Homological Product Codes

Sergey Bravyi
IBM T. J. Watson Research Center
Yorktown Heights, NY 10598
sbravyi@us.ibm.com

Matthew B. Hastings
Microsoft Research, Station Q
CNSI Building, UCSB, CA, 93106
and
Quantum Architectures and Computation Group,
Microsoft Research, Redmond, WA 98052
mahastin@microsoft.com

ABSTRACT

Quantum codes with low-weight stabilizers known as LDPC codes have been actively studied recently due to their potential applications in fault-tolerant quantum computing. However, all families of quantum LDPC codes known to this date suffer from a poor distance scaling limited by the square-root of the code length. This is in a sharp contrast with the classical case where good families of LDPC codes are known that combine constant encoding rate and linear distance. Here we propose the first family of good quantum codes with low-weight stabilizers. The new codes have a constant encoding rate, linear distance, and stabilizers acting on at most $O(\sqrt{n})$ qubits, where n is the code length. For comparison, all previously known families of good quantum codes have stabilizers of linear weight. Our proof combines two techniques: randomized constructions of good quantum codes and the homological product operation from algebraic topology. We conjecture that similar methods can produce good stabilizer codes with stabilizer weight $O(n^\alpha)$ for any $\alpha > 0$.

Categories and Subject Descriptors

E.4 [**Coding and Information Theory**]: Error control codes

General Terms

Theory

Keywords

Quantum error correcting codes, homology theory

1. INTRODUCTION

Classical low density parity check codes are characterized by the property that their parity checks act only on $O(1)$ bits. Such codes have found numerous applications due to their efficient decoding algorithms based on the belief propagation and high transmission rates approaching the channel capacity limit [18, 25]. In addition to showing good practical performance, some families of LDPC codes are good in the coding theory sense featuring a linear minimum distance and, at the same time, constant encoding rate. Some LDPC codes are known to achieve the Gilbert-Varshamov bound on the code parameters [25].

The recently emerged field of quantum error correction attempts to apply coding theory principles to the challenging tasks of fault-tolerant quantum computing and reliable transmission of quantum imformation. A natural question that we investigate here is whether good LDPC codes have a quantum analogue. We shall focus on the simplest construction of quantum codes due to Calderbank, Shor, and Steane (CSS) [10]. A quantum CSS code encoding k qubits into n qubits is constructed from a pair of classical linear codes of length n responsible for detecting bit-flip and phase-flip errors. Let A and B be the parity check matrices of the two classical codes. Each row of A or B gives rise to a stabilizer operator which is a product of Pauli operators Z or X respectively over all qubits in the support of the chosen row. Valid codewords are n-qubit quantum states invariant under the action of any stabilizer, whereas corrupted codewords may violate one or several stabilizers. The requirement that codewords must satisfy both types of stabilizers simultaneously translates to a peculiar condition that rows of A and B must be pairwise orthogonal,

$$AB^T = 0. \tag{1}$$

The number of logical qubits is determined by

$$k = n - \operatorname{rank} A - \operatorname{rank} B. \tag{2}$$

Finally, the code distance d is defined as the minimum weight of a Pauli error that can corrupt a codeword without being detected. For a CSS code $d = \min\{d^X, d^Z\}$, where

$$\begin{aligned} d^X &= \min\{\mathrm{wt}\,(f) \,:\, f \in \ker A \backslash \operatorname{im} B^T\}, \\ d^Z &= \min\{\mathrm{wt}\,(f) \,:\, f \in \ker B \backslash \operatorname{im} A^T\}. \end{aligned} \tag{3}$$

Here and below $\mathrm{wt}\,(f)$ denotes the Hamming weight of a binary vector f. We shall use the standard notation $[[n, k, d]]$ for a CSS code defined above. A family of codes is called *good* if it has a constant encoding rate k/n and a constant relative distance d/n in the limit $n \to \infty$.

When it comes to applications in quantum computing, an important parameter of a code is the *stabilizer weight* w defined as the maximum weight of any row and any column in the parity check matrices A, B. Fault-tolerance considerations strongly favor quantum codes with small stabilizer

STOC '14, May 31 - June 03 2014, New York, NY, USA

http://dx.doi.org/10.1145/2591796.2591870.

weight as it simplifies syndrome measurement at the recovery step [23, 13, 19]. A family of codes is said to be LDPC iff $w = O(1)$ in the limit $n \to \infty$. Quantum LDPC codes are largely responsible for the recent progress in quantum fault-tolerance theory [28, 14, 19]. However, in spite of significant efforts, constructing good quantum LDPC codes or merely proving that such codes exist remains an elusive goal. Here we make a step towards this goal by showing how to combine two previously known techniques: randomized constructions of good codes and homological constructions of LDPC codes. Our main result is as follows.

THEOREM 1. *There exists a family of good CSS codes with stabilizer weight $w \le 2\sqrt{n}$.*

For comparison, all previously known constructions of good quantum codes [10, 2, 29] have stabilizer weight linear in n. While Theorem 1 falls short of proving the existence of good quantum LDPC codes, we believe that it can be improved in several respects; see the discussion below.

The key ingredient in the proof of Theorem 1 is the homological product operation introduced by Freedman and one of the authors [15]. The present paper uses a simplified version of the construction proposed in [15] which we describe in Section 3. The homological product takes as input a pair of CSS codes and produces a larger CSS code that encodes more qubits and typically has larger distance than each of the input codes. To make this more quantitative, the homological product of two CSS codes $[[n_a, k_a, d_a]]$, $a = 1, 2$, is a CSS code $[[n_1 n_2, k_1 k_2, d]]$ with stabilizer weight $w \le n_1 + n_2$. The distances d^X, d^Z of the product code obey $\max\{d_1^\alpha, d_2^\alpha\} \le d^\alpha \le d_1^\alpha d_2^\alpha$, where $\alpha = X, Z$. These properties are proved in Section 3. As was shown in Ref. [15], the homological product is a natural generalization of the hypergraph product construction by Tillich and Zémor [30]. The latter takes as input a pair of *classical* LDPC codes $[n_a, k_a, d_a]$ and produces a quantum LDPC code with parameters $[[O(n_1 n_2), k_1 k_2, d]]$, where $d = \min\{d_1, d_2\}$, see [30, 24]. Since $d_a \le n_a$, the hypergraph product cannot achieve distance growing faster than the square-root of the code length.

We construct the family of codes as stated in Theorem 1 by taking the homological product of two *random* CSS codes with a fixed length $n_1 = n_2 = \sqrt{n}$ and fixed number of logical qubits $k_a = \rho\, n_a$ for some constant encoding rate $\rho > 0$. Note that random CSS codes are good with high probability [10], although their stabilizer weight is linear in the code length. We define a suitable ensemble of random CSS codes and prove their goodness in Section 4. The product of two random codes as above yields a code $[[n, \rho^2 n, d]]$ with stabilizer weight $w \le 2\sqrt{n}$, where the distance d is a random variable. The main technical challenge, addressed in Section 5, is to prove that the product code has a linear distance with high probability, that is, $d \ge cn$ for some constant $c > 0$. As explained there, the standard "first moment method" based on counting the number of low weight logical operators does not work to prove this result. To overcome this, we need two new ingredients. First, we use the so-called Cleaning Lemma which has been previously used to obtain upper bounds on parameters of quantum LDPC codes [9, 8, 6, 21]. Second, we introduce a "uniform low weight" condition which plays the central role in our proof and enables us to derive a strong enough large deviation bound for the weight of logical operators, see Section 5.

A natural question is whether the stabilizer weight $w = O(\sqrt{n})$ in Theorem 1 can be improved by considering m-fold products. The homological product of m input codes $[[n_a, k_a, d_a]]$ has parameters $n = \prod_{a=1}^m n_a$, $k = \prod_{a=1}^m k_a$, and stabilizer weight $w \le \sum_{a=1}^m n_a$. Suppose all input codes have the same length $n_a = n^{1/m}$ and the same number of logical qubits $k_a = \rho n_a$ for some constant $\rho > 0$. Then the product code has encoding rate $k/n = \rho^m$ and stabilizer weight $w \le m n^{1/m}$. Although the distance of the product code is very difficult to compute, we hope that the techniques developed in this paper can be generalized to the m-fold product for $m = O(1)$. Proving that the product code has distance $d = \Omega(n)$ with high probability would establish existence of good quantum codes with stabilizer weight $w \le n^\epsilon$ for any constant $\epsilon > 0$. Furthermore, in the long version of this paper [7] we propose a proof strategy which, if successful, could reduce the stabilizer weight from n^ϵ to $O(1)$ at the cost of slightly increasing the code length.

2. PREVIOUS WORK

The observation that the theory of CSS codes has a natural interpretation in terms of homology, in particular $\mathbb{Z}_2$ homology, goes back to the pioneering works by Kitaev [23], Freedman and Meyer [16], as well as Bombin and Martin-Delgado [5]. Here we review some constructions of quantum LDPC codes focusing on those obtained by homological tools. We leave aside alternative constructions of LDPC codes based on algebraic and graph-theoretic methods [27, 26, 11, 1].

