{i=1}^t |x_i| \leq |Z| \leq \sum_{i=1}^t |x_i|.$$

Proof. Let

$$Z_k = Z - \sum_{i=1}^k x_i,$$

with $Z = Z_0$. Note that since Algorithm 2 completely decomposes Z , we have $Z_t = 0$ and

$$Z = \sum_{i=1}^t x_i.$$

For the decomposition with parameter δ , we have $|Z_{i-1}| - |Z_i| \geq (1 - \delta)|x_i|$ and therefore

$$|Z| \geq (1 - \delta) \sum_{i=1}^t |x_i|.$$

Together, we get the bounds

$$(1 - \delta) \sum_{i=1}^t |x_i| \leq |Z| \leq \sum_{i=1}^t |x_i|.$$

□

Lemma 4.13. *Let Z be a mismatch vector and let $Z_N \in \mathbb{F}_2^Q$ be any vector. Let $\tilde{Z} = Z + Z_N$. Suppose that Z is δ -decomposable with decomposition $\mathcal{F} = \{x_i\}_{i=1}^t$. Let*

$$\mathcal{F}^* = \{x \in \mathcal{F} : |\tilde{Z}| - |\tilde{Z} + x| \geq (1 - \varepsilon)|x|\}.$$

Then

$$\sum_{x \in \mathcal{F}^*} |x| \geq c_1 |Z| - c_2 |Z_N| \quad (7)$$

for constants

$$c_1 = \frac{\varepsilon - 2\delta}{\varepsilon(1 - \delta)} \quad \text{and} \quad c_2 = \frac{2}{\varepsilon}.$$

In particular, if $\mathcal{F}^* = \emptyset$, then $c_1 |Z| \leq c_2 |Z_N|$.

Proof. This proof follows the idea of Lemma 5.1 in Ref. [42]. Given any set $y \in \mathbb{F}_2^Q$, we have

$$|\tilde{Z}| - |\tilde{Z} + y| = |\tilde{Z}| - (|\tilde{Z}| + |y| - 2|\tilde{Z} \cap y|) = 2|\tilde{Z} \cap y| - |y|.$$

For all $y \in \mathcal{F} \setminus \mathcal{F}^*$, we have

$$|\tilde{Z} \cap y| = \frac{1}{2}(|y| + |\tilde{Z}| - |\tilde{Z} + y|) < \left(1 - \frac{\varepsilon}{2}\right) |y|.$$

Define $T = \sum_{x \in \mathcal{F}} |\tilde{Z} \cap x|$. We then have

$$\begin{aligned} T &= \sum_{x \in \mathcal{F}^*} |\tilde{Z} \cap x| + \sum_{y \in \mathcal{F} \setminus \mathcal{F}^*} |\tilde{Z} \cap y| \\ &< \sum_{x \in \mathcal{F}^*} |x| + \left(1 - \frac{\varepsilon}{2}\right) \sum_{y \in \mathcal{F} \setminus \mathcal{F}^*} |y| \\ &= \frac{\varepsilon}{2} \sum_{x \in \mathcal{F}^*} |x| + \left(1 - \frac{\varepsilon}{2}\right) \sum_{y \in \mathcal{F}} |y| \\ &\leq \frac{\varepsilon}{2} \sum_{x \in \mathcal{F}^*} |x| + \frac{2 - \varepsilon}{2(1 - \delta)} |Z|, \end{aligned}$$

where the last inequality follows from Lemma 4.12. On the other hand, we also have

$$\begin{aligned} T &\geq |\tilde{Z} \cap \sum_{x \in \mathcal{F}} x| = |\tilde{Z} \cap Z| \\ &= |Z| - |Z \cap Z_N| \geq |Z| - |Z_N|. \end{aligned}$$

Combining these two inequalities, we get

$$\frac{\varepsilon}{2} \sum_{x \in \mathcal{F}^*} |x| + \frac{2 - \varepsilon}{2(1 - \delta)} |Z| \geq |Z| - |Z_N|,$$

or equivalently

$$\sum_{x \in \mathcal{F}^*} |x| \geq \frac{\varepsilon - 2\delta}{\varepsilon(1 - \delta)} |Z| - \frac{2}{\varepsilon} |Z_N|,$$

as desired. □

Note that Lemma 4.13 will set an implicit bound of $\delta < 1/2$ since we require $\varepsilon - 2\delta > 0$ for the bound (7) to be non-trivial.

Suppose now that the noisy mismatch vector \tilde{Z} is given as input to Algorithm 1 with parameter ε , which terminates after T iterations. Let us denote the residual error by \tilde{e}_T and its associated mismatch by $\tilde{Z}_T = Z_T + Z_N$. If Z_T is δ -decomposable, then Lemma 4.13 implies that $|Z_T| = O(|Z_N|)$. Namely, the sequential decoder terminates only when the mismatch noise Z_N becomes significant. In the following lemma, we further relate the weight of the noiseless residual error e_T with $|Z_T|$.

Lemma 4.14 (Mismatch Correctness and Soundness). *Let e be a V_{10} -weighted error and let Z be an associated mismatch vector. Suppose that Z is δ -decomposable and that*

$$|e|_R + \frac{1}{\kappa(1 - \delta)} |Z| < d. \tag{8}$$

Then we have

$$|Z| \geq (1 - \delta)\kappa |e|_R.$$

Proof. Let $\mathcal{F} = \{x_i\}_{i=1}^t$ denote the decomposition returned for Z by Algorithm 2 with parameter δ . Each x_i is supported on the local view of some vertex v_i and has the further decomposition into column and row codewords as $x_i = c_i + r_i$.

First, we prove that $e \cong \hat{C}_1 + \hat{R}_0$, where \cong denotes equivalence up to stabilizers. Let $e_0 = e$ and define $e_i = e_{i-1} + f_i$ where

$$f_i = \begin{cases} 0, & v \in V_{10}, \\ x_i, & v \in V_{01}, \\ c_i, & v \in V_{11}, \\ r_i, & v \in V_{00}. \end{cases}$$

Note that by construction we have

$$e_t = e_0 + \hat{C}_1 + \hat{R}_0.$$

By Lemma 4.8, the errors e_i are all V_{10} -weighted, and the vector $Z_k = Z + \sum_{i=1}^k x_i$ is a mismatch vector associated with e_i at each step. It follows by the V_{10} -weighting of e_t that

$$\forall v \in V_{01} : \sigma_v(e_t) = 0.$$

Since $Z_t = 0$, it follows by the association of Z_t and e_t that

$$\forall v \in V_{10} : \sigma_v(e_t) = \sigma_v(Z_t) = 0.$$

It follows that e_t has zero syndrome. It remains to show that e_t is a stabilizer, which we can do by bounding its weight. For each flip-set f_i , we have

$$|f_i| \leq |r_i| + |c_i| \leq \Delta(\|r_i\| + \|c_i\|) \leq |x_i|/\kappa, \quad (9)$$

where we use the robustness of the local code in the last inequality. Using Lemma 4.12, we then have

$$|Z| \geq (1 - \delta) \sum_{i=1}^t |x_i| \geq (1 - \delta)\kappa \sum_{i=1}^t |f_i|.$$

