Abstract

In this paper, we present a few simple constructions of quantum locally testable codes that achieve interesting parameters which were previously unknown. We introduce an operation which we give the name check product, and show how this operation gives rise to quantum locally testable codes of constant soundness and linear rate, with varying distance and locality.

1 Introduction

A classical code $C$ is 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 with locality $\ell$ if all of its checks involves at most $\ell$ bits from $w$. The theory of code checking, which began with the pioneering work of Blum, Luby, and Rubinfeld [3], 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 was first proposed and studied by Aharonov and Eldar in [1]. The existence of such codes gained major interest in 2015, when Eldar and Harrow showed in [8] that any quantum locally testable code (henceforth abbreviated as 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 [9].

However, constructing such qLTCs seemed far-fetched at the time, as the best known qLDPC codes 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 (henceforth referred to as check weights), and the number of checks each (qu)bit is involved in (henceforth referred to as (qu)bit degrees), are all bounded by a constant. The first qLTC with unconditional guarantee on soundness is the hypersphere product code constructed by Hastings [11], 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 \([13]\), 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 constant, without reducing the code to have no encoded qubits.

The landscape of qLDPC constructions changed dramatically in 2020, following Hastings, Haah and O'Donnell’s breakthrough construction of fiber bundle codes \([12]\) that achieved \(\tilde{\Omega}(N^{3/5})\) distance. Their ideas were soon generalized to lifted product codes \([16]\) by Panteleev and Kalachev, and balanced product codes \([4]\) by Breuckmann and Eberhardt, culminating in the 2021 result of Panteleev and Kalachev that resolved the problem by constructing the first family of good qLPDC codes using the lifted product \([17]\). Further, they showed that embedded in their construction is a cLDPC code that is locally testable with constant soundness and locality. Independently, at roughly the same time, Dinur, Evra, Livne, Lubotzky and Mozes announced their construction of the left-right Cayley complex codes, which are locally testable with constant soundness, locality, rate and relative distance as well. Both of these groundbreaking constructions resolved the decades-long conjecture of the existence of \(c^3\)-LTCs. Moreover, they together revealed the potential connection between classical local testability and quantum distance. Following their work, a few other good qLDPC codes \([14, 7]\) and \(c^3\)-cLTCs \([15, 14]\) were constructed, and the problem of constructing qLTCs with good parameters became one of major interest to the field. It is worth noting that very recently, Anshu, Breuckmann and Nirkhe \([2]\) succeeded in proving the NLTS conjecture without constructing a qLTC, by a careful analysis of the code Hamiltonian from Leverrier and Zémor’s quantum Tanner codes \([14]\). Nevertheless, constructing a qLTC remains an open problem of great interest and seems closely connected to the quantum PCP conjecture, a major area of research in quantum complexity theory.

In this paper, we take a small step towards this open problem by presenting a few simple constructions of qLTCs that achieve interesting parameters which were previously unknown. Unlike previous works on qLTC, which often had a geometric flavor, our constructions are more algebraic and are based on products of codes. (We are inspired by the move from geometric to algebraic and combinatorial ideas that arguably underlies all the recent breakthroughs in qLDPC and cLTC codes.) 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 linear rate. However, it has the striking deficit of having distance 2.

**Theorem 1.1.** Given a family of classical LDPC codes with parameters \([n, k, d]\) that are locally testable with soundness \(\rho\), there exists a family of quantum LDPC codes that are locally testable with soundness \(2\rho\) 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 \(C' = \{(x, y) \in \mathbb{F}_2^n : x + y \in C\}\) 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 \(C'\). 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 construct

\[2\]
a family of qLTCs with constant soundness, linear rate, and distance scaling with check weights.

**Theorem 1.2.** Assume we have a family of classical LDPC codes with parameters \([n_1, k_1 = rn_1, d_1]\) that are locally testable with soundness \(\rho\). Then for any \(n_2\), there exists a family of quantum locally testable codes with soundness \(4\rho\), parameters \([n_1n_2, (1 + r)n_1n_2/2, \Theta(\min(d_1, n_2))]\), and check weights, qubit degree bounded by \(O(n_2)\).

In particular, we obtain qLTCs of constant soundness, linear rate, \(\Theta(\log(n))\) distance and \(O(\log(n))\) check weights and qubit degrees. We further present how to modify the construction of theorem 1.1 to apply the distance balancing techniques introduced by Hastings [10] in Section 5. This leads to the following 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 \(\rho\), there exists a family of quantum LDPC locally testable codes of soundness \(\Omega(\rho/\ell)\) and parameters \([N = n\ell + m(\ell - 1), k, \min(d, 2\ell)]\).