Notable codes include hyperbolic surface codes and color codes [31, 12] which are generalizations of the toric code [23] defined on a surface of constant negative curvature and large injectivity radius. These codes achieve a constant encoding rate and a slowly growing distance. The toric code has been generalized to higher-dimensional manifolds by Freedman et al [17]. Using a rather complicated 3D manifold the authors of Ref. [17] obtained the first (and currently the only) example of a quantum LDPC code with the distance growing faster than $\sqrt{n}$. This code however has only $O(1)$ logical qubits. In a recent breakthrough work Tillich and Zémor [30] proposed a method of constructing quantum LDPC code from a pair of classical LDPC codes. The hypergraph product codes of Ref. [30] were shown to admit a natural description as a homological product of chain complexes [15]. An improved version of the hypergraph product codes was proposed by Kovalev and Pryadko [24]. Interesting homological constructions of LDPC codes based on knots and links were found by Audoux [3]. There are also examples of LDPC codes, such as Haah's cubic code [20], with a large gap between the best known lower and upper bounds on the distance which leaves a possibility of faster than $\sqrt{n}$ distance scaling. We summarize parameters of the known quantum LDPC codes and the new product codes in Table 1.

3. HOMOLOGICAL PRODUCT CODES

In this section we define the homological product construction needed for the proof of Theorem 1. We refer the reader to Refs. [15, 7] for the interpretation of this construction in terms of the homology theory. Throughout this paper we consider linear vector spaces and linear maps over the binary field. We shall use notations $\ker A$ and $\operatorname{im} A$ for the kernel

	k	d	w
Surface codes	$O(1)$	$O(\sqrt{n})$	4
Hyperbolic surface codes	$\Omega(n)$	$\Omega(\log n)$	$O(1)$
Generalized 3D toric codes	$O(1)$	$\Omega(\sqrt{n \log n})$	$O(1)$
Hypergraph product codes	$\Omega(n)$	$\Omega(\sqrt{n})$	$O(1)$
Homological product codes (new)	$\Omega(n)$	$\Omega(n)$	$O(\sqrt{n})$

Table 1: Parameters of some quantum LDPC codes described in Section 2.

and the image of a linear map A. We shall use a standard notation $[n] \equiv \{1, 2, \ldots, n\}$.

We begin by introducing some terminology. Let $\delta : \mathcal{C} \to \mathcal{C}$ be a linear operator on some space $\mathcal{C}$. We will say that δ is a *boundary operator* iff $\delta^2 = 0$. A *homological dimension* of a boundary operator δ is defined as

$$H(\delta) = \dim(\ker \delta) - \dim(\operatorname{im} \delta). \tag{4}$$

We shall always assume that $\mathcal{C}$ is equipped with the standard basis such that all basis vectors have weight one. Then the transposed operator δ^T is well-defined. The pair $(\mathcal{C}, \delta)$ will be referred to as a *complex*. A vector $f \in \mathcal{C}$ is called a *cycle* or *co-cycle* iff $\delta f = 0$ or $\delta^T f = 0$ respectively. A cycle or co-cycle f is called *trivial* iff $f \in \operatorname{im} \delta$ or $f \in \operatorname{im} \delta^T$ respectively.

Given a complex $(\mathcal{C}, \delta)$ define a quantum code $\mathrm{CSS}(\mathcal{C}, \delta)$ with parity check matrices $A = \delta$ and $B = \delta^T$. Note that the orthogonality condition $AB^T = 0$ is satisfied since $\delta^2 = 0$. From Eqs. (2,3) we infer that $\mathrm{CSS}(\mathcal{C}, \delta)$ has parameters $[[n, k, d]]$ and stabilizer weight w, where $n = \dim(\mathcal{C})$, $k = n - 2\operatorname{rank}(\delta) = H(\delta)$, while $d = \min\{d^X, d^Z\}$ where

$$\begin{aligned} d^Z &= \min\{\mathrm{wt}(f) \,:\, f \in \ker \delta \setminus \operatorname{im} \delta\}, \\ d^X &= \min\{\mathrm{wt}(f) \,:\, f \in \ker \delta^T \setminus \operatorname{im} \delta^T\}. \end{aligned} \tag{5}$$

Note that d^Z and d^X is the minimum weight of any non-trivial cycle and cocyle respectively. The stabilizer weight w is equal to the maximum weight of any column and any row of δ.

Let $(\mathcal{C}_1, \delta_1)$ and $(\mathcal{C}_2, \delta_2)$ be an arbitrary pair of complexes. Define an operator

$$\partial = \delta_1 \otimes I + I \otimes \delta_2 \tag{6}$$

acting on the tensor product space $\mathcal{C}_1 \otimes \mathcal{C}_2$. Here I is the identity operator. We shall always equip the space $\mathcal{C}_1 \otimes \mathcal{C}_2$ with the product basis $i \otimes j$, where i and j are basis vectors of $\mathcal{C}_1$ and $\mathcal{C}_2$. The property $\delta_a^2 = 0$ implies that $\partial^2 = 2\delta_1 \otimes \delta_2 = 0$ since we work with the binary field. Thus ∂ is a boundary operator. We shall refer to the complex $(\mathcal{C}_1 \otimes \mathcal{C}_2, \partial)$ as a product of complexes $(\mathcal{C}_1, \delta_1)$ and $(\mathcal{C}_2, \delta_2)$.

One important property of the product complex is that we can easily compute its homological dimension from the ones of individual complexes. The following simple fact is a special case of the well-known Künneth formula, see for instance Ref. [22].

LEMMA 1. *Let δ_1, δ_2 be any boundary operators and let $\partial = \delta_1 \otimes I + I \otimes \delta_2$. Then*

$$\ker \partial = \ker \delta_1 \otimes \ker \delta_2 + \operatorname{im} \partial \tag{7}$$

and

$$H(\partial) = H(\delta_1) \cdot H(\delta_2). \tag{8}$$

PROOF. Consider any vector $f \in \ker \partial$. Define a vector $g = (\delta_1 \otimes I) f = (I \otimes \delta_2) f$. By construction, $g \in (\operatorname{im} \delta_1 \otimes \mathcal{C}_2) \cap (\mathcal{C}_1 \otimes \operatorname{im} \delta_2) = \operatorname{im} \delta_1 \otimes \operatorname{im} \delta_2$, that is, $g = (\delta_1 \otimes \delta_2) h$ for some $h \in \mathcal{C}_1 \otimes \mathcal{C}_2$. Identities $\delta_a^2 = 0$ then lead to $(\delta_1 \otimes I)(f + \partial h) = 0$ and $(I \otimes \delta_2)(f + \partial h) = 0$, that is, $f + \partial h \in (\ker \delta_1 \otimes \mathcal{C}_2) \cap (\mathcal{C}_1 \otimes \ker \delta_2) = \ker \delta_1 \otimes \ker \delta_2$ This proves the inclusion $\subseteq$ in Eq. (7). The inclusion $\supseteq$ follows trivially from $\delta_a^2 = 0$ and $\partial^2 = 0$. It remains to prove Eq. (8). One can easily check that $\operatorname{im} \delta_1 \otimes \ker \delta_2 \subseteq \operatorname{im} \partial$ and $\ker \delta_1 \otimes \operatorname{im} \delta_2 \subseteq \operatorname{im} \partial$. Thus Eq. (7) implies that $\ker \partial / \operatorname{im} \partial$ has a basis $h_1^i \otimes h_2^j$, where $\{h_a^i\}_i$ is a basis of $\ker \delta_a / \operatorname{im} \delta_a$. This proves Eq. (8). □

Let w_a be the maximum weight of rows and columns of the boundary operator δ_a. Note that any row and any column of $\delta_1 \otimes I$ has weight at most w_1. Likewise, any row and any column of $I \otimes \delta_2$ has weight at most w_2. The triangle inequality implies that any row and any column of ∂ has weight at most $w_1 + w_2$. Combining this observation and Lemma 1 we conclude that the code $\mathrm{CSS}(\mathcal{C}_1 \otimes \mathcal{C}_2, \partial)$ has parameters $[[n, k, d]]$ and stabilizer weight w, where

$$n = \dim(\mathcal{C}_1) \cdot \dim(\mathcal{C}_2), \quad k = H(\delta_1) \cdot H(\delta_2), \quad w \le w_1 + w_2.$$

We shall refer to $\mathrm{CSS}(\mathcal{C}_1 \otimes \mathcal{C}_2, \partial)$ as a *product code*. Unfortunately, the problem of computing the distance d of the product code for a given pair of input complexes $(\mathcal{C}_a, \delta_a)$ appears to be hard. Although it is not necessary for the proof of Theorem 1, below we provide lower and upper bounds on d. In general, neither of these bounds is tight, although the upper bound may be tight in some special cases, see [7] for details and the proof of the lemma.

LEMMA 2. *Let d_a^Z and d_a^X be the minimum weight of non-trivial cycles and co-cycles in the complex $(\mathcal{C}_a, \delta_a)$. Let d^Z and d^X be the minimum weight of non-trivial cycles and co-cycles in the product complex $(\mathcal{C}_1 \otimes \mathcal{C}_2, \partial)$. Then*

$$\max\{d_1^\alpha, d_2^\alpha\} \le d^\alpha \le d_1^\alpha d_2^\alpha, \quad \alpha = X, Z. \tag{9}$$

4. RANDOM CODES FROM RANDOM COMPLEXES

In this section we define a random ensemble of boundary operators used throughout this paper. We will show that the corresponding CSS code is good with high probability. First we derive a canonical form of a boundary operator.