It follows that

$$|e_t|_R = \left| e + \sum_{i=1}^t f_i \right|_R \leq |e|_R + \sum_{i=1}^t |f_i| \leq |e|_R + \frac{1}{\kappa(1 - \delta)} |Z| < d.$$

Therefore $e_t \cong 0$ and hence $e \cong \hat{C}_1 + \hat{R}_0$. Finally, we have

$$|e|_R = \left| \hat{C}_1 + \hat{R}_0 \right|_R \leq \left| \hat{C}_1 + \hat{R}_0 \right| \leq \sum_{i=1}^t |f_i| \leq \frac{1}{\kappa(1 - \delta)} |Z|.$$

□

Now we show that, without surprise, Z_T is δ -decomposable. Let us define the constants

$$A_\varepsilon = \frac{24}{\kappa \Delta(1 - \varepsilon)}, \quad B_\varepsilon = \frac{3\Delta}{\kappa(1 - \varepsilon)}, \quad \text{and} \quad C_\delta = \frac{1}{2^{12}} d_r^2 \delta^3 \kappa \Delta^{-2}.$$

For the purposes of the parallel decoder, it will be convenient to consider a generalized mismatch decomposition procedure which initially starts the decomposition with some weight parameter ε and then switches to some other parameter ε' partway through (see Lemma 4.18). We state the generalized result below in Lemma 4.15, although we will only need the special case where $\varepsilon = \varepsilon'$ for the analysis of the sequential decoder.

Lemma 4.15. *Let e be an error and D a syndrome noise. Let $\tilde{Z} \equiv Z + Z_N$ denote the initial noisy mismatch vector assigned to e and D .*

Let $\varepsilon, \varepsilon' \in (0, 1)$ be constants such that $\varepsilon' \leq \varepsilon$. Consider a modified Algorithm 2 which takes input \tilde{Z} and runs with parameter ε for the first t steps and then switches to parameter ε' until it halts at step $T \geq t$. Let $\tilde{Z}_T \equiv Z_T + Z_N$ denote the final output of this process.

If $A_\varepsilon |e|_R + B_\varepsilon |D|_V \leq C_\delta n$, then Z_T is δ -decomposable.

Proof. Consider the process of running the modified Algorithm 2 with input \tilde{Z} and parameter ε for t steps, and then switching the parameter to ε' until the algorithm finally halts at step T . Let $\{x_1, \dots, x_t\}$ be local codewords obtained with parameter ε , and $\{x_{t+1}, \dots, x_T\}$ the codewords obtained with parameter ε' . Denoting \tilde{Z}_i the mismatch vector at iteration i , we have

$$|\tilde{Z}_{i-1}| - |\tilde{Z}_i| \geq \begin{cases} (1 - \varepsilon)|x_i|, & i \in \{1, \dots, t\}, \\ (1 - \varepsilon')|x_i|, & i \in \{t+1, \dots, T\}. \end{cases} \quad (10)$$

We wish to show that Z_T is δ -decomposable. Suppose that Algorithm 2 returns local codewords $\{y_1, \dots, y_k\}$ when given input Z_T with parameter δ . Let $S_{T+k,ij}$ denote a set of active vertices in V_{ij} for the mismatch

$$Z_{T+k} \equiv Z_T + \sum_{\ell=1}^k y_\ell.$$

For all $k \in [K]$, we have

$$|S_{T+k,ij}| \leq \|Z_{T+k}\| \leq \|Z\| + \sum_{i=1}^T \|x_i\| + \sum_{\ell=1}^k \|y_\ell\|, \quad (11)$$

where the first inequality holds since there exists at least one non-zero row or column for each active vertex. By robustness of the local code, we have $\kappa \Delta \|x_i\| \leq |x_i|$. Continuing the chain of inequalities, we have

$$\begin{aligned} (11) &\leq \|Z\| + \frac{1}{\kappa \Delta} \sum_{i=1}^T |x_i| + \frac{1}{\kappa \Delta} \sum_{\ell=1}^k |y_\ell| \\ &\leq \|Z\| + \frac{1}{\kappa \Delta} \sum_{i=1}^T |x_i| + \frac{1}{\kappa \Delta (1 - \delta)} |Z_T|, \end{aligned} \quad (12)$$

where the first inequality follows by robustness and the second by the fact that $|Z_{T+\ell-1}| - |Z_{T+\ell-1} + y_\ell| \geq (1 - \delta)|y_\ell|$. Using inequality (10), we get

$$|Z_T| = \left| Z + \sum_{i=1}^T x_i \right| \leq |Z| + \sum_{i=1}^T |x_i| \leq |Z| + \frac{1}{1 - \varepsilon} (|\tilde{Z}| - |\tilde{Z}_t|) + \frac{1}{1 - \varepsilon'} (|\tilde{Z}_t| - |\tilde{Z}_T|).$$

Since $\varepsilon' \leq \varepsilon$, it follows that

$$|Z_T| \leq |Z| + \frac{1}{1 - \varepsilon} |\tilde{Z}|. \quad (13)$$

Inserting (13) into (12), we get

$$\begin{aligned} |S_{T+k,ij}| &\leq \|Z\| + \frac{1}{\kappa \Delta (1 - \delta)} |Z| + \frac{1}{\kappa \Delta (1 - \varepsilon)} \left(\frac{2 - \delta}{1 - \delta} \right) |\tilde{Z}| \\ &\leq \|Z\| + \frac{1}{\kappa \Delta (1 - \delta)} |Z| + \frac{1}{\kappa \Delta (1 - \varepsilon)} \left(\frac{2 - \delta}{1 - \delta} \right) (|Z| + |Z_N|) \end{aligned} \quad (14)$$

$$\leq \frac{4}{\kappa\Delta}|e|_R + \frac{4}{\kappa\Delta(1-\delta)}|e|_R + \frac{1}{\kappa\Delta(1-\varepsilon)}\left(\frac{2-\delta}{1-\delta}\right)(4|e|_R + \Delta^2|D|_V), \quad (15)$$

where the last inequality follows by applying Lemma 4.5, together with the fact that $\varepsilon_v(D)$ can be non-zero only when v is in the support of D and hence

$$|Z_N| = \left| \sum_{v \in V_1} \varepsilon_v(D) \right| \leq \sum_{v \in V_1} |\varepsilon_v(D)| \leq |D|_V \max_{v \in V_1} |\varepsilon_v(D)| \leq |D|_V \Delta^2.$$

Simplifying, we finally get

$$\begin{aligned} |S_{T+k,ij}| &\leq \frac{4}{\kappa\Delta} \left(\frac{2-\delta}{1-\delta}\right) \left(\frac{2-\varepsilon}{1-\varepsilon}\right) |e|_R + \frac{\Delta}{\kappa(1-\varepsilon)} \left(\frac{2-\delta}{1-\delta}\right) |D|_V \\ &\leq \frac{12}{\kappa\Delta} \left(\frac{2}{1-\varepsilon}\right) |e|_R + \frac{3\Delta}{\kappa(1-\varepsilon)} |D|_V \\ &\equiv A_\varepsilon |e|_R + B_\varepsilon |D|_V, \end{aligned}$$

where we use the fact that $(2-\delta)/(1-\delta) \leq 3$ for $\delta \in (0, 1/2)$. It follows that if we have $A_\varepsilon |e|_R + B_\varepsilon |D|_V \leq C_\delta n$, then the active vertex condition of Theorem 4.10 is always satisfied so that Algorithm 2 must be able to completely decompose Z_T . \square

It remains for us to check that (8) in Lemma 4.14 holds.