Choosing \(\ell = \log(n)\), we obtain qLDPCs that is locally testable with \(\Omega(1/\log(N))\) soundness, \(\Theta(1/\log(N))\) rate and \(\Theta(\log(N))\) distance. Notably, this distance balancing method increases distance at the expense of soundness. In section 5.2, we present a slight modification to the method so that soundness is preserved, at the cost of a mild increase in the check weights. This is summarized in the following theorem.

**Theorem 1.4.** 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 \(\rho\), 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.

Choosing \(\ell = \log(n)\), we obtain qLTCs with constant soundness, \(\Theta(1/\log(N))\) rate, \(\Theta(\log(N))\) distance and \(O(\log(n))\) check weights and qubit degrees. While this code family is no longer LDPC for any \(\ell\) scaling with \(n\), we note that the check weights and qubit degrees are non-uniform. In particular, we note that the total check weight of all stabilizer generators and the total qubit degree are both \(\Theta(N)\), which means the average check weight and qubit degree are both \(\Theta(1)\).

We further remark that one of the primary goals in [10] was to reduce stabilizer checks of large constant weights to ones of small constant weights. As we are only concerned with the asymptotic behavior of the parameters in this paper, the only distance balancing technique we need from [10] is to consider the homological product of a quantum code with unbalanced distances and a classical repetition code of length \(\ell\). It is unsurprising that without further properties, codes resulting from hypergraph product have diminished soundness. In the proof of theorem 1.4, however, we give a new analysis of the soundness for a special case of the hypergraph product, that shows that constant soundness of the constituent codes is preserved. We hope that our techniques could be extended to showing that other product constructions preserve soundness.

We now present a summary of parameters of known qLTCs and our constructions in the following tables. Since some of these constructions have tweakable components, 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 of these constructions for direct comparison. Note that for the hypersphere product code [11] and the hemicubic code [13], the parameters we record here are exact only in an asymptotic sense. We further remark that in terms of worst case bounds, the parameters of theorem 1.4 are strictly worse than that of theorem 1.2. However, the average check weight and qubit degree of theorem 1.4 are both constant, which is not the case in theorem 1.2.

| Constructions | Hypersphere product code | Hemicubic code | Theorem 1.1 |
|---------------|-------------------------|---------------|-------------|
| Variables     | $n, p$                  | $N$           | $N$         |
| Soundness     | $1/(np)$                | $\Omega(1/\log(N))$ | $\Omega(1)$ |
| Physical qubits | $(2p + o(1))^{2n}$ | $N$           | $N$         |
| Logical qubits | $2$                     | $1$           | $\Theta(N)$ |
| Distance      | $\Theta((p + 1)^{n+1})$ | $\Theta(\sqrt{N})$ | $2$        |
| Check weight/qubit degree | $\Theta(2n)$ | $O(\log(N))$ | $\Theta(1)$ |

| Constructions | Theorem 1.2 | Theorem 1.3 | Theorem 1.4 |
|---------------|-------------|-------------|-------------|
| Variables     | $n_1, n_2$  | $n, \ell$  | $n, \ell$  |
| Soundness     | $\Omega(1)$ | $\Omega(1/\ell)$ | $\Omega(1)$ |
| Physical qubits | $n_1 n_2$ | $O(n \ell)$ | $O(n \ell)$ |
| Logical qubits | $\Theta(n_1 n_2)$ | $\Theta(n)$ | $\Theta(n)$ |
| Distance      | $\Theta(\min(n_1, n_2))$ | $\Theta(\min(n, \ell))$ | $\Theta(\min(n, \ell))$ |
| Check weight/qubit degree | $O(n_2)$ | $\Theta(1)$ | $(\text{avg, max}) = (\Theta(1), \Theta(\ell))$ |

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

| Constructions | Hypersphere product code | Hemicubic code | Theorem 1.1 |
|---------------|-------------------------|---------------|-------------|
| Soundness     | $1/\log(N)^2$          | $\Omega(1/\log(N))$ | $\Omega(1)$ |
| Physical qubits | $N$                | $N$           | $N$         |
| Logical qubits | $2$                   | $1$           | $\Theta(N)$ |
| Distance      | $\Theta(\sqrt{N})$   | $\Theta(\sqrt{N})$ | $2$        |
| Check weight/qubit degree | $\Theta(\log(N)/\log(\log(N)))$ | $O(\log(N))$ | $\Theta(1)$ |

| Constructions | Theorem 1.2 | Theorem 1.3 | Theorem 1.4 |
|---------------|-------------|-------------|-------------|
| Soundness     | $\Omega(1)$ | $\Omega(1/\log(N))$ | $\Omega(1)$ |
| Physical qubits | $N$             | $N$           | $N$         |
| Logical qubits | $\Theta(N)$  | $\Theta(N/\log(N))$ | $\Theta(N/\log(N))$ |
| Distance      | $\Theta(\log(N))$ | $\Theta(\log(N))$ | $\Theta(\log(N))$ |
| Check weight/qubit degree | $O(\log(N))$ | $\Theta(1)$ | $(\text{avg, max}) = (\Theta(1), \Theta(\log(N)))$ |

