Quantum Locally Testable Code with Constant Soundness

Andrew Cross[1], Zhiyang He (Sunny)[1,2], Anand Natarajan[3], Mario Szegedy[4], and Guanyu Zhu[1]

[1]IBM Quantum, IBM T.J. Watson Research Center, Yorktown Heights, NY, United States.
[2]Department of Mathematics, Massachusetts Institute of Technology.
[3]Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology.
[4]Rutgers, The State University of New Jersey, New Brunswick, NJ, United States.

In this paper, we present two constructions of QLTCs with constant soundness. In the first approach, we introduce an operation which we call check product, and show how this operation gives rise to QLTCs of constant soundness, constant rate, and distance scaling with locality. In the second approach, we utilize homological product of codes and prove a special case in which the soundness of component codes is preserved through the homological product. This observation leads us to construct QLTCs of constant soundness, scalable rate and distance, and constant average locality. Our work marks a step towards constructing QLTCs of high soundness and distance, which would give a different construction to the No Low-Energy Trivial States (NLTS) theorem.

1 Introduction

Quantum error correcting codes (QECCs) are essential objects of study in quantum information science due to their broad applications in both practical and theoretical quantum computation. Practically, QECC is the foundation of fault-tolerant quantum computation, which holds the promise to scalable quantum computing. Theoretically, quantum coding theory interacts extensive with quantum complexity theory and information theory, much like how classical coding theory interacts with theoretical computer science. In development of quantum codes for theoretical purposes, we often focus on their asymptotic properties, such as relative rate and distance. In this paper, we study the *testability* of quantum codes and present two novel constructions.

A classical code C is called testable if the syndrome of a proposed code word w reveals more than whether w belongs to the code: the relative weight of the syndrome is also proportional to the relative distance of w from the codespace, and their ratio is called the *soundness* of C. A code is further called *locally testable* if all of its checks involves at most a constant number of bits from w. The theory of code checking, which began with the pioneering work of Blum, Luby, and Rubinfeld [BLR90], has grown into a widely successful area of the theory of computing, affecting PCP theory, combinatorial optimization, combinatorial property testing, program checking and even cryptography.

With the advancement of quantum information science, a quantum notion of locally testable codes (QLTC) was first proposed and studied by Aharonov and Eldar in [AE15].

Zhiyang He (Sunny): szhe@mit.edu

The existence of such codes gained major interest in 2015, when Eldar and Harrow showed in [EH17] that any QLTC with constant soundness, locality and relative distance could be used to construct Hamiltonians with no low-energy trivial states, which would resolve the famous NLTS conjecture of Freedman and Hastings [FH13]. This conjecture is deeply related to the quantum PCP conjecture [AAV13], one of the most important open problems in quantum complexity theory. Further, classical LTCs are important components in the proofs of the classical PCP Theorem [Aro+98; Din07]. Naturally, the connections between QLTCs and the qPCP conjecture became a topic of major importance in the field.

However, constructing QLTCs of high soundness and distance seemed far-fetched at the time, as the best known quantum LDPC codes (QLDPC) had distance $\tilde{\Theta}(\sqrt{N})$ and no bound on soundness. Here we say that a (quantum) code is LDPC if the number of (qu)bits each check involves and the number of checks each (qu)bit is involved in are all bounded by a constant ℓ, which we call the *locality* of the code. The first QLTC with unconditional guarantee on soundness is the hypersphere product code constructed by Hastings [Has17b], which encodes two logical qubits, has soundness $1/\log(N)^2$, locality $\Theta(\log(N))$ and distance $\Theta(\sqrt{N})$. In 2019, Leverrier, Londe and Zémor constructed another family of QLTC called the hemicubic codes [LLZ22], which encodes one qubit and has an improved soundness of $1/\log(N)$, with roughly the same locality and distance. These constructions remain the only known QLTCs, and it was unclear how to improve the soundness to $\Omega(1)$, without reducing the code to have no encoded qubits.

The landscape of QLDPC constructions changed significantly in 2020, following Hastings, Haah and O'Donnell's breakthrough construction of fiber bundle codes [HHO21] that achieved $\tilde{\Omega}(N^{3/5})$ distance. Their ideas were soon generalized to lifted product codes [PK22b] by Panteleev and Kalachev, and balanced product codes [BE21] by Breuckmann and Eberhardt, culminating in the 2021 result of Panteleev and Kalachev that presented the first family of asymptotically good qLPDC codes [PK22a]. It was further shown that embedded in the construction in [PK22a] is a c^3-LTC: asymptotically good classical LDPC code (CLDPC) that is locally testable with constant soundness. Around the same time, Dinur, Evra, Livne, Lubotzky and Mozes announced their construction of a c^3-LTC using left-right Cayley complexes [Din+22]. Building upon their works, two other families of asymptotically good QLDPCs are constructed [LZ22; Din+23]. One such family, namely quantum Tanner codes [LZ22] by Leverrier and Zémor, was utilized by Anshu, Breuckmann and Nirkhe [ABN23] to prove the NLTS conjecture. Following these developments, the problem of constructing QLTCs with good parameters became one of major interest.

In this paper, we take a concrete step towards this open problem by constructing the first few families of QLTCs with constant soundness and varying distance.

1.1 Main Results

We begin by presenting a simple idea that transforms a good classical LDPC locally testable code with constant soundness into a quantum LDPC locally testable code with constant soundness and constant rate. However, it has the striking deficit of having distance 2.

Lemma 1.1. *Given a family of classical LDPC codes with parameters $[n, k, d]$ that are locally testable with soundness ρ, there exists a family of quantum LDPC codes that are locally testable with soundness 2ρ and parameters $[2n, 2k, 2]$.*

It is important to note that the soundness condition is nontrivial, because it concerns the distance of an *arbitrary* state from the codespace, which can be much larger than

the code distance, which is the distance *between* two codewords. For instance, if C is a classical LTC over n bits, then the code $\bar{C} = \{(x, y) \in \mathbb{F}_2^{2n} : x + y \in C\}$ has distance 2 (since it contains (e_i, e_i) for all i), yet if x is far from C, then $(x, 0)$ is far from $\bar{C}$. Our quantum construction is in fact based on this simple classical example. We present this construction in section 3 and discuss how it could be generalized to a new operation which we give the name *check product*. Using this operation and random quantum codes, we obtain the first main result of our paper, a family of QLTCs with constant soundness, constant rate, and distance scaling with locality.

Theorem 1.2. *Suppose we have a family of classical LDPC codes with parameters* $[n_1, k_1 = rn_1, d_1]$ *that are locally testable with soundness* ρ*. Then for any* n_2*, there exists a family of quantum locally testable codes with soundness* 4ρ*, locality bounded by* $O(n_2)$*, and parameters* $[n_1 n_2, (1 + r)n_1 n_2/2, \Theta(\min(d_1, n_2))]$*.*

For instance, taking $n_2 = \log(n_1)$, we obtain QLTCs of constant soundness, constant rate, $\Theta(\log(n))$ distance and $O(\log(n))$ locality.

Our second main result utilizes the distance balancing technique for quantum codes introduced by Hastings [Has17a]. Given a quantum code of distinct X and Z distance, Hastings showed that one could take the hypergraph product of this quantum code with a classical repetition code to obtain a new quantum code with balanced X and Z distance. Notably, this technique balances distance at the expense of soundness – if the original quantum code has soundness ρ and one uses a repetition code of length ℓ in the hypergraph product, the soundness of the resulting quantum code would be ρ/ℓ.

To address this deficiency, we propose a slight yet critical modification to the distance balancing technique such that the soundness of the component quantum code is preserved, at partial expense in locality. We present these results in Section 5, arriving at our second main result.

Theorem 1.3. *Fix integer* $\ell \geq 2$*. Given a family of classical LDPC codes with parameters* $[n, k, d]$ *that are locally testable with* m *checks and soundness* ρ*, there exists a family of quantum locally testable codes of soundness* $\Omega(\rho)$ *and parameters* $[N = n\ell + m(\ell - 1), k, \min(d, 2\ell)]$*, such that a* $1/\ell$ *fraction of* X*-stabilizer generators have weight* $\Theta(\ell)$*, and at most* $1/\ell$ *fraction of the qubits are checked by* $\Theta(\ell)$ Z*-stabilizer generators. All other stabilizer generators are constant weight, and all other qubits are checked by a constant number of stabilizer generators.*

As an example, choosing $\ell = n$, we obtain QLTCs with constant soundness, $\Theta(1/\sqrt{N})$ rate, $\Theta(\sqrt{N})$ distance and $O(\sqrt{N})$ locality. While this code family is no longer LDPC for any ℓ scaling with n, we note that the check weights are non-uniform. In particular, we note that the total check weight of all stabilizer generators is $\Theta(N)$, which means the average locality is $\Theta(1)$. While it is unclear whether average locality is an useful measure, we note the constant average locality here since it is an interesting property that arises naturally from our constructions.

We now present a summary of parameters of known QLTCs and our constructions in the following tables. Since some of these constructions have components whose size can be tweaked (such as the length of the repetition code in Theorem 1.3), in table 1 we present the parameters of the general forms of these constructions, and in table 2 we present the parameters of special cases for direct comparison. We further remark that in terms of worst case bounds, the parameters of Theorem 1.2 are strictly better than that of Theorem 1.3. However, the average locality of Theorem 1.3 are both constant, which is not the case in Theorem 1.2.

