Higher-Dimensional Quantum Hypergraph-Product Codes with Finite Rates

Weilei Zeng and Leonid P. Pryadko

Phys. Rev. Lett. **122**, 230501 — Published 11 June 2019

DOI: 10.1103/PhysRevLett.122.230501

Higher-dimensional quantum hypergraph-product codes with finite rates

Weilei Zeng and Leonid P. Pryadko
Department of Physics & Astronomy, University of California, Riverside, California 92521, USA
(Dated: May 8, 2019)

We describe a family of quantum error-correcting codes which generalize both the quantum hypergraph-product codes by Tillich and Zémor, and all families of toric codes on m-dimensional hypercubic lattices. Parameters of the constructed codes, including the minimum distances, are given explicitly in terms of those of binary codes associated with the matrices used in the construction.

Quantum low-density parity-check (q-LDPC) codes are the only class of codes known to combine finite rates with non-zero fault-tolerant (FT) thresholds[1, 2], to allow scalable quantum computation with a finite multiplicative overhead[3]. However, unlike in the classical case, where capacity-approaching codes can be constructed from random sparse matrices[4–7], matrices suitable for constructing quantum LDPC codes are highly atypical in the corresponding ensembles. Thus, an algebraic ansatz is required to construct large-distance q-LDPC codes. Precious few examples of algebraic constructions are known that give finite rate codes and also satisfy conditions[2] for fault-tolerance: bounded weight of stabilizer generators and minimum distance that scales logarithmically or faster with the block length n. Such constructions include hyperbolic codes on two- and higher-dimensional manifolds[8–12], and quantum hypergraph-product (QHP) & related codes[13–15]. Further, some constructions, e.g., in Refs. 16–20, have finite rates and relatively high distances, with the stabilizer generator weights that grow with n logarithmically. It is not known whether these codes have non-zero FT thresholds. However, such codes can be modified into those with provable FT thresholds with the help of weight reduction[21].

There is more variety for topological codes, which can be viewed as generalizations of the toric code[22–28] invented by Kitaev[29]. Such a code can be constructed from any tessellation of an arbitrary surface or a higher-dimensional manifold. The essential advantage of topological codes is locality: each stabilizer generator involves only the qubits in the immediate vicinity of each other; this makes planar surface codes so practically attractive. However, locality also limits the parameters of topological codes[30–33]. In particular, for a code of length n with generators local in two dimensions, the number of encoded qubits k and the minimal distance d satisfy the inequality[30] $kd^2 \le \mathcal{O}(n)$. This implies asymptotically zero rate, $k/n \to 0$, whenever d diverges with n.

In this work we construct a family of q-LDPC codes that generalize the QHP codes[13, 14] to higher dimensions, and explicitly calculate their parameters, including the minimum distances. Our codes relate to toric codes on hypercubic lattices[24–28] in exactly the same fashion as the QHP codes relate to the square-lattice toric code. Just as different m-dimensional toric codes on a hypercubic lattice are parts of an m-complex[25], here we also construct m-complexes, chain complexes with m non-trivial boundary operators. Our construction is recursive: it defines an m-complex $\mathcal{K}_m$ as a tensor product of a shorter chain complex $\mathcal{K}_{m-1}$ and a 1-complex $\mathcal{K}_1$, a linear map between two binary vector spaces. In particular, the construction of the 2-complex $\mathcal{K}_2$ in terms of two binary matrices is identical to QHP codes[13, 14].

Previously, related constructions have been considered in Refs. 19, 21, and 34. Hastings[21] only considered products with 1-complexes which correspond to classical repetition codes, in essence, the same construction that appears in "space-time" codes used in the analysis of repeated syndrome measurement [1, 2, 35, 36]. On the other hand, Audoux and Couvreur[19] and Campbell[34] only considered products of 2-complexes. Their lower bounds on code distances are not as strong as ours.

In addition to defining new classes of quantum LDPC codes with parameters known explicitly, our construction may be useful for (i) optimizing repeated measurements in the problem of FT quantum error correction[1, 2, 35, 36], (ii) related problem of single-shot error correction[34, 37–39], (iii) analysis of transformations between different QECCs, like the distance-balancing trick by Hastings[21], and (iv) construction of asymmetric quantum CSS codes optimized for operation where error rates for X and Z channels may differ strongly[40–45].

We start with a brief overview of error correcting codes and chain complexes, see, e.g., Refs. 19, 25, 46–50 for much more information. A classical binary linear code $\mathcal{C}$ with parameters $[n, k, d]$ is a k-dimensional subspace of the vector space $\mathbb{F}_2^n$ of all binary strings of length n. The code distance d is the minimal Hamming weight of a nonzero string in the code. A code $\mathcal{C} \equiv \mathcal{C}_G$ can be specified in terms of the generator matrix G whose rows are the basis vectors of the code. All vectors orthogonal to the rows of G form the dual code $\mathcal{C}_G^\perp = \{c \in \mathbb{F}_n^2 | Gc^T = 0\}$. The matrix G is also called the parity check matrix of the code $\mathcal{C}_G^\perp$.