Table 2: Parameters of the 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 \( v \in \mathbb{F}_2^m \), we let \( X^v \) denote the \( n \)-qubit Pauli operator \( X^{v_1} \otimes X^{v_2} \otimes \cdots \otimes X^{v_n} \), where \( X^1 = X \) and \( X^0 = I \). We define \( Z^c \) 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 states

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

for \( \gamma \in C_Z \).

**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 \( d_X := \min\{|c| : c \in C_X \setminus C_X^\perp \} \) and \( d_Z := \min\{|c| : c \in C_Z \setminus C_Z^\perp \} \).

In this paper, we consider the following definition of local testability, which is the same definition as in [13].

**Definition 2.3** (Locally testable code). A linear code \( C \in \mathbb{F}_2^n \) is locally testable with soundness \( \rho \) 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

\[
\frac{1}{m} |Hx| \geq \frac{\rho}{n} d(x, C)
\]

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

We further consider the definition of quantum locally testable codes as in [8]. Given a quantum stabilizer code with stabilizer generators \( S_1, \ldots, S_m \) 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

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

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

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

We then have

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

\[
\frac{1}{m} \sum_{i=1}^m \frac{1}{2} (I - S_i) \geq \frac{\rho}{n} D_Q.
\]
Local testability of quantum CSS codes and the testability of their classical component codes are closely related, as shown by [8]:

**Lemma 2.5** (Fact 17 of [8]). A quantum CSS code CSS($H_X,H_Z$) is a qLTC with soundness $\rho$ if $C_X = \ker(H_X), C_Z = \ker(H_Z)$ are cLTCs of soundness $\rho$. Conversely, if CSS($H_X,H_Z$) is a qLTC with soundness $\rho$, 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 Theorem 1.1.

### 3.1 A Motivating Example

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

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

**Proof.** A way to understand the code $\tilde{C}$ 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 $\tilde{C}$ 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 $z \in \tilde{C}$ as $z = (x, y)$, where $x, y \in \mathbb{F}_2^n$. We show

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

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

Now note that the check weights of $\tilde{C}$ are bounded by $2w$, and each qubit is checked by at most $w$ checks. Therefore $\tilde{C}$ is LDPC. The rate of $\tilde{C}$ 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 $\forall x, y \in \mathbb{F}_2^n$, 

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

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

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

which completes our proof. \[\square\]
**Corollary 3.2.** The quantum code $Q = \text{CSS}(\bar{H}, \bar{H})$ is a qLTC of soundness $2\rho$, 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 $Z^{(1_v, 1_v)}$ and $X^{(1_v, 2_v)}$ for $v \in B$. If $Z^{(1_v, 1_v)}$ 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 $Z^{(1_v, 1_v)}$ and $X^{(1_v, 2_v)}$ are both logical operators. □

By choosing $C$ as a known $c^3$-LTC, for instance the left-right Cayley complex code [6], we obtain Theorem 1.1. It is surprising that such a trivial construction could already give us quantum codes of constant soundness. Moreover, this example demonstrates that, perhaps counter-intuitively, the soundness and distance of a quantum code are not necessarily related. In section 5, we show how to modify this construction so that Hastings’ distance balancing could be applied, and thereby prove Theorem 1.3 and 1.4.

We generalize this construction in the following section.

### 3.2 General Check Products

We begin by making the following observation: the matrix $H = [H, H]$ 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, and we include a proof in the Appendix.

**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 $Q = \text{CSS}(H_X, H_Z)$, we define the check-product of $Q$ and $C$ to be the quantum code $Q \star C = \text{CSS}(H_X \otimes H, H_Z \otimes H)$. 

7
It is straightforward to see that the commutativity condition is satisfied, so this definition is valid. We now discuss the distance of this quantum code.