Constructions	Ref [Has17b]	Ref [LLZ22]	Theorem 1.2	Theorem 1.3
Physical qubits	$N \approx (2p)^{2n}$	N	$N = n_1 n_2$	$N = nl$
Soundness	$1/(np)$	$\Omega(1/\log(N))$	$\Omega(1)$	$\Omega(1)$
Logical qubits	2	1	$n_1 n_2$	n
Distance	$\Theta(p^{n+1})$	$\Theta(\sqrt{N})$	$\Theta(\min(n_1, n_2))$	$\Theta(\min(n, \ell))$
Locality	$\Theta(2n)$	$O(\log(N))$	$O(n_2)$	$\text{avg} = \Theta(1), \max = \Theta(\ell)$

Table 1: Parameters of the general forms of the constructions.

Constructions	Ref [Has17b]	Ref [LLZ22]	Theorem 1.2	Theorem 1.3
Physical qubits	N	N	N	N
Soundness	$1/\log(N)^2$	$\Omega(1/\log(N))$	$\Omega(1)$	$\Omega(1)$
Logical qubits	2	1	$\Theta(N)$	$\Theta(\sqrt{N})$
Distance	$\Theta(\sqrt{N})$	$\Theta(\sqrt{N})$	$\Theta(\log(N))$	$\Theta(\sqrt{N})$
Locality	$O(\log(N))$	$O(\log(N))$	$O(\log(N))$	$\text{avg} = \Theta(1), \max = \Theta(\sqrt{N})$

Table 2: Parameters of special cases of the constructions.

2 Preliminaries

In this section, we introduce the basic definitions of quantum CSS codes and local testability. Given a vector $v \in \mathbb{F}_2^n$, we let X^v denote the n-qubit Pauli operator $X^{v_1} \otimes X^{v_2} \otimes \cdots X^{v_n}$, where $X^1 = X$ and $X^0 = I$. We define Z^v similarly.

Definition 2.1 (CSS Codes)**.** *Let $C_X = \ker(H_X)$ and $C_Z = \ker(H_Z)$ be linear codes of length n such that $C_X^\perp \subseteq C_Z$ (equivalently, $H_X H_Z^T = 0$). The quantum code $Q = \text{CSS}(H_X, H_Z)$ is the stabilizer code where the X-stabilizers have the form X^c for $c \in C_X^\perp$, and the Z-stabilizers have the form Z^c for $c \in C_Z^\perp$. Its code space is spanned by following states, where for γ ranges over C_Z.*

$$|\gamma + C_X^\perp\rangle := \frac{1}{\sqrt{|C_X^\perp|}} \sum_{c \in C_X^\perp} |\gamma + c\rangle \tag{1}$$

Fact 2.2. *If C_X and C_Z are $[n, k_X, d'_X]$ and $[n, k_Z, d'_Z]$ codes, respectively, then $Q = \text{CSS}(H_X, H_Z)$ has dimension $k = k_X + k_Z - n$ and minimum distance $d = \min(d_X, d_Z) \geq \min(d'_X, d'_Z)$ where $d_X := \min\{|c| : c \in C_X \setminus C_Z^\perp\}$ and $d_Z := \min\{|c| : c \in C_Z \setminus C_X^\perp\}$.*

In this paper, we consider the following definition of local testability, which is the same as in [LLZ22].

Definition 2.3 (Locally testable code)**.** *A linear code $C \in \mathbb{F}_2^n$ is locally testable with soundness ρ and check weight w if it has parity check matrix $H \in \mathbb{F}_2^{m \times n}$ with rows of weight w such that for any $x \in \mathbb{F}_2^n$ we have*

$$\frac{1}{m}|Hx| \geq \frac{\rho}{n} d(x, C) \tag{2}$$

where $d(x, C) := \min_{c \in C} d(x, c)$ and $d(\cdot, \cdot)$ denotes the Hamming distance.

We consider the definition of quantum locally testable codes as in [EH17]. Given a quantum stabilizer code with stabilizer generators $S_1, \cdots, S_m$ all having weight at most w,

we define the projector operators $\Pi_i = \frac{1}{2}(I - S_i)$. For a quantum codespace $Q \leq (\mathbb{C}^2)^{\otimes n}$, we define the *t-fattening* of Q as

$$Q_t = \text{Span}\left\{(A_1 \otimes \cdots \otimes A_n)\,|\psi\rangle : |\psi\rangle \in Q, \#\{i \in [n], A_i \neq I\} \leq t\right\}.$$

This is the space of states that are at distance at most t from the codespace Q. Let Π_{Q_t} be the projector onto Q_t, and let

$$D_Q = \sum_{t \geq 1} t(\Pi_{Q_t} - \Pi_{Q_{t-1}}).$$

Definition 2.4 (Quantum Locally Testable Codes)**.** *A n-qubit quantum code Q with stabilizer generators $S_1, \cdots, S_m$ is locally testable with soundness ρ and check weight w if all its stabilizer generators have weight at most w, and*

$$\frac{1}{m}\sum_{i=1}^{m}\frac{1}{2}(I - S_i) \succeq \frac{\rho}{n} D_Q.$$

Local testability of quantum CSS codes and the testability of their classical component codes are closely related, as shown by [EH17]:

Lemma 2.5 (Fact 17 of [EH17])**.** *A quantum CSS code $\text{CSS}(H_X, H_Z)$ is a QLTC with soundness ρ if $C_X = \ker(H_X), C_Z = \ker(H_Z)$ are CLTCs of soundness ρ. Conversely, if $\text{CSS}(H_X, H_Z)$ is a QLTC with soundness ρ, then C_X, C_Z are CLTCs of soundness at least $\rho/2$.*

With this lemma in place, we now proceed to present our constructions.

3 Check Product of Codes

We start by presenting a simple construction that proves Lemma 1.1. All proofs in section 3 and 4, except for that of Claim 3.1, are included in the appendix.

3.1 A Motivating Example

Suppose $C = \ker(H)$, $H \in \mathbb{F}_2^{m \times n}$ is a classical LTC with soundness ρ, rate r, distance d, and in addition an LDPC with weight w. Define $\bar{C} = \ker(\bar{H})$, where $\bar{H} = [H, H]$. Then $\bar{H}\bar{H}^T = 0$, which means $Q = \text{CSS}(\bar{H}, \bar{H})$ is a valid quantum code. We now prove the following claim, which justifies considering this approach.

Claim 3.1. *$\bar{C} = \ker(\bar{H})$ is a LDPC CLTC with soundness 2ρ, rate $\frac{1+r}{2}$, and distance 2.*

Proof. A way to understand the code $\bar{C}$ is through its Tanner graph. Suppose the Tanner graph of C consists of bit vertices B and check vertices K. Then the Tanner graph of $\bar{C}$ is obtained simply by creating a copy v' of each $v \in B$, where v' and v are connected to the same check bits in K. We can therefore represent each $z \in \bar{C}$ as $z = (x, y)$, where $x, y \in \mathbb{F}_2^n$. We show

$$\bar{C} = \{(x, y) : x, y \in \mathbb{F}_2^n, x + y \in C\}. \tag{3}$$

Fix (x, y) such that $x + y \in C$. Then $\bar{H}(x, y) = Hx + Hy = 0$, which means $(x, y) \in \bar{C}$. Similarly, fix $(x, y) \in \bar{C}$, then we have $H(x + y) = \bar{H}(x, y) = 0$. This proves (3). Now we see that $\bar{C}$ has distance 2, because for any $v \in B$, let $\mathbb{1}_v \in \mathbb{F}_2^n$ be the indicator vector of v (meaning that it has a one at index v, and 0 elsewhere), then $(\mathbb{1}_v, \mathbb{1}_{v'}) \in \bar{C}$. We observe that any weight 1 vector $v \in \mathbb{F}_2^{2n}$ will have non-zero syndrome.

Now note that the check weights of $\bar{C}$ are bounded by $2w$, and each qubit is checked by at most w checks. Therefore $\bar{C}$ is LDPC. The rate of $\bar{C}$ is also easy to compute – the number of linearly independent checks stay at $(1-r)n$, while the number of bits is doubled. So the overall rate is $\frac{1+r}{2}$.

The more interesting part is to show local testability. We want to show $\forall x, y \in \mathbb{F}_2^n$,

$$|\bar{H}(x,y)|/m \geq 2\rho \cdot d((x,y), \bar{C})/2n.$$

We first note that $|\bar{H}(x,y)| = |Hx+Hy| = |H(x+y)|$. Moreover, $d((x,y),\bar{C}) = d(x+y, C)$. By local testability of C, we have

$$|H(x+y)|/m \geq \rho \cdot d((x+y), C)/n,$$

which completes our proof. □

Corollary 3.2. *The quantum code $Q = \mathrm{CSS}(\bar{H}, \bar{H})$ is a QLTC of soundness 2ρ, check-weights bounded by $2w$, rate r, and $d_x = d_z = 2$.*

By choosing C as a known c^3-LTC, such as the left-right Cayley complex code [Din+22], we obtain Lemma 1.1. It is surprising that such a simple construction could already give us quantum codes of constant soundness. Moreover, this example demonstrates that the soundness and distance of a quantum code are not necessarily related. We generalize this construction in the following section.

