Asymptotically Good Quantum and Locally Testable Classical LDPC Codes

Pavel Panteleev
Moscow State University
Russia
panteleev@intsys.msu.ru

Gleb Kalachev
Moscow State University
Russia
kalachev@intsys.msu.ru

ABSTRACT

We study classical and quantum LDPC codes of constant rate obtained by the lifted product construction over non-abelian groups. We show that the obtained families of quantum LDPC codes are asymptotically good, which proves the qLDPC conjecture. Moreover, we show that the produced classical LDPC codes are also asymptotically good and locally testable with constant query and soundness parameters, which proves a well-known conjecture in the field of locally testable codes.

CCS CONCEPTS

• **Theory of computation** → **Error-correcting codes**; **Quantum information theory**.

KEYWORDS

quantum codes, LDPC codes, locally testable codes, expander graphs, chain complexes

ACM Reference Format:
Pavel Panteleev and Gleb Kalachev. 2022. Asymptotically Good Quantum and Locally Testable Classical LDPC Codes. In *Proceedings of the 54rd Annual ACM SIGACT Symposium on Theory of Computing (STOC '22), June 20–24, 2022, Rome, Italy*. ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3519935.3520017

1 INTRODUCTION

Classical low-density parity-check (LDPC) codes [20], as well as their quantum counterparts [38], have many important applications in theory and practice. These codes are represented by sparse parity-check matrices, where the term *sparse* usually means that the corresponding Tanner graphs are of bounded degree. Besides numerous applications in data storage and transmission systems, such codes are often used to construct classical and quantum locally testable codes [1, 17, 32], where the sparseness of a code ensures the constant-query property, also known as the constant locality. Informally speaking, a classical locally testable code (LTC) is a code that comes with an efficient non-deterministic procedure that allows to test with high probability whether a given sequence is close to some codeword by looking at a very small, usually constant, number of randomly chosen bits from this sequence. There are several ways how one can formally define LTCs [21]. In this paper, we adopt a very simple combinatorial definition (see [35, Definition 11]) that implies a rather strong form of local testability. According to this definition, a linear code $C \subseteq \mathbb{F}_q^n$ is called (ω, s)-*locally testable* if it has a parity-check matrix $H \in \mathbb{F}_q^{m\times n}$ with rows of weight at most ω such that for any vector $x \in \mathbb{F}_q^n$ we have

$$\frac{1}{m}|Hx| \geqslant \frac{s}{n} d(x, C),$$

where $d(x, C) := \min_{c\in C} d(x, c)$, and we denote by $d(\cdot,\cdot)$ and $|\cdot|$ the Hamming distance and the Hamming weigh. The parameters ω and s are positive real numbers called the *locality* and *soundness*, respectively. As we already mentioned above, this definition implies a strong form of local testability. Indeed, if our test procedure picks uniformly at random a row from H and finds the corresponding syndrome component, then the probability of rejection $\mathrm{rej}_H(x) = \frac{1}{m}|Hx|$ grows *at least* linearly with the *normalized minimum distance* $\delta(x, C) := \frac{1}{n}d(x, C)$ from the tested vector $x \in \mathbb{F}_q^n$ to the code C. In fact, for any family of LDPC codes with $m = \Theta(n)$ where the the weights of rows and columns in H are bounded from above by ω (such codes are called ω-*limited*), it follows that $\frac{1}{m}|Hx|$ can not grow *more* than linearly with $\delta(x, C)$ since for every $x \in \mathbb{F}_q^n$ we get $|Hx| \leqslant \omega \cdot d(x, C)$.

In the case of quantum locally testable codes (qLTCs) introduced in [1], one can give a similar to the above definition if a sparse parity-check matrix H is replaced by a local Hamiltonian $\mathcal{H}$ defining the quantum code. However, for a quantum CSS code Q (see [9, 46]), obtained from a pair of classical codes C_X and C_Z, it is possible [1, 35] to infer the local testability of Q from the local testability of C_X and C_Z. Let us recall that a quantum CSS code Q of *dimension* k is defined by a pair of classical linear codes $C_X, C_Z \subseteq \mathbb{F}_q^n$ such that $C_Z^\perp \subseteq C_X$, and $k = \dim C_X/C_Z^\perp$. Its *minimum distance* d is defined as $\min(d_X, d_Z)$, where d_X and d_Z are the minimal Hamming weights of the vectors from $C_X \setminus C_Z^\perp$ and $C_Z \setminus C_X^\perp$, respectively. In this case, we often say that Q is an $[\![n, k, d]\!]_q$ code. The codes C_X, C_Z are usually represented respectively by parity-check matrices H_X, H_Z, and the condition $C_Z^\perp \subseteq C_X$ is equivalent to $H_X H_Z^* = 0$, where H_Z^* is the transpose of H_Z. It was shown in [35, Lemma 13] that if a CSS code Q is defined by two classical (ω, s)-locally testable codes with parity-check matrices H_X, H_Z, then the quantum code Q is (ω, s')-locally testable, where $s' := s \min\left(\frac{m_X}{m_X+m_Z}, \frac{m_Z}{m_X+m_Z}\right)$, and m_X (resp. m_Z) is the number of rows in the matrix H_X (resp. H_Z).

Classical and quantum LTCs have many interesting applications in theoretical computer science since they are intimately related to a number of important problems in complexity theory [1, 14].

STOC '22, June 20–24, 2022, Rome, Italy

ACM ISBN 978-1-4503-9264-8/22/06…$15.00
https://doi.org/10.1145/3519935.3520017

A major open problem is whether there are such codes of *constant* locality ω, *constant* rate, and *constant* normalized minimum distance, sometimes also known as the c^3*-conjecture* (in the context of classical codes [13]) and *qLTC conjecture* (in the quantum case [1]). In this respect, the situation for classical LTCs is much better than for their quantum counterparts since classical LTCs with almost optimal parameters have been known for a long time [22]. However, in the quantum case, even if the property of local testability is not required, it is still a widely open problem, known as the *qLDPC conjecture* [7], to obtain an *asymptotically good* family of quantum LDPC (qLDPC) codes[1], i.e., with the constant rate and normalized minimum distance. Up until very recently [6, 26, 27, 44], the best provable lower bounds on the distances of qLDPC codes were, up to polylogarithmic factors, at most of the order $\sqrt{n}$ as the number of qubits $n \to \infty$ [12, 18, 19, 23, 33, 48]. At the same time, asymptotically good families of classical LDPC codes have been known since their introduction by Robert Gallager in the 1960s [20].

In the current work, we show the existence of classical LTCs of constant rate, constant locality, and constant normalized minimum distance. In particular, we prove the following theorem, which gives a positive answer to the c^3-conjecture. Let us recall that a classical linear code $C \subseteq \mathbb{F}_q^n$ has the parameters $[n, k, d]_q$ if $k = \dim C$ and $d = \min_{c \in C \setminus \{0\}} |c|$.

Theorem 1. *For every number $R \in (0, 1/2)$ and finite field $\mathbb{F}_q$ it is possible to find universal constants s and ω such that there exists an explicit family of (ω, s)-locally testable classical LDPC codes with the parameters $[n, k \geqslant Rn, d = \Theta(n)]_q$ as $n \to \infty$.*

In the quantum case, we obtained a somewhat weaker analog of the above theorem, given below, which shows the existence of asymptotically good families of qLDPC codes, not necessarily the locally testable ones. This gives an affirmative answer to the qLDPC conjecture.

Theorem 2. *For every number $R \in (0, 1)$ and finite field $\mathbb{F}_q$ there exists an explicit family of quantum LDPC codes over $\mathbb{F}_q$ with the parameters $[\![n, k \geqslant Rn, d = \Theta(n)]\!]_q$ as $n \to \infty$.*

Remark 1. In the case of classical codes from Theorem 1, it is relatively easy to show that an algorithm, similar to the bit-flipping algorithm, corrects in linear time any error of weight up to the constant fraction of the code length n. As for the quantum codes from Theorem 2, we conjecture that it is also possible with a variant of the small-set-flip decoding algorithm from [36] (see also [18]).

The codes from the above two theorems are obtained using the recently introduced lifted product construction [44], which can be seen as a generalization of the (tensor) product construction for classical codes [3, 39] and the hypergraph product construction for quantum codes [49]. This product operation was also given in a more general form in [6] and connected to the balanced product operation from topology. These constructions are best understood in terms of homological algebra[2].

[1]Note that if one goes beyond the standard definition of a quantum LDPC code then codes with very good parameters were already known to exist [2, 4].

[2]In this text, we assume that the reader is familiar with the standard notions of homological algebra such as a (co)chain complex and (co)homology groups. See [8] for a short introduction into this subject.

1.1 Chain complexes and codes

In recent years, ideas from homological algebra found many interesting applications in the field of classical and quantum codes[5, 31, 52]. Let us briefly recall that a *chain complex* is an abelian group $C = \bigotimes_{i \in \mathbb{Z}} C_i$ with some fixed morphism $\partial \colon C \to C$ called the *boundary map* such that $\partial^2 = 0$ and $\partial C_i \subseteq C_{i-1}$ for all $i \in \mathbb{Z}$. A complex (C, ∂) is usually represented by a sequence

$$\cdots \xrightarrow{\partial_{i+1}} C_i \xrightarrow{\partial_i} C_{i-1} \xrightarrow{\partial_{i-1}} \cdots$$

of abelian groups C_i and morphisms[3] $\partial_i := \partial|_{C_i} \colon C_i \to C_{i-1}$ such that $\partial_i \circ \partial_{i+1} = 0$ for all $i \in \mathbb{Z}$. The term C_i in a complex C is called the group of *i-chains* and the assertion $\partial_i \circ \partial_{i+1} = 0$ is equivalent to $\operatorname{im} \partial_{i+1} \subseteq \ker \partial_i$, which allows us to consider for every $i \in \mathbb{Z}$ the quotient group $H_i(C) = \ker \partial_i / \operatorname{im} \partial_{i+1}$ called the *i-th homology group* of the complex C. The elements from $Z_i(C) := \ker \partial_i$ and $B_i(C) := \operatorname{im} \partial_{i+1}$ are called the *i-cycles* and *i-boundaries* of C, respectively. The abelian groups in a complex often come with some additional algebraic structure that makes them vector spaces over a field $\mathbb{F}$ or modules over a ring R, in which case it is further assumed that all boundary maps are linear maps.

In the context of error correcting codes, we are interested in chain complexes C over $\mathbb{F}_q$ with τ non-zero terms (τ*-term* complexes), where each term C_i is *based*, i.e., comes with a distinguished basis $X_i \subseteq C_i$ over $\mathbb{F}_q$, which elements are called *i-cells*. In many cases it is convenient to consider i-chains $c \in C_i$ as formal $\mathbb{F}_q$-linear combinations

$$c = \sum_{x \in X_i} c_x x$$

of i-cells and identify C_i with $\mathbb{F}_q^{n_i}$, where $n_i := |X_i|$. Note that any space of formal linear combinations $\mathbb{F}_q S \cong \mathbb{F}_q^S$ is equipped with the standard *inner product* $\langle a, b \rangle := \sum_{s \in S} a_s b_s$ and the *Hamming norm* $|a| := |\operatorname{supp} a|$, where $\operatorname{supp} a := \{s \in S \mid a_s \neq 0\}$. We usually interpret terms in such chain complexes either as the space of code symbols or parity-checks of the code.

It is convenient to consider the set $X = \bigsqcup_i X_i$ as a graded poset called the *cell poset* of $C = \mathbb{F}_q X$. Let P be a poset with a partial order $\leqslant$. We say that an element $a \in P$ *covers* an element $b \in P$ and write $a \succ b$ or $b \prec a$ if $a < b$, and there is no element $c \in P$ such that $a < c < b$. It is easy to see that any finite poset can be uniquely defined by its covering relation $\prec$ if we let $a \leqslant b$ **iff** there exists a sequence $c_0 \prec c_1 \prec \cdots \prec c_n$ of elements from P such that $c_0 = a$, $c_n = b$, and $n \geqslant 0$. We can define the partial order $\leqslant$ on the distinguished basis X if for every two cells $x, x' \in X$ we put $x' \prec x$ **iff** $x' \in \operatorname{supp} \partial x$. We call the poset X with the relation $\leqslant$ the *cell poset of C*. This poset comes with a natural *grading function* $\rho \colon X \to \mathbb{Z}$ defined as $\rho(x) := i$ if $x \in X_i$, and the sets X_i are called *levels* of X. In many cases, the elements of X can be interpreted as some geometrical objects (points, edges, etc.), and the grading corresponds to their dimension.

Remark 2. In this work, we also view an undirected graph Γ as the graded poset with the levels $V(\Gamma)$ and $E(\Gamma)$, where for every $v \in V(\Gamma)$ and $e \in E(\Gamma)$ we have $v \prec e$ whenever v is incident to e. In fact, 2-level posets are equivalent to the *incidence systems*, and thus

[3]Sometimes when it does not cause confusion we omit the indexes in the boundary maps ∂_i and simply write ∂ instead of ∂_i.

can be used to represent undirected multigraphs and hypergraphs as well.

We can visualize a τ-term complex C by the labeled τ-partite graph $\mathcal{T}$ called its *Tanner graph*, where X_i is the set of vertices of the i-th part, and we have an edge (x, x') labeled by the element $a = \langle x', \partial x\rangle \in \mathbb{F}_q$ whenever $x \succ x'$. One can easily see that $\mathcal{T}$ is just the Hasse diagram of the cell poset X.

Consider several examples. First, we can identify a 2-term chain complex

$$\mathbb{F}_q^n \xrightarrow{\partial_1} \mathbb{F}_q^m$$

with the classical linear code $\ker \partial_1$ defined by the *parity-check matrix* $H := \partial_1$. Here, the space $\mathbb{F}_q^n$ of 1-chains corresponds to the n bits, while the space $\mathbb{F}_q^m$ of 0-chains to the m checks. At the same time, a 3-term chain complex

$$C := \left(\mathbb{F}_q^{m_Z} \xrightarrow{\partial_2} \mathbb{F}_q^n \xrightarrow{\partial_1} \mathbb{F}_q^{m_X}\right)$$

can be naturally identified with the quantum CSS $[\![n, k, d]\!]_q$ code $Q = Q(H_X, H_Z)$ defined by the parity-check matrices $H_X := \partial_1$ and $H_Z := \partial_2^*$, where $\partial_2^* \colon \mathbb{F}_q^n \to \mathbb{F}_q^{m_Z}$ is the transpose of the map $\partial_2 \colon \mathbb{F}_q^{m_Z} \to \mathbb{F}_q^n$. In this case, the space $\mathbb{F}_q^n$ of 1-cells corresponds to the n qubits, and the space $\mathbb{F}_q^{m_X}$ of 0-cells (resp. the space $\mathbb{F}_q^{m_Z}$ of 2-cells) to the X-*checks* (resp. Z-*checks*). The length of Q is equal to $n = \dim \mathbb{F}_q^n$, while its dimension k is equal to the dimension of the first homology group $H_1(C) := \ker \partial_1 / \operatorname{im} \partial_2 = C_X / C_Z^\perp$, where $C_X := \ker \partial_1$ and $C_Z := \ker \partial_2^*$. The minimum distance $d = d(Q)$ can also be described in the language of homology groups if we consider the quotient vector space $H_1(C)$ as a metric space, where the distance $d(A, B)$ between homology classes $A, B \in H_1(C)$ is defined as $d(A, B) := |A - B|$ using the quotient Hamming norm $|A| := \min_{a \in A} |a|$. It is easy to see that $d = \min(d(H_1(C), d(H_1(C^*))$, where

$$C^* := \left(\mathbb{F}_q^{m_X} \xrightarrow{\partial_1^*} \mathbb{F}_q^n \xrightarrow{\partial_2^*} \mathbb{F}_q^{m_Z}\right)$$

is the *dual chain complex* for C. Note that the distances $d(H_1(C))$ and $d(H_1(C^*))$ are sometimes called the 1-*systolic* and 1-*cosystolic distances* of C.