**Lemma 3.5.** Given a quantum code \( Q = \text{CSS}(H_X, H_Z) \), \( Q \star C \) 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

\[
d_x(Q \star C) = \min\{ |w| : w \in C_X \star C \setminus (C_Z \star C)^\perp \} = \min\{ |w| : w \in C_X \otimes \mathbb{F}_2^n + \mathbb{F}_2^{n_q} \otimes C \setminus C_Z^1 \otimes C^\perp \}.
\]

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 \( x \otimes e_i \in C_X \otimes \mathbb{F}_2^n \setminus C_Z^1 \otimes C^\perp \). Similarly, since \( C_Z^1 \neq \mathbb{F}_2^{n_q} \), we can find \( y \in C, |y| = d(C) \), and a standard basis vector \( e_j \in \mathbb{F}_2^{n_q} \setminus C_Z^1 \) such that \( e_j \otimes y \in \mathbb{F}_2^{n_q} \otimes C \setminus C_Z^1 \otimes C^\perp \). 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,

\[
d_x(Q \star C) = \min\{ |w| : w \in C_X \star C \setminus (C_Z \star C)^\perp \} \geq \min\{ |w| : w \in C_X \} = \min(d(C_X), d(C)).
\]

Therefore \( d_x(Q \star C) = \min(d(C_X), d(C)) \). Similarly, we have \( d_y(Q \star C) = \min(d(C_Z), d(C)) \). This lemma then follows. \( \square \)

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, \( \Pi \)):

\[
H' = \begin{bmatrix} I_m \mid R \end{bmatrix} \quad (= GH\Pi) \quad (4)
\]

where \( I_m \) is the \( m \times m \) identity matrix, and \( R \) is a \( m \times (n - m) \) “random-looking” 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. We now show the following claim.

**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 we can just originally permute the bits of the code with $\Pi$, not changing any of its parameters. Given $x \in \mathbb{F}_2^n$, it suffices for us to show that $\frac{d(x, C)}{n} \leq |H'x|/m$. Denote the rows of $H'$ as $r_1, \ldots, r_m$, then $|H'x| = \sum_{i=1}^m r_i \cdot x$ (\(|.| \) meaning the Hamming distance). 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.

Notice that code $C$ in the above claim is not changed at all, only the set of checks. We further note that the check weights are now arbitrary, as we have no control over $R$. Therefore,

**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 check weight and bit degree, 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 check weight and qubit degree, 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 [5], but we only became aware of this correspondence after an initial draft of 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 $\rho$ and check weight, bit degree bounded by $w$. 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 check weight and bit degree are bounded by $w_X$. Then $C_X \star C$ is a cLTC with soundness at least $pm_X/m_X$ and check weights, bit degree bounded by $ww_X$.

**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 check weight and bit degree of $C_X \star C$ follows. The more interesting part is to show that $C_X \star C$ has soundness parameter at least $\rho$.

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 $x \in \mathbb{F}_2^{n_X}$ to be checked, we write it as $x = (x_1, \ldots, x_{m_X})$ where each $x_i \in \mathbb{F}_2$. Fix $1 \leq i \leq m_X$, and consider the collection $\Gamma_i$ 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

$$y_i = \sum_{j \in i\text{th check of } C_X} x_j \pmod{2}.$$


(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 $\Gamma_i$ 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 $\rho$ of $C$ there exists a $y'_i \in \mathbb{F}_2^n$ such that $\rho|y_i - y'_i| \leq \frac{n}{t}|\Gamma'_i|$. Adding now $y_i - y'_i$ to $x_i$, while keeping all $x_j$s for $j \neq i$ the same, we have achieved that all checks in $\Gamma_i$ go through, and also we did not affect those checks that are not in $\Gamma_i$, since their $H_X$ component does not contain the $i$th bit of $C_X$. After having the above done for all $1 \leq i \leq m_X$ we get a word $x'$ that passes all tests, therefore belongs to $C_X \ast C$. Further,

$$\rho|x' - x| \leq \sum_{i=1}^{m_X} \frac{n}{t} |\Gamma'_i| = \frac{n}{t} \sum_{i=1}^{m_X} |\Gamma'_i| = \frac{n}{t} s$$

where $s$ is the number of checks violated by $x$. Relating $s$ to $m_X t$, the number of all checks, we get from (5) that

$$\frac{s}{m_X t} \geq \frac{|x' - x|}{m_X \cdot n} \cdot \rho = \frac{|x' - x|}{n_X \cdot n} \cdot \frac{\rho n_X}{m_X}$$

probability of failed check relative distance of of $x$ from a code word

as needed.

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 $\rho$, dimension $k$, distance $d$ and check weight and bit degree both bounded by $w$, and a $n_q$-qubit quantum code $Q = \text{CSS}(H_X,H_Z)$ of dimension $k_q$, we can reduce $H_X,H_Z$ to have the form in equation (4), and denote the resulting quantum code $\bar{Q} = \text{CSS}(\bar{H}_X,\bar{H}_Z)$. ($Q$ 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 $\bar{Q} \ast C$ has

1. local testability with soundness $\rho \cdot \min(n_X \cdot n_Z, n_Z \cdot n_X)$ (in particular, soundness $\geq \rho$)\(^1\),
2. distance $\min(d,d(C_X),d(C_Z))$, where $C_X = \ker(H_X),C_Z = \ker(H_Z)$.
3. check weight and qubit degree bounded by $w n_q$,
4. and dimension $n n_q - (n - k)(n_q - k_q)$.

