



Quantum LDPC Codes of Almost Linear Distance via Iterated Homological Products

Louis Golowich 

UC Berkeley, CA, USA

Venkatesan Guruswami 

UC Berkeley, CA, USA

Abstract

The first linear-distance quantum LDPC codes were recently constructed by a line of breakthrough works (culminating in the result of Panteleev & Kalachev, 2021). All such constructions, even when allowing for almost-linear distance, are based on an operation called a balanced (or lifted) product, which is used in a one-shot manner to combine a pair of large classical codes possessing a group symmetry.

We present a new construction of almost-linear distance quantum LDPC codes that is iterative in nature. Our construction is based on a more basic and widely used product, namely the homological product (i.e. the tensor product of chain complexes).

Specifically, for every $\epsilon > 0$, we obtain a family of $[[N, N^{1-\epsilon}, N^{1-\epsilon}]]$ (subsystem) quantum LDPC codes via repeated homological products of a constant-sized quantum locally testable code. Our key idea is to remove certain low-weight codewords using subsystem codes (while still maintaining constant stabilizer weight), in order to circumvent a particular obstruction that limited the distance of many prior homological product code constructions to at most $\tilde{O}(\sqrt{N})$.

2012 ACM Subject Classification Theory of computation → Error-correcting codes

Keywords and phrases Quantum Error Correction, Quantum LDPC Code, Homological Product, Iterative Construction

Digital Object Identifier 10.4230/LIPIcs.CCC.2025.25

Related Version *Full Version:* <https://arxiv.org/abs/2411.03646> [14]

Funding Research supported in part by a ONR grant N00014-24-1-2491 and a UC Noyce initiative award. This work was done in part while the authors were attending the Spring 2024 programs at the Simons Institute for the Theory of Computing.

Louis Golowich: Supported by a National Science Foundation Graduate Research Fellowship under Grant No. DGE 2146752.

1 Introduction

Quantum low-density parity-check (qLDPC) codes provide one of the most promising means for achieving efficient quantum fault-tolerance. Such codes are defined to support error detection and correction via sparse queries (i.e. stabilizer measurements) to code states. Each such query involves, and can therefore only propagate errors across, a small number of code components. However, this qLDPC condition has proven difficult to achieve, and asymptotically optimal qLDPC codes were only recently constructed following a line of breakthrough works [16, 28, 8, 27, 22, 11]. The latter three of these works use nearly identical techniques, and still provide the only known asymptotically good qLDPC codes, meaning that the code dimension and distance scale linearly in the block length, and the stabilizers (i.e. parity checks) have constant weight. These codes have led to many applications, including to breakthrough results in both classical and quantum complexity theory [17, 1].



© Louis Golowich and Venkatesan Guruswami;
licensed under Creative Commons License CC-BY 4.0

40th Computational Complexity Conference (CCC 2025).

Editor: Srikanth Srinivasan; Article No. 25; pp. 25:1–25:11

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



The works described above construct qLDPC codes by combining a pair of classical LDPC codes respecting a group action with an operation called a *balanced* (or *lifted*) *product*. However, this operation is fairly rigid, as it requires large, highly symmetric classical codes as inputs. The asymptotically good constructions [27, 22, 11] also require classical codes with a certain strong property called *product-expansion* [18], which is difficult to obtain in practice.

It has remained an open question to find alternative constructions of qLDPC codes with good parameters. Such alternative constructions may yield better practical parameters, have properties useful for other applications to complexity theory and fault-tolerant computation, or be of independent mathematical interest.

In this paper, we develop a new construction of qLDPC codes with close-to-linear dimension and distance. Our construction is inherently iterative: starting from a constant-sized code, we repeatedly apply *homological products* (i.e. tensor products of chain complexes) along with the stabilizer-weight-reduction transformation of [15] to produce a sequence of successively larger qLDPC codes. In contrast, all previous constructions of (even close to) linear distance qLDPC codes were based on a one-shot (non-iterative) application of a balanced product [28, 27, 22, 11].

The homological product is a well-known operation from homological algebra that generalizes the tensor product of classical codes. Such products can be viewed as a more basic version of balanced products, that do not require a group action. Homological products have long been used to construct qLDPC codes, notably including hypergraph product codes [32], which are simply homological products of 2-term chain complexes associated to classical codes. Hypergraph products of good classical LDPC codes give length- N quantum LDPC codes of dimension $\Theta(N)$ and distance $\Theta(\sqrt{N})$ [32]; the well-known surface and Toric codes [21], which also have distance $\Theta(\sqrt{N})$, can be viewed as hypergraph products of repetition codes. However, qLDPC codes previously constructed via homological products generally had distance at most $\tilde{O}(\sqrt{N})$; more technical details regarding this “ \sqrt{N} barrier” can be found in Section 3 below.

We circumvent this barrier by developing a new method of taking homological products that preserves almost-linear distance. Specifically, we observe that this barrier only applies to certain logical operators (i.e. codewords) within the code space. Our key idea is to therefore remove low-weight codewords by using *subsystem codes*, which only encode messages into a subspace of the entire logical code space. We show that appropriate subsystem codes of homological products have good distance; our proof builds on the techniques of [20]. We emphasize that the subsystem codes we consider remain truly LDPC, in that they have constant-weight stabilizers (see Remark 4).