3.2 General Check Products

We begin by making the following observation: the matrix $\bar{H} = [H, H]$ of the previous section could also be written as $[1,1] \otimes H$, where $H_0 = [1,1]$ is the parity check matrix of the repetition code $C_0 = \{00, 11\}$. More generally, for any two classical codes $C_1 = \ker(H_1), C_2 = \ker(H_2)$, we can define the following *check product* of the two codes:

$$C_1 \star C_2 = \ker(H_1 \otimes H_2).$$

The following facts are well known.

Lemma 3.3. *Let C_1, C_2 be classical codes with parameters $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$. The following hold:*

1. *$C_1 \star C_2 = C_1 \otimes \mathbb{F}_2^{n_2} + \mathbb{F}_2^{n_1} \otimes C_2$. Namely, $C_1 \star C_2$ is the dual tensor code of C_1 and C_2.*
2. *$C_1 \star C_2$ has dimension $n_1 n_2 - (n_1 - k_1)(n_2 - k_2)$.*
3. *$C_1 \star C_2$ has distance $\min(d_1, d_2)$.*

With this definition formalized, we can extend it to the check product of a classical code and a quantum code, as follows.

Definition 3.4 (Check-Product of classical and quantum code)**.** *Given a classical code $C = \ker(H)$ and a quantum CSS code given by $Q = \mathrm{CSS}(H_X, H_Z)$, we define the check-product of Q and C to be the quantum code $Q \star C = \mathrm{CSS}(H_X \otimes H, H_Z \otimes H)$.*

It is straightforward to see that the commutativity condition is satisfied, so this definition is valid. We now address the distance of this quantum code.

Lemma 3.5. *Given a quantum code $Q = \mathrm{CSS}(H_X, H_Z)$, the code $Q \star C$ has distance $\min(d(C), d(C_X), d(C_Z))$. In words, its distance is the minimum of all of its component classical codes' distance.*

The natural question to ask now is — what can we say about the soundness of general check product codes? It is straightforward to see that the check product of a CLTC with a classical code that is not locally testable is also not locally testable, and it is also not clear if the check product of two arbitrary CLTCs remains locally testable. However, as we will show in section 4, the check product of CLTCs with a specific form is indeed locally testable. This enables us to prove Theorem 1.2 by considering the check product of a c^3-LTC with random quantum CSS codes.

4 The Check Product of a CLTC and a QLTC

In this section, we present a construction that proves Theorem 1.2. We once again begin by making a simple observation. Given a classical code $C = \ker(H)$, suppose H is a $m \times n$ matrix with linearly independent rows. We may do Gaussian operations on the rows of H, formally multiplying H from the left by a non-singular matrix G, such that the resulting matrix has the form (up to permuting the columns with a permutation matrix, Π):

$$H' = \left[I_m | R\right] \quad (= GH\Pi) \tag{4}$$

where I_m is the $m \times m$ identity matrix, and R is a $m \times (n-m)$ matrix. Note that $\ker(H') = \Pi^{-1} \ker(H) = \Pi^{-1} C$, and the rows of H' can have arbitrary weight due to the row operations.

Claim 4.1. *The code C with check matrix $H'\Pi^{-1}$ has soundness $\geq 1/r$, where r is the rate of C.*

This claim directly implies the following simple corollary, which we include without proof.

Corollary 4.2. *Any classical linear code of rate r can be turned into a CLTC with soundness $\geq 1/r$ at the cost of having arbitrary locality, while keeping the same rate and distance. Similarly, any quantum CSS codes where both component codes are classical linear codes can be turned into a QLTC with soundness $\geq 1/r$ at the cost of having arbitrary locality, while keeping the same rate and distance.*

We note that the same idea of Claim 4.1 was discussed by Campbell in section 5 of [Cam19], but we only became aware of this correspondence after this paper was finished.

In spite of its simplicity, Claim 4.1 has an important application in our check product construction, as shown in the following lemma.

Lemma 4.3. *Suppose $C = \ker(H) \subset \mathbb{F}_2^n$ is a CLTC with soundness ρ and locality w. Let $C_X = \ker(H_X)$ be a classical code where H_X is a $m_X \times n_X$ matrix of the form $[I_{m_X} \mid h_X]$, such that its locality is bounded by w_X. Then $C_X \star C$ is a CLTC with soundness at least $\rho n_X / m_X$ and locality $w w_X$.*

Combining Lemma 4.3 with Lemma 3.3 and Corollary 4.2, we obtain:

Theorem 4.4. *Given a n-bit classical LTC, $C = \ker(H)$, of soundness ρ, dimension k, distance d and locality w, and a n_q-qubit quantum code $Q = \mathrm{CSS}(H_X, H_Z)$ of dimension k_q, we can reduce H_X, H_Z to have the form in equation (4), and denote the resulting quantum code $\bar{Q} = \mathrm{CSS}(\bar{H}_X, \bar{H}_Z)$. ($Q$ and $\bar{Q}$ as sub-spaces are the same. What makes them different is their sets of X and Z checks.) Then the check product code $\bar{Q} \star C$ has*

1. *local testability with soundness* $\rho \cdot \min(\frac{n_q}{m_X}, \frac{n_q}{m_Z})$ *(in particular, soundness* $\geq \rho$*),*
2. *distance* $\min(d, d(C_X), d(C_Z))$*, where* $C_X = \ker(H_X), C_Z = \ker(H_Z)$*.*
3. *locality bounded by* wn_q*,*
4. *and dimension* $nn_q - (n-k)(n_q - k_q)$*.*

While it is tempting to apply this theorem to a c^3-LTC and a good QLDPC code, we note that the result will have constant distance. Indeed, for a quantum CSS code that is LDPC, we necessarily have $d(C_X), d(C_Z) = O(1)$. For instance, to argue that $d(C_X) = O(1)$, we notice that $C_X \geq C_Z^\perp$, and since $C_Z^\perp$ contains all possible checks for C_Z, it also contains the low-weight ones. In fact, to construct QLTC of scalable distance from Theorem 4.4, we want $d(C_X), d(C_Z)$ to be as large as possible, which in turn implies that the quantum code $Q = \mathrm{CSS}(H_X, H_Z)$ has correspondingly large check weights for all possible checks (i.e. checks in $C_X^\perp$ and $C_Z^\perp$). In the following theorem, we show that random codes satisfy this property.

Theorem 4.5. *Let* $C \leq \mathbb{F}_2^n$*,* $C = \ker(H_C)$ *be a random code with dimension* $\frac{3n}{4}$*. Let* $D \leq C$ *be a random subspace of* C *of dimension* $\frac{n}{4}$*. Let* H_D *be the* $\frac{n}{4} \times n$ *matrix such that its rows span the space* D*, then with high probability* C *and* $D^\perp$ *both have linear distances, and the* CSS *code made from the classical codes* C *and* $D^\perp$ *(here check sets do not influence the statement) has rate* $1/2$*.*

Combining Theorem 4.4 and 4.5, we obtain Theorem 1.2.

5 Gauge Fixing and Distance Balancing

Theorem 1.2 shows a family of QLTCs where the quantum distance scales positively with the check weight. In this section, we prove Theorem 1.3 by tweaking our construction in section 3.1 and applying distance balancing with our modifications.

5.1 Modifying Stabilizer and Logical Operators

We briefly recall our earlier construction. Given a LDPC CLTC $C = \ker H \leq \mathbb{F}_2^n$ of soundness ρ, dimension k and distance d, we define $\bar{C} = \ker(\bar{H})$, where $\bar{H} = [H, H]$, and $Q = \mathrm{CSS}(\bar{H}, \bar{H})$. Let us consider the stabilizers and logical operators of Q. Consider the set of Pauli operators

$$\{X^{(e_i, e_i)}, i \in [n] : e_i \text{ are the standard basis vectors of } \mathbb{F}_2^n\}.$$

We observe that exactly k of these operators are independent X-logical operators, and the other $n-k$ of them can be generated from the previous k operators together with the X-stabilizers. There are another set of X-logical operators, namely

$$\{X^{(v,0)} : v \in C\}.$$

Exactly k logical operators in this set are independent, and they all have linear weight. Together, these $2k$ operators generate the complete set of X-logical operators of Q. Similarly, by replacing Xs with Zs, we found the set of Z-logical operators of Q. We see that $d_x = d_z = 2$.

Now suppose we move all the Z-logical operators of weight 2 into the Z-stabilizer group. Then the remaining k Z-logical operators all have linear weight, which means we

have $d_z = O(n)$. On the other hand, all the high-weight X-logical operators of the form $\{X^{(v,0)} : v \in C\}$ are no longer valid logical operators, as they do not compute with all the Z-stabilizers. Therefore, the set of X-logical operators that remain is precisely

$$\{X^{(v,v)} : v \in \mathbb{F}_2^n\}.$$

A more direct way of writing this new code would be the following. Let $H_Z = [I, I], H_X = [H, H]$. Our new code is precisely $Q' = \mathrm{CSS}(H_X, H_Z)$. The code states of Q' can be explicitly written out as

$$|\psi_v\rangle = \sum_{\substack{(a,b)\in\mathbb{F}_2^n \\ a+b\in\ker H}} |v+a, v+b\rangle\,.$$

This code then has $d_z = O(n), d_x = 2$. It is locally testable with soundness 2ρ, LDPC, and has dimension k.