**Proof.** Local testability with soundness $\rho \cdot \min(n_X \cdot n_Z, n_Z \cdot n_X)$ is proved by lemma 4.3, by applying it to both $C_X \ast C$ and $C_Z \ast C$ (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 [8]).

The check weight and qubit degree 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 $\bar{Q} \ast C$ 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 $\bar{Q} \ast C$ is $(n - k)(n_q - k_q)$.

\(^1\)We have used our notational convention, that $\bar{H}_X$ and $\bar{H}_Z$ are $m_X \times n_X$ and $m_Z \times n_Z$ matrices, respectively, where $n_X = n_Z = n_q$, the length of $Q$. Thus $\frac{n_X}{m_X}$ and $\frac{n_Z}{m_Z}$ are reciprocals of the rates of the two classical codes that make $Q$.  

10
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 \(d(C_X), d(C_Z) = O(1)\). To argue for instance, that \(d(C_X) = O(1)\), we notice, that \(C_X \geq C^\perp_Z\), and since \(C^\perp_Z\) contains all possible checks for \(C_Z\), it also contains the low-weight ones, that by our checkability assumption must exist. 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 \(Q = CSS(H_X, H_Z)\) has correspondingly large check weights for all possible checks (i.e. checks in \(C^\perp_X\) and \(C^\perp_Z\)). 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 \(1/2\).

We prove this theorem in the Appendix. Combining theorem 4.4 and 4.5, we obtain theorem 1.2.

5 Gauge Fixing and Distance Balancing

Theorem 1.2 shows an exotic family of qLTCs where the quantum distance scales positively with the check weight. In this section, we prove theorem 1.3 and 1.4 by modifying our construction in section 3.1 and applying distance balancing.

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 \(\rho\), dimension \(k\) and distance \(d\), we define \(\tilde{C} = \ker(\tilde{H})\), where \(\tilde{H} = [H, H]\), and \(Q = CSS(\tilde{H}, \tilde{H})\). Let us consider the stabilizers and logical operators of \(Q\). Consider the set of Pauli operators

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

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 $Q' = \text{CSS}(H_X, H_Z)$. The code states of $Q'$ can be explicitly written out as

$$\{|\psi_{a,b}\rangle = \sum_{v \in F_2^n} |a + v, b + v\rangle : a + b \in \ker H\}.$$ 

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

5.2 Distance Balancing

We can now apply the distance balancing techniques in [10]. Specifically, we consider our code $Q'$ as a chain complex

$$Q = F_2^m \xrightarrow{H_Z^T = [I, I]^T} F_2^{2n} \xrightarrow{H_X = [H, H]} F_2^n,$$

and we take a repetition code of length $\ell$, also viewed as a chain complex

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

where $E = F_2^{\ell-1}, V = F_2^\ell$, and $H_\ell$ is the $\ell \times (\ell - 1)$ matrix of the form

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

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

Now we take the sub-chain complex $C_2 \rightarrow C_1 \rightarrow C_0$, and view it as a quantum code. From [10], 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 $\ell d_x, d_z$. 

12
We refer the readers to [10], statement 7 and 8 of lemma 2 for the proofs. Moreover, it was also shown in [10] that the resulting code is locally testable, albeit having a lower soundness.

Lemma 5.2 (Lemma 7 of [10]). 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 theorem 1.3. 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 5.3 and 5.4. The proof of lemma 5.3 would be a slightly modified version of the proof of lemma 5.1 in [10], and the proof of lemma 5.4 would follow a similar scheme as the proof of lemma 5.2 in [10].

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 check weight and qubit degree. We perform column operation on \( H_\ell \) such that it has the following form.

\[
H_\ell = \begin{bmatrix}
1 & 0 & 0 & 0 & \cdots \\
0 & 1 & 0 & 0 & \cdots \\
0 & 0 & 1 & 0 & \cdots \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 1 \\
1 & 1 & \cdots & 1 & 1 \\
\end{bmatrix}.
\]

Note that as before, \( H_\ell^T \) is a valid parity check matrix for the repetition code. The rest of the construction remains unchanged. We now prove the following lemmas regarding the parameters of \( Q' \).