1.2 Lifted product

In this work, we consider several new families of classical and quantum LDPC codes of constant rate based on the introduced recently lifted product construction [44], which generalizes many known constructions of quantum LDPC codes [24, 25, 34, 38, 49, 52]. The main idea of the lifted product in its general form (see [44, p. 3]) is to extend the standard tensor product $\mathcal{A} \otimes_{\mathbb{F}_q} \mathcal{B}$ of two chain complexes $\mathcal{A}$ and $\mathcal{B}$ over $\mathbb{F}_q$ to a more general product $\mathcal{A} \otimes_R \mathcal{B}$ where $\mathcal{A}, \mathcal{B}$ are free R-modules[4], and $R = \mathbb{F}_q G$ is the group algebra[5] over $\mathbb{F}_q$ for some finite group G.

The idea of the lifted product was used recently in [44] to obtain the first family of qLDPC codes with almost linear distance. In the follow-up paper [6], where some of the ideas from [44] were developed independently, a very similar construction called *balanced product* was used to get qLDPC codes of very large distances[6]. As in the case of lifted product, the balanced product of two chain complexes $\mathcal{A}$ and $\mathcal{B}$ can also be considered as the tensor product complex $\mathcal{A} \otimes_R \mathcal{B}$ over the the group algebra $R = \mathbb{F}_q G$, but this time $\mathcal{A}$ and $\mathcal{B}$ are arbitrary (i.e., not necessary free) R-modules. As it was shown in [6], the G-lifted product and the balanced product can both be viewed as instances of even more general topological idea called a *fiber bundle*, proposed as a way to construct qLDPC codes in the breakthrough paper [27], which first broke the $n^{1/2}\mathrm{polylog}(n)$ barrier on the distance of qLDPC codes. It is also interesting to note that the codes that were actually used to get the main results in [6, 27, 44] are from a more restricted class of lifted product codes, which were previously studied in [43] under the name GHP codes and shown to have surprisingly good practical error-correcting performance under the BP-OSD decoder.

Definition 1 (lifted product)**.** Suppose we have a finite group G. Consider two chain complexes $\mathcal{A} = \bigoplus_{i=0}^m \mathcal{A}_i$ and $\mathcal{B} = \bigoplus_{j=0}^n \mathcal{B}_j$ over $\mathbb{F}_q$ such that the vector spaces $\mathcal{A}_i$ and $\mathcal{B}_j$ are also free R-modules[7] for $R = \mathbb{F}_q G$, and the boundary maps $\partial_{\mathcal{A}} \colon \mathcal{A} \to \mathcal{A}$, $\partial_{\mathcal{B}} \colon \mathcal{B} \to \mathcal{B}$ are R-linear. The *lifted product* of $\mathcal{A}$ and $\mathcal{B}$ over R is their *tensor product complex* $\mathcal{A} \otimes_R \mathcal{B}$ (see [8, p. 7]), where for $k = 0, 1, \ldots, m + n$ the space of k-chains $(\mathcal{A} \otimes_R \mathcal{B})_k$ is equal to $\bigoplus_{i+j=k} \mathcal{A}_i \otimes_R \mathcal{B}_j$, while the boundary map $\partial \colon \mathcal{A} \otimes_R \mathcal{B} \to \mathcal{A} \otimes_R \mathcal{B}$ is defined for $a \in \mathcal{A}_i$, $b \in \mathcal{B}_j$ as[8]

$$\partial(a \otimes_R b) := \partial_{\mathcal{A}} a \otimes_R b + (-1)^i a \otimes_R \partial_{\mathcal{B}} b, \tag{1}$$

and extended by linearity.

Remark 3. Lifted product can also be used with arbitrary finite-dimensional associative algebra R over $\mathbb{F}_q$, not necessary equal to $\mathbb{F}_q G$. The condition that the vector spaces $\mathcal{A}_i$ and $\mathcal{B}_j$ over $\mathbb{F}_q$ are free $\mathbb{F}_q G$-modules is equivalent to the condition that the group G acts freely[9] on their bases over $\mathbb{F}_q$ (from the right for $\mathcal{A}_i$ and from the left for $\mathcal{B}_j$). Moreover, the boundary map ∂ is $\mathbb{F}_q G$-linear **iff** it is an $\mathbb{F}_q$-linear map that commutes with the action of the group G. In the current paper, if $R = \mathbb{F}_q G$ we call this operation *lifted product over* G or G-*lifted product* and denote the complex $\mathcal{A} \otimes_R \mathcal{B}$ by $\mathcal{A} \otimes_G \mathcal{B}$ and $a \otimes_R b$ by $a \otimes_G b$, which is consistent with the notation for balanced products introduced in [6].

Remark 4. When $\mathcal{A}_i$ and $\mathcal{B}_j$ come respectively with distinguished bases X_i and Y_j we assume that these bases are invariant under the action of G. In such cases, by definition, the lifted product complex $\mathcal{A} \otimes_G \mathcal{B}$ has the distinguished basis (over $\mathbb{F}_q$) given by

$$X \times_G Y := \{x \otimes_G y \mid x \in X, y \in Y\},$$

where $X := \bigsqcup_i X_i$, $Y := \bigsqcup_j Y_j$. Hence the basis for the space of k-chains $(\mathcal{A} \otimes_G \mathcal{B})_k$ is $\bigsqcup_{i+j=k} X_i \times_G Y_j$. Recall that if we have a free

[4] The general definition of the *tensor product complex* $\mathcal{A} \otimes_R \mathcal{B}$ over an arbitrary ring R can be found in [8, p. 7].

[5] The elements of $\mathbb{F}_q G$ are formal sums $\sum_{g \in G} \alpha_g g$, where $\alpha_g \in \mathbb{F}_q$. For elements $a = \sum_{g \in G} \alpha_g g$ and $b = \sum_{g \in G} \beta_g g$ from $\mathbb{F}_q G$ their sum $a + b$ and product ab are defined as follows: $a + b := \sum_{g \in G} (\alpha_g + \beta_g) g$, $\quad ab := \sum_{g \in G} \left(\sum_{hr = g} \alpha_h \beta_r\right) g$.

[6] Note that the codes from [44] are CSS codes, while the codes from [6] are in general from a wider class of quantum codes called *subsystem codes*.

[7] If G is not abelian, then we further assume that $R = \mathbb{F}_q G$ acts from the right on $\mathcal{A}$ and from the left on $\mathcal{B}$, i.e., $\mathcal{A}$ is a right free R-module, and $\mathcal{B}$ is a left free R-module.

[8] We should note that the sign $(-1)^i$ in this definition is only relevant in the case of finite fields of odd characteristic.

[9] A *left* (resp. *right*) action of a group G on a set S is called *free* if for every $g \in G$ when we have $gs = s$ (resp. $sg = s$) for some $s \in S$, then g is the identity element of G. Note that the sizes of all orbits of a free action are the same and equal to $|G|$.

action of a group G on a set S, then the size of each orbit is equal to $|G|$, and we can identify S with $(S/G) \times G$, where S/G is the set of all orbits under the action of G. Therefore since the action of G on X and Y is free, and for every $g \in G$ we have $xg \otimes_G y = x \otimes_G gy$, one can identify $X \times_G Y$ with the set $(X/G) \times G \times (Y/G)$.

Remark 5. If the sets X and Y are respectively the cell posets for $\mathcal{A} = \mathbb{F}_q X$ and $\mathcal{B} = \mathbb{F}_q Y$, then one can easily check using (1) that the set $X \times_G Y$ is the cell poset for $\mathcal{A} \otimes_G \mathcal{B} = \mathbb{F}_q X \times_G Y$, where the covering relation $\succ$ for $X \times_G Y$ is defined as follows: we have $(x, g, y) \succ (x', g', y')$ **iff** either $x = x'$ and $(y, g) \succ_Y (y', g')$ or $(x, g) \succ_X (x', g')$ and $y = y'$.

As one can see, the above definition of the partial order on $X \times_G Y$ can be applied to any finite posets X and Y with a free action of G. In the current work, we apply it in the case when X and Y are 2-level posets representing graphs (see Remark 2 and Section 2.1).

Remark 6. If the sets X and Y represent cellulations of some topological spaces M and N, then $X \times_G Y$ represents the cellulation of their balanced product[10] $M \times_G N$ (see [6]).

Remark 7. If G acts on a vector space we say that it is a *G-module*. For any chain complex C we can consider its *dual chain complex* C^* obtained from C if we replace the boundary map ∂ of C by its transpose map ∂^*. It is not hard to see that if C is a left (resp. right) G-module, then C^* is a right (resp. left) G-module. Therefore if chain complexes $\mathcal{A}$ and $\mathcal{B}$ are right G-modules, we can consider the lifted product $\mathcal{A} \otimes_G \mathcal{B}^*$. In fact, for any set S with a left action $(g, s) \mapsto g \cdot s$ (resp. a right action $(s, g) \mapsto s \cdot g$) of a group G we can also consider the corresponding right (resp. left) action of G defined as $(s, g) \mapsto g^{-1} \cdot s$ (resp. $(g, s) \mapsto s \cdot g^{-1}$). Therefore if a group G has a right free action on a chain complex C, then it also has the corresponding left free action on C, and vice versa. This allows us to apply G-lifted product $\mathcal{A} \otimes_G \mathcal{B}$ to two right G-modules $\mathcal{A}$ and $\mathcal{B}$, if we use the corresponding left action of G on $\mathcal{B}$.

Given two classical linear codes invariant under a free action of a group G on their index sets[11], we can represent them by 2-term chain complexes $\mathcal{A}\colon R^{n_a} \xrightarrow{A} R^{m_a}$ and $\mathcal{B}\colon R^{n_b} \xrightarrow{B} R^{m_b}$ over the group algebra $R = \mathbb{F}_q G$, where $A \in R^{m_a \times n_a}$, $B \in R^{m_b \times n_b}$ are the corresponding parity-check matrices[12]. The lifted product $C = \mathcal{A} \otimes_G \mathcal{B}$ is the 3-term complex

$$R^{n_a \times n_b} \xrightarrow{\partial_2} R^{n_a \times m_b} \oplus R^{m_a \times n_b} \xrightarrow{\partial_1} R^{m_a \times m_b}$$

with the boundary map $\partial\colon C \to C$ given by the following diagram

$$\begin{array}{ccc} R^{n_a \times m_b} & \xrightarrow{A \otimes_R \mathrm{id}} & R^{m_a \times m_b} \\ {\scriptstyle -\mathrm{id} \otimes_R B}\uparrow & & \uparrow{\scriptstyle \mathrm{id} \otimes_R B}, \\ R^{n_a \times n_b} & \xrightarrow[A \otimes_R \mathrm{id}]{} & R^{m_a \times n_b} \end{array}$$

which means that $\partial_2 := \begin{bmatrix} -\mathrm{id} \otimes_R B \\ A \otimes_R \mathrm{id} \end{bmatrix}$, $\partial_1 := [A \otimes_R \mathrm{id}, \mathrm{id} \otimes_R B]$. One can easily check that $\partial_1 \circ \partial_2 = A \otimes_R B - A \otimes_R B = 0$, and C is indeed a chain complex. Now we can consider the classical code $\ker \partial_2$ with the parity-check matrix ∂_2 and the quantum CSS code $Q(\partial_1, \partial_2^*)$ where $C_X := \ker \partial_1$ and $C_Z := \ker \partial_2^*$. We can naturally identify these codes with the second homology group $H_2(C)$ and the first homology group $H_1(C)$ of the complex C, and we use them to obtain the classical codes from Theorem 1 and the quantum ones from Theorem 2, respectively. Note that when G is a trivial group, i.e., $|G| = 1$, then $R \cong \mathbb{F}_q$, and one can see that $\ker \partial_2$ and $Q(\partial_1, \partial_2^*)$ are respectively the tensor product and the hypergraph product of the two classical codes $\ker A$ and $\ker B$. Hence the lifted product complex $\mathcal{A} \otimes_G \mathcal{B}$, which we also sometimes denote by $\mathrm{LP}(A, B)$, can be seen as a generalization of these two constructions, where instead of individual symbols from $\mathbb{F}_q$ we have blocks of $|G|$ symbols represented by elements from $\mathbb{F}_q G \cong \mathbb{F}_q^{|G|}$.

1.3 Expander codes and their products

A very important ingredient of the constructions from [6, 44] is expander codes [45], which are the Tanner codes [47] obtained from spectral expander graphs. The individual symbols of the expander code $\mathcal{T}(\Gamma; h)$ defined for a w-regular graph Γ and a parity-check matrix $h \in \mathbb{F}_q^{r \times w}$ are assigned to the edges of Γ, and we get a codeword precisely when for each vertex v from Γ the symbols assigned to the edges connected to v give a codeword of the *local code* $\ker h$.

We usually identify the code $\mathcal{T}(\Gamma; h)$ with the complex

$$\mathbb{F}_q E(\Gamma) \xrightarrow{\partial} \mathbb{F}_q^r V(\Gamma),$$

where ∂ is its parity-check matrix. Here $\mathbb{F}_q E(\Gamma) \cong \mathbb{F}_q^{E(\Gamma)}$ and $\mathbb{F}_q^r V(\Gamma) \cong (\mathbb{F}_q^r)^{V(\Gamma)}$ are respectively the spaces of formal linear combinations of the edges (over $\mathbb{F}_q$) and the vertices (over $\mathbb{F}_q^r$), which we can also view as vector spaces over $\mathbb{F}_q$.

In [44] expander graphs Γ are obtained as *G-lifts* (i.e., regular $|G|$-fold covers) of some small base graphs, where G is a very large group[13]. Recall that a (left)*G-lift* (also called *regular $|G|$-fold cover*) of a *base graph*[14] Γ with some fixed order $<$ of vertices is a graph $\hat{\Gamma}$ obtained if we replace in the base graph each vertex $v \in V(\Gamma)$ with $|G|$ replicas $\hat{v}_g, g \in G$, and replace each edge $e \in E(\Gamma)$ connecting vertices $v, v' \in V(\Gamma)$ where $v < v'$ with $|G|$ replicas $\hat{e}_g, g \in G$, such that $\hat{e}_g$ connects in $\hat{\Gamma}$ the vertices $\hat{v}_g$ and $\hat{v}'_{sg}$, where $s = s(v, v') \in G$.

Every left G-lifted graph $\hat{\Gamma}$ is naturally equipped with a free right action defined as $\hat{v}_g \cdot h := \hat{v}_{gh}$, $\hat{e}_g \cdot h := e_{gh}$ for $h \in G$. It is not hard to see that the obtained in this way expander codes $\mathcal{T}(\Gamma; h)$ are invariant under the free action of G. Let us denote the class of such G-invariant expander codes for a given G-lifted graph $\hat{\Gamma}$ and parity-check matrix h by $\mathfrak{T}_G(\Gamma; h)$. Therefore such codes can be used with the G-lifted product to obtain a 3-term chain complex C, which can also be considered as a quantum CSS code.