Given an *index set* $I \subseteq \{1, 2, \ldots, n\}$ of length $|I| = r$, and a string $c \in \mathbb{F}_2^n$, let $c[I] \in \mathbb{F}_2^r$ be a substring of c with the bits at all positions $i \notin I$ dropped. Similarly, for an n-column matrix G with rows g_j, $G[I]$ is formed by the rows $g_j[I]$. If $\mathcal{C} = \mathcal{C}_G$ is a linear code with the generating matrix G, the *punctured* code $\mathcal{C}_p[I] \equiv \{c[I] : c \in \mathcal{C}\}$ is a linear code of length $|I|$ with the generating matrix $G[I]$. The *shortened* code $\mathcal{C}_s[I]$ is formed similarly, except only from the codewords which have all zero bits outside I, $\mathcal{C}_s[I] = \{c[I] : c = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$ and $c_i = 0$ for each $i \notin I\}$. If $\mathcal{C} = \mathcal{C}_P^\perp$ has the parity check matrix P, $P[I]$ is the parity check matrix of the shortened code $\mathcal{C}_s[I]$.

A *chain complex* is a sequence of finite-dimensional vector spaces $\ldots, \mathcal{A}_{j-1}, \mathcal{A}_j, \ldots$ with *boundary* operators $\partial_j : \mathcal{A}_{j-1} \leftarrow \mathcal{A}_j$ that map between each pair of neighboring spaces, with the requirement $\partial_j \partial_{j+1} = 0$, $j \in \mathbb{Z}$. In this work we only consider vector spaces $\mathcal{A}_j = \mathbb{F}_2^{n_j}$ formed by binary vectors of length $n_j \geq 0$, and define an m-complex $\mathcal{A} \equiv \mathcal{K}(A_1, \ldots, A_m)$, a length-$(m+1)$ chain complex with a basis, in terms of $n_{j-1} \times n_j$ binary matrices A_j serving as the boundary operators,

$$\mathcal{A}: \{0\} \xleftarrow{\partial_0} \mathcal{A}_0 \xleftarrow{A_1} \mathcal{A}_1 \ldots \xleftarrow{A_m} \mathcal{A}_m \xleftarrow{\partial_{m+1}} \{0\}, \qquad (1)$$

where the neighboring matrices must be mutually orthogonal, $A_{j-1} A_j = 0$, $j \in \{1, \ldots, m\}$. In addition to boundary operators given by the matrices A_j, implicit are the trivial operators $\partial_0 : \{0\} \leftarrow \mathcal{A}_0$ and $\partial_{m+1} : \mathcal{A}_m \leftarrow \{0\}$ treated formally as zero $0 \times n_0$ and $n_m \times 0$ matrices.

Elements of the subspace $\mathrm{Im}(\partial_{j+1}) \subseteq \mathcal{A}_j$ are called boundaries; in our case these are linear combinations of columns of A_{j+1} and, therefore, form a binary linear code with the generator matrix A_{j+1}^T, $\mathrm{Im}(A_{j+1}) = \mathcal{C}_{A_{j+1}^T}$. In the singular case $j = m$, $\mathrm{Im}(\partial_{m+1}) = \{0\}$, a trivial vector space. Elements of $\mathrm{Ker}(\partial_j) \subset \mathcal{A}_j$ are called cycles; in our case these are vectors in a binary linear code with the parity check matrix A_j, $\mathrm{Ker}(A_j) = \mathcal{C}_{A_j}^\perp$. In the singular case $j = 0$, $\mathrm{Ker}(\partial_0) = \mathcal{A}_0$.

Because of the orthogonality $\partial_j \partial_{j+1} = 0$, all boundaries are necessarily cycles, $\mathrm{Im}(\partial_{j+1}) \subseteq \mathrm{Ker}(\partial_j) \subseteq \mathcal{A}_j$. The structure of the cycles in $\mathcal{A}_j$ that are not boundaries is described by the jth homology group,

$$H_j(\mathcal{A}) \equiv H(A_j, A_{j+1}) = \mathrm{Ker}(A_j) / \mathrm{Im}(A_{j+1}). \qquad (2)$$

Group quotient here means that two cycles [elements of $\mathrm{Ker}(A_j)$] that differ by a boundary [element of $\mathrm{Im}(A_{j+1})$] are considered equivalent, denoted as $x \simeq y \in \mathcal{A}_j$. Explicitly, $y = x + A_{j+1}\alpha$ for some $\alpha \in \mathcal{A}_{j+1}$. Non-zero elements of $\mathcal{H}_j(\mathcal{A})$ are equivalence classes of homologically non-trivial cycles. The rank of j-th homology group is the dimension of the corresponding vector space; one has

$$k_j \equiv \mathrm{rank}\, H_j(\mathcal{A}) = n_j - \mathrm{rank}\, A_j - \mathrm{rank}\, A_{j+1}. \qquad (3)$$