LEMMA 3. *Consider any complex $(\mathcal{C}, \delta)$ such that δ has homological dimension H and rank L. Then $\delta = U \delta_0 U^{-1}$, where U is some invertible matrix and δ_0 is the canonical boundary operator defined as a block matrix*

$$\delta_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & I \\ 0 & 0 & 0 \end{pmatrix}. \tag{10}$$

Here rows and columns are grouped into blocks of size H, L, L. Furthermore, the number of invertible matrices U such that $\delta = U\delta_0 U^{-1}$ does not depend on δ.

The proof of Lemma 3 is provided in the Appendix. Let us fix integers H, M such that $1 \le H \le M$. Below we consider a random boundary operator δ distributed uniformly on the set of all $M \times M$ matrices satisfying $\delta^2 = 0$ and having a specified homological dimension, $H(\delta) = H$. By Lemma 3, such random boundary operator can be represented as $\delta = U\delta_0 U^{-1}$, where U is a random invertible matrix drawn from the uniform distribution. Define an *encoding rate*

$$\rho = H/M. \tag{11}$$

We shall be interested in the limit $M, H \to \infty$ such that the encoding rate remains constant. Let us show that in this limit a random boundary operator gives a code with linear distance with high probability. For any $r > 0$ define an event

$$\mathcal{E}'_r = \{\exists\, f \in \ker\delta \,:\, \mathrm{wt}\,(f) \le rM\}. \tag{12}$$

LEMMA 4. *For any $\epsilon > 0$ one can choose $r, \rho > 0$ such that*

$$\Pr\left[\mathcal{E}'_r\right] \le O(1)\cdot 2^{-M/2+M\epsilon} \tag{13}$$

for all large enough M and for all $H \le \rho M$.

PROOF. By Lemma 3, we can assume that $\delta = U\delta_0 U^{-1}$, where U is a random invertible matrix. Then $\ker\delta = U\cdot\ker\delta_0$ and $\mathcal{E}'_r = \{\exists f \in \ker\delta_0 \,:\, \mathrm{wt}\,(Uf) \le rM\}$. For a fixed $f \in \ker\delta_0$ the vector Uf is distributed uniformly on the set of all M-bit vectors. Applying a union bound we get

$$\begin{aligned}\Pr\left[\mathcal{E}'_r\right] &\le \sum_{f\in\ker\delta_0} \Pr\left[\mathrm{wt}\,(Uf) \le rM\right] \\ &= |\ker\delta_0|\cdot \sum_{w\le rM} 2^{-M}\binom{M}{w} \\ &\le |\ker\delta_0|\cdot 2^{-M+S(r)M+o(M)},\end{aligned}$$

where $S(r) = -r\log_2(r) - (1-r)\log_2(1-r)$ is the Shannon entropy. Substituting $|\ker\delta_0| = 2^{(M+H)/2}$ gives $\Pr[\mathcal{E}'_r] \le O(1)\cdot 2^{-M/2+H/2+S(r)M+o(M)}$. It remains to choose small enough r and ρ such that $S(r)M + \rho M/2 + o(M) \le \epsilon M$. □

Since δ and δ^T are drawn from the same distribution, the bound Eq. (13) also applies to the event $\{\exists f \in \ker\delta^T \,:\, \mathrm{wt}\,(f) \le rM\}$. Hence the random code $\mathrm{CSS}(\mathcal{C}, \delta)$ has distance less than rM with probability at most $O(1)\cdot 2^{-M/2+M\epsilon}$.

5. PRODUCT OF TWO RANDOM COMPLEXES: DISTANCE BOUNDS

In this section we consider the product of two random complexes $(\mathcal{C}_a, \delta_a)$ defined above. Both complexes have the same dimension, $\dim(\mathcal{C}_1) = \dim(\mathcal{C}_2) = M$, and the same homological dimension $H = H(\delta_1) = H(\delta_2) = \rho M$. Then the product code $\mathrm{CSS}(\mathcal{C}_1\otimes\mathcal{C}_2, \partial)$ defined in Section 3 has parameters $[[M^2, \rho^2 M^2, d]]$ and stabilizer weight $w \le 2M$. Let $0 < c < 1$ be a constant to be chosen later. We would like to show that $d \ge cM^2$ with high probability. Define an event

$$\mathcal{E}_c = \{\exists\, \psi \in \ker\partial \backslash \mathrm{im}\,\partial \,:\, \mathrm{wt}\,(\psi) < cM^2\}. \tag{14}$$

It suffices to prove that for sufficiently small $c > 0$ and $\rho > 0$, the event $\mathcal{E}_c$ has probability $o(1)$ in the limit $M \to \infty$. By analogy with Lemma 4 one could try to bound the probability $\Pr[\mathcal{E}_c]$ using the "first moment" method: if one can show that the average number of low weight cycles ψ is small then with high probability there are no low weight cycles. There are two reasons why this kind of estimate will not work for the product code. One obvious reason is that, by construction, the product code always has low-weight cycles with weight $o(M^2)$. These are trivial cycles obtained as $\partial(i\otimes j) = (\delta_1 i)\otimes j + i\otimes(\delta_2 j)$, where i, j are any basis vectors and any linear combinations of $o(M)$ cycles of this form. Therefore some steps in the proof must differentiate between trivial and non-trivial cycles. The second, less obvious, reason is that, if by chance we pick a poor choice of the boundary operators δ_1, δ_2 such that ∂ has a low-weight non-trivial cycle, then in fact ∂ will have many low-weight non-trivial cycles. To see this, note that if ∂ has a non-trivial cycle ψ with weight $o(M^2)$ then the sum of ψ and any low-weight trivial cycle as above is a non-trivial cycle with weight $o(M^2)$. As a result, even though most codes will not have any low-weight non-trivial cycles, the average number of such cycles will not be small. This problem motivates our introduction of "uniform low weight" condition below.

Assume that a vector $\psi \in \mathcal{C}_1\otimes\mathcal{C}_2$ has weight less than cM^2. We can regard ψ as an M-by-M matrix, with rows corresponding to the first complex and columns corresponding to the second. Choose any constant r such that $c < r < 1$ and let

$$M' = (1-r)M, \qquad b = cr^{-1}/(1-r). \tag{15}$$

Clearly, ψ has at least M' columns with weight at most cMr^{-1}. Similarly, ψ has at least M' rows with weight at most cMr^{-1}. Let ϕ be any submatrix of ψ of size M'-by-M' formed by columns and rows of ψ with weight at most cMr^{-1}. Note that every row and every column of ϕ has weight at most $cMr^{-1} = bM'$. We shall refer to the condition that an M'-by-M' matrix ϕ has weight at most bM' in every row and column as the *uniform low weight* (ULW) condition with a constant b. For brevity we shall write "ϕ has ULW(b)". Note that for any fixed $r > 0$ one can make b arbitrarily small by choosing small enough c.

We shall use a term *reduced matrix* for a subset $\lambda \subset [M]\times[M]$ such that $\lambda = R\times C$ for some subset of M' rows R and some subset of M' columns C. The restriction of ψ onto λ will be called a reduced matrix of ψ and denoted ψ_λ. The above shows that if ψ has weight less than cM^2 then ψ_λ has ULW(b) for at least one reduced matrix λ. First we prove that if ψ is a non-trivial cycle then it cannot have *vanishing* reduced matrix.

LEMMA 5. *Consider any fixed choice of a reduced matrix λ. Suppose each code $\mathrm{CSS}(\mathcal{C}_a, \delta_a)$ has distance at least $M - M' + 1$. Then $\psi_\lambda \ne 0$ for any $\psi \in \ker\partial\backslash\mathrm{im}\,\partial$.*

PROOF. Assume without loss of generality that the reduced matrix λ is formed by the first M' columns and rows. Define $S' = \{1, 2, \ldots, M\}$ and $S = \{M'+1, M'+2, \ldots, M\}$ such that the reduced matrix is $\lambda = S'\times S'$. Consider any non-trivial co-cycle $\bar{h}_a \in \ker\delta_a^T \backslash \mathrm{im}\,\delta_a^T$. Since the size of S is less than the distance of $\mathrm{CSS}(\mathcal{C}_a, \delta_a)$, the Cleaning Lemma of Ref. [9] guarantees that there exists a trivial co-cycle $\bar{\omega}_a \in \mathrm{im}\,\delta_a^T$ such that $\bar{h}_a + \bar{\omega}_a$ has support only on S'. Thus we can choose a basis set of non-trivial co-cycles

$$\ker\delta_a^T = \mathrm{span}\,(\bar{h}_a^1, \bar{h}_a^2, , \ldots, \bar{h}_a^H) + \mathrm{im}\,\delta_a^T \tag{16}$$

such that $\bar{h}_a^i$ have support only on S'. Let us now choose basis sets of non-trivial cycles dual to the ones defined in Eq. (16), that is,

$$\ker \delta_a = \mathrm{span}\,(h_a^1, h_a^2, \ldots, h_a^H) + \mathrm{im}\,\delta_a \tag{17}$$

such that

$$(\bar{h}_a^i, h_a^j) = \delta_{i,j}. \tag{18}$$

Here $(f,g) = \sum_{p=1}^M f_p g_p$ is the binary inner product between vectors f, g. Applying Künneth formula Eq. (7) to ∂ and ∂^T one gets

$$\ker \partial = \mathrm{span}\,\{h_1^i \otimes h_2^j, \quad 1 \le i,j \le H\} + \mathrm{im}\,\partial \tag{19}$$

and

$$\ker \partial^T = \mathrm{span}\,\{\bar{h}_1^i \otimes \bar{h}_2^j, \quad 1 \le i,j \le H\} + \mathrm{im}\,\partial^T. \tag{20}$$