Lemma 4.16. *Assume the hypotheses of Lemma 4.15, and furthermore that*

$$A_\varepsilon |e|_R + B_\varepsilon |D|_V \leq \frac{d}{\Delta}.$$

Then

$$|Z_T| \geq (1-\delta)\kappa|e_T|_R.$$

Proof. By Lemmas 4.7 and 4.8, the error e_T is V_{10} -weighted and Z_T is an associated mismatch vector. Applying Lemma 4.14, it suffices to prove

$$|e_T|_R + \frac{1}{\kappa(1-\delta)}|Z_T| < d. \quad (16)$$

We have

$$|e_T|_R = \left| e_0 + \sum_{i=1}^T f_i \right|_R \leq |e_0|_R + \sum_{i=1}^T |f_i| \leq |e_0|_R + \frac{1}{\kappa} \sum_{i=1}^T |x_i| \leq |e_0|_R + \frac{1}{\kappa(1-\varepsilon)}|\tilde{Z}|,$$

where the second inequality follows from (9). We then get

$$\begin{aligned} |e_T|_R + \frac{1}{\kappa(1-\delta)}|Z_T| &\leq |e_0|_R + \frac{1}{\kappa(1-\varepsilon)}|\tilde{Z}| + \frac{1}{\kappa(1-\delta)}|Z_T| \\ &\leq |e_0|_R + \frac{1}{\kappa(1-\varepsilon)}|\tilde{Z}| + \frac{1}{\kappa(1-\delta)}\left(|Z| + \frac{1}{1-\varepsilon}|\tilde{Z}|\right) \end{aligned}$$

$$= |e_0|_R + \frac{1}{\kappa(1-\delta)}|Z| + \frac{1}{\kappa(1-\varepsilon)}\left(1 + \frac{1}{1-\delta}\right)|\tilde{Z}|,$$

where we use (13) in the second inequality. Next, we may assume without loss of generality that e is a reduced error. Then we have

$$|e_0|_R = |\tilde{e}_0 + Z_N^{01}|_R = \left|e + \sum_{v \in V_{01}} \varepsilon_v\right|_R \leq |e| + \sum_{v \in V_{01}} |e_v| = 2|e| = 2|e|_R,$$

where we use the fact that ε_v are minimum weight corrections in the inequality above and the fact that $e_u \cap e_v = \emptyset$ for distinct vertices $u, v \in V_{01}$ in the second last equality. Following the same steps as from (14) to (15), we therefore get

$$\begin{aligned} |e_T|_R + \frac{1}{\kappa(1-\delta)}|Z_T| &\leq 2|e|_R + \frac{4}{\kappa(1-\delta)}|e|_R + \frac{1}{\kappa(1-\varepsilon)}\left(1 + \frac{1}{1-\delta}\right)(4|e|_R + \Delta^2|D|_V) \\ &\leq \left[2 + \frac{4}{\kappa(1-\varepsilon)}\left(1 + \frac{2-\varepsilon}{1-\delta}\right)\right]|e|_R + \Delta B_\varepsilon|D|_V. \end{aligned}$$

We can simplify the inequality above by noting that $\kappa \leq d_r \leq 1$ [36]. Then we have

$$\begin{aligned} 2 + \frac{4}{\kappa(1-\varepsilon)}\left(1 + \frac{2-\varepsilon}{1-\delta}\right) &= \frac{1}{\kappa}\left[2\kappa + \frac{4}{1-\varepsilon}\left(1 + \frac{2-\varepsilon}{1-\delta}\right)\right] \\ &\leq \frac{1}{\kappa}\left[4 + \frac{4}{1-\varepsilon}\left(1 + \frac{2-\varepsilon}{1-\delta}\right)\right] \\ &= \frac{4}{\kappa}\left(\frac{2-\delta}{1-\delta}\right)\left(\frac{2-\varepsilon}{1-\varepsilon}\right) \\ &\leq \frac{24}{\kappa(1-\varepsilon)} = \Delta A_\varepsilon. \end{aligned}$$

Therefore it suffices to require

$$A_\varepsilon|e|_R + B_\varepsilon|D|_V \leq \frac{d}{\Delta}$$

in order that inequality (16) holds. □

Combining the inequalities, we obtain the main result for sequential decoder.

Theorem 4.17 (Main Theorem for the Sequential Decoder). *Let e be an error and let D be a syndrome error. Suppose that*

$$A_\varepsilon|e|_R + B_\varepsilon|D|_V \leq \min(C_\delta n, d/\Delta).$$

Let $\tilde{\sigma} = \sigma(e) + D$. Then Algorithm 1 with input $\tilde{\sigma}$ and parameter ε will output a correction \hat{f} satisfying

$$|e + \hat{f}|_R \leq \left(1 + \frac{2c_2}{\kappa c_1}\right)\Delta^2|D|_V.$$

Proof. Suppose that Algorithm 1 with parameter ε terminates after T steps with output \hat{f} . Let Z_T denote the state of the mismatch after the algorithm terminates. By Lemma 4.15, Z_T is δ -decomposable. This allows us to apply Lemma 4.13, giving

$$0 \geq c_1|Z_T| - c_2|Z_N|, \quad (17)$$

since the set \mathcal{F}^* must be empty when Algorithm 1 with parameter ε terminates. By Lemma 4.16, we get

$$|Z_T| \geq (1 - \delta)\kappa|e_T|_R. \quad (18)$$

But we know

$$|e_T|_R = |\tilde{e}_T + Z_N^{01}|_R \geq |\tilde{e}_T|_R - |Z_N^{01}|_R \geq |\tilde{e}_T|_R - \Delta^2|D|_V. \quad (19)$$

Combining the inequalities (17), (18), and (19) finally gives

$$\begin{aligned} |e + \hat{f}|_R &= |\tilde{e}_T|_R \\ &\leq |e_T|_R + \Delta^2|D|_V \\ &\leq \frac{1}{(1 - \delta)\kappa}|Z_T| + \Delta^2|D|_V \\ &\leq \frac{c_2}{c_1(1 - \delta)\kappa}|Z_N| + \Delta^2|D|_V \\ &\leq \left(1 + \frac{c_2}{c_1(1 - \delta)\kappa}\right) \Delta^2|D|_V. \end{aligned}$$

Note that the restriction $\delta < 1/2$, as required by Lemma 4.13, implies that $(1 - \delta)^{-1} \leq 2$. \square

This completes our proof of the main theorem for the sequential decoder.