Lemma 5.3. \( Q' \) 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 \( r \)th homology group of a chain complex as \( H_r(C) = \ker \partial_r / \text{im} \partial_{r+1} \), 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 $E = \mathbb{F}_2^\ell$. 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 $Z^c$ 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 $v_\ell \notin \text{im}(H_\ell)$, 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 $r$th homology group of a chain complex as $H^r(C) = \ker \partial_{r+1}^T / \text{im} \partial_r^T$, 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 $u \in \mathbb{F}_2^n \otimes V$. Note that the $H^0(R)$ has dimension 1, which means $v = \sum_{i=1}^r v_i$. Now suppose $u = \sum_{i=1}^\ell u_i \otimes v_i$, and consider the projection of $c$ onto the space $\mathbb{F}_2^n \otimes V$. It has the form

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

Since $\partial_1^T c = 0$, we must have $x + H_X u_i \in H^1(Q)$ for all $i$, which means $|c| \geq \ell d_z(Q)$. 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 $d_x(Q') = \ell d_x(Q)$.

14
For the check weight and qubit degree of $Q'$, we note that $H_X \otimes I$ and $H_Z^2 \otimes I$ are matrices with constant row and column weights. For $I \otimes H_\ell$, exactly $1/\ell$ fraction of its rows have weight $\ell$, 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 $q_1, \ldots, q_{2n}$, and the standard basis vectors of $\mathbb{F}_2^m$ as $c_1, \ldots, c_m$. Then we have

1. All the $Z$-stabilizer generators corresponding to basis vectors of $\mathbb{F}_2^8 \otimes V$ 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 $\ell$ $Z$-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 $\mathbb{F}_2^m \otimes V$ have the form $c_i \otimes v_j$ for $i \in [m], j \in [\ell]$. Generators of the form $c_i \otimes v_\ell$ checks $\ell$ 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. \[ \blacksquare \]

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

**Lemma 5.4.** $Q'$ is locally testable with soundness $\rho/8$ 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

$$
\frac{\left| \partial_1(\bar{c}) \right|}{m\ell} \geq \frac{\rho(|z| + |\bar{y}|)}{8(2n\ell + m(\ell - 1))}. \tag{7}
$$

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

$$
\partial_1(\bar{c}) = (H_X \bar{x}) \otimes v_1 + \sum_{i=1}^{\ell-1} y_i \otimes (H_\ell e_i) = (H_X \bar{x}) \otimes v_1 + \sum_{i=1}^{\ell-1} y_i \otimes v_1 + \sum_{i=1}^{\ell-1} y_i \otimes v_\ell
$$

$$
= (H_X \bar{x}) \otimes v_1 + y_1 \otimes v_1 + \sum_{i=2}^{\ell-1} y_i \otimes v_i + y_1 \otimes v_\ell + \sum_{i=2}^{\ell-1} y_i \otimes v_\ell.
$$
Let \( y' = \sum_{i=2}^{\ell-1} y_i \). For two vectors \( u, v \) denote the vector where \((u \cap v)(i) = 1\) if and only if \( u(i) = v(i) = 1\). Then we have

\[
|\partial_1(\bar{c})| = |H_X\bar{x}| + |y_1| - 2|H_X\bar{x} \cap y_1| + \sum_{i=2}^{\ell-1} |y_i| + |y_1| + |y'| - 2|y' \cap y_1|
\]

\[
= |H_X\bar{x}| - 2|H_X\bar{x} \cap y_1| + |y'| + 2|y_1| - 2|y' \cap y_1| + \sum_{i=2}^{\ell-1} |y_i|.
\]

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

\[
|\partial_1(\bar{c})| \geq \sum_{i=2}^{\ell-1} |y_i| + |y_1| - |y' \cap y_1|,
\]

\[
|\partial_1(\bar{c})| \geq |H_X\bar{x}|.
\]

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

\[
|\partial_1(\bar{c})| \geq |\bar{y}|/3 \geq |\bar{y}| + |H_X\bar{x}| \geq 4 + \frac{|\bar{y}|}{4} + \frac{2\rho md(\bar{x}, \ker H_X)}{4 \cdot 2n},
\]

\[
\frac{|\partial_1(\bar{c})|}{m\ell} \geq \frac{|\bar{y}|}{4m\ell} + \frac{\rho d(\bar{x}, \ker H_X)}{4n\ell}.
\]

Assuming \( \rho \leq 1 \) and \( 8(\ell - 1) \geq 4\ell \), we have equation (7). Now if \(|H_X\bar{x}| \geq |\bar{y}|/3\), we also have