We iteratively apply such homological products along with a stabilizer-weight-reduction transformation of [15] to obtain our main result, stated below:

► **Theorem 1** (Main result; Informal statement of Theorem 6). *For every $\epsilon > 0$, there exists a constant-sized code \mathcal{C} and an infinite sequence of qLDPC subsystem codes $(Q_i)_{i \in \mathbb{N}}$ with parameters¹*

$$[[N_i, N_i^{1-\epsilon}, N_i^{1-\epsilon}]]_2$$

and with constant stabilizer weight $O(1)$ (independent of ϵ), such that each Q_i is obtained by applying the stabilizer-weight-reduction transformation of [15] to the homological product of Q_{i-1} with \mathcal{C} .

¹ Recall that an $[[N, K, D]]_q$ code is a quantum code on qudits of local dimension q with block length N , dimension (i.e. number of logical qudits) K , and distance D .

The weight-reduction step in Theorem 1 is needed to keep the stabilizer weight constant in each iteration, as in general the stabilizer weight of a homological product code grows as the sum of the stabilizer weights of the input codes.

To prove Theorem 1, we set \mathcal{C} to be a constant-sized quantum locally testable code (qLTC) such as one given by [12, 19]; such a qLTC (which we emphasize is just constant-sized) is needed for our homological product distance bound described above. We apply this bound to inductively show that the distance of each Q_i remains close-to-linear (i.e. $\geq N_i^{1-\epsilon}$) in the block length N_i .

Our iterative construction in Theorem 1 is reminiscent of a line of work in classical pseudorandomness, coding theory, and complexity theory, which iteratively builds larger objects with properties of interest from smaller or weaker ones. For instance, [6, 33] constructed classical locally testable codes by iterative tensoring of a small classical code; at a high level, Theorem 1 uses a related approach to construct qLDPC codes. Other notable iterative constructions in the literature include explicit spectral expanders from the zig-zag product [30], Dinur’s proof of the PCP theorem [10], and undirected connectivity in logarithmic space [29]. Theorem 1 can therefore be viewed as an analogue of these results for qLDPC codes. However, our construction does need to start with a strong constant-sized object \mathcal{C} , namely, a constant-sized qLTC with sufficiently good parameters. It is an interesting open question whether there exists an iterative construction with a weaker starting object.

Our bounds on the distance of homological product codes may also be of independent interest. At a foundational level, it is a mathematically interesting question to determine when homological product codes have large distance. Indeed, as quantum codes can be equivalently viewed as chain complexes or as topological spaces (see also [13]), this question can be phrased as asking how the systolic and cosystolic distance of a topological space (see the full version [14]) behave under topological products.

Furthermore, the classical analogue of homological product codes, namely tensor codes, are widely studied and used throughout classical coding theory. Better understanding quantum homological products may yield similar benefits for quantum error correction and beyond.

As mentioned above, many quantum code constructions based on homological products had distance at most $O(\sqrt{N})$. However, a few works have surpassed this barrier, though still with suboptimal parameters. Specifically, [7] showed that a length- N “single-sector” variant of a homological product of two random quantum codes has distance $\Theta(N)$ and stabilizer weight $\Theta(\sqrt{N})$. [20] used homological products of chain complexes from certain high-dimensional expanders [25, 24] to obtain qLDPC codes with distance $\Theta(\sqrt{N} \cdot \text{poly log } N)$ and constant stabilizer weight. [9] also showed how to obtain homological product codes with stabilizer weight w and distance $\Theta(\sqrt{N} \cdot w)$.

In the remainder of this extended abstract, we provide a more detailed technical overview of our results. After presenting some necessary preliminaries in Section 2, we describe the main challenge in obtaining homological product codes of length N and distance $\gg \sqrt{N}$ in Section 3, and then we explain our main idea for circumventing this barrier in Section 4. We then present our bound on the distance of homological product codes in Section 5, and show how we apply this bound in our main iterative code construction in Section 6. We provide some concluding remarks in Section 7. For the complete proofs, the reader is referred to the full version [14].

2 Quantum Code Preliminaries

In this section, we briefly summarize some necessary background on quantum codes; more details can be found in the full version [14].

A length- n quantum CSS code consists of a pair $Q = (Q_X, Q_Z)$ of vector spaces $Q_X, Q_Z \subseteq \mathbb{F}_q^n$ with $Q_X^\perp \subseteq Q_Z$, where $Q_X^\perp := \{c \in \mathbb{F}_q^n : c \cdot x = 0 \ \forall x \in Q_X\}$. The code Q has dimension $k = \dim(Q_Z) - \dim(Q_X^\perp)$ and distance $d = \min_{c \in (Q_X \setminus Q_Z^\perp) \cup (Q_Z \setminus Q_X^\perp)} |c|$. We summarize these parameters by saying that Q is an $[[n, k, d]]_q$ code.