4.4. Parallel decoder. The key idea in analyzing the parallel decoder is to compare the performance of one iteration of parallel decoding to that of a full execution of the sequential decoder. Our convention in this section will be that superscript indices will denote the parallel decoding iteration (always with parameter $1/2$), while subscript indices will denote the sequential decoding iteration. For example, $\tilde{Z}_j^{(k)}$ denotes the mismatch obtained after k iterations of parallel decoding and then j iterations of sequential decoding.

For convenience, we will fix some parameters in this section. Throughout, we will take $\varepsilon = 1/2$ for the parallel decoder. We will write $A = A_{\varepsilon=1/2}$ and $B = B_{\varepsilon=1/2}$.

Lemma 4.18. *Let $\varepsilon' \in (0, 1/6)$. Let $\tilde{Z}^{(k)}$ denote the current state of the (noisy) mismatch vector. Let $\tilde{Z}_T^{(k)}$ denote the residual mismatch after running the sequential decoder with input $\tilde{Z}^{(k)}$ and parameter ε' . Then after one iteration of parallel decoding, the weight of the mismatch is reduced by at least*

$$|\tilde{Z}^{(k)}| - |\tilde{Z}^{(k+1)}| \geq \frac{1}{16}(1 - 6\varepsilon') \left(|\tilde{Z}^{(k)}| - |\tilde{Z}_T^{(k)}| \right).$$

Proof. The proof closely follows the ideas of Lemma 18 in Ref. [33]. For ease of notation we write $\tilde{Z}^{(k)}$ as \tilde{Z} throughout this proof. Suppose that Algorithm 2 runs with input \tilde{Z} and parameter ε' returns local codewords $\{x_i\}_{i=1}^T$ and residual mismatch \tilde{Z}_T . Therefore we can write

$$\tilde{Z} = \sum_{i=1}^T x_i + \tilde{Z}_T.$$

We will analyze the overlap among the sets x_i , and argue that the parallel decoder's output will intersect non-trivially with the sequential decoder's output. Let us define the sets

$$x'_i = \left(\tilde{Z} \cap x_i \right) \setminus \bigcup_{j < i} x_j.$$

Note that the sets x'_i are disjoint, and that they satisfy

$$\bigcup_{i=1}^T x'_i = \tilde{Z} \cap \bigcup_{i=1}^T x_i \supseteq \tilde{Z} \cap \sum_{i=1}^T x_i,$$

which implies

$$\left| \tilde{Z} \setminus \bigcup_{i=1}^T x'_i \right| \leq \left| \tilde{Z} \setminus \left(\tilde{Z} \cap \sum_{i=1}^T x_i \right) \right| = \left| \tilde{Z} \setminus \sum_{i=1}^T x_i \right| \leq \left| \tilde{Z} + \sum_{i=1}^T x_i \right| = |\tilde{Z}_T|.$$

Next, we define the set of “good” indices $G \subseteq [T]$ such that $i \in G$ if and only if

$$|x'_i| \geq \left(1 - \frac{3}{2}\varepsilon' \right) |x_i|.$$

Let $B = [T] \setminus G$ denote the remaining set of “bad” indices. For each $j \in [T]$, let us define

$$\tilde{Z}'_j = \tilde{Z} \setminus \bigcup_{i \leq j} x'_i = \tilde{Z}'_{j-1} \setminus x'_j.$$

We wish to bound the difference between \tilde{Z}_j and \tilde{Z}'_j . Let us denote this difference by

$$A_j = \tilde{Z}_j \setminus \tilde{Z}'_j.$$

To bound the size of A_j , we examine how the size of \tilde{Z} changes as we update it by adding codewords x_j . Since the x_j 's were obtained by running the decoder with parameter ε' , it follows that

$$|\tilde{Z}_{j-1} \cap x_j| \geq (1 - \varepsilon'/2)|x_j|.$$

Referring to Fig. 3, we have $A_j \setminus A_{j-1} = x_j \setminus \tilde{Z}_{j-1}$, and hence

$$|A_j \setminus A_{j-1}| = |x_j \setminus \tilde{Z}_{j-1}| = |x_j| - |x_j \cap \tilde{Z}_{j-1}| \leq |x_j| - \left(1 - \frac{\varepsilon'}{2} \right) |x_j| = \frac{\varepsilon'}{2} |x_j|. \quad (20)$$

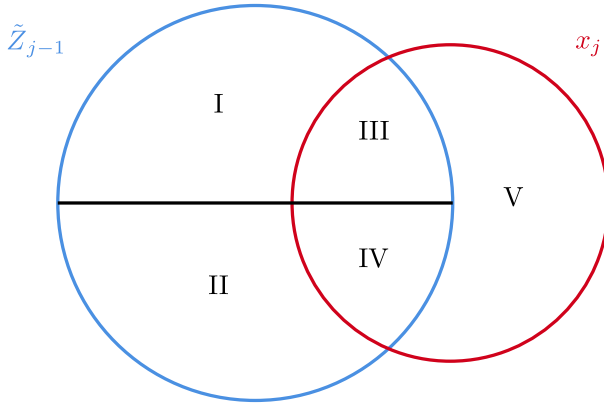


Fig. 3. Reference for sets involved in proof of Lemma 4.18. The regions indicated are: $\text{II} \cup \text{IV} = \tilde{Z}'_{j-1}$, $\text{I} \cup \text{III} = A_{j-1}$, $\text{II} = \tilde{Z}'_j$, $\text{IV} = x'_j$, $\text{III} \cup \text{IV} = \tilde{Z}_{j-1} \cap x_j$, $\text{I} \cup \text{V} = A_j$, and $\text{I} \cup \text{II} \cup \text{V} = \tilde{Z}_j$.

We also have

$$(A_{j-1} \setminus A_j) \sqcup x'_j = \tilde{Z}_{j-1} \cap x_j,$$

corresponding to the unions of regions III and IV in Fig. 3. If $j \in B$ is a “bad” index, then we have

$$|A_{j-1} \setminus A_j| + \left(1 - \frac{3}{2}\varepsilon'\right)|x_j| > |A_{j-1} \setminus A_j| + |x'_j| = |\tilde{Z}_{j-1} \cap x_j| \geq \left(1 - \frac{\varepsilon'}{2}\right)|x_j|,$$

where the first inequality follows from the fact that $j \in B$ and the last from the decoding condition with parameter ε' . It follows that

$$|A_{j-1} \setminus A_j| \geq \varepsilon'|x_j|, \quad (21)$$

and hence

$$|A_{j-1}| - |A_j| = |A_{j-1} \setminus A_j| - |A_j \setminus A_{j-1}| \geq \varepsilon'|x_j| - \frac{\varepsilon'}{2}|x_j| = \frac{\varepsilon'}{2}|x_j|,$$

where we use inequalities (20) and (21) above. It follows that we have

$$\begin{cases} |A_j| - |A_{j-1}| \leq \varepsilon'|x_j|/2, & \forall j \in G, \\ |A_j| - |A_{j-1}| \leq -\varepsilon'|x_j|/2, & \forall j \in B. \end{cases}$$