The homological *distance* d_j is the minimum Hamming weight of a non-trivial element (any representative) in the homology group $H_j(\mathcal{A}) \equiv H(A_j, A_{j+1})$,

$$d_j = \min_{0 \not\simeq x \in H_j(\mathcal{A})} \mathrm{wgt}\, x = \min_{x \in \mathrm{Ker}(A_j) \setminus \mathrm{Im}(A_{j+1})} \mathrm{wgt}\, x. \qquad (4)$$

By this definition, $d_j \geq 1$. To address singular cases, throughout this work we assume that the minimum of an empty set is an infinity; $k_j = 0$ always implies $d_j = \infty$.

In addition to the homology group $H(A_j, A_{j+1})$, there is also a generally distinct *co-homology* group $\tilde{H}_j(\tilde{\mathcal{A}}) = H(A_{j+1}^T, A_j^T)$ of the same rank (3); this is associated with the *co-chain complex* $\tilde{\mathcal{A}}$ formed from the transposed matrices A_j^T taken in the opposite order. A quantum Calderbank-Shor-Steane (CSS) code[51, 52] with generator matrices $G_X = A_j$ and $G_Z = A_{j+1}^T$ is isomorphic with the direct sum of the groups H_j and $\tilde{H}_j$,

$$\mathcal{Q}(A_j, A_{j+1}^T) \cong H(A_j, A_{j+1}) \oplus H(A_{j+1}^T, A_j^T). \qquad (5)$$

The two terms correspond to Z and X logical operators, respectively. The code distance can be expressed as a minimum over the distances d_j and $\tilde{d}_j$ of the two homology groups. Parameters of such a code are written as $[[n_j, k_j, \min(d_j, \tilde{d}_j)]]$.

The tensor product $\mathcal{A} \times \mathcal{B}$ of two chain complexes $\mathcal{A}$ and $\mathcal{B}$ is defined as the chain complex formed by linear spaces decomposed as direct sums of Kronecker products,

$$(\mathcal{A} \times \mathcal{B})_l = \bigoplus\nolimits_{i+j=l} \mathcal{A}_i \otimes \mathcal{B}_j, \qquad (6)$$

with the action of the boundary operators

$$\partial'''(a \otimes b) \equiv \partial_i' a \otimes b + (-1)^i a \otimes \partial_j'' b, \qquad (7)$$

where $a \in \mathcal{A}_i$, $b \in \mathcal{B}_j$, and the boundary operators ∂_i', ∂_j'', and ∂''' act in complexes $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{A} \times \mathcal{B}$, respectively. When both $\mathcal{A}$ and $\mathcal{B}$ are *bounded*, that is, they include finite numbers of non-trivial spaces, the dimension $n_j(\mathcal{C})$ of a space $\mathcal{C}_j$ in the product $\mathcal{C} = \mathcal{A} \times \mathcal{B}$ is

$$n_j(\mathcal{C}) = \sum\nolimits_i n_i(\mathcal{A})\, n_{j-i}(\mathcal{B}). \qquad (8)$$

The homology groups of the product $\mathcal{C} = \mathcal{A} \times \mathcal{B}$ are isomorphic to a simple expansion in terms of those of $\mathcal{A}$ and $\mathcal{B}$ which is given by the Künneth theorem,

$$H_j(\mathcal{C}) \cong \bigoplus\nolimits_i H_i(\mathcal{A}) \otimes H_{j-i}(\mathcal{B}). \qquad (9)$$

One immediate consequence is that the rank $k_j(\mathcal{C})$ of the jth homology group $H_j(\mathcal{C})$ is

$$k_j(\mathcal{C}) = \sum\nolimits_i k_i(\mathcal{A})\, k_{j-i}(\mathcal{B}). \qquad (10)$$

Our first result is an upper bound on the distances of the homological groups in a chain complex $\mathcal{A} \times \mathcal{B}$, an immediate extension of Cor. 2.14 from Ref. 19,

$$d_j(\mathcal{C}) \leq \min_i d_i(\mathcal{A})\, d_{j-i}(\mathcal{B}). \qquad (11)$$