If $H_X \in \mathbb{F}_q^{m_X \times n}$, $H_Z \in \mathbb{F}_q^{m_Z \times n}$ are parity-check matrices for Q_X, Q_Z respectively, meaning that $Q_X = \ker H_X$ and $Q_Z = \ker H_Z$, then the locality (i.e. stabilizer weight) w of Q equals the maximum weight of any row of H_X or H_Z . We say Q is locally testable with locality w and soundness $\rho > 0$ if for $\alpha \in \{X, Z\}$, it holds for every $e \in \mathbb{F}_q^n$ that $|H_\alpha e|/m_\alpha \geq \rho \cdot \text{dis}(e, Q_\alpha)/n$, where $\text{dis}(e, Q_\alpha) = \min_{c \in Q_\alpha} |e - c|$. Thus local testability implies that the weight of an error on a code state can be estimated by simply measuring a random stabilizer.

In this paper, we primarily work with quantum codes using the language of chain complexes:

► **Definition 2.** A *chain complex* \mathcal{C}_* over \mathbb{F}_q consists of a sequence of \mathbb{F}_q -vector spaces $(C_i)_{i \in \mathbb{Z}}$ and linear *boundary maps* $(\partial_i^C : C_i \rightarrow C_{i-1})_{i \in \mathbb{Z}}$ satisfying $\partial_{i-1}^C \partial_i^C = 0$ for all $i \in \mathbb{Z}$. The associated *cochain complex* \mathcal{C}^* has vector spaces $C^i = C_i$ and coboundary maps $\delta_i^C = (\partial_{i+1}^C)^\top$. The *locality* of \mathcal{C}_* is the maximum Hamming weight of any row or column of any ∂_i^C . The *i-homology* (resp. *i-cohomology*) group of \mathcal{C}_* is $H_i(\mathcal{C}) = \ker(\partial_i^C) / \text{im}(\partial_{i+1}^C)$ (resp. $H^i(\mathcal{C}) = \ker(\delta_i^C) / \text{im}(\delta_{i-1}^C)$).

For chain complexes \mathcal{A}, \mathcal{B} , the *homological product* $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$ is the chain complex given by $C_i = \bigoplus_{j \in \mathbb{Z}} A_j \otimes B_{i-j}$ and $\partial_i^C = \bigoplus_{j \in \mathbb{Z}} (\partial_j^A \otimes I + (-1)^j I \otimes \partial_{i-j}^B)$.

We typically work with chain complexes \mathcal{C} that have $C_i = 0$ for every i outside of some sequence of t consecutive integers; we then call \mathcal{C} a t -term chain complex. For every level i with $C_i \neq 0$, there is a naturally associated quantum CSS code Q given by $Q_X = \ker \delta_i^C$ and $Q_Z = \ker \partial_i^C$. Conversely, given a length- n CSS code $Q = (Q_X, Q_Z)$ with parity-check matrices $H_X \in \mathbb{F}_q^{m_X \times n}$, $H_Z \in \mathbb{F}_q^{m_Z \times n}$, we can construct a 3-term chain complex $\mathcal{C} = (\mathbb{F}_q^{m_X} \xrightarrow{H_X^\top} \mathbb{F}_q^n \xrightarrow{H_Z} \mathbb{F}_q^{m_Z})$ with associated quantum code Q at the middle level. By definition, the maximum stabilizer weight of Q is always at most the locality of \mathcal{C} . The dimension (i.e. number of logical qudits) of Q equals $\dim(H^i(\mathcal{C})) = \dim(H_i(\mathcal{C}))$, and elements of $H^i(\mathcal{C})$ and $H_i(\mathcal{C})$ can be viewed as equivalence classes of X and Z logical operators, respectively, up to stabilizers. The distance of Q equals the minimum Hamming weight of any representative of a nontrivial element of $H^i(\mathcal{C})$ or $H_i(\mathcal{C})$.

For $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$, the well-known Künneth formula provides an isomorphism

$$H_i(\mathcal{C}) \cong \bigoplus_{j \in \mathbb{Z}} H_j(\mathcal{A}) \otimes H_{i-j}(\mathcal{B}),$$

which for $a \in \ker(\partial_j^A)$ and $b \in \ker(\partial_{i-j}^B)$ is given by

$$a \otimes b + \text{im}(\partial_i^C) \leftarrow (a + \text{im}(\partial_j^A)) \otimes (b + \text{im}(\partial_{i-j}^B)).$$

The analogous result naturally also applies to cohomology.

3 The \sqrt{N} Distance Barrier

One goal of this paper is to characterize conditions under which homological products preserve good distance (i.e. close to linear in the code length) of the associated quantum codes. However, there is a somewhat fundamental difficulty that arises when we work with finite-length complexes. Recall that for chain complexes \mathcal{A}, \mathcal{B} and integers i, j , the Künneth formula implies that if $a \in \ker(\partial_j^{\mathcal{A}}) \setminus \text{im}(\partial_{j+1}^{\mathcal{A}})$ and $b \in \ker(\partial_{i-j}^{\mathcal{B}}) \setminus \text{im}(\partial_{i-j+1}^{\mathcal{B}})$, then $a \otimes b \in \ker(\partial_i^{\mathcal{C}}) \setminus \text{im}(\partial_{i+1}^{\mathcal{C}})$. Therefore for instance consider the least $j \in \mathbb{Z}$ with $A_j \neq 0$, so that $\partial_j^{\mathcal{A}} = 0$, and assume that $B_{i-j} \neq 0$ (this assumption is without loss of generality if we allow ourselves to swap \mathcal{A} and \mathcal{B} , or instead consider their cochain complexes if necessary). Then unless $\partial_{j+1}^{\mathcal{A}}$ is surjective (which can be difficult to enforce in many settings), we must have some $a \in \ker(\partial_j^{\mathcal{A}}) \setminus \text{im}(\partial_{j+1}^{\mathcal{A}})$ of Hamming weight $|a| = 1$. Therefore $|a \otimes b| = |b|$, which (assuming $\dim(A_j) \approx \dim(B_{i-j})$) will be at most roughly the square root of the length of the quantum code at level i of \mathcal{C} .