Summing the inequalities above, we get

$$0 \leq |A_T| - |A_0| = \sum_{j=1}^T (|A_j| - |A_{j-1}|) \leq \frac{\varepsilon'}{2} \left(\sum_{j \in G} |x_j| - \sum_{j \in B} |x_j| \right),$$

where $|A_0| = 0$ by definition. Therefore

$$\sum_{j \in B} |x_j| \leq \sum_{j \in G} |x_j|.$$

We have

$$\sum_{j \in B} |x'_j| \leq \left(1 - \frac{3}{2}\varepsilon'\right) \sum_{j \in B} |x_j| \leq \left(1 - \frac{3}{2}\varepsilon'\right) \sum_{j \in G} |x_j| \leq \sum_{j \in G} |x'_j|,$$

and hence

$$|\tilde{Z}| - |\tilde{Z}_T| \leq \left| \bigcup_{j=1}^T x'_j \right| = \sum_{j=1}^T |x'_j| = \sum_{j \in B} |x'_j| + \sum_{j \in G} |x'_j| \leq 2 \sum_{j \in G} |x'_j|. \quad (22)$$

Now, consider the iteration of parallel decoding beginning with input $\tilde{Z} \equiv \tilde{Z}^{(k)}$. Let $u \in \mathbb{F}_2^Q$ denote the set of all qubits which have been acted on by the parallel decoder, i.e.,

$$u = \bigcup_{z_v \in \mathcal{F}} z_v,$$

where $\mathcal{F} = \{z_v\}$ is the collection of all local codewords found by the decoder in the current iteration. We now prove that for all $j \in G$, we have $|x_j \cap u| \geq c|x_j|$ for some constant $c > 0$.

Fix some x_j and let v denote its anchoring vertex. Let us write $y = |x'_j \cap u|$. First, let us show that we must have

$$|x'_j \setminus u| < \frac{3}{4}|x_j|.$$

Suppose otherwise. Then let z_v denote the codeword (possibly zero) that the parallel decoder assigns to vertex v . Note that we have $z_v \subseteq u$ by definition, as well as

$$|\bar{Z}| - |\bar{Z} + z_v| \geq \frac{1}{2}|z_v|, \quad (23)$$

where \bar{Z} denotes the current state of the noisy mismatch in the parallel decoder. By definition of u as the execution support of the decoder, the qubits of $x'_j \setminus u$ are untouched by the algorithm. Therefore, since $x'_j \subseteq \tilde{Z}$, it follows that $x'_j \setminus u \subseteq \bar{Z}$ and $x'_j \setminus u \subseteq \bar{Z} + z_v$. Therefore we have

$$x'_j \setminus u = x'_j \setminus u \cap (\bar{Z} + z_v) \subseteq x_j \cap (\bar{Z} + z_v).$$

The addition of x_j to $\bar{Z} + z_v$ therefore removes at least $|x'_j \setminus u| \geq \frac{3}{4}|x_j|$ qubits from \bar{Z} . Consequently, the addition of x_j to $\bar{Z} + z_v$ can add at most $|x_j|/4$ qubits, so that

$$|\bar{Z} + z_v| - |\bar{Z} + z_v + x_j| \geq \frac{1}{2}|x_j|.$$

Adding this inequality to (23), we get

$$|\bar{Z}| - |\bar{Z} + z_v + x_j| \geq \frac{1}{2}(|x_j| + |z_v|) \geq \frac{1}{2}|z_v + x_j|.$$

Similar to the argument above, the addition of x_j to z_v adds at least $|x_j \setminus z_v| \geq |x'_j \setminus u| \geq 3|x_j|/4$ qubits, and hence removes at most $|x_j|/4$ qubits. Therefore

$$|z_v + x_j| - |z_v| \geq \frac{1}{2}|x_j|.$$

Since $|z_v + x_j| > |z_v|$, this contradicts the assumption that z_v is the local codeword selected by the decoder, since the decoder will choose to maximize the Hamming weight of its local codewords. It follows that we've established the inequality

$$|x'_j \setminus u| < \frac{3}{4}|x_j|.$$

This then implies that for all $j \in G$, we have

$$|x'_j \cap u| > |x'_j| - \frac{3}{4}|x_j| \geq \left(1 - \frac{3}{2}\varepsilon'\right)|x_j| - \frac{3}{4}|x_j| = \left(\frac{1}{4} - \frac{3}{2}\varepsilon'\right)|x_j|.$$

Since the x'_j are disjoint, we get

$$\begin{aligned} |u| &\geq \sum_{j \in G} |x'_j \cap u| > \left(\frac{1}{4} - \frac{3}{2}\varepsilon'\right) \sum_{j \in G} |x_j| \\ &\geq \left(\frac{1}{4} - \frac{3}{2}\varepsilon'\right) \sum_{j \in G} |x'_j| \geq \frac{1}{8} (1 - 6\varepsilon') (|\tilde{Z}| - |\tilde{Z}_T|), \end{aligned}$$

where the last inequality follows from (22). Finally, by the decoding criterion (23), the total decrease in mismatch weight is

$$|\tilde{Z}^{(k)}| - |\tilde{Z}^{(k+1)}| \geq \frac{1}{2} \sum_{z_v \in \mathcal{F}} |z_v| \geq \frac{1}{2}|u| \geq \frac{1}{16} (1 - 6\varepsilon') (|\tilde{Z}^{(k)}| - |\tilde{Z}_T^{(k)}|),$$

where we restore the superscript (k) in this last inequality for clarity. \square

Now, as in the sequential case, we bound the weight of the residual mismatch by the weight of measurement noise.

Lemma 4.19. *Let e be an error and D be a syndrome noise. Let \tilde{Z} be the initial mismatch vector assigned to e and D . Let $\tilde{Z}^{(k)}$ denote the state of the mismatch vector after k iterations of parallel decoding. Let $\tilde{Z}_T^{(k)}$ denote the residual mismatch vector obtained by running the sequential decoder with input $\tilde{Z}^{(k)}$ and parameter ε' .*

Suppose that $A|e|_R + B|D|_V \leq C_\delta n$. Then for all $k \in \mathbb{N}^+$ we have

$$|\tilde{Z}_T^{(k)}| \leq \left(1 + \frac{2(1 - \delta)}{\varepsilon' - 2\delta}\right) \Delta^2 |D|_V \equiv (1 + \zeta) \Delta^2 |D|_V.$$

Proof. Suppose that $\mathcal{F} = \{x_i\}_{i=1}^K$ are the codewords which have been found by the parallel decoder after k iterations. Note that we can equivalently consider the same sequence to be obtained by running the sequential decoder with parameter $1/2$, i.e., we can consider $\tilde{Z}^{(k)}$ to be a state of the mismatch after K iterations of sequential decoding with parameter $1/2$. It follows that $\tilde{Z}_T^{(k)}$ is a mismatch obtained by first running the

sequential decoder with input \tilde{Z} and parameter $1/2$ for K iterations, and then switching to parameter ε' for the remaining iterations.

