Higher-dimensional hypergraph-product codes

LPP

A higher-dimensional version of the quantum hypergraph-product ansatz is described. Most important feature are the sharp lower and upper bounds for the minimum distance.

I. INTRODUCTION

The construction is useful for (a) analyzing repeated measurement in a stabilizer code in the problem of fault-tolerant (FT) quantum error correction (e.g., surface code[1], or more general LDPC code[2], (b) related problem of single-shot error correction[3], and (c) analysis and generalization of transformations between QECCs, like the quantum code enlargement trick by Hastings [ref?].

Origin: (a) Higher-dimensional toric codes and (b) Hypergraph-product codes[4]. Present construction generalizes both.

II. CONSTRUCTION OVERVIEW

I want to generalize the QHP construction[4] to produce longer chain complexes from two, three, etc. arbitrary size binary matrices. Here are some examples of intended construction.

- Original QHP construction can be interpreted as a length-two chain complex $\mathcal{K}(A_1, A_2)$: $\{0\} \leftarrow C_0 \overset{A_1}{\leftarrow} C_1 \overset{A_2}{\leftarrow} C_2 \leftarrow \{0\}$ with boundary operators such that $A_1 A_2 = 0$ (below, the indices above and to the left of the double lines label the corresponding sectors),

$$A_1 = \left(\begin{array}{c||c|c} & x & y \\ \hline\hline \cdot & H_1 \otimes E & E \otimes H_2 \end{array}\right), \quad A_2 = \left(\begin{array}{c||c} & xy \\ \hline\hline x & E \otimes H_2 \\ y & H_1 \otimes E \end{array}\right). \tag{1}$$

  Here H_i, $i \in \{1, 2\}$ are binary matrices and E denotes identity matrices of the sizes needed to make the block rows and block columns of matching sizes.

- The following three-chain complex $\mathcal{K}(B_1, B_2, B_3)$ $\{0\} \leftarrow C_0 \overset{B_1}{\leftarrow} C_1 \overset{B_2}{\leftarrow} C_2 \overset{B_3}{\leftarrow} C_3$ with boundary operators $B_1 B_2 = 0$, $B_2 B_3 = 0$ gives a generalization of the 3D toric codes' construction:

$$B_1 = (\cdot \| H_1 \otimes E \otimes E | E \otimes H_2 \otimes E | E \otimes E \otimes H_3) = (A_1 \otimes E | E \otimes H_3),$$

$$B_2 = \left(\begin{array}{c||c|c|c} & xy & xz & yz \\ \hline\hline x & E \otimes H_2 \otimes E & E \otimes E \otimes H_3 & \\ \hline y & H_1 \otimes E \otimes E & & E \otimes E \otimes H_3 \\ \hline z & & H_1 \otimes E \otimes E & E \otimes H_2 \otimes E \end{array}\right) = \left(\begin{array}{c|c} A_2 \otimes E & E \otimes H_3 \\ \hline & A_1 \otimes E \end{array}\right),$$

$$B_3 = \left(\begin{array}{c||c} & xyz \\ \hline\hline xy & E \otimes E \otimes H_3 \\ \hline xz & E \otimes H_2 \otimes E \\ \hline yz & H_1 \otimes E \otimes E \end{array}\right) = \left(\begin{array}{c} E \otimes H_3 \\ \hline A_2 \otimes E \end{array}\right).$$

The simple rule is that the matrix H_1, H_2, or H_3 is placed at the position whose column label differs from the row label by x, y, or z, respectively. The construction has an obvious generalization to higher dimensions. In the following, it is more convenient to use the following recursive definition:

Definition 1 (Dimensional extension of a chain complex)**.** *Given an $(m-1)$-chain complex $\mathcal{A} \equiv \mathcal{K}(A_1,\ldots,A_{m-1})$: $\{0\} \leftarrow C_0 \xleftarrow{A_1} C_1 \xleftarrow{A_2} C_2 \ldots \xleftarrow{A_{m-1}} C_{m-1} \xleftarrow{0_{n_{m-1}\times 0}} \{0\}$ with boundary operators A_j, $j=1,\ldots,m-1$, and an $r\times c$ binary matrix P, the extended m-chain complex $\mathcal{B}\equiv\mathcal{K}(B_1,\ldots,B_m)$ is defined by the boundary operators*

$$B_1 = (A_1\otimes E_r|E_{n_0}\otimes P),\quad B_2 = \left(\begin{array}{c|c} A_2\otimes E_r & E_{n_1}\otimes P \\ \hline & A_1\otimes E_c\end{array}\right),\ldots \tag{2}$$

$$B_j = \left(\begin{array}{c|c} A_j\otimes E_r & E_{n_{j-1}}\otimes P \\ \hline & A_{j-1}\otimes E_c\end{array}\right),\quad \ldots \tag{3}$$

$$B_{m-1} = \left(\begin{array}{c|c} A_{m-1}\otimes E_r & E_{n_{m-2}}\otimes P \\ \hline & A_{m-2}\otimes E_c\end{array}\right), \tag{4}$$

$$B_m = \left(\begin{array}{c} E_{n_{m-1}}\otimes P \\ \hline A_{m-1}\otimes E_c\end{array}\right). \tag{5}$$

Here $E_r\equiv E(r)$ denotes the $r\times r$ identity matrix, and the original linear spaces C_i, $i\in\{0,\ldots,m-1\}$, have dimensions n_i (so that A_i is an $n_{i-1}\times n_i$ binary matrix), with the additional convention $n_j=0$ for $j<0$ and $j\ge m$. The dimension of thus defined j-th level extended linear space $\mathcal{C}_j'$ is $n_j'=n_jr+n_{j-1}c$, $j\in\{0,\ldots,m\}$.

The constructed matrices trivially satisfy the correct orthogonality conditions. The original non-recursive definitions can be recovered by starting with the two-chain complex (1) and extending it sequentially with the help of matrices H_3, H_4, etc.

Let us assume that the rank of the j-th homology group $\mathcal{H}_j\equiv\mathcal{H}_j(\mathcal{A})$ is $k_j=\operatorname{rank}(\mathcal{H}_j)$, and the corresponding *distance*, the minimum weight of a homologically non-trivial cycle in $\mathcal{H}_j$ is $d_j\ge 1$, $1\le j<m$. Here we use the convention that $d_j=\infty$ if $k_j=0$. The distance d_j can be also expressed as the (left or z) distance of a quantum CSS code with generators $G_x=A_j$ and $G_z=A_{j+1}^T$, denoted as $\mathcal{Q}(A_j,A_{j+1}^T)$, that is,

$$d_j(\mathcal{A})\equiv d_j(A_j,A_{j+1}^T)=\min_{\mathbf{e}\in\mathcal{C}_{A_j}^\perp\setminus\mathcal{C}_{A_{j+1}^T}}\operatorname{wgt}\mathbf{e}.$$

The parameters of the CSS code $\mathcal{Q}(A_j,A_{j+1}^T)$ are thus $[[n_j,k_j,\min(d_j,\tilde d_j)]]$, where the distances in the corresponding co-chain complex generated by transposed matrices A_j^T,

$$\tilde{\mathcal{A}}\equiv\{0\}\leftarrow\mathcal{C}_{m-1}\xleftarrow{A_{m-1}^T}\ldots\xleftarrow{A_1^T}\mathcal{C}_0\leftarrow\{0\},$$

are denoted with the tilde, $\tilde d_j\equiv d(A_{j+1}^T,A_j)$.

In the special cases $j=0$ (which formally corresponds to a zero-row matrix A_0) it will be convenient to use $d_0=1$, and with $j=m-1$ (which formally corresponds to a zero-column matrix $A_m=0_{n_{m-1}\times 0}$), use the distance d_{m-1} of a binary code $\mathcal{C}_{A_{m-1}}^\perp$ with the parity check matrix A_{m-1} with the parameters $[n_{m-1},n_{m-1}-\operatorname{rank}A_{m-1},d_m]$.