It is shown in [44, Example 3] that using a G-lifted product of two classical codes it is possible to obtain qLDPC codes of constant rate[15]. In particular, if $\rho := 1 - m/n$ is the design rate of a classical code $\ker A$ represented by the complex $\mathcal{A} := R^n \xrightarrow{A} R^m$, then

[10] The *balanced product* of two topological spaces X and Y with a group G acting on the right on X and on the left on Y is the quotient space $X \times_G Y := X \times Y/\sim$, where the equivalence relation $\sim$ is induced by $(xg, y) \sim (x, gy)$ for $x \in X$, $y \in Y$, $g \in G$.

[11] A classical linear code $C \subseteq \mathbb{F}_q^n$ is *invariant* under an action of a group G on the index set $[n]$ if for every $g \in G$ and $(c_i)_{i \in [n]} \in C$ it follows that $(c_{\pi_g(i)})_{i \in [n]} \in C$, where π_g is the permutation corresponding to the action of g on $[n]$.

[12] If G is non-abelian then when we multiply a vector over $R = \mathbb{F}_q G$ by the matrix A (resp. B), we assume that we multiply by the elements from R from the right (resp. from the left).

[13] In [44] this general idea was applied to cyclic groups to obtain the main result.

[14] In the current paper, we allow in the base graph Γ multiple edges but *not* loops.

[15] A similar observation about balanced products is also made (without a proof) in [6].

the rate of the quantum code represented by $\mathcal{A} \otimes_G \mathcal{A}^*$ is at least $\frac{(n-m)^2}{n^2+m^2} = \frac{\rho^2}{1+(1-\rho)^2}$. Here $\mathcal{A}^* := R^m \xrightarrow{A^*} R^n$ is the *dual chain complex* for $\mathcal{A}$, i.e., A^* is the transpose of the parity-check matrix A, considered as a matrix over $\mathbb{F}_q$. Hence the rate of the quantum codes obtained from $\mathcal{A} \otimes_G \mathcal{A}^*$ can be arbitrary close to 1 as $\rho \to 1$. Moreover, some particular examples of such codes [44, Example 4], indicate that they may also have very large minimal distances, close to the distances of the classical codes $\ker A$ used in the lifted product. However, if the group G is abelian, then the upper bound on the minimum distance of such classical codes [44, Eq. 24] provides strong evidence that to obtain an asymptotically good family of qLDPC codes by a G-lifted product one has to use non-abelian groups.

One particular construction of balanced product codes, analogous to the aforementioned G-lifted product $\mathcal{A} \otimes_G \mathcal{A}^*$, for non-abelian group G, was conjectured in [6] to give an asymptotically good family of qLDPC codes. Unfortunately, our proof strategy does not work for complexes $\mathcal{A} \otimes_G \mathcal{A}^*$, and we can not prove this conjecture with the methods developed here. Instead, we consider similar complexes $\mathcal{A} \otimes_G \mathcal{B}^*$, where 2-term complexes $\mathcal{A}$ and $\mathcal{B}$ correspond respectively to expander codes $\mathcal{T}(\Gamma; h)$ and $\mathcal{T}(\Gamma; h')$ defined for the *same* expander graph Γ but for *different* local codes $\ker h$ and $\ker h'$. It is very simple to show by counting the number of the code symbols and parity-checks in the classical code $\ker \partial_2$ and the quantum code $\mathcal{Q}(\partial_1, \partial_2^*)$ obtained from $\mathcal{A} \otimes_G \mathcal{B}^*$ that these codes have constant rate. However, for our proof of Theorems 1 and 2 to work, the pair of local codes used in $\mathcal{A} \otimes_G \mathcal{B}^*$ can not be arbitrary and should satisfy some special property we call *product-expansion*, which is similar to the *robust testability* property often used in the context of LTCs [3, 16]. We prove that a pair of random linear codes has the product-expansion property with high probability.

1.4 Double covers of Cayley graphs

Informally speaking, the product-expansion property is the *local* property of the complex $\mathcal{A} \otimes_G \mathcal{B}^*$ playing a role similar to the role of the minimal distance of the local codes in the classical proof of Sipser and Spielman [45] that expander codes have linear minimum distances. However, to get the main result we also use the *global* property of $\mathcal{A} \otimes_G \mathcal{B}^*$ related with the *small set expansion*[16] of the graph Γ from the expander codes $\mathcal{T}(\Gamma; h)$ and $\mathcal{T}(\Gamma; h')$. Our main technical result (Proposition 1) shows that the general construction $\mathcal{A} \otimes_G \mathcal{B}^*$ can be used with an arbitrary regular graph Γ obtained as a G-lift of a loop-free base graph if Γ is a sufficiently good small set expander. We prove that spectral expander graphs and their finite covers are good small set expanders. Hence we can let the graph Γ to be the bipartite double-cover of a Cayley graph for some finite group G. Let us remind that, given a finite group G with some symmetric generating set S (i.e. $S = \{s^{-1} \mid s \in S\}$), the corresponding (*left*) *Cayley graph* is the simple graph $\mathrm{Cay}(G, S)$ with the set of vertices $V(\Gamma) := G$ and the set of edges $E(\Gamma) := \{\{g, sg\} \mid g \in G, s \in S\}$. The bipartite double-cover of $\mathrm{Cay}(G, S)$ is the graph $\mathrm{Cay}_2(G, S)$ with the set of vertices $V(\Gamma) := G \times \{0, 1\}$ and the set of edges: $E(\Gamma) := \{\{(g, 0), (sg, 1)\} \mid g \in G, s \in S\}$.

[16] Informally, a graph is a *small set expander* if for every sufficiently small set of vertices S almost all edges connected to it goes outside of S (see Subsection 3.2 for the details).

Note that we have a free right action of the group G on $\mathrm{Cay}_2(G, S)$ defined as $(g, a)t := (gt, a)$ and $\{(g, 0), (sg, 1)\}t := \{(gt, 0), (sgt, 1)\}$, where $g, t \in G$, $s \in S$, and $a \in \{0, 1\}$. This is important for the G-lifted product construction since we need a classical code invariant under a free action of G. Let us fix a parity-check matrix $h \in \mathbb{F}_q^{r \times w}$ and a generating set $S = \{s_1, \ldots, s_w\}$. We can define the expander code $\mathcal{T}(\Gamma; h)$ for $\Gamma = \mathrm{Cay}_2(G, S)$ by its 2-term complex $\mathbb{F}_q E(\Gamma) \xrightarrow{\partial} \mathbb{F}_q^r V(\Gamma)$, where for every $e = \{(g, 0), (s_i g, 1)\} \in E(\Gamma)$ and $i \in [w]$ we put

$$\partial e = h_i \cdot (g, 0) + h_i \cdot (s_i g, 1).$$

Hence, given any Cayley graph, we can get the expander code $\mathcal{T}(\Gamma; h)$ with a free action of G. In our proof we apply this idea (see Example 1) to the Ramanujan Cayley graphs [37, 40], which were also used in the original construction of the expander codes [45] and in the mentioned earlier conjecture from [6].

The main technical tool in our proof of Theorems 1 and 2 is the notion of a *locally minimal* (co)chain, often used in the context of high-dimensional expanders to show expansion properties in simplicial complexes [30]. It is known that such expansion properties can be used to show local testability of a classical code [31] and to give a lower bound on the minimum distance of a quantum code [18]. In the current work, we extend these ideas to a much more general context of (co)chain complexes with local system of coefficients, which can be considered as high-dimensional analogs of the Tanner codes, similar to the ones studied in [41]. Instead of graphs such generalized Tanner codes are defined on high-dimensional complexes, which are usually formally represented by graded posets. Since the G-lifted product is defined for arbitrary complexes, it can naturally be applied to graphs, viewed as 1-dimensional complexes. If we consider graphs Γ and Γ' as topological spaces, their G-lifted product (as a topological space) can be viewed as the balanced product $\Gamma \times_G \Gamma'$ of these spaces [6]. In fact, it can be shown that the products $\Gamma \times_G \Gamma'$ are examples of a well-known class of 2-dimensional complexes called *complete square complexes* [50]. The defining property of a complete square complex is that the links of all its vertices are isomorphic to a *complete* bipartite graph. Since complete bipartite graphs are perfect expanders, then, in some sense, this property is analogous to the well-known property of high-dimensional expanders to have links that are good expanders [30].

Using the discussed above G-lifted products of expander codes over non-abelian groups G we show that it is possible to obtain qLDPC codes with the parameters as in Theorem 2. This gives a positive answer to the questions posed in [44, Conclusion] and in [6, Conjecture] of whether respectively lifted and balanced products of classical codes can give an asymptotically good family of qLDPC codes. Moreover, we also show that, under some additional assumptions, if H_X and H_Z are the parity-check matrices of such qLDPC codes, then the classical code $\ker H_Z^*$ is locally testable with the parameters as in Theorem 1.

Remark. After the first draft of this manuscript was published we became aware that a result similar to our Theorem 1 for the case of binary field $\mathbb{F}_2$ was independently claimed in [15]. The 3-term complex used in [15] to get the main result is equivalent to the balanced product over G of the expander codes [6, 7] defined on *two different* Cayley graphs for the *same* group G. It is interesting to note

that this construction is similar to the lifted product construction we consider in the current work (see Remark 5 from [42]), where instead of the product $\mathcal{A} \otimes_G \mathcal{B}^*$ we propose to use the product $\mathcal{A} \otimes_G \mathcal{B}$ and conjecture that this way it is still possible to get asymptotically good LTCs. The diagrams for $\mathcal{A} \otimes_G \mathcal{B}$ and $\mathcal{A} \otimes_G \mathcal{B}^*$ are given respectively by

$$\begin{array}{ccc} R^{n_a \times m_b} & \xrightarrow{A \otimes_R \mathrm{id}} & R^{m_a \times m_b} \\ {\scriptstyle -\mathrm{id} \otimes_R B}\uparrow & & \uparrow{\scriptstyle \mathrm{id} \otimes_R B} \\ R^{n_a \times n_b} & \xrightarrow[A \otimes_R \mathrm{id}]{} & R^{m_a \times m_b} \end{array}, \qquad \begin{array}{ccc} R^{n_a \times m_b} & \xrightarrow{A \otimes_R \mathrm{id}} & R^{m_a \times m_b} \\ {\scriptstyle -\mathrm{id} \otimes_R B^*}\downarrow & & \downarrow{\scriptstyle \mathrm{id} \otimes_R B^*} \\ R^{n_a \times n_b} & \xrightarrow[A \otimes_R \mathrm{id}]{} & R^{m_a \times n_b} \end{array}.$$

One can easily check that the Tanner graphs of the complexes $\mathcal{A} \otimes_G \mathcal{B}$ and $\mathcal{A} \otimes_G \mathcal{B}^*$ are isomorphic. What is different is the interpretation of the Tanner graph vertices as *code symbols* and *parity-checks* when we make a code out of the complex. In some sense, the product $\mathcal{A} \otimes_G \mathcal{B}$ is better suited for LTCs since it gives classical codes of rate arbitrary close to 1. Hence it is an interesting open question whether the approach used in [15] can also succeed on the codes obtained from $\mathcal{A} \otimes_G \mathcal{B}$. At the same time, the construction $\mathcal{A} \otimes_G \mathcal{B}^*$, which we use to prove the main results, is much better suited for qLDPC codes, since it is symmetric. This symmetry allows us to prove the lower bound on the Z-distance of our qLDPC code in the same way as for the X-distance. Besides, we can get equal number of X-checks and Z-checks, which gives qLDPC codes of rates arbitrary close to 1.

2 PRELIMINARIES

2.1 Products of graphs

If X and Y are two graphs (considered as 2-level posets), then from the geometrical point of view the poset $X \times Y$ corresponds to the direct product of X and Y (as topological graphs). At the same time, the geometrical interpretation of the poset $X \times_G Y$ can be given in terms of the balanced product of graphs [6]. Note that the 1-*skeleton* of $X \times Y$, i.e., its restriction to the first two levels, is the 2-level poset representing the graph $X \square Y$, which is usually called the *Cartesian product* of the graphs X and Y. Recall that for every G-lifted graph Γ the group G acts freely on Γ. Hence, we can also define the *G-lifted Cartesian product* $\hat{X} \square_G \hat{Y}$ for G-lifts $\hat{X}$, $\hat{Y}$ of base graphs X, Y as the 1-skeleton of $\hat{X} \times_G \hat{Y}$. It is not hard to check that the graph $\hat{X} \square_G \hat{Y}$ is a $|G|$-fold cover for the standard Cartesian product $X \square Y$. Furthermore, if G is abelian, then this cover is regular, i.e., $\hat{X} \square_G \hat{Y}$ is a G-lift of $X \square Y$.

Suppose that $\hat{\Gamma}$ is a G-lift of some base graph Γ. We can view Γ as the quotient of $\hat{\Gamma}$ modulo the action of G, i.e., $V(\Gamma) = V(\hat{\Gamma})/G$ and $E(\Gamma) = E(\hat{\Gamma})/G$. Consider the cell poset $\tilde{X} := \hat{\Gamma} \times_G \hat{\Gamma}$, and let us represent its elements by triples $x \cdot g \cdot y$, where $x, y \in V(\Gamma) \cup E(\Gamma)$, and $g \in G$. From the definition of the poset $\hat{\Gamma} \times_G \hat{\Gamma}$ (see Remark 5) it follows that $x' \cdot g' \cdot y' \succ x \cdot g \cdot y$ **iff** one of the following conditions hold:

(1) $\hat{x}'_{g'} \succ_{\hat{\Gamma}} \hat{x}_g$ and $y = y'$;
(2) $x = x'$ and $\hat{y}'_{g'} \succ_{\hat{\Gamma}} \hat{y}_g$;

where $\succ_{\hat{\Gamma}}$ is the covering relation in the graph $\hat{\Gamma}$ considered as a 2-level poset, i.e., its incidence relation. It is convenient to interpret the poset $\tilde{X}$ as a 2-dimensional geometric object. An element $x \cdot g \cdot y \in \tilde{X}$ is called:

- a *vertex* if $x \in V(\Gamma), y \in V(\Gamma)$;
- a *horizontal edge* if $x \in E(\Gamma), y \in V(\Gamma)$;
- a *vertical edge* if $x \in V(\Gamma), y \in E(\Gamma)$;
- a *face* if $x \in E(\Gamma), y \in E(\Gamma)$,

and the corresponding subsets of elements are denoted as $V = V(\tilde{X})$, $E_{\rightarrow} = E_{\rightarrow}(\tilde{X})$, $E_{\uparrow} = E_{\uparrow}(\tilde{X})$, and $F = F(\tilde{X})$. We also define the set $E(\tilde{X}) = E_{\rightarrow}(\tilde{X}) \cup E_{\uparrow}(\tilde{X})$.

If P is a poset we denote by P^* the *dual poset*, i.e., $x \leqslant_{P^*} y$ whenever $y \leqslant_P x$. In what follows, we will also need a poset $X := \hat{\Gamma} \times_G \hat{\Gamma}^*$, which is defined on the *same* set as $\tilde{X} = \hat{\Gamma} \times_G \hat{\Gamma}$ but has *different* partial order. The cell poset $\tilde{X}$ has 3 levels: $\tilde{X}_0 := V$, $\tilde{X}_1 := E_{\uparrow} \cup E_{\rightarrow}$, and $\tilde{X}_2 := F$, while the levels for X are as follows: $X_0 := E_{\uparrow}$, $X_1 := F \cup V$, and $X_2 := E_{\rightarrow}$.