Applying Lemma 4.15 with $\varepsilon = 1/2$, our assumptions on $|e|_R$ and $|D|_V$ imply that $Z_T^{(k)}$ is δ -decomposable. Next, applying Lemma 4.13 (with ε' as ε), it follows that

$$|Z_T^{(k)}| \leq \frac{2(1-\delta)}{\varepsilon' - 2\delta} |Z_N|.$$

We then have

$$\begin{aligned} |\tilde{Z}_T^{(k)}| &= |Z_T^{(k)} + Z_N| \leq |Z_T^{(k)}| + |Z_N| \leq \left(1 + \frac{2(1-\delta)}{\varepsilon' - 2\delta}\right) |Z_N| \\ &\leq \left(1 + \frac{2(1-\delta)}{\varepsilon' - 2\delta}\right) \Delta^2 |D|_V. \end{aligned}$$

□

For simplicity, we take $\varepsilon' = 3\delta$ in the following theorem. Note that this sets an upper bound on δ so that $\delta < 1/18$.

Theorem 4.20 (Main Theorem for the Parallel Decoder). *Let e be an error and D be a syndrome error. Let \tilde{Z} be the initial (noisy) mismatch associated with e and D . Assume that*

$$A|e|_R + B|D|_V \leq \min(C_\delta n, d/\Delta).$$

Then after k iterations of parallel decoding, the decoder returns a correction $\hat{f}^{(k)}$ such that

$$|e + \hat{f}^{(k)}|_R \leq \alpha_k |e|_R + \beta |D|_V,$$

where

$$\alpha_k = \frac{24}{5\kappa} (1-\gamma)^k, \quad \beta = \frac{6}{\kappa\delta} \Delta^2, \quad \text{and} \quad \gamma = (1-18\delta)/16.$$

Proof. Applying Lemmas 4.18 and 4.19, it follows that the mismatch after k iterations of parallel decoding is bounded above as

$$|\tilde{Z}^{(k)}| \leq (1-\gamma) |\tilde{Z}^{(k-1)}| + \gamma(1+\zeta)\Delta^2 |D|_V.$$

Summing this inequality over k gives

$$\begin{aligned} |\tilde{Z}^{(k)}| &\leq (1-\gamma)^k |\tilde{Z}| + \gamma(1+\zeta)\Delta^2 |D|_V \left(1 + (1-\gamma) + (1-\gamma)^2 + \dots + (1-\gamma)^{k-1}\right) \\ &\leq (1-\gamma)^k |\tilde{Z}| + (1+\zeta)\Delta^2 |D|_V. \end{aligned} \tag{24}$$

Next, let $\tilde{e}^{(k)}$ denote the state of the error after k iterations of parallel decoding. Let $\tilde{e}_T^{(k)}$ denote the state of the error after T additional iterations of sequential decoding with parameter ε' . Let us write

$$\tilde{e}_T^{(k)} = \tilde{e}^{(k)} + \sum_{i=1}^T f_i,$$

where $\{f_i\}_{i=1}^T$ are the associated flip-sets with parameter ε' . It follows from Lemma 4.8 that $e_T^{(k)}$ is V_{10} -weighted with associated mismatch $Z_T^{(k)}$. Lemma 4.16 then implies that

$$|e_T^{(k)}|_R \leq \frac{1}{(1-\delta)\kappa} |Z_T^{(k)}| \leq \frac{\zeta}{(1-\delta)\kappa} |Z_N| \leq \frac{\zeta}{(1-\delta)\kappa} \Delta^2 |D|_V. \quad (25)$$

It remains to bound the weight of $|\tilde{e}^{(k)}|_R$. We have

$$|\tilde{e}^{(k)}|_R \leq |e^{(k)}|_R + \Delta^2 |D|_V \quad (26)$$

$$\begin{aligned} &\leq \left| e_T^{(k)} + \sum_{i=1}^T f_i \right|_R + \Delta^2 |D|_V \\ &\leq |e_T^{(k)}|_R + \sum_{i=1}^T |f_i| + \Delta^2 |D|_V \\ &\leq \frac{\zeta}{(1-\delta)\kappa} \Delta^2 |D|_V + \frac{1}{\kappa} \sum_{i=1}^T |x_i| + \Delta^2 |D|_V \end{aligned} \quad (27)$$

$$\leq \left(1 + \frac{\zeta}{(1-\delta)\kappa}\right) \Delta^2 |D|_V + \frac{1}{(1-\varepsilon')\kappa} \left(|\tilde{Z}^{(k)}| - |\tilde{Z}_T^{(k)}|\right) \quad (28)$$

$$\begin{aligned} &\leq \left(1 + \frac{\zeta}{(1-\delta)\kappa}\right) \Delta^2 |D|_V + \frac{1}{(1-\varepsilon')\kappa} |\tilde{Z}^{(k)}| \\ &\leq \left(1 + \frac{\zeta}{(1-\delta)\kappa}\right) \Delta^2 |D|_V + \frac{1+\zeta}{(1-\varepsilon')\kappa} \Delta^2 |D|_V + \frac{(1-\gamma)^k}{(1-\varepsilon')\kappa} |\tilde{Z}|. \end{aligned} \quad (29)$$

In the above, the first inequality (26) follows from (19). Inequality (27) follows from (25) and the κ -product-expansion of the local code. Inequality (28) follows from the fact that each local codeword x_i satisfies the decoding condition with parameter ε' . Finally, inequality (29) follows from (24).

Using the fact that $|\tilde{Z}| \leq 4|e|_R + \Delta^2 |D|_V$, we can rewrite the inequality above in terms of $|e|_R$ and $|D|_V$ following the same steps used in (14) to (15). This gives us

$$|\tilde{e}^{(k)}|_R \leq \left(1 + \frac{\zeta}{(1-\delta)\kappa} + \frac{1+\zeta}{(1-\varepsilon')\kappa} + \frac{(1-\gamma)^k}{(1-\varepsilon')\kappa}\right) \Delta^2 |D|_V + \frac{4(1-\gamma)^k}{(1-\varepsilon')\kappa} |e|_R.$$

Finally, setting $\varepsilon' = 3\delta$, and using the fact that $\kappa \leq 1$ [36], we can relax the inequality above slightly to get $4/((1-\varepsilon')\kappa) \leq 24/(5\kappa)$, as well as

$$\begin{aligned} 1 + \frac{\zeta}{(1-\delta)\kappa} + \frac{1+\zeta}{(1-\varepsilon')\kappa} + \frac{(1-\gamma)^k}{(1-\varepsilon')\kappa} &\leq \frac{1}{\kappa} \left(1 + \frac{2}{\delta} + \frac{2-\delta}{1-3\delta} \cdot \frac{1}{\delta} + \frac{1}{1-3\delta}\right) \\ &\leq \frac{1}{\kappa} \left(1 + \frac{2}{\delta} + \frac{2}{1-3\delta} \cdot \frac{1}{\delta}\right) \\ &\leq \frac{6}{\kappa\delta}, \end{aligned}$$

which holds for $\delta \in (0, 1/18)$. \square

5. Discussion

In our article, we have shown that quantum Tanner codes admit single-shot QEC. Given information from a single round of noisy measurements, the mismatch decomposition decoder [33] is able to output a correction that is close to the data error that occurred. For a variety of noise models, including adversarial or stochastic noise, the single-shot decoder is able to maintain the encoded quantum information for up to an exponential number of correction rounds. The parallelized version of the decoder can be run in constant time while keeping the residual error small. During readout, a logarithmic number of iterations suffices to recover the logical information.