Main result of this work are the exact parameters of the dimensionally-extended chain complex $\mathcal{B}$, expressed in terms of those of the original chain complex $\mathcal{A}$ and the parameters of the two binary codes with parity check matrices P and P^T, respectively: $\mathcal{C}_P^\perp = [c,\kappa,\delta]$ and $\mathcal{C}_{P^T}^\perp = [r,\tilde\kappa,\tilde\delta]$. Here P is an $r\times c$ binary matrix with $\operatorname{rank} P = u$, so that $\kappa = c-u$ and $\tilde\kappa = r-u$; and the distances $\delta\ge 1$, $\tilde\delta\ge 1$. We use the convention that $\delta=\infty$ if $\kappa=0$, and $\tilde\delta=\infty$ if $\tilde\kappa=0$.

With these definitions, the parameters of the dimensionally-extended m-chain complex $\mathcal{B}$ (see Definition 1) are given by the following

Theorem 2. *The dimension of the space* $\mathcal{C}'_j$ *is* $\boxed{n'_j = n_j r + n_{j-1}c,}$ *the rank of the* j *th homology group* $\mathcal{H}_j(\mathcal{B})$ *is* $\boxed{k'_j = k_j\tilde\kappa + k_{j-1}\kappa,}$ *with the minimum distance [weight of the smallest homologically non-trivial cycle in* $\mathcal{H}_j(\mathcal{B})$*]* $\boxed{d'_j = d_{j-1}\delta \text{ if } \tilde\kappa = 0, \text{ otherwise } d'_j = \min(d_j, d_{j-1}\delta).}$

This theorem combines the results of Lemma 3, Theorem 4 (upper distance bounds), and Theorem 6 (lower distance bound) below. The value of n'_j directly follows from the Definition 1.

III. MATRIX RANKS AND DIMENSIONS OF CSS CODES.

Any pair of adjacent matrices A_j and A_{j+1}^T can obviously be used as generators of a quantum CSS code $\mathcal{Q}_j \equiv \mathcal{Q}(A_j, A_{j+1}^T)$, which I assume to encode k_j qubits in n_j. Alternatively, k_j is the rank of the j th homology group in $\mathcal{K}$.

What are the parameters $[[n'_j, k'_j, d'_j]]$ of the codes generated by dimensionally extended matrices, e.g., $\mathcal{Q}'_j \equiv \mathcal{Q}(B_j, B_{j+1}^T)$?

We already know the block length $n'_j = n_j r + n_{j-1}c$. To find k'_j, denote the original ranks $s_j = \operatorname{rank} A_j$, $u \equiv \operatorname{rank} P$, and prove:

Lemma 3. *Given* $A_{j-1}A_j = 0$*, the binary matrix*

$$B_j = \left(\begin{array}{c|c} A_j\otimes E_r & E_{n_{j-1}}\otimes P \\ \hline & A_{j-1}\otimes E_c \end{array}\right)$$

has the rank $s'_j \equiv \operatorname{rank} B_j = s_j(r-u) + s_{j-1}(c-u) + n_{j-1}u.$

Proof. Start by computing the ranks of the upper and lower row blocks using the trick from Ref. 4. Namely, for each block, use row transformations to form distinct zero combinations. The corresponding count for the upper row block is

$$\operatorname{lc} B'_j = (n_{j-1} - s_j)(r-u),$$

and for the lower row block, trivially, $\operatorname{lc} B''_j = (n_{j-2} - s_{j-1})c$. This gives $\operatorname{rank} B'_j = s_j r + n_{j-1}u - s_j u$, and $\operatorname{rank} B''_j = cs_{j-1}$. For matrices of this form, the number of zero linear combinations that involve both row blocks is just the product of the ranks in the right blocks, ,

$$\operatorname{lc}(B'_j, B''_j) = s_{j-1}u.$$

Overall, we get the stated rank of B_j,

$$\begin{aligned} s'_j = \operatorname{rank} B_j &= (n_{j-1}r + n_{j-2}c) - (n_{j-1} - s_j)(r-u) - (n_{j-2} - s_{j-1})c - s_{j-1}u \\ &= n_{j-1}r + n_{j-2}c - n_{j-1}r + rs_j + n_{j-1}u - s_j u - cn_{j-2} + cs_{j-1} - s_{j-1}u \\ &= s_j(r-u) + s_{j-1}(c-u) + n_{j-1}u. \end{aligned}$$