This phenomenon was a major reason behind the “ \sqrt{N} barrier,” as prior to the work of [16] it was a longstanding open question to construct length- N qLDPC codes with distance greater than $\tilde{\Theta}(\sqrt{N})$. This barrier is perhaps easiest to understand with the homological product of two 2-term complexes \mathcal{A}, \mathcal{B} (i.e. the “hypergraph product” of [32]), which can be visualized as a 2×2 grid of vector spaces with maps between them:

$$\begin{array}{ccc} A_1 \otimes B_1 & \xrightarrow{-I \otimes \partial_1^{\mathcal{B}}} & A_1 \otimes B_0 \\ \downarrow \partial_1^{\mathcal{A}} \otimes I & & \downarrow \partial_1^{\mathcal{A}} \otimes I \\ A_0 \otimes B_1 & \xrightarrow{I \otimes \partial_1^{\mathcal{B}}} & A_0 \otimes B_0 \end{array} \quad (1)$$

The diagram above represents the 3-term chain complex $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$, where level 2 is the top left corner $A_1 \otimes B_1$, level 1 contains the diagonal elements $A_0 \otimes B_1 \oplus A_1 \otimes B_0$, and level 0 is the bottom right corner $A_0 \otimes B_0$. The boundary maps of \mathcal{C} are simply the maps shown in the diagram. We let Q be the quantum code at level 1 of \mathcal{C} .

Assume for simplicity that all A_0, A_1, B_0, B_1 all have dimension $\Theta(n)$. If Q is a code of positive dimension, the Künneth formula implies that either $\partial_1^{\mathcal{A}}$ is not surjective and $\partial_1^{\mathcal{B}}$ is not injective, or vice versa; assume the former, as the argument for the latter is analogous. Then as described above, there is some $a \in A_0 \setminus \text{im}(\partial_1^{\mathcal{A}})$ of weight $|a| = 1$, and there is some $b \in \ker(\partial_1^{\mathcal{B}})$, so $a \otimes b \in \ker(\partial_1^{\mathcal{C}}) \setminus \text{im}(\partial_2^{\mathcal{C}}) = Q_Z \setminus Q_X^\perp$ has Hamming weight $|a \otimes b| = |b| \leq O(n)$. But Q is a code of length $N = \Theta(n^2)$, and thus Q has distance $D \leq O(\sqrt{N})$.

Thus homological products of 2-term chain complexes cannot yield codes of good distance. We could consider using complexes \mathcal{A}, \mathcal{B} with $t^{\mathcal{A}}, t^{\mathcal{B}} \geq 2$ terms, and letting Q be the quantum code at some level i of the product complex $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$. However, a similar issue will arise. Specifically, the 2×2 grid in (1) would be replaced by a $t^{\mathcal{A}} \times t^{\mathcal{B}}$ grid, but if we look at vector spaces around the edge of this grid, we may again find codewords in $\ker(\partial_i^{\mathcal{C}}) \setminus \text{im}(\partial_{i+1}^{\mathcal{C}}) = Q_Z \setminus Q_X^\perp$ of the form $a \otimes b$ with $|a| = 1$, so that $|a \otimes b| = |b| \leq O(n) = O(\sqrt{N})$.

[7] circumvented this barrier using *single-sector chain complexes*, which can be viewed as infinitely long complexes $\cdots \xrightarrow{\partial} C \xrightarrow{\partial} C \xrightarrow{\partial} \cdots$ with the same boundary map ∂ at every level. These complexes therefore do not have such low-distance codewords in vector spaces on the edges of the grid described above. However, single-sector complexes are somewhat restrictive, as they only have a single boundary map, and we were not able to obtain good bounds on the distance of single-sector homological products of qLDPC codes with constant locality; the products of [7] have locality $\Theta(\sqrt{N})$. Instead, we took an alternative approach to circumventing this barrier, using subsystem codes as described below.