One may also ask about the possibility of single-shot QEC with other decoders for good QLDPC codes. Due to the close connection between the decoders analyzed here and the potential-based decoder for quantum Tanner codes in Ref. [22] (for example, the ability to map between candidate flip sets for both types of decoders), a corollary of the proofs presented here is that the potential-based decoder also has the single-shot property. Likewise, under the mapping of errors shown in Ref. [21], the decoders considered here are applicable to the original good QLDPC codes by Panteleev and Kalachev [17]. Our analysis does not straightforwardly carry over to the code and decoder proposed in Ref. [19], and it remains to be seen whether that construction also admits single-shot decoding.

We further remark that all known constructions of asymptotically good QLDPC codes admit a property called small-set (co)boundary expansion [43], which in the case of quantum Tanner codes, was used to prove the No Low-Energy Trivial States (NLTS) conjecture (see Property 1 of reference [44]). Small-set (co)boundary expansion is also equivalent to the notion of soundness [45], which lower bounds the syndrome weight by some function of reduced error weight. Indeed, soundness is a strong indication of single-shot decodability. Similarly, quantum locally testable codes [46–50] admit analogous soundness properties, although decoders for such codes are unexplored. Note that in our proof, what we needed was a notion of soundness for the mismatch vector (see Lemma 4.14), which is distinct from the usual notion of soundness for the syndrome. The weight of the mismatch is in general incomparable to the weight of the syndrome, so the precise relation between these two definitions of soundness is not well understood.

In conclusion, our results can be viewed as a step toward making general QLDPC codes more practical. While many challenges still remain, there have been promising developments in this direction [41, 51–53]. We believe that quantum LDPC codes, similar to classical LDPC codes, will constitute the gold standard for future quantum telecommunication technologies and form the backbone of resource-efficient quantum fault-tolerant protocols.

Acknowledgments We would like to thank Robert König, Anthony Leverrier and Chris Pattison for inspiring discussions on single-shot QEC and QLDPC codes. S.G. acknowledges funding from the U.S. Department of Energy (DE-AC02-07CH11359), and the National Science Foundation (PHY-1733907). The Institute for Quantum Information and Matter is an NSF Physics Frontiers Center. E.T. acknowledges funding from the Sloan Foundation, DARPA 134371-5113608, and DOD KK2014. L.C. and S.C. gratefully acknowledge support by the European Research Council under grant agreement no. 101001976 (project EQUIPTNT). Z.H. would like to thank NSF grant CCF 1729369 for support.

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52**, R2493 (1995). <https://doi.org/10.1103/PhysRevA.52.R2493>
2. Steane, A.M.: Error correcting codes in quantum theory. *Phys. Rev. Lett.* **77**, 793 (1996). <https://doi.org/10.1103/PhysRevLett.77.793>
3. Gottesman, D.: Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A* **54**, 1862 (1996). <https://doi.org/10.1103/PhysRevA.54.1862>
4. Kitaev, A.: Fault-tolerant quantum computation by Anyons. *Ann. Phys.* **303**, 2 (2003). [https://doi.org/10.1016/S0003-4916\(02\)00018-0](https://doi.org/10.1016/S0003-4916(02)00018-0)
5. Dennis, E., Kitaev, A., Landahl, A., Preskill, J.: Topological quantum memory. *J. Math. Phys.* **43**, 4452 (2002). <https://doi.org/10.1063/1.1499754>
6. Bombin, H., Martin-Delgado, M.A.: Topological quantum distillation. *Phys. Rev. Lett.* **97**, 180501 (2006). <https://doi.org/10.1103/PhysRevLett.97.180501>
7. Bombin, H., Martin-Delgado, M.: Exact topological quantum order in $D = 3$ and beyond: Branyons and brane-net condensates. *Phys. Rev. B* **75**, 075103 (2007). <https://doi.org/10.1103/PhysRevB.75.075103>
8. Kubica, A.: The ABCs of the Color Code: A Study of Topological Quantum Codes as Toy Models for Fault-Tolerant Quantum Computation and Quantum Phases Of Matter, Ph.D. thesis, Caltech (2018). <https://doi.org/10.7907/059V-MG69>
9. Bravyi, S., Terhal, B.: A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes. *New J. Phys.* **11**, 043029 (2009). <https://doi.org/10.1088/1367-2630/11/4/043029>
10. Bravyi, S., Poulin, D., Terhal, B.: Tradeoffs for reliable quantum information storage in 2D systems. *Phys. Rev. Lett.* **104**, 050503 (2010). <https://doi.org/10.1103/PhysRevLett.104.050503>
11. Baspin, N., Krishna, A.: Quantifying nonlocality: how outperforming local quantum codes is expensive. *Phys. Rev. Lett.* **129**, 050505 (2022). <https://doi.org/10.1103/PhysRevLett.129.050505>
12. Breuckmann, N.P., Eberhardt, J.N.: Quantum low-density parity-check codes. *PRX Quantum* **2**, 040101 (2021). <https://doi.org/10.1103/prxquantum.2.040101>
13. Evra, S., Kaufman, T., Zémor, G.: Decodable quantum ldpc codes beyond the \sqrt{n} distance barrier using high-dimensional expanders. *SIAM J. Comput.* FOCS20 (2022). <https://doi.org/10.1137/20M1383689>
14. Hastings, M.B., Haah, J., O'Donnell, R.: Fiber bundle codes: breaking the $n^{1/2}\text{polylog}(n)$ barrier for quantum LDPC codes. In: Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing, pp. 1276–1288 (2021). <https://doi.org/10.1145/3406325.3451005>
15. Panteleev, P., Kalachev, G.: Quantum LDPC codes with almost linear minimum distance. *IEEE Trans. Inf. Theory* **68**, 213 (2022). <https://doi.org/10.1109/tit.2021.3119384>
16. Breuckmann, N.P., Eberhardt, J.N.: Balanced product quantum codes. *IEEE Trans. Inf. Theory* **67**, 6653 (2021). <https://doi.org/10.1109/tit.2021.3097347>
17. Panteleev, P., Kalachev, G.: Asymptotically good quantum and locally testable classical LDPC codes. In: Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing, pp. 375–388 (2022). <https://doi.org/10.1145/3519935.3520017>
18. Leverrier, A., Zémor, G.: Quantum Tanner codes. In: 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS) (IEEE, 2022), pp. 872–883. <https://doi.org/10.1109/FOCS54457.2022.00117>
19. Dinur, I., Hsieh, M.-H., Lin, T.-C., Vidick, T.: Good quantum LDPC codes with linear time decoders (2022). [arXiv:2206.07750](https://arxiv.org/abs/2206.07750)
20. Terhal, B.M.: Quantum error correction for quantum memories. *Rev. Mod. Phys.* **87**, 307 (2015). <https://doi.org/10.1103/RevModPhys.87.307>