5.2 Distance Balancing

We can now apply the distance balancing techniques in [Has17a]. Specifically, we consider our code Q' as a chain complex

$$Q = \mathbb{F}_2^n \xrightarrow{H_Z^T=[I,I]^T} \mathbb{F}_2^{2n} \xrightarrow{H_X=[H,H]} \mathbb{F}_2^m,$$

and we take a repetition code of length ℓ, also viewed as a chain complex

$$R = E \xrightarrow{H_\ell} V,$$

where $E = \mathbb{F}_2^{\ell-1}, V = \mathbb{F}_2^\ell$, and H_ℓ is the $\ell \times (\ell-1)$ matrix of the form

$$H_\ell = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots \\ 1 & 1 & 0 & 0 & \cdots \\ 0 & 1 & 1 & 0 & \cdots \\ & & \cdots & & \\ & & \cdots & & \\ 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}. \tag{5}$$

We take the homological product of the two complexes, and the resulting chain complex $Q \times R$ is

$$\begin{array}{ccccc} & & \mathbb{F}_2^{2n}\otimes E & \xrightarrow{H_X\otimes I} & \mathbb{F}_2^m\otimes E \\ & \nearrow^{H_Z^T\otimes I} & & \searrow^{I\otimes H_\ell} & \\ \mathbb{F}_2^n\otimes E & & \oplus & & \oplus \quad \mathbb{F}_2^m\otimes V \\ & \searrow_{I\otimes H_\ell} & & \nearrow_{H_Z^T\otimes I} & \\ & & \mathbb{F}_2^n\otimes V & \xrightarrow{H_X\otimes I} & \mathbb{F}_2^{2n}\otimes V \end{array} \tag{6}$$

$$C_3 \xrightarrow{\partial_3} C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0$$

Now we take the sub-chain complex $C_2 \to C_1 \to C_0$, and view it as a quantum code. From [Has17a], the following holds.

Lemma 5.1. *If the original quantum code Q is a $2n$-qubit LDPC quantum code with dimension k and distance d_x, d_z, then this new code Q' is a $2n\ell + m(\ell-1)$-qubit LDPC quantum code with dimension k and distance $\ell d_x, d_z$.*

We refer the readers to [Has17a], statement 7 and 8 of Lemma 2 for the proofs. Moreover, it was also shown in [Has17a] that the resulting code is locally testable, albeit having a lower soundness.

Lemma 5.2 (Lemma 7 of [Has17a])**.** *If Q is a QLTC with constant soundness, then the code Q' is a QLTC with soundness $\Omega(1/\ell)$.*

Combining these two lemmas, we obtain the following corollary.

Corollary 5.3. *Fix integer $\ell \geq 2$. Given a family of classical LDPC codes with paramaters $[n, k, d]$ that are locally testable with m checks and soundness ρ, there exists a family of quantum LDPC locally testable codes of soundness $\Omega(\rho/\ell)$ and parameters $[N = n\ell + m(\ell-1), k, \min(d, 2\ell)]$.*

We choose not to include direct proofs of these two lemmas in this paper, because in the following section we would present a slight modification to the above construction and prove Lemma 5.4 and 5.5. The proof of Lemma 5.4 would be a slightly modified version of the proof of Lemma 5.1 in [Has17a], and the proof of Lemma 5.5 would follow a similar scheme as the proof of Lemma 5.2 in [Has17a].

5.3 Preserving Soundness

As the primary goal of this paper is to achieve constant soundness, we present a simple modification to the above distance balancing technique that preserves soundness, while sacrificing some locality. We perform column operation on H_ℓ such that it has the following form.

$$H_\ell = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots \\ 0 & 1 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & \cdots \\ & & \cdots & & \\ & & \cdots & & \\ 0 & 0 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 & 1 \end{bmatrix}. \tag{7}$$

Note that as before, H_ℓ^T is a valid parity check matrix for the repetition code. The rest of the construction remains unchanged.

While this modification seems superficial on first glance, it actually follows important geometric insights. To see that, we construct two graphs from the two matrices in equation (5) and (7). We create a vertex for each bit of the repetition code, which corresponds to rows of H_l, and for each column in H_l, we create an edge that connects the two vertices that has entry 1 at that column. Then the previous matrix (5) gives a line segment, while the new matrix (7) gives a star graph. Intuitively, the star graph has better soundness than a line segment since any collection of edges S in the star graph must have at least the same number of vertices on its boundary ∂S, while in a line segment a partial line segment have only two vertices on its boundary. This intuition can be formally formulated as boundary and co-boundary expansion of chain complexes, which are directly related to the soundness of classical and quantum codes derived from such chain complexes.

We now prove the following lemmas regarding the parameters of Q'. We suggest that the readers follow the chain complex in equation (6) when reading the following lemmas and proofs.

Lemma 5.4. *Q' is a $2n\ell + m(\ell-1)$-qubit quantum code with dimension k and distance $\ell d_x, d_z$. A $1/\ell$ fraction of X-stabilizer generators have weight $\Theta(\ell)$, and at most $1/\ell$ fraction of the qubits are checked by $\Theta(\ell)$ Z-checks. All other checks are constant weight, and all other qubits are checked by a constant number of checks.*

Proof. To show the dimension of the new code, we cite the Künneth formula from algebraic topology. Define the rth homology group of a chain complex as $H_r(C) = \ker \partial_r / \operatorname{im} \partial_{r+1}$, then the number of logical qubits of a quantum code is precisely $\dim(H_1(C))$. From the Künneth formula, we have

$$H_1(Q \times R) = (H_1(Q) \otimes H_0(R)) \oplus (H_0(Q) \otimes H_1(R)).$$

Note that $\dim(H_1(Q)) = k, \dim(H_0(R)) = 1$, and $\dim(H_1(R)) = 0$. Therefore $\dim(H_1(Q \times R)) = k$.

For the Z distance of Q', let $c = (x, y) \in C_1$ such that $x \in \mathbb{F}_2^{2n} \otimes V$, $y \in \mathbb{F}_2^m \otimes E$, and $Z^{(x,y)}$ is a Z-logical operator. Let $v_1, \cdots, v_\ell$ be the standard basis vector of $V = \mathbb{F}_2^\ell$, and $e_1, \cdots, e_{\ell-1}$ be the standard basis vector of $E = \mathbb{F}_2^{\ell-1}$. Write $x = \sum_{i=1}^{\ell} x_i \otimes v_i$. We describe a simplification procedure that turns x into the form $\bar{x} \otimes v_1$, such that $|\bar{x}| \leq \sum_{i=1}^{\ell} |x_i|$.

We begin with $x_\ell \otimes v_\ell$. Consider $\partial_2(x_\ell \otimes e_1) = (x_\ell \otimes (v_1 + v_\ell), (H_X x_\ell) \otimes e_1)$, then

$$(\sum_{i=1}^{\ell} x_i \otimes v_i, y) + \partial_2(x_\ell \otimes e_1) = ((x_1 + x_\ell) \otimes v_1 + \sum_{i=2}^{\ell-1} x_i \otimes v_i, y + (H_X x_\ell) \otimes e_1).$$

In the stabilizer formalism, this step correspond to multiplying the logical operator $Z^{(x,y)}$ with the Z-stabilizer $Z^{\partial_2(x_\ell \otimes e_1)}$. Now for all other $i = 2, \cdots, \ell - 1$, we multiply by the Z-stabilizer specified by $\partial_2(x_i \otimes (e_1 + e_i)) = (x_i \otimes (v_1 + v_i), (H_X x_i) \otimes (e_1 + e_i))$ and the final vector in C_1 will have the form

$$\bar{c} = ((\sum_{i=1}^{\ell} x_i) \otimes v_1, \bar{y})$$

for some $\bar{y} \in \mathbb{F}_2^n \otimes E$. Since $Z^{\bar{c}}$ is a valid logical operator, we must have $\partial_1(\bar{c}) = 0$, which means

$$H_X(\sum_{i=1}^{\ell} x_i) \otimes v_1 + (I \otimes H_\ell)\bar{y} = 0.$$

However, note that $v_1 \notin \operatorname{im}(H_\ell)$, which means for the above equation to hold we must have $\bar{y} = 0$ and $\sum_{i=1}^{\ell} x_i \in \ker H_X$. This implies that $Z^{\sum_{i=1}^{\ell} x_i}$ must be a Z-logical operator of Q. Therefore

$$|c| = |x| + |y| \geq |\sum_{i=1}^{\ell} x_i| + |y| \geq d_z(Q),$$

which means $d_z(Q') \geq d_z(Q)$. We also note that $d_z(Q') \leq d_z(Q)$ since if Z^x is a Z-logical operator of Q, then $Z^{x \otimes v_1}$ is a Z-logical operator of Q'. We conclude that $d_z(Q') = d_z(Q)$.