Proof of Eq. (11). This is a consequence of a version of the Künneth theorem for a pair of chain complexes with chosen bases, see Proposition 1.13 in Ref. 19. Namely, if, for each $r \in \mathbb{Z}$, the sets $X_r \subset \mathcal{A}_r$ and $Y_r \subset \mathcal{B}_r$ induce bases for $H_r(\mathcal{A})$ and $H_r(\mathcal{B})$, respectively, then, for every $j \in \mathbb{Z}$, the vectors in the set

$$Z_j = \{x \otimes y | i \in \mathbb{Z}, x \in X_i, y \in Y_{j-i}\} \qquad (12)$$

induce a basis for $H_j(\mathcal{A}\otimes\mathcal{B})$. Now, if we choose each of the sets X_r and Y_r to contain the corresponding minimum-weight vectors, minimum weight of the elements of the set (12) equals to the r.h.s. in Eq. (11). The homology group is trivial, $k_j(\mathcal{A}\otimes\mathcal{B})=0$ and $Z_j=\emptyset$, only if at least one of the sets in each pair $\{a_i, b_{j-i}\}$, $i\in\mathbb{Z}$ is empty, which implies that the corresponding product $d_i(\mathcal{A})d_{j-i}(\mathcal{B})$ be infinite, consistent with the result given by our convention, $d_j(\mathcal{C})=\infty$ whenever $k_j(\mathcal{C})=0$. □

Our second result is a lower bound on the distance for the special case where $\mathcal{B}=\mathcal{K}(P)$ is a 1-complex induced by an $r\times c$ binary matrix P. This bound matches the upper bound in Eq. (11), and thus ensures the equality for the case where $\mathcal{B}$ is a 1-complex. This expression,

$$d_j(\mathcal{A}\times\mathcal{B})=\min\bigl(d_j(\mathcal{A})\,d_0(\mathcal{B}), d_{j-1}(\mathcal{A})\,d_1(\mathcal{B}),\bigr), \quad (13)$$

where $\mathcal{B}=\mathcal{K}(P)$ is a 1-complex, is our main result.

With $\mathcal{A}$ the m-complex in Eq. (1), the tensor product $\mathcal{C}\equiv\mathcal{A}\times\mathcal{B}$ can be written as an $(m+1)$-complex, $\mathcal{C}=\mathcal{K}(C_1,\ldots,C_{m+1})$, with the block matrices

$$C_{j+1}=\left(\begin{array}{c|c} A_{j+1}\otimes E_r & (-1)^j E_{n_j}\otimes P \\ \hline & A_j\otimes E_c\end{array}\right), \quad (14)$$

where E_r denotes the $r\times r$ identity matrix. The sign in the top-right corner ensures orthogonality $C_jC_{j+1}=0$; in our case spaces are binary and signs have no effect. We also notice that since ∂_0 and ∂_{m+1} in $\mathcal{A}$ are both trivial, matrices C_1 and C_{m+1}, respectively, will be missing the lower and the left block pairs. If we denote $u\equiv\operatorname{rank}P$, the two homology groups associated with $\mathcal{B}$ have ranks $\kappa_0\equiv k_0(\mathcal{B})=r-u$ and $\kappa_1\equiv k_1(\mathcal{B})=c-u$, respectively. Equations (8) and (10) give in this case,

$$n_j'=n_jr+n_{j-1}c \;\text{ and }\; k_j'=k_j\kappa_0+k_{j-1}\kappa_1, \quad (15)$$

where we use the primes to denote the parameters of $\mathcal{C}$, $n_j'\equiv n_j(\mathcal{C})$ and $k_j'\equiv k_j(\mathcal{C})$. We now prove the claimed lower bound for the distance[53]:

Theorem 1. *Consider m-complex $\mathcal{A}$ in Eq. (1), and assume that homological groups $H_j(\mathcal{A})$ have distances d_j, $0\le j\le m$. Given an $r\times c$ binary matrix P of rank u, construct matrices C_j in Eq. (14). Denote δ the minimum distance of a binary code with the parity check matrix P; by our convention, $\delta=\infty$ if $u=c$. The minimum distance $d_j'\equiv d_j(\mathcal{C})$ of the homology group $H(C_j,C_{j+1})$, $0\le j\le m+1$, satisfies the following lower bounds:*
(i) *if $r>u$, $d_j'\ge\min(d_j,d_{j-1}\delta)$, otherwise,*
(ii) *if $r=u$, $d_j'\ge d_{j-1}\delta$.*

We notice that in Eq. (13), $d_j(\mathcal{A})\equiv d_j$, $d_1(\mathcal{B})=\delta$, while $d_0(\mathcal{B})=1$ in case (i) and it is infinite in case (ii).

Proof of Theorem 1. Start with (i). Take a block vector $e=(e_1|e_2)$, with $e_1\in\mathbb{F}_2^{n_jr}$, $e_2\in\mathbb{F}_2^{n_{j-1}c}$, with component weights $w_1\equiv\operatorname{wgt}(e_1)<d_j$, and $w_2\equiv\operatorname{wgt}(e_2)<d_{j-1}\delta$, and assume $C_je^T=0$. We are going to show that e is a linear combination of columns of C_{j+1}.