4 Circumventing the Barrier with Subsystem Codes

Our key observation for circumventing the \sqrt{N} distance barrier described above is that it only applies to certain subspaces of the code space. For instance, consider a homological product of 3-term chain complexes \mathcal{A}, \mathcal{B} as a 3×3 grid:

$$\begin{array}{ccccc}
 A_2 \otimes B_2 & \xrightarrow{I \otimes \partial_2^{\mathcal{B}}} & A_2 \otimes B_1 & \xrightarrow{I \otimes \partial_1^{\mathcal{B}}} & A_2 \otimes B_0 \\
 \downarrow \partial_2^{\mathcal{A}} \otimes I & & \downarrow \partial_2^{\mathcal{A}} \otimes I & & \downarrow \partial_2^{\mathcal{A}} \otimes I \\
 A_1 \otimes B_2 & \xrightarrow{-I \otimes \partial_2^{\mathcal{B}}} & A_1 \otimes B_1 & \xrightarrow{-I \otimes \partial_1^{\mathcal{B}}} & A_1 \otimes B_0 \\
 \downarrow \partial_1^{\mathcal{A}} \otimes I & & \downarrow \partial_1^{\mathcal{A}} \otimes I & & \downarrow \partial_1^{\mathcal{A}} \otimes I \\
 A_0 \otimes B_2 & \xrightarrow{I \otimes \partial_2^{\mathcal{B}}} & A_0 \otimes B_1 & \xrightarrow{I \otimes \partial_1^{\mathcal{B}}} & A_0 \otimes B_0
 \end{array} \tag{2}$$

Let Q be the quantum code at the middle level ($i = 2$) of the 5-term chain complex $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$, so that Q_X, Q_Z are codes within the vector space $C_2 = A_0 \otimes B_2 \oplus A_1 \otimes B_1 \oplus A_2 \otimes B_0$ consisting of the three spaces in the bottom-left to top-right diagonal of the grid in (2). By the Künneth formula,

$$H_2(\mathcal{C}) \cong H_0(\mathcal{A}) \otimes H_2(\mathcal{B}) \oplus H_1(\mathcal{A}) \otimes H_1(\mathcal{B}) \oplus H_2(\mathcal{A}) \otimes H_0(\mathcal{B}),$$

where for simplicity here we restrict attention to homology (i.e. Z logical operators); the analogous reasoning also applies to cohomology (i.e. X logical operators). The reasoning in Section 3 suggests that elements of $H_0(\mathcal{A}) \otimes H_2(\mathcal{B})$ and $H_2(\mathcal{A}) \otimes H_0(\mathcal{B})$ may have low-weight representatives. However, there is no apparent obstruction to having the homology classes associated to nonzero elements of $H_1(\mathcal{A}) \otimes H_1(\mathcal{B})$ having only high-weight representatives (and analogously for cohomology). In the language of quantum codes, while the code Q at level 2 of \mathcal{C} may have low-weight logical operators, we may hope to guarantee that the subspace of logical operators associated to the middle element of the grid in (2) all have high weight. In Theorem 5 below, we realize this hope for \mathcal{A}, \mathcal{B} satisfying appropriate conditions.

This idea of a code where we restrict attention to a subspace of logical operators has been studied in the quantum error correction literature, where it is called a *subsystem code*, defined below.

► **Definition 3.** A *quantum subsystem code* is a pair (Q, L) consisting of a CSS code $Q = (Q_X, Q_Z)$ together with a pair $L = (L_X, L_Z)$ of tuples $L_X = (c^1, \dots, c^k) \in Q_X^k$, $L_Z = (c_1, \dots, c_k) \in Q_Z^k$ of the same length k , such that $c^i \cdot c_j = \mathbb{1}_{i=j}$ for all $i, j \in [k]$.

The dimension of the subsystem code (Q, L) is k , the distance is

$$d := \min_{c \in (Q_X \setminus \text{span}\{L_Z\}^\perp) \cup (Q_Z \setminus \text{span}\{L_X\}^\perp)} |c|,$$

and the locality w equals the the locality (i.e. stabilizer weight) of Q .

► **Remark 4.** In Definition 3, we define the locality of a subsystem code to equal the maximum stabilizer weight for the chosen parity-check matrices of the underlying CSS code Q . Therefore for our purposes, a subsystem code with constant locality is simply a qLDPC code with constant-weight stabilizers, but where we only encode message qudits into certain logical operators. Such codes can typically be used for fault-tolerant computation analogously to non-subsystem qLDPC codes.

In contrast, some works (e.g. [4]) have studied subsystem codes where the locality is measured by the weight of generators for the groups $Q_X \cap \text{span}\{L_Z\}^\perp$ and $Q_Z \cap \text{span}\{L_X\}^\perp$, which are often called “gauge operators.” Codes with such a weaker locality property can

be more difficult to use for applications to fault-tolerance, as while a high-weight stabilizer can be measured by decomposing it into low-weight gauge operators, many different gauge operators may need to be measured for each stabilizer.

5 Bounds on Products of QLDPC Subsystem Codes

In Theorem 5 below, we characterize conditions under which good subsystem QLDPC code distance is preserved by homological products. Following the intuition described in Section 4 above, we restrict attention to logical operators in the middle terms of homological products of complexes of length ≥ 3 . In fact, we take the product of a 3-term complex \mathcal{A} with a 5-term complex \mathcal{B} ; for both complexes, we assume that the middle level is indexed $i = 0$.