To discuss the X distance, we define cohomologies and cite the Künneth formula again. For a chain complex C, define the rth homology group of a chain complex as $H^r(C) = \ker \partial_{r+1}^T / \operatorname{im} \partial_r^T$, and the Künneth formula in this case states

$$H^1(Q \times R) = (H^1(Q) \otimes H^0(R)) \oplus (H^0(Q) \otimes H^1(R)).$$

Since $H^1(R) = 0$, we have $H^1(Q \times R) = (H^1(Q) \otimes H^0(R))$, which means any X-logical operator (which corresponds to a chain c in $H^1(Q \times R)$) can be written in the form

$$c = x \otimes v + \partial_1^T(u)$$

where $x \in H^1(Q), v \in H^0(R)$, and $u \in \mathbb{F}_2^m \otimes V$. Note that the $H^0(R)$ has dimension 1, which means $v = \sum_{i=1}^{\ell} v_i$. Now suppose $u = \sum_{i=1}^{\ell} u_i \otimes v_i$, and consider the projection of c onto the space $\mathbb{F}_2^{2n} \otimes V$. It has the form

$$c\,|_{\mathbb{F}_2^{2n}\otimes V} = \sum_{i=1}^{\ell} (x + H_X^T u_i) \otimes v_i.$$

Since $\partial_2^T c = 0$, we must have $x + H_X^T u_i \in H^1(Q)$ for all i, which means $|c| \geq \ell d_x(Q)$. This shows $d_x(Q') \geq \ell d_x(Q)$. We also note that $d_x(Q') \leq \ell d_x(Q)$ since if X^x is a X-logical operator of Q, then $X^{x \otimes (\sum_{i=1}^{\ell} v_i)}$ is a X-logical operator of Q'. We conclude that $d_x(Q') = \ell d_x(Q)$.

For the locality of Q', we note that $H_X \otimes I$ and $H_Z^T \otimes I$ are matrices with constant row and column weights. For $I \otimes H_\ell$, exactly $1/\ell$ fraction of its rows have weight ℓ, while the other rows have weight 1, and all its columns have weight 2. Let us enumerate the standard basis vector of $\mathbb{F}_2^{2n}$ as $q_1, \cdots, q_{2n}$, and the standard basis vectors of $\mathbb{F}_2^m$ as $c_1, \cdots, c_m$. Then we have

1. All the Z-stabilizer generators corresponding to basis vectors of $\mathbb{F}_2^n \otimes V$ have constant weight;

2. All the Z-stabilizer generators corresponding to basis vectors of $\mathbb{F}_2^{2n} \otimes E$ have constant weight, because $I \otimes H_\ell^T$ has constant row weight;

3. The qubits corresponding to $\mathbb{F}_2^{2n} \otimes V$ have the form $q_i \otimes v_j$ for $i \in [2n], j \in [\ell]$. Qubits of the form $q_i \otimes v_\ell$ are checked by ℓ Z-stabilizer generators from $\mathbb{F}_2^{2n} \otimes E$. All other qubits have constant degree (in both X and Z stabilizer generator checks).

4. The X-stabilizer generators corresponding to $\mathbb{F}_2^m \otimes V$ has the form $c_i \otimes v_j$ for $i \in [m], j \in [\ell]$. Generators of the form $c_i \otimes v_\ell$ checks ℓ qubits from $\mathbb{F}_2^m \otimes E$. All other X-stabilizer generators have constant weight.

In short summary, at most $1/\ell$ fraction of the qubits are checked by $\Theta(\ell)$ Z-stabilizer generators, and exactly $1/\ell$ fraction of the X-stabilizer generators have $\Theta(\ell)$ weight. All other check weights and qubit degrees are constant. □

Finally, we prove a lower bound on soundness. Recall that our code Q has soundness 2ρ.

Lemma 5.5. *Q' is locally testable with soundness $\min(\rho, 1)/8$ for Z-operators, and soundness $1/3$ for X-operators.*

Proof. Given a Z-operator Z^c where $c \in C_1$, we once again turn c into the following form by multiplying with Z-stabilizers:

$$\bar{c} = (\bar{x} \otimes v_1, \bar{y}).$$

Let $z \in \mathbb{F}_2^{2n}$ be such that $|z| = d(\bar{x}, \ker H_X)$ and $\bar{x} + z \in \ker H_X$. Then we see that

$$\partial_1(\bar{c}) = \partial_1((z \otimes v_1, \bar{y})).$$

Therefore, it suffices for us to show that

$$\frac{|\partial_1(\bar{c})|}{m\ell} \geq \frac{\min(\rho, 1) \cdot (|z| + |\bar{y}|)}{8(2n\ell + m(\ell - 1))}. \tag{8}$$

Write $\bar{y} = \sum_{i=1}^{\ell-1} y_i \otimes e_i$. Then we have

$$\begin{aligned}\partial_1(\bar{c}) &= (H_X\bar{x}) \otimes v_1 + \sum_{i=1}^{\ell-1} y_i \otimes (H_\ell e_i) \\ &= (H_X\bar{x}) \otimes v_1 + \sum_{i=1}^{\ell-1} y_i \otimes v_i + (\sum_{i=1}^{\ell-1} y_i) \otimes v_\ell \\ &= (H_X\bar{x}) \otimes v_1 + y_1 \otimes v_1 + \sum_{i=2}^{\ell-1} y_i \otimes v_i + y_1 \otimes v_\ell + (\sum_{i=2}^{\ell-1} y_i) \otimes v_\ell.\end{aligned}$$

Let $y' = \sum_{i=2}^{\ell-1} y_i$. For two vectors u, v, let $u \cap v$ denote the vector where $(u \cap v)(i) = 1$ if and only if $u(i) = v(i) = 1$. Then we have

$$\begin{aligned}|\partial_1(\bar{c})| &= |H_X\bar{x}| + |y_1| - 2|H_X\bar{x} \cap y_1| + \sum_{i=2}^{\ell-1} |y_i| + |y_1| + |y'| - 2|y' \cap y_1| \\ &= |H_X\bar{x}| - 2|H_X\bar{x} \cap y_1| + |y'| + 2|y_1| - 2|y' \cap y_1| + \sum_{i=2}^{\ell-1} |y_i|.\end{aligned}$$

We first observe that since $|u|, |v| \geq |u \cap v|$ for any u, v,

$$\begin{aligned}|\partial_1(\bar{c})| &\geq \sum_{i=2}^{\ell-1} |y_i| + |y_1| - |y' \cap y_1|, \\ |\partial_1(\bar{c})| &\geq |H_X\bar{x}|.\end{aligned}$$

The first inequality implies $|\partial_1(\bar{c})| \geq |\bar{y}/3|$, for the following reason. If $|y_1| \leq 2|\bar{y}|/3$, then $|\partial_1(\bar{c})| \geq \sum_{i=2}^{\ell-1} |y_i| \geq |\bar{y}|/3$; otherwise if $|y_1| \geq 2|\bar{y}|/3$, then $|y'| < \sum_{i=2}^{\ell-1} |y_i| < |\bar{y}|/3$, which again implies $|\partial_1(\bar{c})| \geq |\bar{y}|/3$.

Therefore, if $|H_X\bar{x}| \leq |\bar{y}|/3$, then by soundness of H_X,

$$\begin{aligned}|\partial_1(\bar{c})| \geq |\bar{y}|/3 \geq \frac{|\bar{y}| + |H_X\bar{x}|}{4} \geq \frac{|\bar{y}|}{4} + \frac{2\rho m d(\bar{x}, \ker H_X)}{4 \cdot 2n}, \\ \frac{|\partial_1(\bar{c})|}{m\ell} \geq \frac{|\bar{y}|}{4m\ell} + \frac{\rho d(\bar{x}, \ker H_X)}{4n\ell}.\end{aligned}$$

Assuming $8(\ell - 1) \geq 4\ell$, we have equation (8). Now if $|H_X\bar{x}| \geq |\bar{y}|/3$, we also have

$$|\partial_1(\bar{c})| \geq |H_X\bar{x}| \geq \frac{|\bar{y}| + |H_X\bar{x}|}{4},$$

and the same calculations as above follows. Therefore, Q' is locally testable with soundness $\rho/8$ for Z-operators.

For X-operators X^c where $c \in C_1$, suppose $c = (x, \sum_{j=1}^{\ell-1} y_j \otimes e_j)$. Note that since $\operatorname{im} H_\ell^T = \mathbb{F}_2^{\ell-1} = E$, we can multiply X^c by X-stabilizers of the form X^r, where

$$r = \partial_1^T(\sum_{j=1}^{\ell-1} y_j \otimes v_j) = (\sum_{j=1}^{\ell-1} H_X^T y_j \otimes v_j, \sum_{j=1}^{\ell-1} y_j \otimes e_j).$$

Then $c + r = (\bar{x}, 0)$ for some $\bar{x}$. In other words, we may assume without loss of generality that all X-operators X^c has the form

$$c = (\sum_{i=1}^{\ell} x_i \otimes v_i, 0).$$

We will show that $|\partial_2^T(c)| \geq (\sum_{i=1}^{\ell} |x_i|)/2$. To prove this, we need to use the fact that our H_Z has the form $[I, I]$. For notation purposes, we let

$$x_i = (x_i^1, x_i^2) = (x_i^1(1), \cdots, x_i^1(n), x_i^2(1), \cdots, x_i^2(n)) \in \mathbb{F}_2^{2n}.$$

Further, without loss of generality, we may assume $x_\ell^1 \cap x_\ell^2 = 0$ because if $x_\ell^1 \cap x_\ell^2 \neq 0$, we can add $((x_\ell^1 \cap x_\ell^2, x_\ell^1 \cap x_\ell^2) \otimes (\sum_{i=1}^{\ell} v_i), 0)$ to c. Note here that $\partial_2^T((x_\ell^1 \cap x_\ell^2, x_\ell^1 \cap x_\ell^2) \otimes (\sum_{i=1}^{\ell} v_i), 0) = 0$. Now we are ready for the proof.