Step 1: This step is needed if d_j is finite; otherwise let $C_j'=C_j$, $C_{j+1}'=C_{j+1}$, $e'=e$, and proceed to step 2. Mark the columns in A_j which are incident on non-zero positions in e_1. That is, write

$$e_1=\sum\nolimits_{i=1}^r a_i\otimes x_i,$$

where $a_i\in\mathbb{F}_2^{n_j}$, and $x_i\in\mathbb{F}_2^r$ with the only non-zero bit at position i. Take I_0 the union of the supports of all vectors a_i. Denote the corresponding submatrix of A_j as $A_j^{(0)}=A_j[I_0]$; this is the generating matrix of a code $\mathcal{C}_{A_j}$ punctured at the positions not in I_0. Further, denote $A_{j+1}^{(0)}$ a transposed generating matrix of the code $\mathcal{C}_{A_{j+1}^T}$ shortened to I_0; it is obtained from a linear combination of columns of A_{j+1} by dropping rows not in I_0.

By construction, $n_j^{(0)}\equiv|I_0|\le w_1$; since $w_1<d_j$, the homology group $H(A_j^{(0)},A_{j+1}^{(0)})$ is trivial. Now, increase I_0 by adding indices of all linearly independent columns of A_j to get $I_1\supseteq I_0$ and $A_j'=A_j[I_1]$, such that $|I_1|-|I_0|=\operatorname{rank}(A_j')-\operatorname{rank}(A_j^{(0)})$ and in addition $\operatorname{rank}(A_j')=\operatorname{rank}(A_j)$. Similarly, denote A_{j+1}' a transposed generating matrix of the code $\mathcal{C}_{A_{j+1}^T}$ shortened to I_1; it satisfies $\operatorname{rank}(A_{j+1}')=\operatorname{rank}(A_{j+1}^{(0)})$. Then $H(A_j',A_{j+1}')$ still has zero rank, and $H(A_{j-1},A_j)=H(A_{j-1},A_j')$. Use Eq. (14) to construct the corresponding matrices C_j' and C_{j+1}' and define the punctured vectors $e_1'=\sum_i a_i[I_1]\otimes x_i$, $e'=(e_1'|e_2)$. Since we only removed zero positions, the new vector satisfies $C_j'(e')^T=0$. Also, if there exists a vector $\alpha'\in\mathcal{C}_{j+1}'$ such that $(e')^T=C_{j+1}'(\alpha')^T$, then necessarily $e^T=C_{j+1}\alpha^T$ with some $\alpha\in\mathcal{C}_{j+1}$.

Step 2: Consider the decomposition

$$e_2=\sum\nolimits_{\ell=1}^c f_\ell\otimes y_\ell,\; f_\ell\in\mathbb{F}_2^{n_{j-1}}, \quad (16)$$

where $y_\ell\in\mathbb{F}_2^c$ has the only non-zero bit at ℓ. The identity $C_j'(e')^T=0$ implies $A_{j-1}f_\ell^T=0$ for any $1\le\ell\le c$. For those ℓ where f_ℓ^T is linearly dependent with the columns of A_j', $f_\ell^T=A_j'\alpha_\ell^T$ with some $\alpha_\ell\in\mathcal{C}_j'=\mathbb{F}_2^{n_j'}$, render this vector to zero by the equivalence transformation

$$(e')^T\to(e')^T+C_{j+1}'(0|\alpha_\ell\otimes y_\ell)^T.$$

Such a transformation only affects one vector f_ℓ. It may also modify the first block of e', which is of no importance since $H(A_j',A_{j+1}')$ is trivial. The resulting vector $\bar{e}'=(\bar{e}_1'|e_2')$ has the second block of weight $\operatorname{wgt}(e_2')\le\operatorname{wgt}(e_2)<d_{j-1}\delta$, it satisfies $C_j'(\bar{e}')^T=0$, and in its block representation (16) the remaining non-zero vectors $f_\ell\in H(A_{j-1},A_j')$ have weights d_{j-1} or larger.

Step 3: For sure, there remains fewer than δ of non-zero vectors f_ℓ. Thus, in a decomposition, $e_2'=\sum_{j=1}^{n_{j-1}}z_j\otimes$

c_j, where $z_j \in \mathbb{F}_2^{n_{j-1}}$ have the only non-zero bit at j, and $c_j \in \mathbb{F}_2^c$, the union of supports of the vectors c_j, I_2, has size $c' \equiv |I_2| < \delta$. Indeed, I_2 is just the set of the indices ℓ corresponding to the remaining non-zero vectors f_ℓ. Construct a matrix $P' = P[I_2]$ by dropping the columns of P outside of I_2. Since there are fewer than δ columns left, $c' < \delta$, the resulting classical code contains no non-zero vectors, $c' = \operatorname{rank} P'$. Construct the modified matrices C''_j and C''_{j+1} and define the punctured vectors $e''_2 = \sum_{j=1}^{n_0} z_j \otimes c_j[I_2]$ and $e'' = (\bar{e}'_1|e''_2)$ such that $C''_j(e'')^T = 0$. Now, after we trimmed the columns of both A_j and of P, according to Eq. (15), the homology group $H(C''_j, C''_{j+1})$ is trivial. This implies that e'' must be a linear combination of the columns of C''_{j+1}, that is, $(e'')^T = C''_{j+1}\beta^T$, for some binary vector β.