Remark 8. As we will see in Section 3.3, the poset $X = \hat{\Gamma} \times_G \hat{\Gamma}^*$ corresponds to the lifted product complex $\mathcal{T}(\Gamma; h) \otimes_G \mathcal{T}^*(\Gamma; h')$, which we use to show the main result. However the levels in the poset X do not correspond to the natural geometrical dimension of the cells, and in the proof of our main result it is more convenient to work with the poset $\tilde{X} = \hat{\Gamma} \times_G \hat{\Gamma}$ defined on the same set as X, but giving it a natural geometrical interpretation as a 2-dimensional complex. To this end we define the incidence relation $\mathrm{inc}(\cdot, \cdot)$ on the set $V \cup E_{\rightarrow} \cup E_{\uparrow} \cup F$ in a standard geometrical sense, i.e., we assume that $\mathrm{inc}(x, y)$ **iff** $x \leqslant y$ or $y \leqslant x$, where $\leqslant$ is the partial order of the poset $\tilde{X} = \hat{\Gamma} \times_G \hat{\Gamma}$. If $x \in X$ and $S, T \subseteq X$, then we also use the following notations:

$$S_x := \{y \in S \mid \mathrm{inc}(x, y)\},$$
$$S_T := \{y \in S \mid \mathrm{inc}(x, y) \text{ for some } x \in T\}.$$

Hence S_x is the subset of the elements from X incident to x, and S_T is the the subset of the elements from S incident to some element from T. For example, $X_v = \{v\} \cup E_v \cup F_v$ is the set of all cells incident to v called the *star* of v, where E_v (resp. F_v) is the set of edges (resp. faces) incident to v.

For the proof of our main result we will also need the 1-skeleton $\Lambda := \hat{\Gamma} \square_G \hat{\Gamma}$ of $\hat{\Gamma} \times_G \hat{\Gamma}$ with the set of vertices $V(\Lambda) := V(\tilde{X})$ and the set of edges $E(\Lambda) := E(\tilde{X})$.

Remark 9. In the proof of the main result in Section 3, when we mention sets V, E, $E_{\rightarrow}$, $E_{\uparrow}$, F or a graph Λ, we refer to the corresponding sets and the graph defined for the poset $\hat{\Gamma} \times_G \hat{\Gamma}$ in this section unless otherwise stated.

2.2 Complexes with local system of coefficients

In this subsection, we describe expander codes, which are Tanner codes obtained from expander graphs. We adopt a very convenient way, used in [41], [6] to represent these codes in the language of chain complexes and local systems. If $\mathcal{F}$ is some abelian group and X is some n-element set, then we denote by $\mathcal{F}X$ the abelian group of all formal linear combinations $\sum_{x \in X} a_x x$ of the elements $x \in X$ with coefficients $a_x \in \mathcal{F}$. When $n = 1$, and $X = \{x\}$, we usually write $\mathcal{F}x$ instead of $\mathcal{F}\{x\}$. If $\mathcal{F} = \mathbb{F}_q$ then the group $\mathcal{F}X$ is isomorphic to the vector space $\mathbb{F}_q^n$. When $\mathcal{F} = \mathbb{F}_q^m$, the group $\mathcal{F}X$ can be identified with the vector space $\mathbb{F}_q^{mn}$ of block vectors $(v_1, \ldots, v_n)$ with the blocks $v_i \in \mathbb{F}_q^m$, $i \in [n]$. We denote by $\mathbf{wt}(a)$ the standard Hamming weight of a, considered as a vector over $\mathbb{F}_q$.

We also consider the *block weight* $\mathbf{wt}_X(a)$ defined as the number non-zero blocks in a, viewed as a block vector $(a_x)_{x\in X}$, i.e. we have

$$\mathbf{wt}_X(a) := \operatorname{card}\{x \in X \mid a_x \neq 0\}.$$

Sometimes we need to take into account only the blocks that correspond to some subset $S \subseteq X$. In this case, we can define the *block weight* $\mathbf{wt}_S(a) := \operatorname{card}\{x \in S \mid a_x \neq 0\}$ *relative* to the subset $S \subseteq X$. We also define $\operatorname{supp} a := \{x \in X \mid a_x \neq 0\}$ and $a|_S := \sum_{x\in S} a_x$, where $a = \sum_{x\in X} a_x x$.

Let $\partial\colon \mathcal{F}X \to \mathcal{F}X$ be the boundary map of C. In some cases, we want to restrict the domain and codomain of ∂. For every $S, T \subseteq X$ we consider the map $\partial_{S\to T}\colon \mathcal{F}S \to \mathcal{F}T$ defined as $a \mapsto (\partial a)|_T$. From the definition it is clear that for every $a \in \mathcal{F}X$ we have:

$$(\partial(a|_S))|_T = \partial_{S\to T}(a|_S). \tag{2}$$

Local systems can be used to obtain a high-level view of a chain complex over $\mathbb{F}_q$. The main idea is to allow for each element x of a cell poset X to have its own vector space of coefficients $\mathcal{F}_x$. For example, we can represent a Tanner code $\mathcal{T}(\Gamma; h)$ for a graph Γ (considered as a 2-level poset $\Gamma = V \sqcup E$) by the complex $\mathcal{F}\Gamma$ defined by the diagram

$$\mathbb{F}_q E \xrightarrow{\partial} \mathbb{F}_q^r V,$$

where for every $v \in V$ we have $\mathcal{F}_v := \mathbb{F}_q^r$ and for every $e \in E$ we have $\mathcal{F}_e := \mathbb{F}_q$.

If we have a free action of G on the cell posets X and Y of the complexes $\mathcal{A} = \mathcal{F}X$ and $\mathcal{B} = \mathcal{G}Y$ with local systems $\mathcal{F}$ and $\mathcal{G}$ respectively, then it is not hard to see that the complex $\mathcal{A} \otimes_G \mathcal{B}$ can be described as $(\mathcal{F} \otimes \mathcal{G})X \times_G Y$, where $\mathcal{F} \otimes \mathcal{G}$ is the local system for $X \times_G Y$ defined as $(\mathcal{F} \otimes \mathcal{G})_{x\otimes_G y} = \mathcal{F}_x \otimes_{\mathbb{F}_q} \mathcal{G}_y$.

Let us we show that the lifted product over G of two Tanner codes invariant under a free action of G can also be represented as a complex with a local system on the poset $\hat{\Gamma} \times_G \hat{\Gamma}^*$ from Subsection 2.1.

$$\begin{array}{ccc} \mathbb{F}_q E & \xrightarrow{A} & \mathbb{F}_q^r V \\ \otimes_G & & \\ \mathbb{F}_q E & \xrightarrow{B^*} & \mathbb{F}_q^{r'} V \end{array} = \begin{array}{ccc} \mathbb{F}_q E & \xrightarrow{A\otimes_G \mathrm{id}} & \mathbb{F}_q^r V \times_G E \\ \downarrow -\mathrm{id}\otimes_G B^* & & \downarrow \mathrm{id}\otimes_G B^* \\ \mathbb{F}_q^{r'} E \times_G V & \xrightarrow[A\otimes_G \mathrm{id}]{} & \mathbb{F}_q^{r\times r'} V \times_G V \end{array}$$

3 PROOF OF THE MAIN RESULTS

This section contains the proofs of the main results. The proofs of several lemmas are omitted due to space limitations. They can be found in the full version of the paper [42].

3.1 Local minimality

One of the key ideas used in the proof of our main result is the idea of local minimality. It was used previously in the context of cohomology of simplicial complexes with $\mathbb{F}_2$-coefficients [18, 30]. In the current work, we extend this idea to a much more general context of (co)homology of complexes with local systems of coefficients.

Consider an abstract cell complex X and a based chain complex $C = \mathcal{F}X$ of vector spaces

$$\cdots \xrightarrow{\partial_{i+1}} C_i \xrightarrow{\partial_i} C_{i-1} \xrightarrow{\partial_{i-1}} \cdots$$

over $\mathbb{F}_q$, where $\mathcal{F}$ is a local system on X. Denote by $|\cdot|$ the block weight $\mathbf{wt}_X(\cdot)$, which makes each term C_i in this complex a normed abelian group with the norm $|\cdot|$ and allows us to define the distance in the standard way: $d(a, b) := |a - b|$, $d(a, \mathcal{B}) := \min_{b\in\mathcal{B}} |a - b|$. We also use $|\cdot|$ to define for every $i \in \mathbb{Z}$ the corresponding quotient norm on the i-th homology group $H_i(C) = Z_i(C)/B_i(C)$ called the *systolic norm* by the formula $|\mathcal{A}| := \min_{a\in\mathcal{A}} |a|$, where $\mathcal{A} \in H_i(C)$, $B_i(C) = \operatorname{im}\partial_{i+1}$, $Z_i(C) = \ker\partial_i$. This in turn allows us to define the distance on $H_i(C)$ as $d(\mathcal{A}, \mathcal{B}) := |\mathcal{A} - \mathcal{B}|$ and consider the minimal distance of $H_i(C)$ given by the standard formulas:

$$\begin{aligned} d(H_i(C)) &:= \min_{\substack{\mathcal{A}\neq\mathcal{B} \\ \mathcal{A},\mathcal{B}\in H_i(C)}} d(\mathcal{A}, \mathcal{B}) \\ &= \min_{\mathcal{A}\in H_i(C)\setminus\{B_i(C)\}} |\mathcal{A}| = \min_{a\in Z_i(C)\setminus B_i(C)} |a|. \end{aligned}$$

These distances are related to the minimal distance $d(Q)$ of the quantum CSS code $Q = Q(\partial_i, \partial_{i+1}^*)$ over $\mathbb{F}_q$ defined by three consecutive terms of the complex

$$C_{i+1} \xrightarrow{\partial_{i+1}} C_i \xrightarrow{\partial_i} C_{i-1}.$$

It is easy to see that $d(Q) \geqslant \min(d(H_i(C)), d(H_i(C^*)))$, where we have the equality if $\mathcal{F}_x = \mathbb{F}_q$ for all $x \in X$ since the block Hamming weight $\mathbf{wt}_X(\cdot)$ is less than or equal to the corresponding Hamming weight $\mathbf{wt}(\cdot)$.

Definition 2. We say that an i-chain $c \in C_i$, $i \in \mathbb{Z}$, is *locally minimal* (*with respect to* X) if $|c + \partial a x| \geqslant |c|$ for all $x \in X_{i+1}$ and $a \in \mathcal{F}_x$. We also define the value

$$d^{(i)}_{\mathrm{LM}}(C) := \min\{|c| \mid c \in Z_i(C) \setminus \{0\}, c \text{ is locally minimal}\},$$

which we call the *i-th locally minimal distance* of C. If we do not have non-zero locally minimal i-cycles, then we assume that $d^{(i)}_{\mathrm{LM}}(C) = \infty$.

Note that in general the locally minimal distance $d^{(i)}_{\mathrm{LM}}(C)$ is not equal to the minimal distance of $Z_i(C)$ since the codewords of minimal weight from $Z_i(C)$ are not necessarily locally minimal. For example, in the context of w-limited qLDPC codes where $|\partial x| \leqslant w$ for every $x \in Xi + 1$, and thus we have $\partial x \in Z_i(C)$ and $d(Z_i(C)) \leqslant w$, one can see that the codeword $c = \partial x$ is not locally minimal since $|c - \partial x| = 0 < |c|$.

The next lemma connects the locally minimal distance of the complex to the properties of the corresponding quantum and classical codes obtained from it. The first assertion can be used to obtain the lower bound on the minimal distance $d(Q)$ of the corresponding quantum CSS code Q, while the second one can be used to show that the space $Z_{i+1}(C)$ is a locally testable code.

Lemma 1. *Let $C = \mathcal{F}X$ be a chain complex, where $\mathcal{F}$ is a local system on X. Then for every $i \in \mathbb{Z}$ we have*

$$d(H_i(C)) \geqslant d^{(i)}_{\mathrm{LM}}(C),$$

and for every chain $c \in C_{i+1}$ such that $|\partial c| < d^{(i)}_{\mathrm{LM}}(C)$ we have

$$|\partial c| \geqslant d(c, Z_{i+1}(C)). \tag{3}$$

Proof. By definition we have

$$d(H_i(C)) = |c_0|, \quad \text{where} \quad c_0 := \operatorname*{arg\,min}_{c\in Z_i(C)\setminus B_i(C)} |c|.$$

Since the element c_0 has the minimal norm in the coset $c_0+B_i(C)$, it is also locally minimal. Hence we have $d(H_i(C)) = |c_0| \geqslant d^{(i)}_{\mathrm{LM}}(C)$.

We prove the second claim by induction on $|\partial c|$. If $|\partial c| = 0$ then $d(c, Z_{i+1}(C)) = 0$, and (3) is true. Consider $c \in C_{i+1}$ such that $0 < |\partial c| < d^{(i)}_{\mathrm{LM}}(C)$. Since $\partial c \in Z_i(C)$ and $|\partial c| < d^{(i)}_{\mathrm{LM}}(C)$, we see that ∂c cannot be locally minimal, and hence there exists $a \in \mathcal{F}_x$ where $x \in X_{i+1}$ such that $|\partial(c + ax)| \leqslant |\partial c| - 1$. Therefore by the induction hypothesis we have $|\partial(c+ax)| \geqslant d(c+ax, Z_{i+1}(C))$. Thus we obtain

$$d(c, Z_{i+1}(C)) \leqslant d(c+ax, Z_{i+1}(C))+|ax| \leqslant |\partial(c+ax)|+\underbrace{|ax|}_{=1} \leqslant |\partial c|,$$

which completes the proof of the second claim. □

3.2 Graph expansion

Let Γ be a graph[17] with the set of vertices $V(\Gamma)$ and the set of edges $E(\Gamma)$. If vertices $v, v' \in V(\Gamma)$ are connected by an edge $e \in E(\Gamma)$, we call v, v' *adjacent* and denote this fact by $v \leftrightarrow v'$ or by $v \leftrightarrow_e v'$ when we want to emphasize the edge e. A graph Γ is called *w-regular* if all its vertices have degree w. The *adjacency matrix* of a graph Γ with $V(\Gamma) = \{v_1, \dots, v_n\}$ is the matrix $A(\Gamma) = (a_{ij})_{n\times n}$, where a_{ij} is the number of edges $e \in E(\Gamma)$ such that $v_i \leftrightarrow_e v_j$. Since $A(\Gamma)$ is a symmetric matrix, it has n real-valued eigenvalues $\lambda_1 \geqslant \dots \geqslant \lambda_n$. Let $\lambda_2(\Gamma) := \lambda_2$, and $\lambda(\Gamma) := \max(|\lambda_2|, |\lambda_n|)$. It is obvious that $\lambda_2(\Gamma) \leqslant \lambda(\Gamma)$.

Definition 3. We say that a graph Γ is an *(n, w, λ)-expander* if it is a simple w-regular graph on n vertices such that $\lambda = \lambda(G)$.