For clarity purposes, in the following equations, we denote "addition mod 2" as $+_m$. We have

$$\begin{aligned}
\partial_2^T(c) &= \sum_{i=1}^{\ell} (x_i^1 +_m x_i^2) \otimes v_i +_m \sum_{i=1}^{\ell} (x_i^1, x_i^2) \otimes (H_\ell^T v_i) \\
&= \sum_{i=1}^{\ell} (x_i^1 +_m x_i^2) \otimes v_i +_m \sum_{i=1}^{\ell-1} (x_i^1, x_i^2) \otimes e_i +_m (x_\ell^1, x_\ell^2) \otimes (\sum_{i=1}^{\ell-1} e_i).
\end{aligned}$$

$$\begin{aligned}
|\partial_2^T(c)| &= \sum_{i=1}^{\ell} |x_i^1 +_m x_i^2| + \sum_{i=1}^{\ell-1} (|x_i^1| + |x_i^2|) + \sum_{i=1}^{\ell-1} (|x_\ell^1| + |x_\ell^2|) - 2 \sum_{i=1}^{\ell-1} (|x_i^1 \cap x_\ell^1| + |x_i^2 \cap x_\ell^2|), \\
&= |x_\ell^1 +_m x_\ell^2| + \sum_{i=1}^{\ell-1} \sum_{j=1}^{n} [(x_i^1(j) +_m x_i^2(j)) + x_i^1(j) + x_i^2(j) + x_\ell^1(j) + x_\ell^2(j) \\
&\qquad - 2(x_i^1 \cap x_\ell^1)(j) - 2(x_i^2 \cap x_\ell^2)(j)].
\end{aligned}$$

We abbreviate the above equation into

$$|\partial_2^T(c)| = |x_\ell^1 +_m x_\ell^2| + \sum_{i=1}^{\ell-1} \sum_{j=1}^{n} c_{i,j}.$$

We now prove $|\partial_2^T(c)| \geq \frac{1}{2} \sum_{i=1}^{\ell} \sum_{j=1}^{n} |x_i^1(j)| + |x_i^2(j)|$ by a counting argument. In particular, for any $i \leq \ell - 1, j \in [n]$, if at least one of $x_i^1(j)$, $x_i^2(j)$ is 1, then regardless of the values of $x_\ell^1(j)$, $x_\ell^2(j)$, we have $c_{i,j} \geq 1$. This can be seen from the following table. Note that by our assumptions, $x_\ell^1(j)$, $x_\ell^2(j)$ cannot both be 1.

$x_i^1(j)$	$x_i^2(j)$	$x_\ell^1(j)$	$x_\ell^1(j)$	$c_{i,j}$
1	0	0	0	2
1	0	1	0	1
1	0	0	1	3
1	1	0	0	2
1	1	1	0	1
1	1	0	1	1
0	1	0	0	2
0	1	1	0	3
0	1	0	1	1

Table 3: Table of possible values of the four variables and $c_{i,j}$.

The only case that remains is $i = l$, and we observe that since $x_\ell^1 \cap x_\ell^2 = 0$, $|x_\ell^1 + x_\ell^2| =$

$|x^1_\ell| + |x^2_\ell|$. Combining this observation with the values in table 3, we see that

$$|\partial_2^T(c)| \geq \frac{1}{2}\sum_{i=1}^{\ell}\sum_{j=1}^{n} |x_i^1(j)| + |x_i^2(j)| = (\sum_{i=1}^{\ell} |x_i|)/2$$

$$\frac{|\partial_2^T(c)|}{n\ell + 2n(\ell-1)} \geq \frac{\sum_{i=1}^{\ell}|x_i|}{2n\ell + 4n(\ell-1)} \geq \frac{1}{3}\frac{\sum_{i=1}^{\ell}|x_i|}{2n\ell + m(\ell-1)}.$$

Therefore, Q' is locally testable with soundness $1/3$ for X-operators. □

Together, Lemma 5.4 and 5.5 gives Theorem 1.3.

Acknowledgements

We thank Ted Yoder for the discussion on gauge fixing of the check product codes.

Z.H and A.N. thank Eugene Tang and the QLDPC reading group at MIT, especially Aram Harrow and Peter Shor for many helpful discussions. Z.H. also thanks Nikolas Breuckmann for many insightful conversations. Part of this work was done while Z.H. was at IBM T.J. Watson Research Center.

A.C. thanks Aram Harrow and the QLDPC reading group at MIT for helpful discussions. A.C and G.Z. are supported by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Co-design Center for Quantum Advantage (C2QA) under contract number DE-SC0012704.

References

[AAV13] Dorit Aharonov, Itai Arad, and Thomas Vidick. "Guest column: the quantum PCP conjecture". In: *SIGACT News* 44.2 (June 2013), pp. 47–79. ISSN: 0163-5700. DOI: 10.1145/2491533.2491549.

[ABN23] Anurag Anshu, Nikolas P. Breuckmann, and Chinmay Nirkhe. "NLTS Hamiltonians from Good Quantum Codes". In: New York, NY, USA: Association for Computing Machinery, 2023. ISBN: 9781450399135. DOI: 10.1145/3564246.3585114.

[AE15] Dorit Aharonov and Lior Eldar. "Quantum Locally Testable Codes". In: *SIAM Journal on Computing* 44.5 (2015), pp. 1230–1262. DOI: 10.1137/140975498.

[Aro+98] Sanjeev Arora et al. "Proof verification and the hardness of approximation problems". In: 45.3 (1998). ISSN: 0004-5411. DOI: 10.1145/278298.278306.

[BE21] Nikolas P. Breuckmann and Jens N. Eberhardt. "Balanced Product Quantum Codes". In: *IEEE Transactions on Information Theory* 67.10 (2021), pp. 6653–6674. DOI: 10.1109/TIT.2021.3097347.

[BLR90] M. Blum, M. Luby, and R. Rubinfeld. "Self-testing/correcting with applications to numerical problems". In: *Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing*. STOC '90. Baltimore, Maryland, USA: Association for Computing Machinery, 1990, pp. 73–83. ISBN: 0897913612. DOI: 10.1145/100216.100225.

[Cam19] Earl T Campbell. "A theory of single-shot error correction for adversarial noise". In: *Quantum Science and Technology* 4.2 (Feb. 2019), p. 025006. DOI: 10.1088/2058-9565/aafc8f.

[Din+22] Irit Dinur et al. “Locally testable codes with constant rate, distance, and locality”. In: *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*. STOC 2022. Rome, Italy: Association for Computing Machinery, 2022, pp. 357–374. ISBN: 9781450392648. DOI: 10.1145/3519935.3520024.

[Din+23] Irit Dinur et al. “Good Quantum LDPC Codes with Linear Time Decoders”. In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. STOC 2023. Orlando, FL, USA: Association for Computing Machinery, 2023, pp. 905–918. ISBN: 9781450399135. DOI: 10.1145/3564246.3585101.

[Din07] Irit Dinur. “The PCP theorem by gap amplification”. In: *J. ACM* 54.3 (June 2007), 12–es. ISSN: 0004-5411. DOI: 10.1145/1236457.1236459.

[EH17] L. Eldar and A. W. Harrow. “Local Hamiltonians Whose Ground States Are Hard to Approximate”. In: *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*. Los Alamitos, CA, USA: IEEE Computer Society, Oct. 2017, pp. 427–438. DOI: 10.1109/FOCS.2017.46.

[FH13] Michael Freedman and Matthew Hastings. “Quantum Systems on Non-k-Hyperfinite Complexes: A Generalization of Classical Statistical Mechanics on Expander Graphs”. In: *Quantum Information and Computation* 14 (Jan. 2013). DOI: 10.26421/QIC14.1-2-9.

[Has17a] Mathew B. Hastings. “Weight reduction for quantum codes”. In: *Quant. Inf. Comput.* 17.15-16 (2017), pp. 1307–1334. DOI: 10.26421/QIC17.15-16-4.

[Has17b] Matthew B. Hastings. “Quantum Codes from High-Dimensional Manifolds”. In: *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*. Ed. by Christos H. Papadimitriou. Vol. 67. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2017, 25:1–25:26. ISBN: 978-3-95977-029-3. DOI: 10.4230/LIPIcs.ITCS.2017.25.

[HHO21] Matthew B. Hastings, Jeongwan Haah, and Ryan O’Donnell. “Fiber bundle codes: breaking the $n^{1/2}$ polylog(n) barrier for Quantum LDPC codes”. In: *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. STOC 2021. Virtual, Italy: Association for Computing Machinery, 2021, pp. 1276–1288. ISBN: 9781450380539. DOI: 10.1145/3406325.3451005.