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

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 \( \im H^T_\ell = \mathbb{F}_2^{\ell-1} = E \), we can multiply \( X^c \) by \( X \)-stabilizers of the form \( X^r \), where

\[
r = \partial^T_1 \left( \sum_{j=1}^{\ell-1} y_j \otimes v_j \right) = \left( \sum_{j=1}^{\ell-1} H^T_X y_j \otimes v_j, \sum_{j=1}^{\ell-1} y_j \otimes e_j \right).
\]

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

\[
x_i = (x^1_i, x^2_i) = (x^1_i(1), \cdots, x^1_i(n), x^2_i(1), \cdots, x^2_i(n)) \in \mathbb{F}_2^n.
\]
Further, without loss of generality, we may assume $x_i^1 \cap x_i^2 = 0$ because if $x_i^1 \cap x_i^2 \neq 0$, we can add $(x_i^1 \cap x_i^2, x_i^1 \cap x_i^2) \otimes (\sum_{i=1}^{\ell} v_i), 0)$ to $c$. Note here that $\partial_T^2 ((x_i^1 \cap x_i^2, x_i^1 \cap x_i^2) \otimes (\sum_{i=1}^{\ell} v_i), 0) = 0$. Now we are ready for the proof.

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

$$\partial_T^2 (c) = \sum_{i=1}^{\ell} (x_i^1 + m x_i^2) \otimes v_i + m \sum_{i=1}^{\ell} (x_i^1, x_i^2) \otimes (H^T T \mathcal{E} v_i)$$

$$= \sum_{i=1}^{\ell} (x_i^1 + m x_i^2) \otimes v_i + m \sum_{i=1}^{\ell-1} (x_i^1, x_i^2) \otimes e_i + m (x_i^1, x_i^2) \otimes (\sum_{i=1}^{\ell-1} e_i).$$

$$|\partial_T^2 (c)| = \sum_{i=1}^{\ell} |x_i^1 + m x_i^2| + \sum_{i=1}^{\ell-1} (|x_i^1| + |x_i^2|) + \sum_{i=1}^{\ell-1} (|x_i^1| + |x_i^2|) - 2 \sum_{i=1}^{\ell-1} (|x_i^1 \cap x_i^2| + |x_i^2 \cap x_i^2|),$$

$$= |x_i^1 + m x_i^2| + \sum_{i=1}^{\ell-1} \sum_{j=1}^{n} (x_i^1(j) + m x_i^2(j)) + x_i^1(j) + x_i^2(j) + x_i^2(j) + x_i^1(j) + x_i^2(j) + x_i^2(j)$$

$$- 2(x_i^1 \cap x_i^2)(j) - 2(x_i^2 \cap x_i^2)(j).$$

We abbreviate the above equation into

$$|\partial_T^2 (c)| = |x_i^1 + m x_i^2| + \sum_{i=1}^{\ell-1} \sum_{j=1}^{n} c_{i,j}.$$  

We now prove $|\partial_T^2 (c)| \geq \frac{1}{2} \sum_{i=1}^{\ell} \sum_{j=1}^{n} |x_i^1(j)| + |x_i^2(j)|$ 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 $x_i^1(j), x_i^2(j)$, we have $c_{i,j} \geq 1$. This can be seen from the following table. Note that by our assumptions, $x_i^1(j), x_i^2(j)$ cannot both be 1.

| $x_i^1(j)$ | $x_i^2(j)$ | $x_i^1(j)$ | $x_i^2(j)$ | $c_{i,j}$ |
|-----------|-----------|-----------|-----------|---------|
| 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       |

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

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

17
Combining this observation with the values in table 3, we see that

\[ |\partial^2 T_2(c)| \geq \frac{1}{2} \sum_{i=1}^{\ell} \sum_{j=1}^{n} |x_1(j)| + |x_2(j)| = \left( \sum_{i=1}^{\ell} |x_i| \right)/2 \]

\[ \frac{|\partial^2 T_2(c)|}{n\ell + 2n(\ell - 1)} \geq \frac{\sum_{i=1}^{\ell} |x_i|}{2n\ell + 4n(\ell - 1)} \geq \frac{1}{3} \frac{\sum_{i=1}^{\ell} |x_i|}{2n\ell + m(\ell - 1)}. \]

Therefore, \( Q' \) is locally testable with soundness 1/3 for \( X \)-operators.

Together, lemma 5.3 and 5.4 gives theorem 1.4.

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

[1] Dorit Aharonov and Lior Eldar. Quantum locally testable codes. *SIAM Journal on Computing*, 44(5):1230–1262, 2015.

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

[3] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, pages 73–83, 1990.

[4] Nikolas P Breuckmann and Jens N Eberhardt. Balanced product quantum codes. *IEEE Transactions on Information Theory*, 67(10):6653–6674, 2021.

[5] Earl T Campbell. A theory of single-shot error correction for adversarial noise. *Quantum Science and Technology*, 4(2):025006, 2019.