► **Theorem 5.** *Let \mathcal{A} be a 3-term chain complex of locality $w^{\mathcal{A}}$ with an associated $[[n^{\mathcal{A}}, k^{\mathcal{A}}, d^{\mathcal{A}}]]$ subsystem code at the middle level ($i = 0$). Let \mathcal{B} be a 5-term chain complex of locality $w^{\mathcal{B}}$ with an associated $[[n^{\mathcal{B}}, k^{\mathcal{B}}, d^{\mathcal{B}}]]$ CSS code at the middle level ($i = 0$) that is locally testable with soundness $\rho^{\mathcal{B}}$. Then the homological product $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$ is a 7-term chain complex of locality $w^{\mathcal{C}} \leq w^{\mathcal{A}} + w^{\mathcal{B}}$ with an associated $[[N, K, D]]$ subsystem code at the middle level for*

$$\begin{aligned} N &\leq n^{\mathcal{A}}n^{\mathcal{B}} + 2n'^{\mathcal{A}}n'^{\mathcal{B}} \\ K &= k^{\mathcal{A}}k^{\mathcal{B}} \\ D &\geq \frac{d^{\mathcal{A}}d^{\mathcal{B}}}{(w^{\mathcal{A}}/\rho^{\mathcal{B}}) \cdot (n^{\mathcal{B}}/d'^{\mathcal{B}})}, \end{aligned}$$

where we assume that the CSS codes at levels $i = \pm 1$ of \mathcal{B} (resp. \mathcal{A}) have length $\leq n'^{\mathcal{B}}$ (resp. $\leq n'^{\mathcal{A}}$) and distance $\geq d'^{\mathcal{B}}$.

Theorem 5 provides a way to obtain good larger QLDPC codes from smaller ones. For instance, if $n'^{\mathcal{A}}, k^{\mathcal{A}}, d^{\mathcal{A}} = \Theta(n^{\mathcal{A}})$, $n'^{\mathcal{B}}, k^{\mathcal{B}}, d^{\mathcal{B}}, d'^{\mathcal{B}} = \Theta(n^{\mathcal{B}})$, and if $w^{\mathcal{A}}, w^{\mathcal{B}}, \rho^{\mathcal{B}}$ are all bounded by constants, so that \mathcal{A} and \mathcal{B} have asymptotically good parameters, then Theorem 5 provides a subsystem QLDPC code of length $N = \Theta(n^{\mathcal{A}}n^{\mathcal{B}})$ associated to the product $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$ that also has asymptotically good parameters.

Under stronger conditions on \mathcal{A} and \mathcal{B} , we can also bound the local testability of the product \mathcal{C} ; see the full version [14] for details. A similar result also holds for complexes with arbitrarily many terms, though for simplicity in this paper we use the minimum length complexes that suffice for our purposes. As discussed below, a proof of a similar result for longer complexes can be found in [20].

The proof of Theorem 5 goes by a diagram-chasing argument inspired by [20]. Specifically, [20] proved a related result, which they applied to show good Z -distance (i.e. high weight for logical Z operators) for quantum codes obtained as homological products of chain complexes from high-dimensional expanders [25, 24]. However, [20] did not use subsystem codes, and the X -distance of their product codes was only polylogarithmic in the block length.² Thus after applying a distance-balancing procedure, [20] obtained QLDPC codes of distance $\sqrt{N} \cdot \text{poly}(\log N)$, which only barely surpasses the \sqrt{N} barrier.

If both \mathcal{A} and \mathcal{B} have associated codes with large distance, then Theorem 5 yields a large distance bound on the subsystem product code whenever \mathcal{A} has good (small) locality $w^{\mathcal{A}}$ and \mathcal{B} has good (large) soundness $\rho^{\mathcal{B}}$. At a high level, our proof of Theorem 5 (inspired by [20])

² Such poor X -distance was in part due to the fact that the cochain complexes they considered from high-dimensional expanders have much better distance and expansion properties than the associated chain complexes. However, as [20] did not use subsystem codes, it seems difficult to obtain product codes with close-to-linear distance from their results, even when applied to products of different complexes.

argues that by the Künneth formula, codewords of the product code can be expressed as tensor products of codewords of \mathcal{A} and \mathcal{B} , plus elements in the image of the boundary map $\partial^{\mathcal{C}}$ (i.e. stabilizers). Classical tensor product codes have good distance, so we just need to argue that the distance is not significantly reduced by adding in elements in $\text{im}(\partial^{\mathcal{C}})$. This final step goes by a diagram-chasing argument that bounds the loss in distance in terms of $w^{\mathcal{A}}$ and $\rho^{\mathcal{B}}$; the reader is referred to the full version [14] for more details.

6 Main Result via Iterated Products and Locality Reduction

In Theorem 6 below, we iteratively apply Theorem 5 starting with a constant-sized chain complex from [12, 19] to obtain an infinite family of qLDPC codes with close-to-linear dimension and distance. Below, we view qLDPC codes Q interchangeably with their associated 3-term chain complexes, as described previously.

► **Theorem 6.** *For every $\epsilon > 0$, there exists a constant-sized 5-term chain complex \mathcal{C} and an infinite explicit sequence of qLDPC subsystem codes $(Q_i, L_i)_{i \in \mathbb{N}}$ with parameters*

$$[[N_i, K_i \geq N_i^{1-\epsilon}, D_i \geq N_i^{1-\epsilon}]]_2$$

and locality $w_i = O(1)$, such that each Q_i is obtained by applying the stabilizer-weight-reduction transformation of [15] to the middle 3 terms of the homological product $Q_{i-1} \otimes \mathcal{C}$.