For any graph Γ we denote by Γ^2 the graph with $V(\Gamma^2) = V(\Gamma)$ and $A(\Gamma^2) = (A(\Gamma))^2$, i.e., the number of edges connecting two vertices in Γ^2 is equal to the number of length 2 paths connecting them in Γ. In this section, we prove several technical lemmas to establish expanding properties of the graphs Λ and Λ^2, where Λ is the graph defined in Subsection 2.1. If $\Gamma = (V, E)$ is a graph (possibly with multiple edges), and $S, T \subseteq E$, then by $E_\Gamma(S, T)$, we denote the set of oriented edges from S to T, i.e. $E_\Gamma(S, T) := \{(s, e, t) \mid e \in E; s \in S, t \in T; s \leftrightarrow_e t\}$ (every edge connecting $s, t \in S \cap T$ is counted twice). We also usually write $E(S, T)$ instead of $E_\Gamma(S, T)$ if the graph Γ is clear from the context.

Let us now state without proof a well-known variant of the expander mixing lemma for (n, w, λ)-regular graphs [28, Lemma 2.5].

Lemma 2 (Expanding mixing lemma)**.** *If $\Gamma = (V, E)$ is an (n, w, λ)-expander graph, then for every $S, T \subseteq V$ we have:*

$$\left||E(S, T)| - w\frac{|S|\,|T|}{n}\right| \leqslant \lambda\sqrt{|S|\,|T|}.$$

Example 1. Let us now consider the infinite family of $(p + 1)$-regular non-bipartite Ramanujan graphs $X^{p,q}$ from [37], where p and q are two unequal primes such that $q > 2\sqrt{p}$, $p \equiv q \equiv 1 \pmod 4$, and $p^{(q-1)/2} \equiv 1 \pmod q$. The graph $X^{p,q}$ is obtained in [37] as the Cayley graph $\mathrm{Cay}(G, S_{p,q})$, where[18] $G := \mathrm{PSL}(\mathbb{F}_q^2)$ and $S_{p,q}$ is some specific symmetric set of $p + 1$ generators. Denote by $\bar{X}^{p,q}$ the corresponding double-cover $\mathrm{Cay}_2(G, S_{p,q})$. Hence $\bar{X}^{p,q}$ is a $(p + 1)$-regular bipartite graph with $n = 2\,|G|$ vertices, where $|G| = q(q^2 - 1)/2$. Since it is proved in [37] that $\lambda(X^{p,q}) \leqslant 2\sqrt{p}$, then we also have $\lambda_2(\bar{X}^{p,q}) \leqslant 2\sqrt{p}$.

In what follows, it will be convenient to define a property called (a, λ)-edge-expansion, which captures the edge expansion on small sets of vertices in a graph.

Definition 4. We say that a graph Γ is *(a, λ)-edge-expanding* if for any $S, T \subseteq V(\Gamma)$ such that $|S|, |T| \leqslant a$ the following condition holds:

$$|E(S, T)| \leqslant \lambda\sqrt{|S||T|}.$$

Note that $E(S, S)$ is twice the number of the edges connecting the vertices inside the set S in Γ. Hence if $\lambda = o(w)$, and Γ is a w-regular (a, λ)-edge-expanding graph, then for all sufficiently small sets S we have $|\mathrm{E(S,S)}| \leqslant \lambda|S|$, i.e., almost all edges goes outside of S in Γ.

Lemma 3. *If Γ is an (n, w, λ)-expander graph, then it is $(\lambda n/w, 2\lambda)$-edge-expanding.*

Proof. If Γ is w-regular, then from Lemma 2 it follows that for any $S, T \subseteq V(\Gamma)$ such that $|S|, |T| \leqslant \lambda n/w$ we have

$$\left||E(S, T)| - w\frac{|S||T|}{n}\right| \leqslant \lambda\sqrt{|S||T|}.$$

Hence we get

$$|E(S, T)| \leqslant w\frac{|S||T|}{n} + \lambda\sqrt{|S||T|} \leqslant \left(\frac{\lambda n}{w}\cdot\frac{w}{n} + \lambda\right)\sqrt{|S||T|} = 2\lambda\sqrt{|S||T|},$$

and the lemma is proved. □

Lemma 4. *If for some finite group G a graph $\hat{\Gamma}$ is a G-lift of an (a, λ)-edge-expanding base graph Γ, then $\hat{\Gamma}$ is $(a, |G| \cdot \lambda)$-edge-expanding.*

Proof. Consider subsets $\hat{S}, \hat{T} \subseteq V(\hat{\Gamma})$ such that $|\hat{S}|, |\hat{T}| \leqslant a$, and let $S, T \subseteq V(\Gamma)$ be their projections[19] to the base graph Γ. Since each edge of Γ is the projection of $m = |G|$ edges from $\hat{\Gamma}$, then using the edge-expansion of the base graph Γ we have:

$$|E(\hat{S}, \hat{T})| \leqslant m|E(S, T)| \leqslant m\lambda\sqrt{|S||T|} \leqslant m\lambda\sqrt{|\hat{S}||\hat{T}|}.$$ □

Lemma 5. *Every graph $\bar{X}^{w-1,t}$ from Example 1 is $(n/\sqrt{w}, 8\sqrt{w})$-edge-expanding, where $n = t(t^2 - 1)$ is the number of its vertices.*

Proof. Since the Ramanujan graph $X^{w-1,t}$ is an $(n/2, w, 2\sqrt{w})$-graph, then by Lemma 3 it is $(n/\sqrt{w}, 4\sqrt{w})$-edge-expanding. Moreover, since the graph $\bar{X}^{w-1,t}$ is a 2-lift of $X^{w-1,t}$, then by Lemma 4 it is $(n/\sqrt{w}, 8\sqrt{w})$-edge-expanding. □

Lemma 6. *Let $x_1, \dots, x_n \in \mathbb{R}_+$, $y_1, \dots, y_n \in \mathbb{R}_+$ be sequences of non-negative real numbers. Then $\min_{i\in[n]} x_i y_i \leqslant \bar{x}\bar{y}$, where $\bar{x} = \frac{1}{n}\sum_{i=1}^n x_i$, $\bar{y} = \frac{1}{n}\sum_{i=1}^n y_i$.*

Proof. The proof follows from the Cauchy–Schwarz inequality for the vectors $(\sqrt{x_i})_{i=1}^n$ and $(\sqrt{y_i})_{i=1}^n$. □

Lemma 7. *If a w-regular graph Γ is (a, λ)-edge-expanding, then the graph Γ^2 is $(a/w, 2\lambda^2(1 + \ln w))$-edge-expanding.*

[17] It may have multiple edges but we do not allow loops in the current work.

[18] The group $\mathrm{PSL}(\mathbb{F}_q^2)$ is the *projective special linear* group for $\mathbb{F}_q^2$, i.e. the quotient of the group of matrices $A \in \mathbb{F}_q^{2\times 2}$ with $\det A = 1$ modulo its subgroup $\{\pm\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)\}$.

[19] The *projection* of a vertex $(v, g) \in V(\tilde{\Gamma})$ is the vertex $v \in V(\Gamma)$.

Proof. Let $S, T \subseteq V(\Gamma)$ and $|S|, |T| \leqslant a/w$. There are at most $w|S| \leqslant a$ vertices adjacent to the vertices from S. Let $v_1, v_2, \dots$ be the sequence of the vertices incident to S in the decreasing order of the number of length 2 paths from S to T that goes through each of these vertices. Consider the set $U_j = \{v_1, \dots, v_j\}$ of size $j \leqslant a$. By the edge-expansion property of the graph Γ we have

$$|E_\Gamma(U_j, S)| \leqslant \lambda\sqrt{j|S|}, \qquad |E_\Gamma(U_j, T)| \leqslant \lambda\sqrt{j|T|}.$$

Hence, using Lemma 6 with $n = j, x_i = |E_\Gamma(\{v_i\}, S)|, y_i = |E_\Gamma(\{v_i\}, T)|$ the number of length 2 paths through the vertex v_j is

$$x_j y_j = \min_{i \in [j]} x_i y_i \leqslant \frac{|E_\Gamma(U_j, S)|}{j} \cdot \frac{|E_\Gamma(U_j, T)|}{j} \leqslant \frac{\lambda^2\sqrt{|S||T|}}{j}.$$

On the other hand, the degree of each vertex in Γ is w, and hence the total number of pairs of edges incident to each vertex is w^2. Hence, if we let $\mu := \lambda^2\sqrt{|S||T|}$, then the total number of length 2 paths from S to T can be estimated as

$$\begin{aligned} |E_{\Gamma^2}(S, T)| &\leqslant \sum_{j=1}^{\lfloor \mu \rfloor} \min\left(w^2, \mu/j\right) = w^2 \cdot \frac{\mu}{w^2} + \mu \sum_{j=\lceil \mu/w^2 \rceil}^{\lfloor \mu \rfloor} \frac{1}{j} \\ &< \mu(2 + \ln \mu - \ln(\mu/w^2)) \\ &= 2\mu(1 + \ln w) = 2\lambda^2(1 + \ln w)\sqrt{|S||T|}. \end{aligned}$$

Above we truncate the summation at $j = \lfloor \mu \rfloor$ since for $j > \mu$ the number of length 2 paths going through the vertex v_j is less or equal to $\min(w^2, \mu/j) < 1$, and therefore is equal to 0. Thus there exist at most $2\lambda^2(1 + \ln w)\sqrt{|S||T|}$ edges from S to T in Γ^2, and Γ^2 is $(a/w, 2\lambda^2(1 + \ln w))$-edge-expanding. □

3.3 Proof outline

In this subsection, we give some definitions and an informal idea of the proof of our main results. Let $\hat{\Gamma} = (\hat{E}, \hat{V})$ be a G-lift of some base graph Γ. We assume that $\hat{\Gamma}$ is a w-regular (a, λ)-edge-expanding simple graph with n vertices. For example, we can use an infinite family of graphs $\bar{X}^{w-1,t}$ from Example 1, where by Lemma 5 we have $a = n/\sqrt{w}$, $\lambda = 8\sqrt{w}$.

Let $h \in \mathbb{F}_q^{r \times w}$, $h' \in \mathbb{F}_q^{r' \times w}$ be some full rank matrices, and $\mathcal{A} \in \mathfrak{T}_G(\hat{\Gamma}, h)$, $\mathcal{B} \in \mathfrak{T}_G(\hat{\Gamma}, h')$ be the corresponding G-lifted Tanner codes:

$$\mathcal{A} = \left(\mathbb{F}_q\hat{E} \xrightarrow{\partial_A} \mathbb{F}_q^r\hat{V}\right), \qquad \mathcal{B} = \left(\mathbb{F}_q\hat{E} \xrightarrow{\partial_B} \mathbb{F}_q^{r'}\hat{V}\right).$$

Now since G acts freely on $\mathcal{A}$ and $\mathcal{B}$, we can consider their G-lifted product complex $C := \mathcal{A} \otimes_G \mathcal{B}^*$ over $\mathbb{F}_q$ shown below:

$$\underbrace{\mathbb{F}_q\hat{E} \otimes_G \mathbb{F}_q^{r'}\hat{V}}_{C_2} \xrightarrow{\partial_2} \underbrace{\overbrace{\mathbb{F}_q\hat{E} \otimes_G \mathbb{F}_q\hat{E}}^{C_F} \oplus \overbrace{\mathbb{F}_q^r\hat{V} \otimes_G \mathbb{F}_q^{r'}\hat{V}}^{C_V}}_{C_1} \xrightarrow{\partial_1} \underbrace{\mathbb{F}_q^r\hat{V} \otimes_G \mathbb{F}_2\hat{E}}_{C_0}.$$

It is convenient to represent C as the the chain complex $\mathcal{F}X$, where $\mathcal{F}$ is the local system on $X := \hat{\Gamma} \times_G \hat{\Gamma}^*$. Since the poset X has three levels: $X_2 = E_\rightarrow$, $X_1 = F \cup V$, and $X_0 = E_\uparrow$, it is not hard to see that $\mathcal{F}X$ has the following form:

$$\underbrace{\mathbb{F}_q^{r'}E_\rightarrow}_{C_2} \xrightarrow{\partial_2} \underbrace{\overbrace{\mathbb{F}_qF}^{C_F} \oplus \overbrace{\mathbb{F}_q^{r \times r'}V}^{C_V}}_{C_1} \xrightarrow{\partial_1} \underbrace{\mathbb{F}_q^rE_\uparrow}_{C_0},$$

where we identify $\mathbb{F}_q^r \otimes \mathbb{F}_q^{r'}$ with $\mathbb{F}_q^{r \times r'}$.

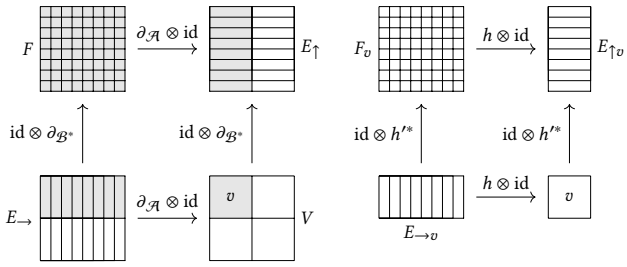

Figure 1: High-level view of the tensor product complex $\mathcal{A} \otimes \mathcal{B}^*$ over $\mathbb{F}_2$, where $\mathcal{A} \in \mathfrak{T}(D_w; h)$, $\mathcal{B} \in \mathfrak{T}(D_w; h')$, and $w = 8$ (on the right); and its part that corresponds to the elements from X incident to the vertex v (on the left).

Remark 10. As we can see, $\mathcal{F}X$ gives us a high-level representation of the complex C. For example, on the left of Fig. 1 you can find a graphical representation of the tensor product complex $\mathcal{A} \otimes \mathcal{B}^*$, where $\mathcal{A} \in \mathfrak{T}(D_w; h)$, $\mathcal{B} \in \mathfrak{T}(D_w; h')$, and $w = 8$. For simplicity we consider in this example the tensor product instead of the G-lifted product. On the right of Fig. 1 you can see the "part" of this complex corresponding to the faces and edges incident to one particular vertex $v \in V$.

Now we consider the classical code $Z_2(C) = \ker \partial_2$ and the quantum code $\mathcal{Q}(C) := \mathcal{Q}(\partial_1, \partial_2^*)$, and show that for some sufficiently large number w we can choose the matrices h, h' such that $Z_2(C)$ and $\mathcal{Q}(C)$ satisfy the requirements of Theorems 1 and 2, respectively. The most difficult part of the proof is to show that $Z_2(C)$ is locally testable, and $\mathcal{Q}(C)$ has linear minimum distance. However, from Lemma 1 it easily follows that if C has the locally minimal distance $d^{(1)}_{\mathrm{LM}}(C) = \Theta(n)$ as $n \to \infty$, then both $Z_2(C)$ and $\mathcal{Q}(C)$ have the desired properties. Therefore we need to show that for every locally minimal 1-cycle $c \in Z_1(C)$ such that $|c| = o(n)$ as $n \to \infty$ we have $c = 0$, where $|c| = \mathbf{wt}_X(c)$ is the block weight of c.

Let us fix some non-zero locally minimal 1-cycle

$$c = \sum_{x \in X_1} c_x x \in Z_1(C).$$

Hence we get $c \neq 0$ and $\partial c = 0$. We have $c = c_F + c_V$, where $c_F := c|_F$ and $c_V := c|_V$. Below we give a number of important definitions used in the rest of the paper. Note that some of them depend on the fixed 1-cycle c. However, for brevity, we usually do not mention c.

Definition 5. An element $x \in X_1$ (a vertex or a face) is called *active* if $c_x \neq 0$. A vertical edge $e \in X(0)$ is called *active* if it is incident to an active vertex or an active face. Furthermore, e is called *face-active* if it is not incident to any active vertex (only to an active face).