The transformation to C''_{j+1} and e'' amounts to dropping some columns and rows from the matrix C'_{j+1}, and some matching positions from $\bar{e}'$. All non-zero bits of $\bar{e}'$ are preserved, as are all involved columns of P. This implies that $\bar{e}'$ can be also obtained as a linear combination of columns of C'_{j+1}. Combined with the equivalence transformation in Step 2, we get $(e')^T = C'_{j+1}(\alpha')^T$; the construction of Step 1 then implies existence of $\alpha \in \mathcal{C}_{j+1}$ such that $e^T = C_{j+1}\alpha^T$ for the original two-block vector $e = (e_1|e_2)$. Thus, any such e with block weights $w_1 < d_j$ and $w_2 < d_{j-1}\delta$ which satisfies $C_j e^T = 0$ is necessarily a linear combination of the columns of C_{j+1}. This guarantees $d'_j \geq \min(d_j, d_{j-1}\delta)$.

To complete the proof, consider the case (ii). Here, step 1 can be omitted; the matrices resulting from steps 2 and 3 alone would give trivial homology group, regardless of the weight $\operatorname{wgt}(e_1)$ of the first block. Thus, in this case we get the lower bound $d'_j \geq d_{j-1}\delta$. $\square$

Let us now consider tensor products of several 1-complexes. The space dimensions, row and column weights, and homology group distances do not depend on the order of the terms in the product. Further, if the matrices used to construct one-complexes are (υ, ω)-sparse, that is, their column and row weights do not exceed υ and ω, respectively, the matrices in the resulting m-chain complex are $(m\upsilon, m\omega)$-sparse. In particular, when $\mathcal{K} = \mathcal{K}(R)$ is a 1-complex associated with a circulant check matrix R of the repetition code, $\mathcal{K}^{\times D}$ recovers all the D-dimensional toric codes.

Next, consider an $r \times c$ full-row rank binary matrix P with $r < c$, and assume that a binary code $\mathcal{C}_P^\perp$ has distance δ. The 1-complex $\mathcal{K} \equiv \mathcal{K}(P)$ has two non-trivial spaces of dimensions r and c; the corresponding homology groups have ranks 0, κ and distances ∞, δ. The 1-complex $\tilde{K} \equiv \mathcal{K}(P^T)$ generated by the transposed matrix has equivalent spaces taken in the opposite order, with the same homology group ranks, but the distances are now 1 and ∞, respectively. For $(a+b)$-complex $\mathcal{K}^{(a,b)} \equiv \mathcal{K}^{\times a} \times \tilde{\mathcal{K}}^{\times b}$ constructed as tensor products of $\mathcal{K}$ and/or $\tilde{\mathcal{K}}$ in any order, the only non-trivial homology group $H_a(\mathcal{K}^{(a,b)})$, acting in the space of dimension

$$n_a(\mathcal{K}^{(a,b)}) = \sum_{i=0}^{a} c^{2i} r^{a+b-2i} \binom{a}{i}\binom{b}{i} < (r+c)^{a+b},$$

has rank κ^{a+b} and distance δ^a. The corresponding quantum CSS code has distance $\min(\delta^a, \delta^b)$, and its stabilizer generators have weights not exceeding $(a+b)\max(\upsilon, \omega)$.

Good weight-limited classical codes with finite rates κ/c and finite relative distances δ/c can be obtained from ensembles of large random matrices[4–7]. Any of these can be used in the present construction. Then, for any pair (a, b) of natural numbers, we can generate weight-limited q-LDPC codes with finite rates and the distances $d_X = \delta^a$, $d_Z = \delta^b$ whose product scales linearly with the code length. QHP codes are a special case of this construction with $a = b = 1$.

Unlike in the case of QHP codes, with any $a > 1$, $b > 1$, the rows of matrices $G_X = K_a \equiv K_a(\mathcal{K}^{(a,b)})$, $G_Z = K_{a+1}^T$ satisfy a large number of linear relations resulting from the orthogonality with the matrices K_{a-1} and K_{a+2}, respectively. These can be used to correct syndrome measurement errors. Even though the resulting syndrome codes do not have large distances (with a finite probability some errors remain), the use of such codes in repeated measurement setting could simplify the decoding and/or improve the decoding success probability in the case of adversarial noise[34]. Such improvements with stochastic noise have been demonstrated numerically in the case of $D = 4$ toric codes in Ref. 54.