□

The same result can also be obtained considering column blocks. Check:

$$\begin{aligned} s'_j &= n_j r + n_{j-1} c - (n_{j-1} - s_{j-1})(c-u) - (n_j - s_j) r - s_j u \\ &= n_{j-1} u + c s_{j-1} - s_{j-1} u + r s_j - s_j u = \boxed{s_j(r-u) + s_{j-1}(c-u) + n_{j-1} u.} \end{aligned}$$

These expressions give

$$\begin{aligned} k'_j &= n'_j - \operatorname{rank} B_j - \operatorname{rank} B_{j+1} \\ &= n_j r + n_{j-1} c - s_j(r-u) - s_{j-1}(c-u) - n_{j-1} u - s_{j+1}(r-u) - s_j(c-u) - n_j u \\ &= (n_j - s_j - s_{j+1})(r-u) + (n_{j-1} - s_{j-1} - s_j)(c-u) \\ &= k_j \tilde\kappa + k_{j-1} \kappa, \end{aligned} \tag{6}$$

where $\kappa \equiv c - u$ and $\tilde\kappa \equiv r - u$ respectively are the dimensions of the binary codes using P and P^T as check matrices.

For the length-two chain complex (1) this gives (setting $s_0 = 0$):

$$k_0^{(2)} = r_1 r_2 - \operatorname{rank} B_1 = (r_1 - u_1)(r_2 - u_2) = \tilde\kappa_1 \tilde\kappa_2, \tag{7}$$

$$k_1^{(2)} = (c_1 - u_1)(r_2 - u_2) + (r_1 - u_1)(c_2 - u_2) = \tilde\kappa_1 \kappa_2 + \kappa_1 \tilde\kappa_2, \tag{8}$$

$$k_2^{(2)} = c_1 c_2 - \operatorname{rank} B_2 = (c_1 - u_1)(c_2 - u_2) = \kappa_1 \kappa_2, \tag{9}$$

where the k_0 and k_2 correspond to classical codes with check matrices B_1^T and B_2, respectively. The value of $k_1^{(2)}$ coincides with the result in Ref. 4. For length-3 chain complex one gets, explicitly:

$$\begin{aligned} k_0^{(3)} &= \tilde\kappa_1 \tilde\kappa_2 \tilde\kappa_3, \\ k_1^{(3)} &= \kappa_1 \tilde\kappa_2 \tilde\kappa_3 + \tilde\kappa_1 \kappa_2 \tilde\kappa_3 + \tilde\kappa_1 \tilde\kappa_2 \kappa_3, \\ k_2^{(3)} &= \kappa_1 \kappa_2 \tilde\kappa_3 + \kappa_1 \tilde\kappa_2 \kappa_3 + \tilde\kappa_1 \kappa_2 \kappa_3, \\ k_3^{(3)} &= \kappa_1 \kappa_2 \kappa_3. \end{aligned}$$

Generally, $k_j^{(m)}$ is a sum of all the products of distinct κ_s, $s \in \{1, \ldots, m\}$ with all possible placements of $(m-j)$ tildes.