Suppose now that $h \in \ker \partial$ is a cycle with the vanishing reduced matrix. Using Eq. (19), one can write h as

$$h = \sum_{i,j=1}^{H} x_{i,j}\, h_1^i \otimes h_2^j + \omega, \tag{21}$$

for some $\omega \in \mathrm{im}\,\partial$ and some coefficients $x_{i,j} \in \{0,1\}$. Since $(\omega, \bar{h}_1^i \otimes \bar{h}_2^j) = 0$ for all i,j, the duality Eq. (18) implies that $x_{i,j} = (h, \bar{h}_1^i \otimes \bar{h}_2^j)$. However, since $\bar{h}_1^i \otimes \bar{h}_2^j$ has support only on the reduced matrix and h has vanishing reduced matrix, $x_{i,j} = 0$ for all i,j. This shows that any cycle with the vanishing reduced matrix must be trivial. □

For any reduced matrix λ and any integer $0 \le R \le M'$ define an event

$$\mathcal{E}_{b,R,\lambda} = \{\exists\, \psi \in \ker\partial \backslash \mathrm{im}\,\partial \,:\, \psi_\lambda \text{ has ULW}(b) \\ \text{and} \quad \mathrm{rank}\,(\psi_\lambda) = R\}. \tag{22}$$

The above arguments and a union bound imply

$$\Pr\left[\mathcal{E}_c\right] \le \sum_{\lambda} \sum_{R=0}^{M'} \Pr\left[\mathcal{E}_{b,R,\lambda}\right], \tag{23}$$

where the first sum is over all $\binom{M}{M'}^2$ reduced matrices λ. Note that the probability $\Pr\left[\mathcal{E}_{b,R,\lambda}\right]$ does not depend on the choice of λ since the distribution of ∂ is invariant under permutations of qubits in the input complexes. We shall treat the terms with $R = 0$ and $R > 0$ separately. The event $\mathcal{E}_{b,0,\lambda}$ occurs only if the reduced matrix of ψ is vanishing, $\psi_\lambda = 0$. By Lemma 5, this is possible only if at least one of the codes $\mathrm{CSS}(\mathcal{C}_a, \delta_a)$ has distance at most $M - M' = rM$. In other words, the event $\mathcal{E}'_r$ defined in Eq. (12) must occur for at least one of the boundary operators δ_a. Applying Lemma 4 and a union bound we get

$$\Pr\left[\mathcal{E}_{b,0,\lambda}\right] \le 2 \cdot \Pr\left[\mathcal{E}'_r\right] \le O(1) \cdot 2^{-M/2 + \epsilon M} \le 2^{-M/3} \tag{24}$$

for large M, since ϵ can be made arbitrarily small by choosing small enough r and ρ, see Lemma 4.

To bound the probability $\Pr\left[\mathcal{E}_{b,R,\lambda}\right]$ for $R \ge 1$ we shall need the following technical lemmas proved in the Appendix (with Lemma 7 being by far the most difficult one).

Lemma 6. *Let ϕ be a random rank-R matrix of size M'-by-M' drawn from the uniform distribution on the set of such matrices. For any $\epsilon > 0$ one can choose $b > 0$ such that*

$$\Pr\left[\phi \textit{ has ULW}(b)\right] \le O(1) \cdot 2^{R^2 - 2(1-\epsilon)M'R} \tag{25}$$

for all integers $1 \le R \le M'$.

To state the next two lemmas fix any reduced matrix λ and define a set $\mathcal{Z}_R(\delta_1, \delta_2)$ which includes all rank-R matrices ϕ of size M'-by-M' such that $\phi = \psi_\lambda$ for some cycle $\psi \in \ker\partial$. We shall refer to elements of $\mathcal{Z}_R(\delta_1, \delta_2)$ as *reduced cycles*. Let us say that the boundary operator δ_a is *good* iff the code $\mathrm{CSS}(\mathcal{C}_a, \delta_a)$ has distance at least $M - M' + 1$.

Lemma 7. *There exists a function $\Gamma(R)$ such that the set $\mathcal{Z}_R(\delta_1, \delta_2)$ has cardinality $\Gamma(R)$ for all pairs of good boundary operators δ_1, δ_2. Furthermore,*

$$\Gamma(R) \le O(1) \cdot 2^{(M+H)R - R^2} \quad \textit{if} \quad R \le H, \tag{26}$$

$$\Gamma(R) \le O(1) \cdot 2^{(M+H/2)R - R^2/2} \quad \textit{if} \quad R \ge H. \tag{27}$$

Lemma 8. *One can parameterize reduced cycles in each set $\mathcal{Z}_R(\delta_1, \delta_2)$ by integers $j = 1, \ldots, \Gamma(R)$ such that the following properties hold.*
(1) The parameterization is defined for any good pair δ_1, δ_2.
(2) Choose random boundary operators δ_1, δ_2 from the distribution defined in Section 4 and let $1 \le j \le \Gamma(R)$ be a fixed integer. Conditioned on δ_1, δ_2 being good, the j-th reduced cycle in $\mathcal{Z}_R(\delta_1, \delta_2)$ is distributed uniformly on the set of all $M' \times M'$ matrices with rank R.

Consider any $R \ge 1$. By Lemma 8, the event $\mathcal{E}_{b,R,\lambda}$ occurs only if one of the boundary operators δ_a is not good or if there exists $1 \le j \le \Gamma(R)$ such that the j-th reduced cycle in $\mathcal{Z}_R(\delta_1, \delta_2)$ has ULW(b). Note that here we no longer differentiate between trivial and non-trivial cycles. This is justified since we just need an upper bound on the probability $\Pr\left[\mathcal{E}_{b,R,\lambda}\right]$. Furthermore, for any fixed j the j-th reduced cycle in $\mathcal{Z}_R(\delta_1, \delta_2)$ is distributed uniformly on the set of all M'-by-M' matrices with rank R, see Lemma 8. Combining a union bound and Lemma 6 we arrive at

$$\Pr\left[\mathcal{E}_{b,R,\lambda}\right] \le 2^{-M/3} + O(1) \cdot \Gamma(R) \cdot 2^{R^2 - 2(1-\epsilon)M'R}, \tag{28}$$

where ϵ can be made arbitrarily small by choosing small enough b and the term $2^{-M/3}$ accounts for the possibility that one of the boundary operators δ_a is not good. We shall split the sum over $R \ge 1$ in Eq. (23) into two parts,

$$\Sigma_1 \equiv \sum_{R=1}^{H} \Pr\left[\mathcal{E}_{b,R,\lambda}\right] \quad \text{and} \quad \Sigma_2 \equiv \sum_{R=H}^{M'} \Pr\left[\mathcal{E}_{b,R,\lambda}\right]. \tag{29}$$

Combining Eqs. (15,26,28) we get

$$\Sigma_1 \le M \cdot 2^{-M/3} + O(1) \cdot \sum_{R=1}^{\infty} 2^{-MR(1-\rho-2\epsilon')}, \tag{30}$$

where $\epsilon' = 1 - (1-\epsilon)(1-r)$. The sum over R can be upper bounded, up to a factor $O(1)$, by its first term $O(1) \cdot 2^{-M(1-\rho-\epsilon')}$. Hence for sufficiently small r, ϵ, ρ we have $\Sigma_1 \le O(1) \cdot 2^{-M/4}$.

Combining Eqs. (15,27,28) we get

$$\Sigma_2 \le M \cdot 2^{-M/3} + O(1) \cdot \sum_{R=H}^{M'} 2^{-MR(1/2-\sigma)}, \tag{31}$$

where $\sigma = 2\epsilon' + \rho/2$. Here we used a trivial bound $2^{R^2/2} \le 2^{RM/2}$. Note that σ can be made arbitrarily small by choosing small enough r, ρ, b. Let us make $\sigma < 1/2$. Then the sum over R in Eq. (31) can be upper bounded, up to a factor $O(1)$, by its first term $O(1) \cdot 2^{-MH(1/2-\sigma)} \equiv F(M,H)$.

Note that for any fixed M the function $F(M,H)$ is monotone decreasing for $H \geq 0$. Since H is a non-negative integer, one has $F(M,H) \leq F(M,1) = O(1) \cdot 2^{-M(1/2-\sigma)}$. If we make $\sigma < 1/4$ then $F(M,H) \leq O(1) \cdot 2^{-M/4}$ and thus $\Sigma_2 \leq O(1) \cdot 2^{-M/4}$.

Combining all contributions to the sum in Eq. (23) and taking into account that there are $\binom{M}{M'}^2$ choices of the reduced matrix λ we arrive at

$$\Pr\left[\mathcal{E}_c\right] \leq O(1) \cdot \binom{M}{M'}^2 \cdot 2^{-M/4} \leq 2^{-M/4+S(r)M+o(M)} = o(1)$$

for small enough r. Finally, since ∂ and ∂^T are drawn from the same distribution, the same arguments as above show that $\Pr\left[\exists\, \psi \in \ker \partial^T \setminus \operatorname{im} \partial^T \,:\, \operatorname{wt}(\psi) < cM^2\right] = o(1)$. Hence for sufficiently large M the product code is unlikely to have non-trivial cycles or co-cycles with weight less than cM^2. This completes the proof of Theorem 1.