[LLZ22] Anthony Leverrier, Vivien Londe, and Gilles Zémor. “Towards local testability for quantum coding”. In: *Quantum* 6 (Feb. 2022), p. 661. ISSN: 2521-327X. DOI: 10.22331/q-2022-02-24-661.

[LZ22] A. Leverrier and G. Zemor. “Quantum Tanner codes”. In: *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*. Los Alamitos, CA, USA: IEEE Computer Society, Nov. 2022, pp. 872–883. DOI: 10.1109/FOCS54457.2022.00117.

[PK22a] Pavel Panteleev and Gleb Kalachev. “Asymptotically good Quantum and locally testable classical LDPC codes”. In: *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*. STOC 2022. Rome, Italy: Association for Computing Machinery, 2022, pp. 375–388. ISBN: 9781450392648. DOI: 10.1145/3519935.3520017.

[PK22b] Pavel Panteleev and Gleb Kalachev. “Quantum LDPC Codes With Almost Linear Minimum Distance”. In: *IEEE Transactions on Information Theory* 68.1 (2022), pp. 213–229. DOI: 10.1109/TIT.2021.3119384.

Appendix

Omitted Proofs in Section 3

Corollary 3.2. *The quantum code $Q = \mathrm{CSS}(\bar{H}, \bar{H})$ is a QLTC of soundness 2ρ, check-weights bounded by $2w$, rate r, and $d_x = d_z = 2$.*

Proof. We note that the soundness follows from Lemma 2.5, and the LDPC property follows from the fact that both of its component codes are LDPC. The rate can be calculated from the number of checks: there are $2n$ qubits and $2(1-r)n$ checks, which gives rate r.

The quantum distance can be seen from the following fact. Consider $Z^{(\mathbb{1}_v, \mathbb{1}_v)}$ and $X^{(\mathbb{1}_v, \mathbb{1}_v)}$ for $v \in B$. If $Z^{(\mathbb{1}_v, \mathbb{1}_v)}$ is in the stabilizer group for all $v \in B$, then H must be a matrix of rank n. Equivalently, H can be transformed into the $n \times n$ identity matrix I by row operations, which means the original code C is trivial. Therefore there exists some v such that $Z^{(\mathbb{1}_v, \mathbb{1}_v)}$ and $X^{(\mathbb{1}_v, \mathbb{1}_v)}$ are both logical operators. □

Lemma 3.3. *Let C_1, C_2 be classical codes with parameters $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$. The following hold:*

1. *$C_1 \star C_2 = C_1 \otimes \mathbb{F}_2^{n_2} + \mathbb{F}_2^{n_1} \otimes C_2$. Namely, $C_1 \star C_2$ is the dual tensor code of C_1 and C_2.*
2. *$C_1 \star C_2$ has dimension $n_1 n_2 - (n_1 - k_1)(n_2 - k_2)$.*
3. *$C_1 \star C_2$ has distance $\min(d_1, d_2)$.*

Proof. To prove the first claim, we see that the row space of $H_1 \otimes H_2$ is exactly $C_1^\perp \otimes C_2^\perp$. Therefore, the dual of its row space is exactly the dual tensor code $C_1 \otimes \mathbb{F}_2^{n_2} + \mathbb{F}_2^{n_1} \otimes C_2$. The rate of the new code is also easy to compute, as the number of linearly independent checks is simply $(n_1 - k_1)(n_2 - k_2)$.

To argue about the distance of $C_1 \star C_2$ (item *2.*) is not hard either. Let $0 \neq x \in C_1 \star C_2$, and imagine x as an $n_1 \times n_2$ matrix M over $\mathbb{F}_2$. We will have shown that $|x| \geq \min(d_1 d_2)$ if we find any $v \in \mathbb{F}_2^{n_1}$ or $w \in \mathbb{F}_2^{n_2}$ such that $|v^T M| \geq d_2$ or $|Mw| \geq d_1$ ($|.|$ is the Hamming weight).

Let us now run v through all checks of C_1 (i.e. rows of H_1), and w through all checks of C_2 (i.e. rows of H_2). There are two possibilities.

1. Either all of the above matrix-vector products give the zero vector. In that case x is not only in $C_1 \star C_2$, but also in the smaller $C_1 \otimes C_2$, and therefore its distance from the zero vector is at least $d_1 d_2 \geq \min(d_1, d_2)$.
2. One of the above matrix-vector products is non-zero. Notice that for any v that is a C_1-check (any w that is a a C_2-check), we have $v^T M \in C_2$ ($Mw \in C_1$), by definition, since M represents an $x \in C_1 \star C_2$, and now we get a $\min(d_1 d_2)$ bound for that reason.

This proves that the distance is at least $\min(d_1, d_2)$. To prove equality, take $x \in C_2$ and $y \in C_1$ with minimum distances (d_2 and d_1, respectively) from zero. Then $\underbrace{(1, 0, \cdots, 0)}_{n_1} \otimes x$ and $y \otimes \underbrace{(1, 0, \cdots, 0)}_{n_2}$ are both valid codewords of $C_1 \star C_2 = C_1 \otimes \mathbb{F}_2^{n_2} + \mathbb{F}_2^{n_1} \otimes C_2$. This concludes the proof of our claims. □

Lemma 3.5. *Given a quantum code $Q = \mathrm{CSS}(H_X, H_Z)$, the code $Q \star C$ has distance $\min(d(C), d(C_X), d(C_Z))$. In words, its distance is the minimum of all of its component classical codes' distance.*

Proof. Suppose Q has n_q physical qubits. We have from Lemma 3.3

$$\begin{aligned} d_x(Q \star C) &= \min\{|w| : w \in C_X \star C \setminus (C_Z \star C)^\perp\} \\ &= \min\{|w| : w \in C_X \otimes \mathbb{F}_2^n + \mathbb{F}_2^{n_q} \otimes C \setminus C_Z^\perp \otimes C^\perp\}. \end{aligned}$$

Since $C^\perp \neq \mathbb{F}_2^n$, we can find $x \in C_X, |x| = d(C_X)$, and a standard basis vector $e_i \in \mathbb{F}_2^n \setminus C^\perp$ such that $x \otimes e_i \in C_X \otimes \mathbb{F}_2^n \setminus C_Z^\perp \otimes C^\perp$. Similarly, since $C_Z^\perp \neq \mathbb{F}_2^{n_q}$, we can find $y \in C, |y| = d(C)$, and a standard basis vector $e_j \in \mathbb{F}_2^{n_q} \setminus C_Z^\perp$ such that $e_j \otimes y \in \mathbb{F}_2^{n_q} \otimes C \setminus C_Z^\perp \otimes C^\perp$. This shows that $d_x(Q \star C) \leq \min(d(C_X), d(C))$. On the other hand, we note that from Fact 3 of Lemma 3.3,

$$\begin{aligned} d_x(Q \star C) &= \min\{|w| : w \in C_X \star C \setminus (C_Z \star C)^\perp\} \\ &\geq \min\{|w| : w \in C_X \star C\} = \min(d(C_X), d(C)). \end{aligned}$$

Thus $d_x(Q \star C) = \min(d(C_X), d(C))$. Similarly, we have $d_z(Q \star C) = \min(d(C_Z), d(C))$. This lemma then follows. □

Omitted Proofs in Section 4

Claim 4.1. *The code C with check matrix $H'\Pi^{-1}$ has soundness $\geq 1/r$, where r is the rate of C.*

Proof. Without loss of generality we assume $\Pi = I_n$, since Π simply permute the bits of the code without changing any of its parameters. Given $x \in \mathbb{F}_2^n$, it suffices for us to show that $\frac{n}{m} d(x, C)/n \leq |H'x|/m$. Denote the rows of H' as $r_1, \cdots, r_m$, then $|H'x| = \sum_{i=1}^m r_i \cdot x$. Now suppose $r_1 \cdot x = 1$, then let $x' = x + e_1$, where e_1 is the standard basis vector, and we see that $|H'x'| = |H'x| - 1$. We may now repeat this procedure for all rows that give syndrome-bit 1 with respect to x, until in $|H'x|$ steps we arrive at a code word. Finally we notice that $n/m = 1/r$. More explicitly, let $S \subset [m]$ be the indices of rows violated by x. Define

$$y = x + \sum_{i \in S} e_i.$$

Then $|H'y| = 0$, since $H'x = H'(\sum_{i \in S} e_i)$. Thus, $d(x, C) \leq d(x, y) = |S| = |H'x|$, which proves our claim. □

Lemma 4.3. *Suppose $C = \ker(H) \subset \mathbb{F}_2^n$ is a CLTC with soundness ρ and locality w. Let $C_X = \ker(H_X)$ be a classical code where H_X is a $m_X \times n_X$ matrix of the form $[I_{m_X} \mid h_X]$, such that its locality is bounded by w_X. Then $C_X \star C$ is a CLTC with soundness at least $\rho n_X/m_X$ and locality ww_X.*

Proof. The check matrix of $C_X \star C$ is $H_X \otimes H$, and since the latter has row and column weight bounded by ww_X, the bound on the locality of $C_X \star C$ follows. The more interesting part is to show that $C_X \star C$ has soundness parameter at least ρ.