We also need another type of vertices we call *labeled* that include active vertices as a special case. However, the number of the labeled vertices is $O(|c|)$, and we can still use the expansion properties of the graphs involved in the proof. We define the set of labeled vertices as the minimal set of vertices such that:

(1) every active vertex is labeled;
(2) every vertex of a face-active edge adjacent in Λ to at least m labeled vertices is labeled.

We also consider 2 types of labeled vertices:

(1) a vertex is called *m-edge-expanding* if there are at least m edges connecting it to the labeled vertices in Λ;
(2) a vertex is called *s-face-expanding* if there are at least s edges connecting it to the labeled vertices in Λ^2.

In the proof outlined below, we consider classical codes that are duals of the product codes. In Subsection 3.4 we define a special property of such codes called (s, m, β)*-product-expansion*.

Fix $\varepsilon := 1/6$, and put $m := w^{1/2+\varepsilon}$, $s := w^{1+\varepsilon}$. From Lemma 10 it follows that we can find a sufficiently large number w and choose matrices h and h' with w columns such that both pairs $(\operatorname{im} h^*, \ker h')$ and $(\ker h, \operatorname{im} h'^*)$ are $(s, 2m, \beta)$-product-expanding.

In the proof, we often use expansion properties of the graphs Λ and Λ^2, where $\Lambda := \hat{\Gamma} \square_G \hat{\Gamma}$ is the graph defined in Subsection 2.1. Using the edge expansion of $\hat{\Gamma}$ we show in Lemma 11 that Λ is $(\Theta(n), \lambda')$-edge-expanding where $\lambda' = \Theta(w^{1/2})$. We also show in Lemma 12 that Λ^2 is $(\Theta(n), \lambda'')$-edge-expanding, where $\lambda'' = \Theta(w \ln w)$.

Suppose that $|c| = o(n)$, i.e., the number of the active vertices and faces is relatively small. Then the proof by contradiction contains the following steps.

(1) Since each labeled vertex is either active itself or incident to an active face, then the number of the labeled vertices is $O(|c|) = o(n)$. Hence we can use the expansion properties of the graphs Λ and Λ^2 for subsets of labeled vertices.
(2) Using the expansion properties of the graph $\hat{\Gamma}$ it is possible to show that each face-active edge is incident to a labeled vertex (Lemma 14).
(3) Note that, by definition, each labeled non-active vertex is m-edge-expanding.
(4) Using local minimality of c and $(s, 2m, \beta)$-product-expansion of $(\operatorname{im} h, \ker h')$ we can show that each active vertex is either m-edge-expanding or s-face-expanding (Lemma 15—the key lemma).
(5) From the previous 2 items we have that each labeled vertex is either m-edge-expanding or s-face-expanding (Corollary 1).
(6) Thus using the expansion properties of Λ and Λ^2 we obtain a contradiction (Lemma 16):
   (a) from the $(\Theta(n), \lambda')$-edge expansion of Λ we obtain that the fraction of the m-edge-expanding labeled vertices is $\Theta(\lambda'/m) < 1/2$ for a sufficiently large w since $\lambda' = \Theta(w^{1/2})$ and $m = \Theta(w^{1/2+\varepsilon})$;
   (b) from the $(\Theta(n), \lambda'')$-edge expansion of Λ^2 we obtain that the ratio of the s-face-expanding labeled vertices is $\Theta(\lambda''/s) < 1/2$ for a sufficiently large w since $\lambda'' = \Theta(w \ln w)$ and $s = \Theta(w^{1+\varepsilon})$;
   (c) the ratio of the labeled vertices that are either m-edge-expanding or s-face expanding is less than 1, which can be true only when the 1-cycle c is zero.

Since we obtained a contradiction, we have that $|c| = \Theta(n)$, i.e., the locally minimal distance $d^{(1)}_{\mathrm{LM}}(C) = \Theta(n)$ as $n \to \infty$, which is in turn of the same order as the length of the classical or quantum codes obtained from the chain complex C. Hence by Lemma 1 we get what we need.

3.4 Local expansion

In this section, we consider the dual code to the classical product code [11, 51] and study its properties[20]. Such codes are related to the local properties of the G-lifted product of two Tanner codes. Let $\ker h \subseteq \mathbb{F}_q^w$ and $\ker h' \subseteq \mathbb{F}_q^w$ be linear codes with parity-check matrices h and h' respectively. Consider the code $C = \ker(h \otimes h') \subseteq \mathbb{F}_q^w \otimes \mathbb{F}_q^w$. We will identify the elements of $\mathbb{F}_q^w \otimes \mathbb{F}_q^w$ with the matrices $x = (x^i_j)^w_{i,j=1} \in \mathbb{F}_q^{w \times w}$ and denote by x^i (resp. x_j) the i-th row (resp. the j-th column) of x. Note that the matrix $h \otimes h'$ is also a generator matrix for the product of the codes $(\ker h)^\perp = \operatorname{im} h^*$ and $(\ker h')^\perp = \operatorname{im} h'^*$ with the generator matrices h, h' respectively, which means that C is the dual to this product code.

Remark 11. Using matrix representation, it is not hard to check that the codewords of C are precisely the matrices $x \in \mathbb{F}_q^{w \times w}$ such that $h' x h^* = 0$. Therefore if $x \in C$ then every row of the matrix $s_\uparrow := h'x$ is a codeword from $\ker h$ and every column of the matrix $s_\rightarrow := xh^*$ is a codeword from $\ker h'$.

Definition 6. A codeword $x \in C = \ker(h \otimes h')$ is called Δ*-minimal* if the following conditions hold:

(1) $\mathbf{wt}(x^i) \leqslant d(x^i, \ker h) + \Delta$ for all $i \in [w]$,
(2) $\mathbf{wt}(x_j) \leqslant d(x_j, \ker h') + \Delta$ for all $j \in [w]$,

which means that we cannot decrease the weight of the matrix x by more than Δ if we add any codeword from $\ker h$ (resp. $\ker h'$) to some row (resp. column) of x. A pair of codes $(\ker h, \ker h')$ is called (s, m, β)*-product-expanding* if for each non-zero βw-minimal codeword $x \in C$ and for each $A, B \subseteq [w]$ such that $|A|, |B| \geqslant w - m$ we have $\mathbf{wt}_{A \times B}(x) \geqslant s$, where $\mathbf{wt}_{A \times B}(x) := \mathbf{wt}(x|_{A \times B})$.

In this section, we often use the following short-hand notations: $x^I := x|_{I \times [w]}$, $x_J := x|_{[w] \times J}$, and $x^I_J := x|_{I \times J}$, where $x \in \mathbb{F}_q^{w \times w}$, $I, J \subseteq [w]$.

Lemma 8. *Let $h \in \mathbb{F}_q^{r \times w}$, $h' \in \mathbb{F}_q^{r' \times w}$ be parity-check matrices such that $\min(d(\ker h), d(\ker h')) \geqslant d$, and $x = (x^i_j)^w_{i,j=1} \in \mathbb{F}_q^{w \times w}$ be a $d/3$-minimal codeword of $\ker(h \otimes h')$. If there exist $A, B \subseteq [w]$ such that $|A| > w - d/3$, $|B| \geqslant w - d + 1$ and $x^B_A = 0$ or $x^A_B = 0$, then $x = 0$.*

Lemma 9. *Let $h \in \mathbb{F}_q^{r \times w}$, $h' \in \mathbb{F}_q^{r' \times w}$, $d = \min(d(\ker h), d(\ker h'))$, $m \leqslant d/6$. Suppose $x \in \ker(h \otimes h')$ is a $d/3$-minimal non-zero codeword such that $\mathbf{wt}_{A \times B}(x) < s$ for some $A, B \subseteq [w]$, $|A| = |B| = w - m$. Then $\operatorname{rk} h'x \geqslant \frac{5}{36} \cdot \frac{d^2}{s}$.*

Lemma 10. *Let $\varepsilon \in (0, 1/4)$, $\alpha > 0$, $\gamma > 0$, $R_1 \in (0, 1)$, $R_2 \in (0, 1)$. Then there exist $\beta > 0$ and $\delta > 0$ such that for random[21] matrices*

[20] The property we consider is similar to the *robust testability* property of tensor product codes, often studied in the literature on LTCs [3, 16].
[21] We suppose that the entries of the both matrices are chosen uniformly and independently at random from $\mathbb{F}_q$.

$h \in \mathbb{F}_q^{\lfloor R_1 w \rfloor \times w}$, $g' \in \mathbb{F}_q^{\lfloor R_2 w \rfloor \times w}$ the following three conditions hold with high probability as $w \to \infty$:

1. $\min(d(\ker h), d(\operatorname{im} g'^*)) \geqslant \delta w$;
2. *the matrices h and g' have full rank;*
3. *the pair of codes $(\ker h, \operatorname{im} g'^*)$ is $(\alpha w^{1+\varepsilon}, \gamma w^{1/2+\varepsilon}, \beta)$-product-expanding.*

3.5 Global expansion

In this subsection, the graph Λ is the graph from Subsection 2.1.

Lemma 11. *The graph Λ is $(a, 2\lambda)$-edge-expanding.*

Lemma 12. *The graph Λ^2 is $(a/2w, 8\lambda^2(\ln w + 2))$-edge-expanding.*

In the rest of this subsection, we assume that c is some fixed locally minimal 1-cycle in the complex $\mathcal{F}X$ from Subsection 3.3.

Lemma 13. *If $\partial c = 0$, then each face-active vertical edge is incident to at least $d(\ker h)$ active faces.*

Proof. Consider a face-active vertical edge e. Then F_e is the set of faces incident to e, and V_e is the set of (two) vertices incident to e. Since e is face-active, $c|_{V_e} = 0$ but $c|_{F_e} \neq 0$. Since $(\partial c)|_e$ depends only on $c|_{F_e}$ and $c|_{V_e}$, then using (2) we have

$$0 = (\partial c)|_e = (\partial(c|_{F_e} + \underbrace{c|_{V_e}}_{=0}))|_e = \partial_{F_e \to e}(c|_{F_e})$$

Since $\partial_{F_e \to e} \sim h$, $c|_{F_e} \neq 0$, and $\partial_{F_e \to e}(c|_{F_e}) = 0$, we have that the number of active faces incident to the edge e is

$$\mathbf{wt}(c|_{F_e}) \geqslant d(\ker \partial_{F_e \to e}) = d(\ker h),$$

and the lemma is proved. □

Lemma 14. *If $d(\ker h) \geqslant 2m + \lambda$, $\partial c = 0$ and $\mathbf{wt}_X(c) \leqslant a/w$, then every active edge is incident to a labeled vertex.*

Proof. The number of active vertical edges is at most $\mathbf{wt}_X(c)w \leqslant a$. Let $S \subseteq E_\uparrow$ be the set of active edges that are not incident to a labeled vertex, and $A \subseteq E_\uparrow$ be the set of all active edges. If an active edge is not incident to labeled vertices, then it is not incident to active vertices (every active vertex is labeled). Then, by definition it is face-active, and hence S is a subset of face-active edges.

Consider the subposet $\Lambda_\square = E_\uparrow \cup F$ of the poset X. Since each face from F is incident to exactly two vertical edges from $E_\uparrow$, $\Lambda_\square$ can be interpreted as a graph with $V(\Lambda_\square) = E_\uparrow$ and $E(\Lambda_\square) = F$. We have

$$\Lambda_\square = \{x \cdot g \cdot y \mid x \in V(\Gamma) \cup E(\Gamma), y \in E(\Gamma), g \in G\} = \bigsqcup_{y \in E(\Gamma)} \Lambda_\square^{(y)}$$

where

$$\Lambda_\square^{(y)} = \{x \cdot g \cdot y \mid x \in V(\Gamma) \cup E(\Gamma), g \in G\} \simeq \hat{\Gamma}.$$

It is not hard to see that $\Lambda_\square$ has the same edge expansion as $\hat{\Gamma}$, i.e. it is (a, λ)-edge-expanding. The sets S and A can be interpreted as sets of vertices of graph $\Lambda_\square$. From the edge expansion of $\Lambda_\square$ we have $|E_{\Lambda_\square}(S, S)| \leqslant \lambda|S|$.

On the other hand, by Lemma 13 since each edge $e \in S$ is face-active, it is incident to at least $d = d(\ker h)$ active faces, hence in the graph $\Lambda_\square$ it is adjacent to at least $d \geqslant 2m + \lambda$ active edges, therefore $|E_{\Lambda_\square}(S, A)| \geqslant (\lambda + 2m)|S|$. Thus

$$|E_{\Lambda_\square}(S, A \setminus S)| = |E_{\Lambda_\square}(S, A)| - |E_{\Lambda_\square}(S, S)| \geqslant (\lambda + 2m)|S| - \lambda|S| = 2m|S|.$$

Suppose, $|S| \neq \varnothing$. Then there exists an edge $e \in S$ adjacent to $2m$ edges $e_1, \ldots, e_{2m} \in A \setminus S$ in $\Lambda_\square$. By the definition of A and S each of the edges e_i is incident to some labeled vertex x_i, which is adjacent to one of the two vertices of e in Λ. Hence, there are $2m$ different labeled vertices adjacent to one of the vertices of the edge e, and therefore one of these vertices is adjacent to at least m labeled vertices, therefore it is labeled by definition. This contradicts the fact that the edge e is from S and cannot be incident to labeled vertices. Hence $S = \varnothing$, and the lemma is proved. □

Lemma 15 (key lemma)**.** *Suppose the pair of codes $(\ker h, \operatorname{im} h'^*)$ is $(s, 2m, \beta)$-product-expanding, h' has full rank, $\beta w \geqslant 4m + 3$, $d \geqslant 4m$, and $m \geqslant \max(4s/d, \lambda)$ where $d = \min(d(\ker h), d(\operatorname{im} h'^*))$. If c is a locally minimal 1-cycle, and $\mathbf{wt}_X(c) \leqslant a/w$, then for each active vertex v one of the following conditions holds:*

1. *v is m-edge-expanding (i.e., it is adjacent to at least m labeled vertices in Λ);*
2. *v is s-face-expanding (i.e., it is adjacent to at least s labeled vertices in Λ^2).*

Proof. □

From Lemma 15 and the definition of the labeled vertices we obtain the following result.

Corollary 1. *Suppose the pair of codes $(\ker h, \operatorname{im} h'^*)$ is $(s, 2m, \beta)$-product-expanding, $\beta w \geqslant 4m + 3$, $d = \min(d(\ker h), d(\operatorname{im} h'^*)) \geqslant 4m$, and $m \geqslant \max(4s/d, \lambda)$. If c is a locally minimal 1-cycle, and $\mathbf{wt}_X(c) \leqslant a/w$, then for each labeled vertex v one of the following conditions holds:*

1. *v is m-edge-expanding (i.e. it is adjacent to at least m labeled vertices in Λ);*
2. *v is s-face-expanding (i.e. it is adjacent to at least s labeled vertices in Λ^2).*

Proof. If the vertex v is active, then the lemma assertion is true by Lemma 15. Otherwise, by definition, the vertex v is adjacent to at least m active vertices in Λ, and hence it is m-edge-expanding. □

Lemma 16. *Suppose the pair of codes $(\ker h, \operatorname{im} h'^*)$ is $(s, 2m, \beta)$-product-expanding, $\beta w \geqslant 4m + 3$, $d = \min(d(\ker h), d(\operatorname{im} h'^*)) \geqslant 4m$, $m \geqslant \max(4s/d, 2\lambda')$, and $s \geqslant 2\lambda''$ where[22] $\lambda' = 2\lambda$ and $\lambda'' = 8\lambda^2(\ln w + 2)$. If c is a locally minimal 1-cycle, and $\mathbf{wt}_X(c) \leqslant \frac{a}{2w}$, then $c = 0$.*

Proof. Let L be the set of labeled vertices. Then by Corollary 1 each vertex $v \in L$ is either m-edge-expanding or s-face-expanding, i.e. $L = L_e \cup L_f$ where L_e is the set of m-edge-expanding vertices, L_f is the set of s-face-expanding vertices. By definition we have

$$|E_\Lambda(L_e, L)| \geqslant m|L_e|, \qquad |E_{\Lambda^2}(L_f, L)| \geqslant s|L_f|. \tag{4}$$

[22] The parameters λ' and λ'' correspond to the edge expansion of the graphs Λ and Λ^2.