In conclusion, we derived an explicit expression for the distances of the homology groups in a tensor product of two chain complexes assuming one of the complexes has length two. Immediate use of this result is in theory of quantum LDPC codes. Our result greatly extends the family of QHP codes whose parameters are known explicitly. Higher-dimensional QHP codes can be especially useful in fault-tolerant quantum computation, to optimize repeated syndrome measurement in the presence of measurement errors.

In addition, we believe that the lower distance bound in Theorem 1 can be extended to a general product of two chain complexes. If this is the case, the r.h.s. in Eq. (11) would give explicitly the distances, not just an upper bound. Such a result could have substantial applications in many areas of science where homology is used.

LPP is grateful to Jean-Pierre Tilich for illuminating discussions, and to the Institute Henri Poincaré for hospitality. This research was supported in part by the NSF Division of Physics via Grants No. 1416578 and 1820939.

[1] A. A. Kovalev and L. P. Pryadko, "Fault tolerance of quantum low-density parity check codes with sublinear distance scaling," Phys. Rev. A **87**, 020304(R) (2013).

[2] I. Dumer, A. A. Kovalev, and L. P. Pryadko, "Thresholds for correcting errors, erasures, and faulty syndrome measurements in degenerate quantum codes," Phys. Rev. Lett. **115**, 050502 (2015), 1412.6172.

[3] D. Gottesman, "Fault-tolerant quantum computation with constant overhead," Quant. Information and Computation **14**, 1338–1371 (2014), 1310.2984.

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

[5] R. G. Gallager, *Low-Density Parity-Check Codes* (M.I.T. Press, Cambridge, Mass., 1963).

[6] S. Litsyn and V. Shevelev, "On ensembles of low-density parity-check codes: asymptotic distance distributions," IEEE Trans. Inf. Theory **48**, 887–908 (2002).

[7] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," Information Theory, IEEE Transactions on **47**, 619–637 (2001).

[8] G. Zémor, "On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction," in *Coding and Cryptology: Second International Workshop, IWCC 2009, Proc.*, edited by Y. M. Chee, C. Li, S. Ling, H. Wang, and C. Xing (Springer, Berlin, Heidelberg, 2009) pp. 259–273.

[9] N. Delfosse and G. Zémor, "Quantum erasure-correcting codes and percolation on regular tilings of the hyperbolic plane," in *Information Theory Workshop (ITW), 2010 IEEE* (2010) pp. 1–5.

[10] N. P. Breuckmann and B. M. Terhal, "Constructions and noise threshold of hyperbolic surface codes," IEEE Trans. on Inf. Th. **62**, 3731–3744 (2016), 1506.04029.

[11] N. P. Breuckmann, C. Vuillot, E. Campbell, A. Krishna, and B. M. Terhal, "Hyperbolic and semi-hyperbolic surface codes for quantum storage," Quantum Science and Technology **2**, 035007 (2017).

[12] L. Guth and A. Lubotzky, "Quantum error correcting codes and 4-dimensional arithmetic hyperbolic manifolds," Journal of Mathematical Physics **55**, 082202 (2014), arXiv:1310.5555.

[13] J.-P. Tillich and G. Zemor, "Quantum LDPC codes with positive rate and minimum distance proportional to $\sqrt{n}$," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)* (2009) pp. 799–803.

[14] J.-P. Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength," IEEE Transactions on Information Theory **60**, 1193–1202 (2014).

[15] A. A. Kovalev and L. P. Pryadko, "Quantum Kronecker sum-product low-density parity-check codes with finite rate," Phys. Rev. A **88**, 012311 (2013).

[16] A. Couvreur, N. Delfosse, and G. Zémor, "A construction of quantum LDPC codes from Cayley graphs," CoRR **abs/1206.2656** (2012), arXiv:1206.2656.

[17] Sergey Bravyi and Matthew B. Hastings, "Homological product codes," (2013), unpublished, arXiv:1311.0885.

[18] B. Audoux, "An application of Khovanov homology to quantum codes," Ann. Inst. Henri Poincare **1**, 185223 (2014).

[19] B. Audoux and A. Couvreur, "On tensor products of CSS codes," (2015), to appear in Ann. Inst. Henri Poincaré D, arXiv:1512.07081.

[20] M. B. Hastings, "Quantum codes from high-dimensional manifolds," (2016), unpublished, arXiv:1608.05089.

[21] M. B. Hastings, "Weight reduction for quantum codes," (2016), unpublished, arXiv:1611.03790.

[22] S. B. Bravyi and A. Yu. Kitaev, "Quantum codes on a lattice with boundary," (1998), unpublished, quant-ph/9811052.

[23] M. H. Freedman and D. A. Meyer, "Projective plane and planar quantum codes," Foundations of Computational Mathematics **1**, 325332 (2001), quant-ph/9810055.