IV. BOUNDS ON CODES' DISTANCES

For a CSS code with binary generator matrices P and Q, such that $PQ^T = 0$, consider two distances different by the order of the generators:

$$d(P,Q) = \min_{\mathbf{x} \in \mathcal{C}_P^\perp \setminus \mathcal{C}_Q} \operatorname{wgt} \mathbf{x}, \quad d(Q,P) = \min_{\mathbf{x} \in \mathcal{C}_Q^\perp \setminus \mathcal{C}_P} \operatorname{wgt} \mathbf{x},$$

so that the actual CSS code distance is the minimum of the two. I will use the convention[4] that an empty code has infinite distance, which is the same as stating $\min(\emptyset) = \infty$. Notice that if one takes the right matrix zero, one can also get the distances of the classical binary code associated with the matrix P (dimensions $r \times c$),

$$d_P = d(P, 0_{0 \times c}).$$

In any case, the distance of the code (quantum or classical, empty or not) cannot be zero.

Again, consider an $(m-1)$-chain complex

$$\mathcal{A} = \{0\} \stackrel{0_{0\times n_0}}{\leftarrow} C_0 \stackrel{A_1}{\leftarrow} C_1 \leftarrow \ldots \leftarrow C_{m-2} \stackrel{A_{m-1}}{\leftarrow} C_{m-1} \stackrel{0_{n_{m-1}\times 0}}{\leftarrow} \{0\},$$

and its associated dimensionally-extended m-chain complex $\mathcal{B}$, see Definition 1. Let the CSS code $\mathcal{Q}(A_j, A_{j+1}^T)$ have parameters $[[n_j, k_j]]$ and the left and right distances $d(A_j, A_{j+1}^T) = d_j$, $d(A_{j+1}^T, A_j) = \tilde{d}_j$, and the binary codes with the check matrices P and P^T have distances δ and $\tilde{\delta}$, respectively. We have the following upper bounds on the distances in K':

Theorem 4. *The following upper bounds apply to codes in* $\mathcal{B}$*:*

(a) If $\tilde{\kappa} \equiv r - u > 0$*, then* $d'_j \equiv d(B_j, B_{j+1}^T) \le d_j \equiv d(A_j, A_{j+1}^T)$.

(b) If $k_0 \equiv n_0 - \operatorname{rank} A_1 > 0$*, then* $d'_1 \le \delta$.

(c) For $j > 1$*,* $d'_j \equiv d(B_j, B_{j+1}^T) \le d_{j-1}\delta \equiv d(A_{j-1}, A_j^T)\,\delta$.

The proofs are based on Lemma 3 and its generalization, the following Lemma:

Lemma 5. *Consider two pairs of matrices:* A*,* B *of dimensions* $n_0\times n_1$*,* $n_1\times n_2$ *respectively, such that* $AB = 0$*, and* P*,* Q *of dimensions* $m_0\times m_1$*,* $m_1\times m_2$ *respectively, such that* $PQ = 0$*. Then the rank of the following block matrix*

$$M = \left(\begin{array}{c|c|c} B_{n_1\times n_2}\otimes E(m_0) & E(n_1)\otimes P_{m_0\times m_1} & \\ \hline & A_{n_0\otimes n_1}\otimes E(m_1) & E(n_0)\otimes Q_{m_1\times m_2}\end{array}\right) \quad \textit{is}$$

$$\begin{aligned}\operatorname{rank} M = {} & m_0 \operatorname{rank} B + n_1 \operatorname{rank} P - \operatorname{rank} B \operatorname{rank} P \\ & + m_1 \operatorname{rank} A + n_0 \operatorname{rank} Q - \operatorname{rank} A \operatorname{rank} Q - \operatorname{rank} A \operatorname{rank} P.\end{aligned}$$

In this expression, the first and second three terms are the ranks of the upper and lower row blocks, respectively; the last term is the number of rows that enter non-trivial linear combinations between the two blocks.