21. Leverrier, A., Zémor, G.: Efficient decoding up to a constant fraction of the code length for asymptotically good quantum codes. In: *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)* (SIAM, 2023), pp. 1216–1244. <https://doi.org/10.1137/1.9781611977554.ch45>
22. Gu, S., Pattison, C.A., Tang, E.: An efficient decoder for a linear distance quantum LDPC code. In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, series and number STOC 2023* (publisher Association for Computing Machinery, address New York, NY, USA, 2023), pp. 919–932. <https://doi.org/10.1145/3564246.3585169>
23. Shor, P.: Fault-tolerant quantum computation. In: *Proceedings of 37th Conference on Foundations of Computer Science* (publisher IEEE Comput. Soc. Press, 1996), pp. 56–65. <https://doi.org/10.1109/SFCS.1996.548464>
24. Bombín, H.: Single-shot fault-tolerant quantum error correction. *Phys. Rev. X* **5**, 031043 (2015). <https://doi.org/10.1103/PhysRevX.5.031043>
25. Fawzi, O., Grospellier, A., Leverrier, A.: Constant overhead quantum fault-tolerance with quantum expander codes. In: *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (publisher IEEE, 2018). <https://doi.org/10.1109/focs.2018.00076>
26. Kubica, A., Vasmer, M.: Single-shot quantum error correction with the three-dimensional subsystem toric code. *Nat. Commun.* **13**, 6272 (2022). <https://doi.org/10.1038/s41467-022-33923-4>
27. Bridgeman, J.C., Kubica, A., Vasmer, M.: Lifting topological codes: three-dimensional subsystem codes from two-dimensional Anyon models (2023). [arXiv:2305.06365](https://arxiv.org/abs/2305.06365)
28. Bombín, H.: Gauge color codes: optimal transversal gates and gauge fixing in topological stabilizer codes. *New J. Phys.* **17**, 083002 (2015). <https://doi.org/10.1088/1367-2630/17/8/083002>
29. Campbell, E.T.: A theory of single-shot error correction for adversarial noise. *Quantum Sci. Technol.* **4**, 025006 (2019). <https://doi.org/10.1088/2058-9565/aafc8f>
30. Fujiwara, Y.: Ability of stabilizer quantum error correction to protect itself from its own imperfection. *Phys. Rev. A* **90**, 062304 (2014). <https://doi.org/10.1103/PhysRevA.90.062304>
31. Ashikhmin, A., Lai, C.Y., Brun, T.A.: Quantum Data-Syndrome Codes. *IEEE J. Sel. Areas Commun.* **38**, 449 (2020). <https://doi.org/10.1109/JSAC.2020.2968997>
32. Delfosse, N., Reichardt, B.W., Svore, K.M.: Beyond single-shot fault-tolerant quantum error correction. *IEEE Trans. Inf. Theory* **68**, 287 (2022). <https://doi.org/10.1109/tit.2021.3120685>
33. Leverrier, A., Zémor, G.: Decoding quantum tanner codes. *IEEE Trans. Inform. Theory* (2023). <https://doi.org/10.1109/TIT.2023.3267945>
34. Ben-Sasson, E., Sudan, M.: Robust locally testable codes and products of codes. *Random Struct. Algor.* **28**, 387 (2006). <https://doi.org/10.1002/rsa.20120>
35. Dinur, I., Evra, S., Livne, R., Lubotzky, A., Mozes, S.: Locally testable codes with constant rate, distance, and locality. In: *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing* (2022), pp. 357–374. <https://doi.org/10.1145/3519935.3520024>
36. Kalachev, G., Panteleev, P.: Two-sided robustly testable codes (2022). [arXiv:2206.09973](https://arxiv.org/abs/2206.09973)
37. Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. *Phys. Rev. A* **54**, 1098 (1996). <https://doi.org/10.1103/PhysRevA.54.1098>
38. Steane, A.: Multiple-particle interference and quantum error correction. *Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci.* **452**, 2551 (1996). <https://doi.org/10.1098/rspa.1996.0136>
39. Knill, E.: Quantum computing with realistically noisy devices. *Nature* **434**, 39 (2005). <https://doi.org/10.1038/nature03350>
40. Steane, A.M.: Active stabilization, quantum computation, and quantum state synthesis. *Phys. Rev. Lett.* **78**, 2252 (1997). <https://doi.org/10.1103/physrevlett.78.2252>
41. Gottesman, D.: Fault-tolerant quantum computation with constant overhead. *Quantum Info. Comput.* **14**, 1338–1372 (2014). <https://doi.org/10.5555/2685179.2685184>
42. Grospellier, A.: Constant time decoding of quantum expander codes and application to fault-tolerant quantum computation, Ph.D. thesis, School Sorbonne Université (2019). <https://theses.hal.science/tel-03364419v3>
43. Kaufman, T., Lubotzky, A.: High dimensional expanders and property testing (2013). [arXiv:1312.2367](https://arxiv.org/abs/1312.2367)
44. Anshu, A., Breuckmann, N., Nirkhe, C.: NLTS Hamiltonians from good quantum codes (2022). [arXiv:2206.13228](https://arxiv.org/abs/2206.13228)
45. Quintavalle, A.O., Vasmer, M., Roffe, J., Campbell, E.T.: Single-shot error correction of three-dimensional homological product codes. *PRX Quantum* **2**, 020340 (2021). <https://doi.org/10.1103/PRXQuantum.2.020340>
46. Aharonov, D., Eldar, L.: Quantum locally testable codes. *SIAM J. Comput.* **44**, 1230 (2015). <https://doi.org/10.1137/140975498>
47. Hastings, M. B.: Quantum codes from high-dimensional manifolds. In: *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)* (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017). <https://doi.org/10.4230/LIPIcs.ITCS.2017.25>

48. Leverrier, A., Londe, V., Zémor, G.: Towards local testability for quantum coding. *Quantum* **6**, 661 (2022). <https://doi.org/10.1137/140975498>
49. Cross, A., He, Z., Natarajan, A., Szegedy, M., Zhu, G.: Quantum locally testable code with exotic parameters (2022). [arXiv:2209.11405](https://arxiv.org/abs/2209.11405)
50. Wills, A., Lin, T.-C., Hsieh, M.-H.: General distance balancing for quantum locally testable codes (2023). [arXiv:2305.00689](https://arxiv.org/abs/2305.00689)
51. Cohen, L.Z., Kim, I.H., Bartlett, S.D., Brown, B.J.: Low-overhead fault-tolerant quantum computing using long-range connectivity. *Sci. Adv.* **8**, eabn1717 (2022). <https://doi.org/10.1126/sciadv.abn1717>
52. Tremblay, M.A., Delfosse, N., Beverland, M.E.: Constant-overhead quantum error correction with thin planar connectivity. *Phys. Rev. Lett.* **129**, 050504 (2022). <https://doi.org/10.1103/physrevlett.129.050504>
53. Pattison, C.A., Krishna, A., Preskill, J.: Hierarchical memories: simulating quantum LDPC codes with local gates (2023). [arXiv:2303.04798](https://arxiv.org/abs/2303.04798)

Communicated by E. Smith