6. ACKNOWLEDGMENTS

We would like to thank Michael Freedman and Alexey Kitaev for helpful discussions. We thank Maris Ozols and Alex Vargo for valuable suggestions on numerical computation of the product code distance. We thank Aram Harrow for sharing with us a preliminary version of the manuscript Ref. [4]. SB is supported in part by the DARPA QuEST program under contract number HR0011-09-C-0047, and IARPA QCS program under contract number D11PC20167.

7. REFERENCES

[1] S. A. Aly. A class of quantum LDPC codes constructed from finite geometries. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5. IEEE, 2008.

[2] A. Ashikhmin, S. Litsyn, and M. Tsfasman. Asymptotically good quantum codes. *arXiv preprint quant-ph/0006061*, 13, 2000.

[3] B. Audoux. An application of Khovanov homology to quantum codes. *arXiv preprint arXiv:1307.4677*, 2013.

[4] D. Bacon, S. T. Flammia, A. W. Harrow, and J. Shi. *unpublished preprint.*

[5] H. Bombin and M. Martin-Delgado. Homological error correction: classical and quantum codes. *J. Math. Phys.*, 48:052105, 2007.

[6] S. Bravyi. Subsystem codes with spatially local generators. *Phys. Rev. A*, 83(1):012320, 2011.

[7] S. Bravyi and M. B. Hastings. Homological product codes. *arXiv preprint arXiv:1311.0885*, 2013.

[8] S. Bravyi, D. Poulin, and B. Terhal. Tradeoffs for reliable quantum information storage in 2D systems. *Phys. Rev. Lett.*, 104(5):050503, 2010.

[9] S. Bravyi and B. Terhal. A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes. *New J. of Phys.*, 11(4):043029, 2009.

[10] R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54(2):1098, 1996.

[11] T. Camara, H. Ollivier, and J.-P. Tillich. Constructions and performance of classes of quantum LDPC codes. *arXiv preprint quant-ph/0502086*, 2005.

[12] N. Delfosse. Tradeoffs for reliable quantum information storage in surface codes and color codes. *arXiv preprint arXiv:1301.6588*, 2013.

[13] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill. Topological quantum memory. *J. of Math. Phys.*, 43:4452, 2002.

[14] A. Fowler, A. Stephens, and P. Groszkowski. High-threshold universal quantum computation on the surface code. *Phys. Rev. A*, 80(5):052312, 2009.

[15] M. Freedman and M. Hastings. Quantum systems on non-k-hyperfinite complexes: A generalization of classical statistical mechanics on expander graphs. *arXiv preprint arXiv:1301.1363*, 2013.

[16] M. Freedman and D. Meyer. Projective plane and planar quantum codes. *Foundations of Computational Mathematics*, 1(3):325–332, 2001.

[17] M. Freedman, D. Meyer, and F. Luo. Z2-systolic freedom and quantum codes. *Mathematics of quantum computation, Chapman & Hall/CRC*, pages 287–320, 2002.

[18] R. Gallager. Low-density parity-check codes. *IRE Trans. on Inf. Theory*, 8(1):21–28, 1962.

[19] D. Gottesman. What is the overhead required for fault-tolerant quantum computation? *arXiv preprint arXiv:1310.2984*, 2013.

[20] J. Haah. Local stabilizer codes in three dimensions without string logical operators. *Phys. Rev. A*, 83(4):042330, 2011.

[21] J. Haah and J. Preskill. Logical-operator tradeoff for local quantum codes. *Phys. Rev. A*, 86(3):032308, 2012.

[22] A. Hatcher. *Algebraic topology*. Cambridge UP, Cambridge, 2002.

[23] A. Kitaev. Fault-tolerant quantum computation by anyons. *Ann. of Phys.*, 303(1):2–30, 2003.

[24] A. A. Kovalev and L. P. Pryadko. Improved quantum hypergraph-product LDPC codes.

[25] D. MacKay. Good error-correcting codes based on very sparse matrices. *IEEE Trans. Inf. Theory*, 45(2):399–431, 1999.

[26] D. MacKay, G. Mitchison, and P. McFadden. Sparse-graph codes for quantum error correction. *IEEE Trans. on Inf. Theory*, 50(10):2315–2330, 2004.

[27] M. Postol. A proposed quantum low density parity check code. *arXiv preprint quant-ph/0108131*, 2001.

[28] R. Raussendorf and J. Harrington. Fault-tolerant quantum computation with high threshold in two dimensions. *Phys. Rev. Lett.*, 98:190504, 2007.

[29] P. Sarvepalli and K. R. Brown. Topological subsystem codes from graphs and hypergraphs. *Phys. Rev. A*, 86(4):042336, 2012.

[30] J.-P. Tillich and G. Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to $n^{1/2}$. *IEEE International Symposium on Inf. Theory*, pages 799–803, 2009.

[31] G. Zémor. On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction. In *Coding and Cryptology*, pages 259–273. Springer, 2009.

APPENDIX

In this section we prove all lemmas stated in the main part. For convenience of the reader, we repeat the statement of each lemma.

Proof of Lemma 3

LEMMA 3. *Consider any complex $(\mathcal{C}, \delta)$ such that δ has homological dimension H and rank L. Then $\delta = U\delta_0 U^{-1}$, where U is some invertible matrix and δ_0 is the canonical boundary operator defined as a block matrix*

$$\delta_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & I \\ 0 & 0 & 0 \end{pmatrix}. \tag{32}$$

Here rows and columns are grouped into blocks of size H, L, L. Furthermore, the number of invertible matrices U such that $\delta = U\delta_0 U^{-1}$ does not depend on δ.

PROOF. Let $M = \dim(\mathcal{C})$. By definition of the homological dimension, Eq. (4), one has $L + H = \dim(\ker\delta) = M - L$, that is, $M = 2L + H$. Choose an arbitrary H-dimensional subspace $\mathcal{H}$ such that $\ker\delta = \mathcal{H} \oplus \operatorname{im}\delta$ is a direct sum. Let $I^1, I^2, \ldots, I^{L+H}$ be any basis of $\ker\delta$ such that $I^1, \ldots, I^H$ span $\mathcal{H}$ and $I^{H+1}, \ldots, I^{H+L}$ span $\operatorname{im}\delta$. Then $I^{H+j} = \delta(I^{H+L+j})$ for some vectors $I^{H+L+1}, \ldots, I^M$. Let $\mathcal{M}$ be the subspace spanned by $I^{H+L+1}, \ldots, I^M$. Since $\delta \cdot \mathcal{M} = \operatorname{im}\delta$, $\dim(\mathcal{M}) \le L$, and $\dim(\operatorname{im}\delta) = L$, one must have $\dim(\mathcal{M}) = L$. The property $\delta^2 = 0$ implies that $\mathcal{M} \cap \ker\delta = 0$, as otherwise $\delta \cdot \mathcal{M}$ would have dimension less than L. Thus vectors $I^1, \ldots, I^M$ form a basis of the full space $\mathcal{C}$. In this basis δ has the desired form Eq. (32). Hence $\delta = U\delta_0 U^{-1}$ for some invertible U.

To prove the last statement, define a normalizer group $G = \{U : U\delta_0 U^{-1} = \delta_0\}$. Then $U\delta U^{-1} = V\delta V^{-1}$ implies $V^{-1}U \in G$. Thus for any a given δ there are $|G|$ invertible matrices U such that $\delta = U\delta_0 U^{-1}$. □

Proof of Lemma 6

To simplify the notations, we set $M' = M$ below.

LEMMA 6. *Let ϕ be a random rank-R matrix of size M-by-M drawn from the uniform distribution on the set of such matrices. For any $\epsilon > 0$ one can choose $b > 0$ such that*

$$\Pr[\phi \text{ has ULW}(b)] \le O(1) \cdot 2^{R^2 - 2(1-\epsilon)MR}$$

for all integers $1 \le R \le M$.

PROOF. Let A, B be random rank-R matrices of size $M \times R$ drawn from the uniform distribution on the set of such matrices. Then $\phi = AB^T$ is uniformly distributed on the set of rank-R matrices of size $M \times M$. Below we fix some pair A, B and define two submatrices of ϕ; one of size $M \times R$ and the other of size $R \times M$.

Since ϕ has rank R, one can choose an $M \times R$ submatrix of ϕ which has rank R. Let ϕ_{red} be any such submatrix. Since each column of ϕ is a linear combination of columns of A, we conclude that $\phi_{red} = AU$ for some invertible $R \times R$ matrix U. For each matrix A as above let A_{red} be some fixed $R \times R$ submatrix of A with rank R (say, order all $R \times R$ submatrices of A lexicographically and choose A_{red} as the first submatrix with rank R). Note that $A_{red}B^T$ is a submatrix of ϕ which has size $R \times M$.

Let say that a vector has *low weight* if the fraction of non-zero entries in this vector is at most b. Define three classes of matrices. A matrix is Column-Low-Weight (CLW) if each of its columns has low weight. A matrix is Row-Low-Weight (RLW) if each of its rows has low weight. Finally, a matrix is Column-Row-Low-Weight (CRLW) if it is both CLW and RLW. Our goal is to bound the probability that $\phi = AB^T$ is CRLW.