The weight-reduction transformation of [15] provides a means of reducing the locality of a CSS code from a given value w to an absolute constant $O(1)$, at the cost of increasing the code length and decreasing the distance by a factor of $\text{poly}(w)$. We apply this transformation after every application of the homological product because the distance bound in Theorem 5 decays with the locality of \mathcal{A} . Therefore by maintaining constant locality, we are able to inductively maintain a good distance bound in each iteration.

The starting complex in Theorem 6 is a constant-sized instance of the construction of [12, 19], which provides chain complexes whose associated CSS codes are quantum LTCs with nearly optimal asymptotic parameters. As Theorem 6 only needs a constant-sized such starting object \mathcal{C} , it is an interesting question to instantiate it with alternative constructions.

7 Conclusion

In this paper, we provide a new construction of qLDPC codes of almost linear distance. Constructions of such objects were out of reach of known techniques until the breakthrough line of work [16, 28, 8, 27, 22, 11] that developed over the past few years.³ The constructions from these works are based on a sort of balanced product (also called a lifted product) that applies to only certain codes with a particular group symmetry. In contrast, our constructions are based on iterative applications of the more basic homological product, which is generically defined with no group symmetries. Indeed, the classical analogue of our construction, namely iterated tensor products of classical codes, immediately gives classical LDPC codes of close-to-linear distance, and has also been shown to yield properties such as local testability [6, 33].

³ We remark that [15] applies locality reduction to construct qLDPC codes of length N and distance $\tilde{\Omega}(N^{2/3})$. Therefore these codes surpass the “ $\tilde{O}(\sqrt{N})$ distance barrier” (see Section 3), but do not approach linear distance.

It is perhaps surprising that we are able to obtain similar parameters as in the classical case with just homological/tensor products, especially given that for many years, qLDPC codes constructed with similar techniques were not able to achieve distance greater than $\tilde{O}(\sqrt{N})$ (see Section 3). We obtain our distance bounds by combining conceptual insights (e.g. the use of subsystem codes) with certain strong properties of the base code in our iterative construction. Specifically, we assume that the starting code is a constant-sized qLTC. Currently, the only known appropriate such qLTCs, given by [12, 19], are themselves based on balanced products following the line of work described above. We leave it as an interesting direction for future work to find alternative instantiations of the starting code. We also emphasize that the iterative nature of our construction may be of independent interest. Indeed, iterative constructions in the past have led to a number of breakthrough results in pseudorandomness, complexity theory, and coding theory (e.g. [30, 10, 29, 5, 31]), including some cases ([30], [10]) where algebraic constructions ([23, 26], [3, 2]) were previously known.

References

- 1 Anurag Anshu, Nikolas P. Breuckmann, and Chinmay Nirkhe. NLTS Hamiltonians from Good Quantum Codes. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023*, pages 1090–1096, New York, NY, USA, June 2023. Association for Computing Machinery. doi:10.1145/3564246.3585114.
- 2 Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, May 1998. doi:10.1145/278298.278306.
- 3 Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: a new characterization of NP. *J. ACM*, 45(1):70–122, January 1998. doi:10.1145/273865.273901.
- 4 Dave Bacon, Steven T. Flammia, Aram W. Harrow, and Jonathan Shi. Sparse Quantum Codes from Quantum Circuits. *IEEE Transactions on Information Theory*, 63(4):2464–2479, April 2017. arXiv:1411.3334 [quant-ph]. doi:10.1109/TIT.2017.2663199.
- 5 Avraham Ben-Aroya and Amnon Ta-Shma. A Combinatorial Construction of Almost-Ramanujan Graphs Using the Zig-Zag Product. *SIAM Journal on Computing*, 40(2):267–290, January 2011. doi:10.1137/080732651.
- 6 Eli Ben-Sasson and Madhu Sudan. Robust Locally Testable Codes and Products of Codes. In Klaus Jansen, Sanjeev Khanna, José D. P. Rolim, and Dana Ron, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, Lecture Notes in Computer Science, pages 286–297, Berlin, Heidelberg, 2004. Springer. doi:10.1007/978-3-540-27821-4_26.
- 7 Sergey Bravyi and Matthew B. Hastings. Homological product codes. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing, STOC '14*, pages 273–282, New York, NY, USA, May 2014. Association for Computing Machinery. doi:10.1145/2591796.2591870.
- 8 Nikolas P. Breuckmann and Jens N. Eberhardt. Balanced Product Quantum Codes. *IEEE Transactions on Information Theory*, 67(10):6653–6674, October 2021. Conference Name: IEEE Transactions on Information Theory. doi:10.1109/TIT.2021.3097347.
- 9 Nicolas Delfosse and Matthew B. Hastings. Union-Find Decoders For Homological Product Codes. *Quantum*, 5:406, March 2021. Publisher: Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften. doi:10.22331/q-2021-03-10-406.
- 10 Irit Dinur. The PCP theorem by gap amplification. *Journal of the ACM*, 54(3):12-es, June 2007. doi:10.1145/1236457.1236459.
- 11 Irit Dinur, Min-Hsiu Hsieh, Ting-Chun Lin, and Thomas Vidick. Good Quantum LDPC Codes with Linear Time Decoders. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023*, pages 905–918, New York, NY, USA, June 2023. Association for Computing Machinery. doi:10.1145/3564246.3585101.