[6] Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes. Locally testable codes with constant rate, distance, and locality. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 357–374, 2022.
[7] Irit Dinur, Min-Hsiu Hsieh, Ting-Chun Lin, and Thomas Vidick. Good quantum ldpc codes with linear time decoders. *arXiv preprint arXiv:2206.07750*, 2022.

[8] Lior Eldar and Aram W Harrow. Local Hamiltonians whose ground states are hard to approximate. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 427–438. IEEE, 2017.

[9] Michael H Freedman and Matthew B Hastings. Quantum systems on non-k-hyperfinite complexes: a generalization of classical statistical mechanics on expander graphs. *Quantum Information & Computation*, 14(1-2):144–180, 2014.

[10] Mathew B Hastings. Weight reduction for quantum codes. *Quantum Information & Computation*, 17(15-16):1307–1334, 2017.

[11] Matthew B Hastings. Quantum codes from high-dimensional manifolds. In *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*, volume 67, page 25. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2017.

[12] Matthew B Hastings, Jeongwan Haah, and Ryan O'Donnell. 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*, pages 1276–1288, 2021.

[13] Anthony Leverrier, Vivien Londe, and Gilles Zémor. Towards local testability for quantum coding. *Quantum*, 6:661, 2022.

[14] Anthony Leverrier and Gilles Zémor. Quantum Tanner codes. *arXiv preprint arXiv:2202.13641*, 2022.

[15] Ting-Chun Lin and Min-Hsiu Hsieh. $c^3$-local testable codes from lossless expanders. *arXiv preprint arXiv:2201.11369*, 2022.

[16] Pavel Panteleev and Gleb Kalachev. Quantum ldpc codes with almost linear minimum distance. *IEEE Transactions on Information Theory*, 68(1):213–229, 2021.

[17] 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*, pages 375–388, 2022.

Appendix

**Proof of Lemma 3.3**

**Lemma.** 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. $C_1 \star C_2 = C_1 \otimes F_2^{n_2} + F_2^{n_1} \otimes C_2$. 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 $n_1n_2 - (n_1 - k_1)(n_2 - k_2)$.
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 $|M w| \geq d_1$ ($|.|$ 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 $(1, 0, \ldots, 0) \otimes x$ and $y \otimes (1, 0, \ldots, 0)$ 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. \hfill \Box

**Dual Classical Codes of Linear Distance**

Here we prove Theorem 4.5. 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 $\frac{3n}{4} - \frac{1}{2}n$ qubits, therefore it has rate $1/2$.

Next we will show that both $C$ and $D^\perp$ have linear distances with high probability. Let $\delta$ 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 $\delta'$, then a random linear code with rate $1 - H(\delta') - \epsilon$ will achieve that, where $\epsilon$ 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 $\frac{3}{4}$ rows and $n$ columns. The minimum distance of $C$ is the minimum number of columns of $M$ that sum to zero. To argue for relative distance $\delta'$ slightly below $\delta$, we use the well-known fact, that

$$\log_2 \left( \frac{n}{\delta' n} \right) = H(\delta) \left( n - \omega(\log n) \right) \quad \text{when} \quad \delta' \to \delta \quad \text{appropriately, as} \quad n \to \infty$$
The number of ways to select \( 1 \leq k \leq \delta' n \) columns is then \( \leq \delta' n \cdot 2^{\left(\frac{H(\delta)}{2}(n-o(\log n))\right)} = o\left(2^{H(\delta)n}\right) \),
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 \( n - \dim D = \frac{3}{4} n \), 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 \( \frac{3}{4} n \) 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 \( W = \begin{pmatrix} N \\ M \end{pmatrix} \). Here \( N \) and \( M \) are random, and the rows of \( W \) generate \( D^\perp \). (Warning: Here we do not condition on that \( M \) satisfies our first criterion. We will simply take the intersection of the two favorable events in the end.) We calculate the probability that the rows of \( W \) generate any vector of weight less than \( \delta' n \), where \( \delta' \) is appropriately, but only slightly less, than \( \delta \).

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 \( 2^{0.75 n} \). Thus:

\[
\Pr_W\left(\text{there are rows of } W \text{ that add up to some } w \text{ with weight } \leq \delta n\right) \leq o\left(2^{H(\delta)n}\right) \cdot 2^{0.75 n} \cdot 2^{-n} = o(1)
\]

Thus, the probability that the minimum distance of \( D^\perp \) is at least \( \delta n \) 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 \( \delta' \), for a randomly chosen \( W = \begin{pmatrix} N \\ M \end{pmatrix} \) becomes arbitrarily small, as \( n \) goes to infinity.