Clearly, if ϕ is CRLW then any $R \times M$ submatrix of ϕ must be RLW and any $M \times R$ submatrix of ϕ must be CLW. The above arguments and the union bound imply that

$$\Pr[\ AB^T \text{ is CRLW }] \le \sum_U \Pr[\ A_{red}B^T \text{ is RLW and } AU \text{ is CLW }], \tag{33}$$

where the sum runs over all $R \times R$ invertible matrices U. Note that the number of such matrices is at most 2^{R^2}. Furthermore, for any fixed A the matrix $A_{red}B^T$ is distributed uniformly on the set of all $R \times M$ matrices of rank R. Likewise, for any fixed U the matrix AU is distributed uniformly on the set of all $M \times R$ matrices of rank R. This shows that

$$\Pr[\ AB^T \text{ is CRLW }] \le 2^{R^2} \cdot \Pr[\ B^T \text{ is RLW }] \cdot \Pr[\ A \text{ is CLW }]. \tag{34}$$

Let us show that for any $\epsilon > 0$ one can choose $b > 0$ such that

$$\Pr[\ A \text{ is CLW }] \le O(1) \cdot 2^{-MR(1-\epsilon)} \tag{35}$$

for all integers $1 \le R \le M$. Indeed, let $\tilde{A}$ be a random $M \times R$ matrix drawn form the uniform distribution on the set of all such matrices. Since columns of $\tilde{A}$ are independent and uniformly distributed, one can easily check that

$$\Pr[\ \tilde{A} \text{ is CLW }] \le 2^{-MR(1-\epsilon)}, \tag{36}$$

where ϵ can be made arbitrarily small by choosing small enough b. On the other hand, A and $\tilde{A}$ have the same distribution conditioned on the event $\operatorname{rank}(\tilde{A}) = R$. Thus

$$\Pr[\ A \text{ is CLW }] = \Pr[\ \tilde{A} \text{ is CLW } \mid \operatorname{rank}(\tilde{A}) = R\ ] \le \frac{\Pr[\ \tilde{A} \text{ is CLW }]}{\Pr[\ \operatorname{rank}(\tilde{A}) = R\ ]}. \tag{37}$$

It is well-known that a random uniformly distributed matrix has full rank with probability $\Omega(1)$. Thus the denominator in Eq. (37) is $\Omega(1)$. Combining Eqs. (36,37) proves Eq. (35). Applying exactly the same arguments to B one can show that $\Pr[\ B^T \text{ is RLW }] \le O(1) \cdot 2^{-MR(1-\epsilon)}$. The lemma now follows from Eq. (34). □

Proof of Lemma 7

Below we consider the reduced matrix λ formed by the first M' rows and columns. Recall that the boundary operator δ_a is *good* iff the code $\mathrm{CSS}(\mathcal{C}_a, \delta_a)$ has distance at least $M - M' + 1$.

LEMMA 7. *There exists a function $\Gamma(R)$ such that the set $\mathcal{Z}_R(\delta_1, \delta_2)$ has cardinality $\Gamma(R)$ for all pairs of good boundary operators δ_1, δ_2. Furthermore,*

$$\Gamma(R) \le O(1) \cdot 2^{(M+H)R - R^2} \quad \text{if} \quad R \le H, \tag{38}$$

$$\Gamma(R) \le O(1) \cdot 2^{(M+H/2)R - R^2/2} \quad \text{if} \quad R \ge H. \tag{39}$$

The proof, which is rather complicated, is based on defining a reduced boundary operator ∂' acting on a properly defined coarse-grained space. We will show that the task of counting reduced cycles with a given rank is closely related to counting matrices in $\ker \partial'$ with a given rank.

PROOF. Let $\mathcal{C} = \mathrm{span}\,\{1, 2, \ldots, M\}$ be the full M-dimensional binary space. We begin by defining several subspaces of $\mathcal{C}$ and linear operators acting on those subspaces. First, decompose

$$\mathcal{C} = \mathcal{V} \oplus \mathcal{V}^>, \quad \mathcal{V} = \mathrm{span}\,\{j \,:\, 1 \le j \le M'\}, \\ \mathcal{V}^> = \mathrm{span}\,\{j \,:\, M' < j \le M\}. \tag{40}$$

Let W and $W^>$ be projectors onto the sectors $\mathcal{V}$ and $\mathcal{V}^>$ in Eq. (40). Here by a projector we mean a linear operator on $\mathcal{C}$ that sends all vectors in one sector to zero and acts as the identity on the other sector. Thus $W + W^> = I$ is the identity operator on $\mathcal{C}$.

Let $\delta : \mathcal{C} \to \mathcal{C}$ be one of the boundary operators δ_1, δ_2. Recall that $\delta^2 = 0$. Define subspaces

$$\mathcal{S}^> = W\delta(\mathcal{V}^>) \subseteq \mathcal{V} \quad \text{and} \quad \mathcal{V}' = \mathcal{V}/\mathcal{S}^>.$$

By definition, vectors of the quotient space $\mathcal{V}'$ are cosets $x + \mathcal{S}^>$, where $x \in \mathcal{V}$. The following lemma defines a *reduced boundary operator* δ' which will play the key role in what follows.

LEMMA 9. *There exists a unique linear operator $\delta' : \mathcal{V}' \to \mathcal{V}'$ such that $(\delta')^2 = 0$ and*

$$\delta'(x + \mathcal{S}^>) = W\delta(x) + S^> \quad \textit{for any } x \in \mathcal{V}. \tag{41}$$

PROOF. Let us first show that

$$\mathrm{im}\,(W\delta W\delta) \subseteq \mathcal{S}^>. \tag{42}$$

Indeed, suppose $x = W\delta W\delta(y)$ for some y. Then $x = W\delta(I + W)\delta(y) = W\delta W^>\delta(y) \in W\delta(\mathcal{V}^>) = \mathcal{S}^>$ which proves Eq. (42). To show that Eq. (41) indeed defines a linear operator on $\mathcal{V}'$ we need to check that the right-hand side of Eq. (41) depends only on the coset of x. Equivalently, we need to check that $W\delta(\mathcal{S}^>) \subseteq \mathcal{S}^>$. However, this follows from Eq. (42) since $W\delta(\mathcal{S}^>) = (W\delta W\delta)(\mathcal{V}^>) \subseteq \mathrm{im}\, W\delta W\delta$. Thus δ' is well-defined. The property $(\delta')^2 = 0$ follows trivially from Eq. (42). □

We first establish some basic properties of δ'. Given a vector $h \in \mathcal{V}$, let $h' \in \mathcal{V}'$ be the coset of h, that is, $h' = h + \mathcal{S}^>$.

LEMMA 10. *For any vector $g \in \mathcal{C}$ one has $(W\delta g)' = \delta'(Wg)'$. Furthermore,*

$$\ker \delta' = \{(Wg)' \,:\, \delta g \in \mathcal{V}^>\} \quad \textit{and} \\ \mathrm{im}\,\delta' = \{(Wg)' \,:\, g \in \mathrm{im}\,\delta\}. \tag{43}$$

PROOF. Indeed, $(W\delta g)' = W\delta g + \mathcal{S}^> = W\delta(W + W^>)g + \mathcal{S}^> = W\delta W g + \mathcal{S}^> = \delta'(Wg)'$. Here we used the fact that $W\delta W^> g \in W\delta(\mathcal{V}^>) = \mathcal{S}^>$.

Let us show that $\ker\delta' = \{(Wg)' \,:\, \delta g \in \mathcal{V}^>\}$. Indeed, suppose $\delta' h = 0$. Then the coset h has a representative $f \in \mathcal{V}$ such that $W\delta f \in \mathcal{S}^>$, that is, $W\delta(f + k) = 0$ for some $k \in \mathcal{V}^>$. Let $g = f + k$. Then $\delta g \in \mathcal{V}^>$ and $h = f + \mathcal{S}^> = Wg + \mathcal{S}^>$ proving that $h = (Wg)'$ has the desired form. Conversely, if $\delta g \in \mathcal{V}^>$ then $\delta'(Wg)' = (W\delta g)' = 0$ since $W\mathcal{V}^> = 0$. The second equality in Eq. (43) follows trivially from the identity $(W\delta g)' = \delta'(Wg)'$. □

Recall that we define a homological dimension of a boundary operator δ as $H(\delta) = \dim(\ker\delta) - \dim(\mathrm{im}\,\delta)$. Below we show that the boundary operators δ and δ' have the same homological dimension, as long as δ is good. Note that the condition of being good can be rephrased as

$$\ker\delta \cap \mathcal{V}^> = 0. \tag{44}$$

LEMMA 11. *Suppose a boundary operator δ is good. Then $\dim\mathcal{V}' = 2M' - M$ and*

$$\dim(\ker\delta') = \dim(\ker\delta) - (M - M'), \\ \dim(\mathrm{im}\,\delta') = \dim(\mathrm{im}\,\delta) - (M - M'). \tag{45}$$

PROOF. Since $\dim\mathcal{V}' = M' - \dim\mathcal{S}^>$, it suffices to show that $\dim\mathcal{S}^> = M - M'$. By definition, $\mathcal{S}^> = W\delta(\mathcal{V}^>)$ and thus $\dim\mathcal{S}^> \le \dim\mathcal{V}^> = M - M'$. Suppose $\dim\mathcal{S}^> < \dim\mathcal{V}^>$. Then there must exist a non-zero vector $g \in \mathcal{V}^>$ such that $W\delta(g) = 0$. From Eq. (44) we infer that $h = \delta(g) \ne 0$ but $Wh = 0$, that is, $h \in \mathcal{V}^>$. This contradicts to Eq. (44) since $\delta h = \delta^2(g) = 0$.