[24] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, "Topological quantum memory," J. Math. Phys. **43**, 4452 (2002).

[25] H. Bombin and M. A. Martin-Delgado, "Homological error correction: Classical and quantum codes," Journal of Mathematical Physics **48**, 052105 (2007).

[26] C. Castelnovo and C. Chamon, "Topological order in a three-dimensional toric code at finite temperature," Phys. Rev. B **78**, 155120 (2008).

[27] D. Mazáč and A. Hamma, "Topological order, entanglement, and quantum memory at finite temperature," Annals of Physics **327**, 2096 – 2111 (2012).

[28] H. Bombin, R. W. Chhajlany, M. Horodecki, and M. A. Martin-Delgado, "Self-correcting quantum computers," New Journal of Physics **15**, 055023 (2013).

[29] A. Yu. Kitaev, "Fault-tolerant quantum computation by anyons," Ann. Phys. **303**, 2 (2003).

[30] S. Bravyi and B. Terhal, "A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes," New Journal of Physics **11**, 043029 (2009).

[31] S. Bravyi, D. Poulin, and B. Terhal, "Tradeoffs for reliable quantum information storage in 2D systems," Phys. Rev. Lett. **104**, 050503 (2010), 0909.5200.

[32] N. Delfosse, "Tradeoffs for reliable quantum information storage in surface codes and color codes," in *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on* (IEEE, 2013) pp. 917–921.

[33] S. T. Flammia, J. Haah, M. J. Kastoryano, and I. H. Kim, "Limits on the storage of quantum information in a volume of space," Quantum **1**, 4 (2017), 1610.06169.

[34] E. T. Campbell, "A theory of single-shot error correction for adversarial noise," (2018), to be published in Quantum Science and Technology (2019), 1805.09271.

[35] C. Wang, J. Harrington, and J. Preskill, "Confinement-Higgs transition in a disordered gauge theory and the accuracy

threshold for quantum memory," Annals of Physics **303**, 31 – 58 (2003).

[36] Ruben S. Andrist, *Understanding topological quantum error-correction codes using classical spin models*, Ph.D. thesis, ETH Zürich, Dep. of Physics, ETH Zürich (2012).

[37] Y. Fujiwara, "Ability of stabilizer quantum error correction to protect itself from its own imperfection," Phys. Rev. A **90**, 062304 (2014).

[38] A. Ashikhmin, C. Y. Lai, and T. A. Brun, "Robust quantum error syndrome extraction by classical coding," in *2014 IEEE International Symposium on Information Theory* (2014) pp. 546–550.

[39] A. Ashikhmin, C. Y. Lai, and T. A. Brun, "Correction of data and syndrome errors by stabilizer codes," in *2016 IEEE International Symposium on Information Theory (ISIT)* (2016) pp. 2274–2278, arXiv:1602.01545.

[40] Lev Ioffe and Marc Mézard, "Asymmetric quantum error-correcting codes," Phys. Rev. A **75**, 032345 (2007).

[41] Z. W. E. Evans, A. M. Stephens, J. H. Cole, and L. C. L. Hollenberg, "Error correction optimisation in the presence of x/z asymmetry," (2007), arXiv:0709.3875.

[42] A. M. Stephens, Z. W. E. Evans, S. J. Devitt, and L. C. L. Hollenberg, "Asymmetric quantum error correction via code conversion," Phys. Rev. A **77**, 062335 (2008).

[43] P. Aliferis and J. Preskill, "Fault-tolerant quantum computation against biased noise," Phys. Rev. A **78**, 052331 (2008).

[44] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler, "Asymmetric quantum codes: constructions, bounds and performance," Proc. R. Soc. A **465**, 1645–72 (2009).

[45] D. K. Tuckett, S. D. Bartlett, and S. T. Flammia, "Ultrahigh error threshold for surface codes with biased noise," Phys. Rev. Lett. **120**, 050505 (2018).

[46] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, Vol. 38 (Cambridge University Press, Cambridge, 1994).

[47] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1981).

[48] Daniel Gottesman, *Stabilizer Codes and Quantum Error Correction*, Ph.D. thesis, Caltech (1997).

[49] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Infomation* (Cambridge Unive. Press, Cambridge, MA, 2000).

[50] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," IEEE Trans. Info. Theory **44**, 1369–1387 (1998).

[51] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A **54**, 1098–1105 (1996).

[52] A. M. Steane, "Simple quantum error-correcting codes," Phys. Rev. A **54**, 4741–4751 (1996).

[53] See Supplemental Material at [URL] for a more detailed version of the proof.

[54] N. P. Breuckmann, K. Duivenvoorden, D. Michels, and B. M. Terhal, "Local decoders for the 2D and 4D toric code," Quantum Inf. Comput. **17**, 0181 (2017), 1609.00510.