Since each labeled vertex v is either active ($v \in \operatorname{supp} c_V$) or incident to a face-active edge, and hence adjacent to at least d active faces, we get

$$|L| \leqslant \mathbf{wt}_X(c_V)+4\mathbf{wt}_X(c_F)/d \leqslant \mathbf{wt}_X(c_V)+\mathbf{wt}_X(c_F) = \mathbf{wt}_X(c) \leqslant \frac{a}{2w}$$

Hence by (a, λ')-edge-expansion of Λ we have

$$|E(L_e, L)| \leqslant \lambda'\sqrt{|L||L_e|}.$$

Similarly, from $(a/2w, \lambda'')$-edge-expansion of Λ^2 we obtain

$$|E(L_f, L)| \leqslant \lambda''\sqrt{|L||L_f|}.$$

Taking into account (4), we obtain

$$m|L_e| \leqslant \lambda'\sqrt{|L||L_e|}, \qquad s|L_f| \leqslant \lambda''\sqrt{|L||L_f|},$$

and hence

$$|L_e| \leqslant \left(\frac{\lambda'}{m}\right)^2 |L| \leqslant \frac{|L|}{4}, \qquad |L_f| \leqslant \left(\frac{\lambda''}{s}\right)^2 |L| \leqslant \frac{|L|}{4}.$$

Since $|L| = |L_e \cup L_f| \leqslant |L|/2$, we obtain $|L| = 0$. Since each active vertical edge by Lemma 14 contains labeled vertices, we have that the number of active vertical edges is 0, and hence $c = 0$. □

3.6 Proof of the theorems

Proposition 1. *For every finite field $\mathbb{F}_q$, intervals $(\rho_0, \rho_1), (\rho'_0, \rho'_1) \subseteq (0, 1)$, constant $\mu > 0$, and infinite set $W \subseteq \mathbb{N}$, there exist matrices $h \in \mathbb{F}_q^{r\times w}$, $h' \in \mathbb{F}_q^{r'\times w}$ for sufficiently large $w \in W$ such that $r/w \in (\rho_0, \rho_1)$, $r'/w \in (\rho'_0, \rho'_1)$, and for every G-lifted w-regular $(a, \mu\sqrt{w})$-edge-expanding simple graph $\hat\Gamma$ and Tanner codes $\mathcal{A} \in \mathfrak{T}_G(\hat\Gamma; h)$, $\mathcal{B} \in \mathfrak{T}_G(\hat\Gamma; h')$ with a free action of a group G we have*

$$d^{(1)}_{\mathrm{LM}}(\mathcal{A} \otimes_G \mathcal{B}^*) \geqslant a/2w,$$
$$d^{(1)}_{\mathrm{LM}}(\mathcal{B} \otimes_G \mathcal{A}^*) \geqslant a/2w.$$

Proof. Let w be a parameter which we will fix later. Define $\varepsilon := 1/6$, $m := w^{1/2+\varepsilon}$, $s := w^{1+\varepsilon}$, $r := \left\lfloor \frac{1}{2}(\rho_0 + \rho_1)w \right\rfloor$, $r' := \left\lfloor \frac{1}{2}(\rho'_0 + \rho'_1)w \right\rfloor$. By Lemma 10 with $\alpha := 1$, $\gamma := 2$, there exist $\beta_1, \beta_2 > 0$ and $\delta_1, \delta_2 > 0$ such that for random matrices $h \in \mathbb{F}_q^{r\times w}$, $h' \in \mathbb{F}_q^{r'\times w}$ as $w \to \infty$ the following three conditions hold with high probability[23]:

(1) the matrices h and h' have maximal rank, i.e. $\operatorname{rk} h = r$, $\operatorname{rk} h' = r'$;
(2) the pair $(\ker h, \operatorname{im} h'^*)$ is $(s, 2m, \beta_1)$-product-expanding and $\min(d(\ker h), d(\operatorname{im} h'^*)) \geqslant \delta_1 w$;
(3) the pair $(\operatorname{im} h^*, \ker h')$ is $(s, 2m, \beta_2)$-product-expanding and $\min(d(\ker h'), d(\operatorname{im} h^*)) \geqslant \delta_2 w$.

Therefore by the union bound for a sufficiently large $w_0 \in \mathbb{N}$ for every $w \geqslant w_0$ there exists a pair (h, h') that satisfies these three conditions. Let $\beta := \min(\beta_1, \beta_2)$, $d := \min(\delta_1, \delta_2)w$, $\lambda := \mu\sqrt{w}$, $\lambda' := 2\lambda$, $\lambda'' := 8\lambda^2(\ln w + 2)$. We have

$$d = \Theta(w), \qquad \lambda' = \Theta(w^{\frac{1}{2}}) = o(m),$$
$$m = \Theta(w^{\frac{1}{2}+\varepsilon}) = o(w) \qquad \lambda'' = \Theta(w \ln w) = o(s),$$

as $w \to \infty$. Hence there exists w_1 such that for every $w \geqslant w_1$ the following inequalities hold:

$$d > 4m, \quad \beta w \geqslant 4m + 3, \quad m > \max\left(\frac{4s}{d}, 2\lambda'\right), \quad s > 2\lambda''. \tag{5}$$

Since the set W is infinite, we can take $w := \min\{w \in W \mid w \geqslant \max(w_0, w_1)\}$ and fix some pair (h, h') that satisfy the conditions 1–3. Now consider a G-lifted (a, λ)-edge-expanding graph $\hat\Gamma$ and some G-lifted Tanner codes $\mathcal{A} \in \mathfrak{T}_G(\hat\Gamma; h)$, $\mathcal{B} \in \mathfrak{T}_G(\hat\Gamma; h')$.

Since $\min(d(\ker h), d(\ker h'), d(\operatorname{im} h^*), d(\operatorname{im} h'^*)) \geqslant d$, and conditions (5) hold, we can apply Lemma 16 to the pair of codes (h, h') and obtain that every non-zero locally minimal 1-cycle of the chain complex $\mathcal{A} \otimes_G \mathcal{B}^*$ has the weight at least $a/2w$. Hence we have

$$d^{(1)}_{\mathrm{LM}}(\mathcal{A} \otimes_G \mathcal{B}^*) \geqslant a/2w.$$

Since lemma 16 is also applicable to the pair (h', h), we have

$$d^{(1)}_{\mathrm{LM}}(\mathcal{B} \otimes_G \mathcal{A}^*) \geqslant a/2w,$$

which completes the proof of the proposition. □

Theorem 1. *For every number $R \in (0, 1/2)$ and finite field $\mathbb{F}_q$ it is possible to find universal constants s and ω such that there exists an explicit family of (ω, s)-locally testable classical LDPC codes with the parameters $[n, k \geqslant Rn, d = \Theta(n)]_q$ as $n \to \infty$.*

Proof. Fix some $R \in (0, 1/2)$ and put $\varepsilon := (1 - 2R)/(6 - 2R)$. Note that for any w from the infinite set $W := \{p + 1 \in \mathbb{N} \mid p \equiv 1 \mod 4$ and p is prime$\}$ there exist infinite family of graphs $\bar X^{w-1,t}$ from Example 1. By Lemma 5 every graph $\Gamma = \bar X^{w-1,t}$ is $(n_0(t)/\sqrt{w}, 8\sqrt{w})$-edge-expanding, where $n_0(t) = t(t^2 - 1) = |V(\Gamma)|$. Consider the chain complex

$$C := \mathcal{T}(\Gamma, h) \otimes_G \mathcal{T}^*(\Gamma; h'),$$

with the boundary operator ∂, where $G := \mathrm{PSL}(\mathbb{F}_t^2)$, and h, h' are the parity-check matrices of the local codes, which we will fix later. Let $|\cdot|$ be the block weight norm $\mathbf{wt}_X(\cdot)$ defined on C, considered as a chain complex with a local system on the cell poset $X = \Gamma \times_G \Gamma^*$. By Proposition 1 for the intervals $(1-\varepsilon, 1)$, $(0, \varepsilon)$ and the parameter $\mu = 8$ there exist $w \in W$ and matrices $h \in \mathbb{F}_q^{r\times w}$, $h' \in \mathbb{F}_q^{r'\times w}$ such that for every $\Gamma = \bar X^{w-1,t}$ we have

$$d^{(1)}_{\mathrm{LM}}(C) \geqslant n_0(t)/2w\sqrt{w}$$

where $r/w > 1-\varepsilon$, $r'/w < \varepsilon$. Let $n := \dim C_2$ and $m := \dim C_1$, then $n = n_0(t)rw$, $m = \frac{1}{2}n_0(t)(w^2 + 4rr')$. Hence $d^{(1)}_{\mathrm{LM}}(C) \geqslant \frac{n}{2w^2 r\sqrt{w}} > \frac{n}{2w^{7/2}}$. By Lemma 1 for all $c \in C_2$ we have

$$|\partial c| \geqslant \min(d^{(1)}_{\mathrm{LM}}(C), |c + Z_2(C)|).$$

Since $|y| \leqslant \mathbf{wt}(y)$ for $y \in C$ and $\mathbf{wt}(c) \leqslant r|c| \leqslant w|c|$ for $c \in C_2$, taking into account that $n \geqslant \mathbf{wt}(c + Z_2(C))$ finally we obtain

$$\mathbf{wt}(\partial c) \geqslant \min\left(\frac{n}{2w^{7/2}}, \frac{\mathbf{wt}(c + Z_2(C))}{w}\right) \geqslant \frac{1}{2w^{7/2}}\mathbf{wt}(c + Z_2(C)).$$

We have

$$\frac{m}{n} = \frac{w^2 + 4rr'}{2rw} = \frac{1 + 4\frac{r}{w}\cdot\frac{r'}{w}}{2r/w} \leqslant \frac{1 + 4\varepsilon}{2(1 - \varepsilon)} = 1 - R.$$

[23] Note that Lemma 10 is used here twice. First time h is interpreted as a parity-check matrix, but h' as a generator matrix, and the second time vice versa.

In particular, we have $m < n$, and hence

$$\frac{1}{m}\mathbf{wt}(\partial c) \geqslant \frac{w^{-7/2}}{2m}\mathbf{wt}(c + Z_2(C)) \geqslant \frac{w^{-7/2}}{2n}\mathbf{wt}(c + Z_2(C)).$$

Therefore the code $Z_2(C)$ is (ω, s)-locally testable where $\omega := 2w$ and $s := \frac{1}{2}w^{-7/2}$. For the dimension $k = \dim Z_2(C)$ we have $k \geqslant n - m \geqslant Rn$.

To complete the proof we also need to show that the linear code $Z_2(C)$ has the minimal distance $\Theta(n)$ as $n \to \infty$. It is not hard to see that the minimal distance of $Z_2(C)$ is not less than the distance of the component Tanner code $\mathcal{T}(\bar{X}^{w-1,t}, h)$, which is a classical expander code [45]. Thus, as it follows from the proof of Proposition 1, we can fix a sufficiently large number w such that $d(\ker h) > \lambda_2(\bar{X}^{w-1,t})$ and obtain that $d(\mathcal{T}(\bar{X}^{w-1,t}, h)) = \Theta(n)$ as $n \to \infty$. □

Theorem 2. *For every number $R \in (0, 1)$ and finite field $\mathbb{F}_q$ there exists an explicit family of quantum LDPC codes over $\mathbb{F}_q$ with the parameters $[\![n, k \geqslant Rn, d = \Theta(n)]\!]_q$ as $n \to \infty$.*

Proof. Fix some $R \in (0, 1)$. Note that for every w from the infinite set $W := \{p + 1 \in \mathbb{N} \mid p \equiv 1 \mod 4 \text{ and } p \text{ is prime}\}$ there exist infinite family of graphs $\bar{X}^{w-1,t}$ from Example 1. By Lemma 5 the graph $\Gamma = \bar{X}^{w-1,t}$ is $(n_0(t)/\sqrt{w}, 8\sqrt{w})$-edge-expanding where $n_0(t) = t(t^2 - 1) = |V(\Gamma)|$. As in the proof of Theorem 1, we consider the complex $C = \mathcal{T}(\Gamma; h) \otimes_G \mathcal{T}^*(\Gamma; h')$ with the boundary operator ∂ where $G = \mathrm{PSL}(\mathbb{F}_t^2)$. Let $|\cdot|$ be the block weight defined on C. By Proposition 1 for $\rho_0 = \rho_0' = 0$, $\rho_1 = \rho_1' = (1 - R)/4$, and $\mu = 8$ there exist $w \in W$ and matrices $h \in \mathbb{F}_q^{r \times w}$, $h' \in \mathbb{F}_q^{r' \times w}$ such that for all $\Gamma = \bar{X}^{w-1,t}$ we have

$$d^{(1)}_{\mathrm{LM}}(C) \geqslant n_0(t)/2w\sqrt{w}, \qquad d^{(1)}_{\mathrm{LM}}(C^*) \geqslant n_0(t)/2w\sqrt{w}$$

where $r/w < (1 - R)/4$, $r'/w < (1 - R)/4$. Let $n := \dim C_1$, then $n = \frac{1}{2}n_0(t)(w^2 + 4rr') < w^2 n_0(t)$. The chain complex C defines the quantum CSS code $Q = Q(H_X, H_Z)$ with the parity-check matrices $H_X := \partial_1$ and $H_Z := \partial_2^*$. By Lemma 1 for the complex C we have

$$d_X(Q) = d(H_1(C)) \geqslant d^{(1)}_{\mathrm{LM}}(C) \geqslant \frac{n_0(t)}{2w\sqrt{w}} > \frac{n}{2w^{7/2}}.$$

Similarly, since the dual chain complex C^* is isomorphic[24] to the chain complex $\mathcal{B} \otimes_G \mathcal{A}^*$, then by Lemma 1 we have

$$d_Z(Q) = d(H_1(C^*)) \geqslant d^{(1)}_{\mathrm{LM}}(C^*) > \frac{n}{2w^{7/2}},$$

and hence $d(Q) = \min(d_X(Q), d_Z(Q)) \geqslant \frac{1}{2}n/w^{7/2}$. To complete the proof we also need to estimate the dimension $k = \dim(H_1(C))$ of the quantum code Q. We have

$$\dim C_0 = n_0(t)rw = 2n\frac{rw}{w^2 + 4rr'} < n(1 - R)/2,$$

$$\dim C_2 = n_0(t)r'w = 2n\frac{r'w}{w^2 + 4rr'} < n(1 - R)/2,$$

and therefore

$$k = \dim(H_1(C)) \geqslant n - \dim C_0 - \dim C_2 > n - n(1 - R)/2 - n(1 - R)/2 = nR.$$

Thus Q is a w-limited quantum CSS code with the parameters $[\![n, k \geqslant Rn, d \geqslant \frac{1}{2}n/w^{7/2}]\!]_q$. □

CONCLUSIONS

In this work, we showed that there exist asymptotically good families of quantum LDPC codes, which proves the well-known qLDPC conjecture. We also conjecture that a decoder, similar to the small-set-flip decoding algorithm from [36] (see also [18]), can be used to correct in linear time any adversarial errors up to the constant fraction of the code length.