The goodness condition implies that $\delta g \in \mathcal{V}^>$ is only possible for $\delta g = 0$. Thus the first equality in Eq. (43) becomes $\ker\delta' = \{(Wg)' \,:\, g \in \ker\delta\}$. Noting that $\mathcal{S}^> \subseteq W(\mathrm{im}\,\delta) \subseteq W(\ker\delta)$ and using Eq. (43) we arrive at

$$\dim(\ker\delta') = \dim(W\ker\delta) - \dim(\mathcal{S}^>) \quad \text{and} \\ \dim(\mathrm{im}\,\delta') = \dim(W\,\mathrm{im}\,\delta) - \dim(\mathcal{S}^>).$$

Using the goodness condition again one can easily show that $\dim(W\ker\delta) = \dim(\ker\delta)$ and $\dim(W\,\mathrm{im}\,\delta) = \dim(\mathrm{im}\,\delta)$. It remains to substitute $\dim(\mathcal{S}^>) = M - M'$. □

The above lemma implies that $H(\delta') = H(\delta)$ whenever δ is good. From now on we consider a pair of good boundary operators $\delta_1, \delta_2 : \mathcal{C} \to \mathcal{C}$ such that

$$\dim(\mathrm{im}\,\delta_a) = L, \quad \dim(\ker\delta_a) = L + H, \quad L \equiv (M - H)/2.$$

Define subspaces $\mathcal{S}_a^>$ and $\mathcal{V}_a'$ as above for each boundary operator δ_a. Let $\delta_a' : \mathcal{V}_a' \to \mathcal{V}_a'$ be the corresponding reduced boundary operator. By Lemma 11 we have

$$\dim\mathcal{V}_a' = 2M' - M \equiv K. \tag{46}$$

Consider a tensor product space $\mathcal{C} \otimes \mathcal{C}$ and define

$$\partial' = \delta_1' \otimes I + I \otimes \delta_2' \tag{47}$$

acting on the space $\mathcal{V}_1' \otimes \mathcal{V}_2'$. Note that

$$\mathcal{V}_1' \otimes \mathcal{V}_2' \cong (\mathcal{V} \otimes \mathcal{V})/\mathcal{S}_{12}^>, \quad \text{where} \quad \mathcal{S}_{12}^> = \mathcal{S}_1^> \otimes \mathcal{V} + \mathcal{V} \otimes \mathcal{S}_2^>. \tag{48}$$

Given any vector $h \in \mathcal{V} \otimes \mathcal{V}$, let $h' \in \mathcal{V}_1' \otimes \mathcal{V}_2'$ be the coset $h + \mathcal{S}_{12}^>$. One can easily check that $(f \otimes g)' = f' \otimes g'$ for any $f, g \in \mathcal{V}$. The lemma below shows that a coset is a cycle for the reduced boundary operator ∂' iff it has a representative which is a reduced matrix of a cycle for ∂.

LEMMA 12. *Suppose δ_a are good. Then*

$$\ker\partial' = \{((W \otimes W)g)' \,:\, g \in \ker\partial\} \quad \textit{and} \\ \mathrm{im}\,\partial' = \{((W \otimes W)g)' \,:\, g \in \mathrm{im}\,\partial\}. \tag{49}$$

PROOF. Let us show that $\partial'((W\otimes W)h)' = ((W\otimes W)\partial h)'$ for any $h \in \mathcal{C}\otimes\mathcal{C}$. By linearity, it suffices to consider product vectors $h = g_1 \otimes g_2$. Then $((W \otimes W)\partial h)'$ is equal to

$$(W\delta_1 g_1)' \otimes (Wg_2)' + (Wg_1)' \otimes (W\delta_2 g_2)' \\ = \delta_1'(Wg_1)' \otimes (Wg_2)' + (Wg_1)' \otimes \delta_2'(Wg_2)' \\ = \partial'((Wg_1)' \otimes (Wg_2)') = \partial'((W \otimes W)h)'. \tag{50}$$

Here the second equality uses Lemma 10. This immediately proves the second equality in Eq. (49) and the inclusion $\ker\partial' \supseteq \{((W\otimes W)g)' : g\in\ker\partial\}$.

It remains to prove $\ker\partial' \subseteq \{((W\otimes W)g)' : g\in\ker\partial\}$. Suppose $\partial' f = 0$ for some coset $f \in \mathcal{V}'_1\otimes\mathcal{V}'_2$. We need to show that f has a representative g which is a reduced matrix of a cycle. By Künneth formula, $\ker\partial' = \operatorname{im}\partial' + \ker\delta'_1\otimes\ker\delta'_2$. By linearity, it suffices to consider two cases. *Case 1:* $f\in\operatorname{im}\partial'$. Then the second equality in Eq. (49) implies that f has a representative which is a reduced matrix of a trivial cycle. *Case 2:* $f\in\ker\delta'_1\otimes\ker\delta'_2$. Since δ_a are good, Lemma 10 implies that $\ker\delta'_a = \{(Wg)' : g\in\ker\delta_a\}$. Hence f has a representative $g = (W\otimes W)g_{full}$, where $g_{full}\in\ker\delta_1\otimes\ker\delta_2$. Clearly, g_{full} is a cycle and we are done. □

The first equality in Eq. (49) implies that the set of rank-R matrices of size $M'\times M'$ which are reduced matrices of cycles coincides with the set of rank-R matrices $g\in\mathcal{V}\otimes\mathcal{V}$ such that the coset g' is a cycle for the reduced boundary operator. Thus

$$\Gamma(R) = \sum_{h\in\ker\partial'} \#\{g\in\mathcal{V}\otimes\mathcal{V} : \operatorname{rank}(g) = R \quad\text{and}\quad g' = h\}. \tag{51}$$

Choose any basis set of cosets $h_a^1,\dots,h_a^K\in\mathcal{V}'_a$ and let $g_a^i\in\mathcal{V}$ be any fixed vector in the coset h_a^i. One can always choose a basis of $\mathcal{V}$ such that the first K basis vectors are $g_a^1,\dots,g_a^K$ and the last $M'-K = M-M'$ basis vectors belong to $\mathcal{S}_a^>$. Then any vector $g\in\mathcal{V}\otimes\mathcal{V}$ in the coset h can be regarded as an $M'\times M'$ matrix that contains a given $K\times K$ matrix h in the first K rows and columns.

Definition 1. *Let X and Y be arbitrary matrices of size $a\times a$ and $A\times A$ respectively. We will say that Y is an extension of X iff Y contains X in the first a rows and columns. Let $E_{a,r}^{A,R}$ be the number of rank-R extensions Y of a given rank-r matrix X.*

Note that the number of rank-R matrices Y extending a given matrix X is invariant under a transformation $X\to UXV$, where U, V are arbitrary invertible matrices. This means that the number of rank-R extensions Y depends only on the rank of X and thus the coefficient $E_{a,r}^{A,R}$ is well-defined.

Proposition 1.

$$E_{a,r}^{A,R} \le O(1)\cdot 2^{(2A-a)R-ar-R^2+(r+R)^2/4} \tag{52}$$

and

$$E^{A,R} \equiv E_{0,0}^{A,R} = O(1)\cdot 2^{2AR-R^2}. \tag{53}$$

Note that $E^{A,R}$ is the total number of rank-R matrices of size $A\times A$. The proof of Proposition 1 can be found in the full version of this paper [7]. Using these notations, Eq. (51) can be written as

$$\Gamma(R) = \sum_{r=0}^{\min\{K,R\}} \#\{h\in\ker\partial' : \operatorname{rank}(h) = r\}\cdot E_{K,r}^{M',R}. \tag{54}$$

The remaining step is to compute the number of matrices $h\in\ker\partial'$ with a given rank r. This is done in the next lemma; while the lemma is stated in terms of ∂, we will apply it to the reduced boundary operator ∂', using $\dim(\operatorname{im}\delta'_a) = L-(M-M')$.