By definition, every check of $C_X \star C$ is a tensor product of a check for C_X and a check for C. The i^{th} check of C_X contains the i^{th} bit of the checked word and some other bits that have index beyond m_X, due to the $[I_{m_X} \mid h_X]$ structure of H_X. Given a word $x \in \mathbb{F}_2^{n_x \times n}$ to be checked, we write it as $x = (x_1, \cdots, x_{n_X})$ where each $x_i \in \mathbb{F}_2^n$. Fix

$1 \le i \le m_X$, and consider the collection Γ_i of all those checks of $C_X \star C$ that have the i^{th} check of C_X as their first component. Then $|\Gamma_i|$ is exactly the number t of all checks for C (hence t is independent of i). Define

$$y_i = \sum_{j \in\, i^{\text{th}} \text{ check of } C_X} x_j \qquad (\in \mathbb{F}_2^n)$$

(in particular, $j = i$ is one of the participant indices on the r.h.s.). Let $\Gamma_i' \subseteq \Gamma_i$ be the checks in Γ_i that x violates. These violated checks, due to the tensor product construction, correspond to those checks of C that y_i violates. Therefore, due to the soundness parameter ρ of C there exists a $y_i' \in C$ such that $\rho|y_i - y_i'| \le \frac{n}{t}|\Gamma_i'|$. Adding now $y_i' - y_i$ to x_i, while keeping all x_js for $j \neq i$ the same, we have achieved that all checks in Γ_i go through, and also we did not affect those checks that are not in Γ_i, since their H_X component does not contain the i^{th} bit of C_X. After having the above done for all $1 \le i \le m_X$ we get a word x' that passes all tests, therefore belongs to $C_X \star C$. Further,

$$\rho|x' - x| \;\le\; \sum_{i=1}^{m_X} \frac{n}{t}\,|\Gamma_i'| \;=\; \frac{n}{t} \sum_{i=1}^{m_X} |\Gamma_i'| \;=\; \frac{n}{t} s \tag{9}$$

where s is the number of checks violated by x. Relating s to $m_X t$, the number of all checks, we get from (9) that

$$\underbrace{\frac{s}{m_X t}}_{\text{probability of failed check}} \;\ge\; \frac{|x' - x|}{m_X \cdot n} \cdot \rho \;=\; \underbrace{\frac{|x' - x|}{n_X \cdot n}}_{\substack{\text{relative distance of} \\ \text{of } x \text{ from a code word}}} \cdot \underbrace{\frac{\rho\, n_X}{m_X}}_{\text{soundness}}$$

as needed. □

Theorem 4.4. *Given a n-bit classical LTC, $C = \ker(H)$, of soundness ρ, dimension k, distance d and locality w, and a n_q-qubit quantum code $Q = \mathrm{CSS}(H_X, H_Z)$ of dimension k_q, we can reduce H_X, H_Z to have the form in equation (4), and denote the resulting quantum code $\bar{Q} = \mathrm{CSS}(\bar{H}_X, \bar{H}_Z)$. ($Q$ and $\bar{Q}$ as sub-spaces are the same. What makes them different is their sets of X and Z checks.) Then the check product code $\bar{Q} \star C$ has*

1. *local testability with soundness $\rho \cdot \min(\frac{n_q}{m_X}, \frac{n_q}{m_Z})$ (in particular, soundness $\ge \rho$),*
2. *distance $\min(d, d(C_X), d(C_Z))$, where $C_X = \ker(H_X), C_Z = \ker(H_Z)$.*
3. *locality bounded by wn_q,*
4. *and dimension $nn_q - (n-k)(n_q - k_q)$.*

Proof. Local testability with soundness $\rho \cdot \min(\frac{n_q}{m_X}, \frac{n_q}{m_Z})$ is proved by Lemma 4.3, by applying it to both $C_X \star C$ and $C_Z \star C$ (where the check sets associated with C_X and C_Z are $\bar{H}_X$ and $\bar{H}_Z$)) and taking the minimum. That the minimum of the respective soundness of the two classical parts is a lower bound on the soundness of the CSS code is proven in Lemma 2.5 (originally Fact 17 in [EH17]). The locality bounds also follow from Lemma 4.3, where we use the trivial n_q upper bound on the row and column weights of $\bar{H}_X$ and $\bar{H}_Z$). Since Q and $\bar{Q}$ are the same code, they have the same rate and distance, and therefore the distance of $\bar{Q} \star C$ is easily given by Lemma 3.3. The dimension can be calculated as follows: the number of stabilizer generators in $\bar{Q}$ is $n_q - k_q$, and therefore the number of stabilizer generators in $\bar{Q} \star C$ is $(n-k)(n_q - k_q)$. □

Theorem 4.5. *Let $C \leq \mathbb{F}_2^n$, $C = \ker(H_C)$ be a random code with dimension $\frac{3n}{4}$. Let $D \leq C$ be a random subspace of C of dimension $\frac{n}{4}$. Let H_D be the $\frac{n}{4} \times n$ matrix such that its rows span the space D, then with high probability C and $D^\perp$ both have linear distances, and the* CSS *code made from the classical codes C and $D^\perp$ (here check sets do not influence the statement) has rate* $1/2$.

Proof. First recall that in our construction $C \leq \mathbb{F}_2^n$ is a random code with dimension $\frac{3n}{4}$ and $D \leq C$ is a random subspace of C of dimension $\frac{n}{4}$. Due to the above parameters the quantum CSS code made from classical codes C and $D^\perp$ encodes $\frac{3}{4}n - \frac{1}{2}n$ qubits, therefore it has rate $1/2$.

Next we will show that both C and $D^\perp$ have linear distances with high probability. Let δ be such that $H(\delta) = 0.25$, where $H(\delta) = \delta \log_2 \frac{1}{\delta} + (1-\delta)\log_2 \frac{1}{1-\delta}$ is the entropy function. We show that with probability very close to one both C and $D^\perp$ have minimum distance at least $\delta' n$, where $\delta' \to \delta$ (from below) as n tends to infinity.

That C has the above distance is simply the Gilbert-Varshamov (GV) bound for linear codes. This says that if we want to achieve relative distance δ', then a random linear code with rate $1 - H(\delta') - \epsilon$ will achieve that, where ϵ is arbitrary small as n grows.

The proof of the GV bound is simple, and the code construction that leads to it, telling the proof with our parameters for simplicity, is the following: We select a random parity check matrix, M with $\frac{n}{4}$ rows and n colums. The minimum distance of C is the minimum number of columns of M that sum to zero. To argue for relative distance δ' slightly below δ, we use the well-known fact, that

$$\log_2 \binom{n}{\delta' n} = H(\delta)\,(n - \omega(\log n)) \qquad \text{when } \delta' \to \delta \text{ appropriately, as } n \to \infty$$

The number of ways to select $1 \leq k \leq \delta' n$ columns is then $\leq \delta' n \cdot 2^{(H(\delta)\,(n-\omega(\log n))} = o\left(2^{H(\delta)n}\right)$, for large n. The probability that any select k columns (no restriction on k) of a random matrix with $\frac{1}{4}n$ rows add up to zero is $2^{-\frac{1}{4}n}$, and we can simply finish the proof by the union bound, since $o\left(2^{H(\delta)n}\right) \cdot 2^{-\frac{1}{4}n} = o(1)$.

Let us now estimate the distance of $D^\perp$ in a similar way. The dimension of the linear space $D^\perp$ is $n - \dim D = \frac{3n}{4}$, but at this time we have the restriction that D must be a subspace of C. The way to create a random subspace of C of dimension $\frac{n}{4}$ is to add $\frac{n}{2}$ extra rows to the parity check matrix of C. Therefore, to continue the construction, we select an additional $\frac{1}{2}n$ rows. The added new rows constitute a matrix N of dimensions $\frac{1}{2}n \times n$. When we concatenate N and M (put them together into an $n \times \frac{3}{4}n$ matrix, we get a matrix $W = \left(\frac{N}{M}\right)$. Here N and M are random, and the rows of W generate $D^\perp$. We calculate the probability that the rows of W generate any vector of weight less than $\delta' n$, where δ' is appropriately, but only slightly less, than δ.

The number of vectors with weight $\delta' n$ is upper bounded by $o\left(2^{H(\delta)n}\right)$ similarly to our previous calculation. The probability that any fixed select rows of W (over the randomness of W) add up to a any particular vector w is 2^{-n}. The number of ways we can select a subset of rows of w is $2^{0.75n}$. Thus:

$$\begin{aligned} &\text{Prob}_W(\text{there are rows of } W \text{ that add up to some } w \text{ with weight} \leq \delta n) \\ &\qquad \leq\ o\left(2^{H(\delta)n}\right) \cdot 2^{0.75n} \cdot 2^{-n} = o(1) \end{aligned}$$

Thus, the probability that the minimum distance of $D^{\perp}$ is at least δn is arbitrarily close to 1 when n is sufficiently large.

By the union bound (at this time applied only on two terms), the probability that the minimum relative distance of either of C or $D^{\perp}$ fails to be at least δ', for a randomly chosen $W = \binom{N}{M}$ becomes arbitrarily small, as n goes to infinity. □