The constructed qLDPC codes were obtained from the G-lifted product of two G-lifted Tanner codes, and to obtain qLDPC codes of linear minimum distance a non-abelian group G was used. In fact, it is not hard to see that Proposition 1 implies that using the $\mathbf{C}_\ell$-lifted product of two $\mathbf{C}_\ell$-lifted Tanner codes from [44], where $\mathbf{C}_\ell$ is the cyclic group of size $\ell = \Theta(n/\log n)$, one can obtain qLDPC codes with the parameters $[\![n, k = \Theta(n), d = \Theta(n/\log n)]\!]_q$ as $n \to \infty$. Note that very recent results on explicit $\mathbf{C}_\ell$-lifted expander graphs from [29] implies that the construction of these qLDPC codes can also be made explicit.

In addition, as a byproduct of our proof of the qLDPC conjecture, we show that the second homology groups of the constructed in this work chain complexes can be used to obtain asymptotically good families of classical LDPC codes, which are also locally testable with constant query and soundness parameters. This resolves an important conjecture in the field of locally-testable codes[25].

Though all the constructions we propose here can be considered as explicit, the constant size local codes used in our expander codes are still obtained by probabilistic methods. We think that it is an interesting open problem to find an explicit construction of such codes. One possible option would be to use MDS codes such as Reed-Solomon codes. In fact, such non-binary local codes can be used even if we want to get codes over $\mathbb{F}_2$ since every classical and quantum code over $\mathbb{F}_{2^s}$ can be also considered as a code over $\mathbb{F}_2$, and the rate and minimal distance of such a code is at least as good as for the non-binary one. However, it is not clear whether one can find a pair of MDS codes that satisfies the product-expansion property required for our proof to work.

We also hope that some of the methods developed in the current work can be used to show the existence of locally-testable qLDPC codes required to prove the qLTC conjecture, which in turn implies [17] the NLTS conjecture. A natural candidate for such a code would be a 5-term chain complex, where the three middle terms corresponds to a good qLDPC code, and the remaining two terms represents its X- and Z-meta-checks (i.e., checks on checks). In fact, similar 5-term complexes were already used in the context of single-shot decoding of qLDPC codes [10, Figure 1].

ACKNOWLEDGMENT

We would like to thank Nikolas Breuckmann and Jens Eberhardt for very helpful and insightful discussions of possible ways to get good qLDPC codes, and for an opportunity to report our results in the QCDA seminar. We want to express our gratitude to many people, including Thomas Vidick, Sergey Sadov, Victor Albert, Shouzhen

[24] We say that two based chain complexes C and C' over $\mathbb{F}_q$ with distinguished bases X and X' are *isomorphic* if there exists a one-to-one $\mathbb{F}_q$-linear map $f\colon C \to C'$ such that $f(X_i) = X'_i$ for every $i \in \mathbb{Z}$.

[25] An independent solution to this problem was also proposed in [15].

Gu, who read our manuscript and made a number of valuable comments. We also want to thank anonymous reviewers for indicating several unclear places in our work and for pointing out the connection of our product-expansion property to the robust testability of tensor product codes.

This work was supported by the Ministry of Science and Higher Education of the Russian Federation (Grant 075-15-2020-801).

REFERENCES

[1] Dorit Aharonov and Lior Eldar. 2015. Quantum Locally Testable Codes. *SIAM J. Comput.* 44, 5 (Jan. 2015), 1230–1262. https://doi.org/10.1137/140975498

[2] D. Bacon, S. T. Flammia, A. W. Harrow, and J. Shi. 2017. Sparse quantum codes from quantum circuits. *IEEE Transactions on Information Theory* 63, 4 (2017), 2464–2479. https://doi.org/10.1109/TIT.2017.2663199

[3] Eli Ben-Sasson and Madhu Sudan. 2006. Robust locally testable codes and products of codes. *Random Structures & Algorithms* 28, 4 (2006), 387–402. https://doi.org/10.1002/rsa.20120

[4] Thomas C. Bohdanowicz, Elizabeth Crosson, Chinmay Nirkhe, and Henry Yuen. 2019. Good approximate quantum LDPC codes from spacetime circuit Hamiltonians. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing (STOC 2019)*. Association for Computing Machinery, New York, NY, USA, 481–490. https://doi.org/10.1145/3313276.3316384

[5] Sergey Bravyi and Matthew B. Hastings. 2014. Homological product codes. In *Proceedings of the forty-sixth annual ACM symposium on theory of computing (STOC '14)*. ACM, New York, NY, USA, 273–282. https://doi.org/10.1145/2591796.2591870

[6] Nikolas P. Breuckmann and Jens N. Eberhardt. 2021. Balanced Product Quantum Codes. *IEEE Transactions on Information Theory* 67, 10 (Oct. 2021), 6653–6674. https://doi.org/10.1109/TIT.2021.3097347

[7] Nikolas P. Breuckmann and Jens Niklas Eberhardt. 2021. Quantum Low-Density Parity-Check Codes. *PRX Quantum* 2, 4 (Oct. 2021), 040101. https://doi.org/10.1103/PRXQuantum.2.040101

[8] Kenneth S. Brown. 1982. Some Homological Algebra. In *Cohomology of Groups*, Kenneth S. Brown (Ed.). Springer, New York, NY, 4–32. https://doi.org/10.1007/978-1-4684-9327-6_2

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

[10] Earl T. Campbell. 2019. A theory of single-shot error correction for adversarial noise. *Quantum Science and Technology* 4, 2 (Feb. 2019), 025006. https://doi.org/10.1088/2058-9565/aafc8f

[11] R. Chien and S. Ng. 1973. Dual Product Codes for Correction of Multiple Low-Density Burst Errors. *IEEE Transactions on Information Theory* 19, 5 (Sept. 1973), 672–677. https://doi.org/10.1109/TIT.1973.1055085

[12] Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill. 2002. Topological quantum memory. *J. Math. Phys.* 43, 9 (2002), 4452–4505. https://doi.org/10.1063/1.1499754

[13] Yotam Dikstein, Irit Dinur, Prahladh Harsha, and Noga Ron-Zewi. 2020. Locally testable codes via high-dimensional expanders. arXiv:2005.01045 [cs]

[14] Irit Dinur. 2007. The PCP theorem by gap amplification. *J. ACM* 54, 3 (June 2007), 12–es. https://doi.org/10.1145/1236457.1236459

[15] Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes. 2021. Locally Testable Codes with constant rate, distance, and locality. arXiv:2111.04808 [cs, math]

[16] Irit Dinur, Madhu Sudan, and Avi Wigderson. 2006. Robust Local Testability of Tensor Products of LDPC Codes. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (Lecture Notes in Computer Science)*, Josep Díaz, Klaus Jansen, José D. P. Rolim, and Uri Zwick (Eds.). Springer, Berlin, Heidelberg, 304–315. https://doi.org/10.1007/11830924_29

[17] Lior Eldar and Aram W. Harrow. 2017. Local Hamiltonians Whose Ground States Are Hard to Approximate. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, Berkeley, CA, USA, 427–438. https://doi.org/10.1109/FOCS.2017.46

[18] Shai Evra, Tali Kaufman, and Gilles Zémor. 2020. Decodable quantum LDPC codes beyond the square root distance barrier using high dimensional expanders. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, Durham, NC, USA, 218–227. https://doi.org/10.1109/FOCS46700.2020.00029

[19] Michael H Freedman, David A Meyer, and Feng Luo. 2002. $\mathbb{Z}_2$-systolic freedom and quantum codes. In *Mathematics of quantum computation*, Ranee K. Brylinski and Goong Chen (Eds.). Chapman & Hall/CRC, New York, Chapter 12, 287–320. https://doi.org/10.1201/9781420035377

[20] R. G. Gallager. 1963. *Low-density parity-check codes*. M.I.T. Press, Cambridge, MA. https://doi.org/10.7551/mitpress/4347.001.0001

[21] Oded Goldreich. 2010. Short Locally Testable Codes and Proofs: A Survey in Two Parts. In *Property Testing: Current Research and Surveys*, Oded Goldreich (Ed.). Springer, Berlin, Heidelberg, 65–104. https://doi.org/10.1007/978-3-642-16367-8_6

[22] O. Goldreich and M. Sudan. 2002. Locally testable codes and PCPs of almost-linear length. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.* IEEE, Vancouver, BC, Canada, 13–22. https://doi.org/10.1109/SFCS.2002.1181878

[23] Larry Guth and Alexander Lubotzky. 2014. Quantum error correcting codes and 4-dimensional arithmetic hyperbolic manifolds. *J. Math. Phys.* 55, 8 (Aug. 2014), 082202. https://doi.org/10.1063/1.4891487

[24] Jeongwan Haah. 2011. Local stabilizer codes in three dimensions without string logical operators. *Physical Review A* 83, 4 (April 2011), 042330. https://doi.org/10.1103/PhysRevA.83.042330

[25] M. Hagiwara and H. Imai. 2007. Quantum quasi-cyclic LDPC codes. In *2007 IEEE international symposium on information theory*. IEEE, Nice, France, 806–810. https://doi.org/10.1109/ISIT.2007.4557323

[26] M. B. Hastings. 2021. On Quantum Weight Reduction. arXiv:2102.10030 [quant-ph]

[27] Matthew B. Hastings, Jeongwan Haah, and Ryan O'Donnell. 2021. Fiber bundle codes: breaking the $N^{1/2}$ polylog(N) barrier for Quantum LDPC codes. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. Association for Computing Machinery, New York, NY, USA, 1276–1288. https://doi.org/10.1145/3406325.3451005

[28] Shlomo Hoory, Nathan Linial, and Avi Wigderson. 2006. Expander Graphs and Their Applications. *Bull. Amer. Math. Soc.* 43, 04 (Aug. 2006), 439–562. https://doi.org/10.1090/s0273-0979-06-01126-8

[29] Fernando Granha Jeronimo, Tushant Mittal, Ryan O'Donnell, Pedro Paredes, and Madhur Tulsiani. 2022. Explicit Abelian Lifts and Quantum LDPC Codes. In *13th Innovations in Theoretical Computer Science Conference (ITCS 2022) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 215)*, Mark Braverman (Ed.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 88:1–88:21. https://doi.org/10.4230/LIPIcs.ITCS.2022.88

[30] Tali Kaufman, David Kazhdan, and Alexander Lubotzky. 2014. Ramanujan Complexes and Bounded Degree Topological Expanders. In *2014 IEEE 55th Annual Symposium on Foundations of Computer Science*. IEEE, Philadelphia, PA, USA, 484–493. https://doi.org/10.1109/FOCS.2014.58

[31] Tali Kaufman and Alexander Lubotzky. 2014. High dimensional expanders and property testing. In *Proceedings of the 5th conference on Innovations in theoretical computer science (ITCS '14)*. Association for Computing Machinery, New York, NY, USA, 501–506. https://doi.org/10.1145/2554797.2554842

[32] Tali Kaufman and Madhu Sudan. 2007. Sparse Random Linear Codes are Locally Decodable and Testable. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*. IEEE, Providence, RI, USA, 590–600. https://doi.org/10.1109/FOCS.2007.8

[33] Tali Kaufman and Ran J. Tessler. 2021. 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*. Association for Computing Machinery, New York, NY, USA, 1317–1329. https://doi.org/10.1145/3406325.3451029

[34] Alexey A. Kovalev and Leonid P. Pryadko. 2013. Quantum Kronecker sum-product low-density parity-check codes with finite rate. *Physical Review A* 88, 1 (July 2013), 012311. https://doi.org/10.1103/PhysRevA.88.012311

[35] Anthony Leverrier, Vivien Londe, and Gilles Zémor. 2022. Towards local testability for quantum coding. *Quantum* 6 (Feb. 2022), 661. https://doi.org/10.22331/q-2022-02-24-661

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

[37] A. Lubotzky, R. Phillips, and P. Sarnak. 1988. Ramanujan graphs. *Combinatorica* 8, 3 (Sept. 1988), 261–277. https://doi.org/10.1007/BF02126799

[38] D. J. C. MacKay, G. Mitchison, and P. L. McFadden. 2004. Sparse-graph codes for quantum error correction. *IEEE Transactions on Information Theory* 50, 10 (Oct. 2004), 2315–2330. https://doi.org/10.1109/TIT.2004.834737

[39] F. J. MacWilliams and N. J. A. Sloane. 1977. *The Theory of Error-Correcting Codes* (first ed.). North Holland Publishing Co., Amsterdam.

[40] Grigorii Aleksandrovich Margulis. 1988. Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators. *Problemy peredachi informatsii* 24, 1 (1988), 51–60.

[41] Roy Meshulam. 2018. Graph codes and local systems. arXiv:1803.05643 [math]

[42] Pavel Panteleev and Gleb Kalachev. 2021. Asymptotically Good Quantum and Locally Testable Classical LDPC Codes. arXiv:2111.03654 [quant-ph] http://arxiv.org/abs/2111.03654

[43] Pavel Panteleev and Gleb Kalachev. 2021. Degenerate Quantum LDPC Codes With Good Finite Length Performance. *Quantum* 5 (Nov. 2021), 585. https://doi.org/10.22331/q-2021-11-22-585

[44] Pavel Panteleev and Gleb Kalachev. 2022. Quantum LDPC Codes With Almost Linear Minimum Distance. *IEEE Transactions on Information Theory* 68, 1 (Jan. 2022), 213–229. https://doi.org/10.1109/TIT.2021.3119384

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

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

[47] R. Tanner. 1981. A recursive approach to low complexity codes. *IEEE Transactions on Information Theory* 27, 5 (Sept. 1981), 533–547. https://doi.org/10.1109/TIT.1981.1056404

[48] J. Tillich and G. Zémor. 2009. Quantum LDPC codes with positive rate and minimum distance proportional to $n^{1/2}$. In *2009 IEEE international symposium on information theory*. IEEE, Seoul, Korea (South), 799–803. https://doi.org/10.1109/ISIT.2009.5205648

[49] J. Tillich and G. Zémor. 2014. Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength. *IEEE Transactions on Information Theory* 60, 2 (Feb. 2014), 1193–1202. https://doi.org/10.1109/TIT.2013.2292061

[50] Daniel T. Wise. 2007. Complete square complexes. *Commentarii Mathematici Helvetici* 82, 4 (Dec. 2007), 683–724. https://doi.org/10.4171/cmh/107

[51] J. Wolf. 1965. On Codes Derivable from the Tensor Product of Check Matrices. *IEEE Transactions on Information Theory* 11, 2 (April 1965), 281–284. https://doi.org/10.1109/TIT.1965.1053771

[52] Weilei Zeng and Leonid P. Pryadko. 2019. Higher-dimensional quantum hypergraph-product codes with finite rates. *Physical Review Letters* 122, 23 (June 2019), 230501. https://doi.org/10.1103/PhysRevLett.122.230501