- 12 Irit Dinur, Ting-Chun Lin, and Thomas Vidick. Expansion of higher-dimensional cubical complexes with application to quantum locally testable codes, April 2024. arXiv:2402.07476 [quant-ph]. doi:10.48550/arXiv.2402.07476.
- 13 Michael Freedman and Matthew Hastings. Building manifolds from quantum codes. *Geometric and Functional Analysis*, 31(4):855–894, August 2021. doi:10.1007/s00039-021-00567-3.
- 14 Louis Golowich and Venkatesan Guruswami. Quantum LDPC Codes of Almost Linear Distance via Homological Products, November 2024. arXiv:2411.03646 [quant-ph]. doi:10.48550/arXiv.2411.03646.
- 15 M. B. Hastings. On Quantum Weight Reduction, July 2023. arXiv:2102.10030 [quant-ph]. doi:10.48550/arXiv.2102.10030.
- 16 Matthew B. Hastings, Jeongwan Haah, and Ryan O’Donnell. Fiber bundle codes: breaking the $n^{1/2} \log(n)$ barrier for Quantum LDPC codes. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2021, pages 1276–1288, New York, NY, USA, June 2021. Association for Computing Machinery. doi:10.1145/3406325.3451005.
- 17 Max Hopkins and Ting-Chun Lin. Explicit Lower Bounds Against $\Omega(n)$ -Rounds of Sum-of-Squares. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 662–673. IEEE Computer Society, October 2022. doi:10.1109/FOCS54457.2022.00069.
- 18 Gleb Kalachev and Pavel Panteleev. Two-sided Robustly Testable Codes, August 2023. arXiv:2206.09973 [cs, math]. doi:10.48550/arXiv.2206.09973.
- 19 Gleb Kalachev and Pavel Panteleev. Maximally Extendable Product Codes are Good Coboundary Expanders, January 2025. arXiv:2501.01411 [cs]. doi:10.48550/arXiv.2501.01411.
- 20 Tali Kaufman and Ran J. Tessler. New cosystolic expanders from tensors imply explicit Quantum LDPC codes with $\Omega(\sqrt{n} \log^k n)$ distance. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2021, pages 1317–1329, New York, NY, USA, June 2021. Association for Computing Machinery. doi:10.1145/3406325.3451029.
- 21 A. Yu. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2–30, January 2003. doi:10.1016/S0003-4916(02)00018-0.
- 22 Anthony Leverrier and Gilles Zémor. Quantum Tanner codes. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 872–883. IEEE Computer Society, October 2022. doi:10.1109/FOCS54457.2022.00117.
- 23 A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, September 1988. doi:10.1007/BF02126799.
- 24 Alexander Lubotzky, Beth Samuels, and Uzi Vishne. Explicit constructions of Ramanujan complexes of type \tilde{A}_d . *European Journal of Combinatorics*, 26(6):965–993, August 2005. doi:10.1016/j.ejc.2004.06.007.
- 25 Alexander Lubotzky, Beth Samuels, and Uzi Vishne. Ramanujan complexes of type \tilde{A}_d . *Israel Journal of Mathematics*, 149(1):267–299, December 2005. doi:10.1007/BF02772543.
- 26 M. Morgenstern. Existence and Explicit Constructions of $q + 1$ Regular Ramanujan Graphs for Every Prime Power q . *Journal of combinatorial theory. Series B*, 62(1):44–62, 1994. Place: SAN DIEGO Publisher: Elsevier Inc. doi:10.1006/jctb.1994.1054.
- 27 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, pages 375–388, New York, NY, USA, June 2022. Association for Computing Machinery. doi:10.1145/3519935.3520017.
- 28 Pavel Panteleev and Gleb Kalachev. Quantum LDPC Codes With Almost Linear Minimum Distance. *IEEE Transactions on Information Theory*, 68(1):213–229, January 2022. Conference Name: IEEE Transactions on Information Theory. doi:10.1109/TIT.2021.3119384.
- 29 Omer Reingold. Undirected connectivity in log-space. *Journal of the ACM*, 55(4):17:1–17:24, September 2008. doi:10.1145/1391289.1391291.
- 30 Omer Reingold, Salil Vadhan, and Avi Wigderson. Entropy Waves, the Zig-Zag Graph Product, and New Constant-Degree Expanders. *The Annals of Mathematics*, 155(1):157, January 2002. doi:10.2307/3062153.

- 31 Amnon Ta-Shma. Explicit, almost optimal, epsilon-balanced codes. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 238–251, Montreal Canada, June 2017. ACM. doi:10.1145/3055399.3055408.
- 32 Jean-Pierre Tillich and Gilles Zemor. Quantum LDPC codes with positive rate and minimum distance proportional to $n^{1/2}$. *IEEE Transactions on Information Theory*, 60(2):1193–1202, February 2014. arXiv:0903.0566. doi:10.1109/TIT.2013.2292061.
- 33 Michael Viderman. A combination of testability and decodability by tensor products. *Random Structures & Algorithms*, 46(3):572–598, 2015. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/rsa.20498>, doi:10.1002/rsa.20498.