Lemma 13. *Let δ_1,δ_2 be boundary operators such that $\dim(\operatorname{im}\delta_a) = L$ and $\dim(\ker\delta_a) = L+H$. Define a boundary operator $\partial = \delta_1\otimes I + I\otimes\delta_2$ and let $Z(r)$ be the number of rank-r matrices in $\ker\partial$. Then $Z(r)$ is only a function of r, L, H and*

$$Z(r) \le O(1)\cdot 2^{2(H+L)r-r^2}\cdot \sum_{f=0}^{\min(r/2,L)} 2^{-2f^2+2f(r-H)}. \tag{55}$$

Proof. By Lemma 3, there exist invertible matrices U_a such that a transformation $\delta_a\to U_a\delta_a U_a^{-1}$ brings δ_a into the canonical form

$$\delta_a = \begin{bmatrix} 0 & 0 & 0\\ 0 & 0 & I\\ 0 & 0 & 0\end{bmatrix}, \tag{56}$$

where rows and columns are grouped into blocks of size H, L, L. Let $U = U_1\otimes U_2$. Noting that $(U_1\delta_1U_1^{-1})\otimes I + I\otimes(U_2\delta_2U_2^{-1}) = U\partial U^{-1}$ and $\ker(U\partial U^{-1}) = U\cdot\ker\partial$, it suffices to count rank-r matrices in $\ker\partial$ for the special case when both matrices δ_a have the canonical form. Using Künneth formula Eq. (7) one can easily check that $\ker\partial$ coincides with the set of matrices h having the following form:

$$h = \begin{bmatrix} A & B & 0\\ C & D & F\\ 0 & F & 0\end{bmatrix}. \tag{57}$$

As above, we group rows and columns into blocks of size H, L, L. Consider the set of matrices h as above where the block F has some fixed rank f. For a fixed choice of F let S_{row} and S_{col} be the set of first f linearly independent rows and columns of F respectively. Choose any invertible $L\times L$ matrices U and V such that UFV has zero rows outside S_{row} and zero columns outside S_{col}. A transformation

$$h\to \begin{bmatrix} I & 0 & 0\\ 0 & U & 0\\ 0 & 0 & U\end{bmatrix}\cdot h\cdot \begin{bmatrix} I & 0 & 0\\ 0 & V & 0\\ 0 & 0 & V\end{bmatrix}$$

does not change rank of h and preserves its block structure. Keeping in mind that there are $E^{L,f}$ choices of F with a given rank f, see Eq. (53), we can now assume that F has zero rows outside of S_{row} and zero columns outside S_{col}. Removing all rows of S_{row} and all columns of S_{col} from h reduced its rank by $2f$ regardless of the choice of the remaining blocks A, B, C, D. After this removal the non-zero part of h forms a matrix of size $(H+L-f)\times(H+L-f)$ which can be completely arbitrary as long as its rank is $r-2f$. Combining all these observations we arrive at

$$Z(r) = \sum_{f=0}^{\min(r/2,L)} E^{L,f}\cdot 2^{2f(H+L)-f^2}\cdot E^{H+L-f,r-2f}. \tag{58}$$

Here the factor $2^{2f(H+L)-f^2}$ represents possible choices of A, B, C, D in f rows of S_{row} and in f columns of S_{col}. Substituting Eq. (53) and collecting similar terms gives Eq. (55). □

We conclude that the number of reduced cycles with a given rank R is

$$\Gamma(R) = \sum_{r=0}^{\min\{K,R\}} Z(r)\cdot E_{K,r}^{M',R}. \tag{59}$$

This shows that $\Gamma(R)$ does not depend on δ_a as long as δ_a are good. From Eq. (52) we get

$$E_{K,r}^{M',R} = O(1) \cdot 2^{MR-(2M'-M)r-R^2+(r+R)^2/4}. \quad (60)$$

Applying Lemma 13 to the reduced boundary operators δ'_a and noting that $\dim(\operatorname{im}\delta'_a) = L-(M-M')$, see Eq. (45), we can rewrite Eq. (59) as

$$\Gamma(R) \le O(1) \cdot 2^{MR-3R^2/4} \sum_{r=0}^{R} 2^{(H+R/2)r-3r^2/4} \cdot \sum_{f=0}^{\infty} 2^{-2f^2+2f(r-H)}. \quad (61)$$

Here we extended the range of the sum over f in Eq. (55) to all integers $f \ge 0$ since we just need an upper bound on $\Gamma(R)$. Likewise, we extended the range of the sum over r in Eq. (59) to $0 \le r \le R$. The function $2^{-2f^2+2f(r-H)}$ has maximum at $f = f_0 = (r-H)/2$ and decays exponentially away from f_0. Note that f_0 is in the range of the sum over f iff $r \ge H$. If this is the case, then the sum over f can be approximated, up to a factor $O(1)$, by the single term $2^{-2f_0^2+2f_0(r-H)} = 2^{(r-H)^2/2}$. In the remaining case, $r < H$, the sum over f can be approximated by a constant $O(1)$. Let $\Gamma_1(R)$ and $\Gamma_2(R)$ be contributions to the righthand side of Eq. (61) that come from the terms with $r \le H$ and $r \ge H$ respectively. We have

$$\Gamma_1(R) = O(1) \cdot 2^{MR-3R^2/4} \sum_{r=0}^{\min\{H,R\}} 2^{(H+R/2)r-3r^2/4}. \quad (62)$$

The function $2^{(H+R/2)r-3r^2/4}$ achieves maximum at $r = r_0 = (2/3)H + R/3$ and decays exponentially away from r_0. Note that $r_0 \ge \min\{H,R\}$ with the equality iff $H = R$. Hence the sum over r can be approximated, up to a factor $O(1)$, by the last term $r = \min\{H,R\}$. Simple algebra shows that

$$\Gamma_1(R) \le O(1) \cdot 2^{(M+H/2)R-R^2/2} \quad \text{if } R \ge H, \quad (63)$$

and

$$\Gamma_1(R) \le O(1) \cdot 2^{(M+H)R-R^2} \quad \text{if } R \le H. \quad (64)$$

Next let us bound $\Gamma_2(R)$. Note that terms with $r \ge H$ can only appear for $R \ge H$. Replacing the sum over f by $O(1) \cdot 2^{(r-H)^2/2}$ in Eq. (61) and simplifying the resulting expression one gets

$$\Gamma_2(R) = O(1) \cdot 2^{MR-3R^2/4+H^2/2} \sum_{r=H}^{R} 2^{-r^2/4+Rr/2}. \quad (65)$$

The function $2^{-r^2/4+Rr/2}$ achieves maximum at $r = R$ and decays exponentially away from the maximum. Approximating the sum over r by the last term $r = R$, we get

$$\Gamma_2(R) = O(1) \cdot 2^{MR-R^2/2+H^2/2} \le O(1) \cdot 2^{(M+H/2)R-R^2/2}, \quad (66)$$

since $R \ge H$. This proves Eqs. (38,39).

Proof of Lemma 8

Below we consider a fixed reduced matrix λ formed by the first M' columns and rows. We shall use the notations introduced in the previous section.

LEMMA 8. *One can parameterize reduced cycles in each set $\mathcal{Z}_R(\delta_1,\delta_2)$ by integers $j = 1,\dots,\Gamma(R)$ such that the following properties hold.*
(1) The parameterization is defined for any good pair δ_1,δ_2.
(2) Choose random boundary operators δ_1,δ_2 from the distribution defined in Section 4 and let $1 \le j \le \Gamma(R)$ be a fixed integer. Conditioned on δ_1,δ_2 being good, the j-th reduced cycle in $\mathcal{Z}_R(\delta_1,\delta_2)$ is distributed uniformly on the set of all $M' \times M'$ matrices with rank R.

PROOF. Consider block-diagonal $M \times M$ matrices

$$U_a = \begin{pmatrix} U'_a & 0 \\ 0 & I \end{pmatrix}, \quad (67)$$

where U'_1 and U'_2 are arbitrary invertible $M' \times M'$ matrices. Given a pair of good boundary operators δ_1,δ_2, define

$$\tilde{\delta}_a = U_a \delta_a U_a^{-1}. \quad (68)$$

Using the block-diagonal structure of U_a one can easily check that $\tilde{\delta}_a$ are good boundary operators. Define $\tilde{\partial} = \tilde{\delta}_1 \otimes I + I \otimes \tilde{\delta}_2$. Noting that $\tilde{\partial} = (U_1 \otimes U_2)\partial(U_1 \otimes U_2)^{-1}$ one gets $\ker\tilde{\partial} = (U_1 \otimes U_2)\ker\partial$ which implies

$$\mathcal{Z}_R(\tilde{\delta}_1,\tilde{\delta}_2) = (U'_1 \otimes U'_2)\mathcal{Z}_R(\delta_1,\delta_2). \quad (69)$$

Consider some fixed good pair δ_1,δ_2. By Lemma 7, the set $\mathcal{Z}_R(\delta_1,\delta_2)$ has size $\Gamma(R)$. Choose an arbitrary parameterization of the set $\mathcal{Z}_R(\delta_1,\delta_2)$ by integers $j = 1,\dots,\Gamma(R)$. Let ψ_j be the j-th reduced cycle in $\mathcal{Z}_R(\delta_1,\delta_2)$. Then consider all possible pairs $\tilde{\delta}_1,\tilde{\delta}_2$ as defined in Eqs. (67,68) and choose $(U'_1 \otimes U'_2)\psi_j$ as the j-th reduced cycle of $\mathcal{Z}_R(\tilde{\delta}_1,\tilde{\delta}_2)$. By Eq. (69), this parameterizes the sets $\mathcal{Z}_R(\tilde{\delta}_1,\tilde{\delta}_2)$. Next choose any good pair δ_1,δ_2 which has not been considered yet. Choose an arbitrary parameterization on the set $\mathcal{Z}_R(\delta_1,\delta_2)$ and extend it to all sets $\mathcal{Z}_R(\tilde{\delta}_1,\tilde{\delta}_2)$ as described above. Repeating these steps we can parameterize the sets $\mathcal{Z}_R(\delta_1,\delta_2)$ for all good pairs δ_1,δ_2.

It remains to note that we choose boundary operators from a distribution invariant under the transformation $\delta_a \to \tilde{\delta}_a$. Hence the distribution of the j-th reduced cycle ψ_j is invariant under a transformation $\psi_j \to (U'_1 \otimes U'_2)\psi_j$, where U'_a are arbitrary invertible matrices. This is only possible if ψ_j is distributed uniformly on the set of all rank-R matrices. □