Proof of Theorem 4. For convenience, quote the definitions

$$B_1 = (A_1\otimes E_r | E_{n_0}\otimes P),\ B_2 = \left(\begin{array}{c|c} A_2\otimes E_r & E_{n_1}\otimes P \\ & A_1\otimes E_c\end{array}\right),\ B_j = \left(\begin{array}{c|c} A_j\otimes E_r & E_{n_{j-1}}\otimes P \\ & A_{j-1}\otimes E_c\end{array}\right), \ldots$$

Part *(a)*: We only need to consider the case where $k_j \ne 0$. In this case we can find a minimum-weight codeword $\mathbf{c} \in \mathbb{F}_2^{n_j}$, $\operatorname{wgt}(\mathbf{c}) = d_j$, such that $A_j\mathbf{c}^T = 0$ but $\mathbf{c} \ne \alpha A_{j+1}^T$ for any $\alpha \in \mathbb{F}_2^{n_{j+1}}$. Clearly, $\mathbf{x} = (\mathbf{c}\otimes\mathbf{y}|0)$ satisfies $B_j\mathbf{x}^T = 0$ with every $\mathbf{y} \in \mathbb{F}_2^r$. We want a $\mathbf{y}$ of weight one, such that $\mathbf{x}$ is not a linear combination of rows of B_{j+1}^T. To see that this is guaranteed by the condition $\tilde{\kappa} > 0$, consider the matrix B'_{j+1} constructed from the original A_j and a modified matrix A'_{j+1} of dimension $n_j \times (n_{j+1}+1)$, which is A_{j+1} with an added column $\mathbf{c}^T$; one has $\operatorname{rank} A'_{j+1} = \operatorname{rank} A_{j+1} + 1$. By construction, $A_jA'_{j+1} = 0$. According to Lemma 3, the modified matrix B'_{j+1} has $\operatorname{rank} B'_{j+1} = \operatorname{rank} B_{j+1} + r - u$, which guarantees that at least $\tilde{\kappa} = r - u > 0$ of the added columns are indeed linearly independent from the columns of the original B_{j+1}. That is, we can find a weight-one vector $\mathbf{y}$ so that $\mathbf{x}$ is a valid codeword of weight d_j in $\mathcal{Q}(B_j, B_{j+1})$, which proves the upper bound.

Proof of Part *(b)* is similar, except now the trial vector has the form $\mathbf{x} = (0, \mathbf{y}\otimes\mathbf{b})$, where $P\mathbf{b}^T = 0$ (we only need to consider the case $\kappa > 0$). Any such vector clearly satisfies $B_1\mathbf{x}^T = 0$. We want $\mathbf{y}\in\mathbb{F}_2^{n_0}$ of unit weight, such that $\mathbf{x}^T$ be linearly independent from the columns of B_2. Instead of analyzing each possible $\mathbf{y}$, consider the rank of the matrix B_2' obtained from B_2 by adding a block $E(n_0)\otimes\mathbf{b}^T$ in the second block row (and a zero block of size $n_{j-1}r\times n_0$ above it). Resulting matrix B_2' satisfies the conditions of Lemma 5, which gives $\operatorname{rank} B_2' = \operatorname{rank} B_2 + (n_0 - \operatorname{rank} A_1)$; indeed, whenever $k_0 > 0$, we can find a codeword of weight δ.

Part *(c)*: Again, we only need to consider the case $k_{j-1} > 0$ and $\kappa > 0$, so that minimum-weight codewords $\mathbf{c}\in\mathcal{Q}(A_{j-1}, A_j^T)$ and $\mathbf{b}\in\mathcal{C}_P^\perp$ cab be found; $d_{j-1} = \operatorname{wgt}(\mathbf{c})$, $\delta = \operatorname{wgt}(\mathbf{b})$. The trial codeword has the block form $\mathbf{x} = (0|\mathbf{c}\otimes\mathbf{b})$, it satisfies $B_j\mathbf{x}^T = 0$. Also, since $\mathbf{c}^T$ is linearly independent from the columns of A_{j-1}, it follows from Lemma 5 that $\mathbf{x}^T$ is linearly independent from the columns of B_{j+1}. Indeed, it is easy to see that if we took instead of the $\mathbf{c}^T$ a linear combination of the columns of A_{j-1}, the additional block would not affect the rank since it may be eliminated by column transformations. If the same were true for the vector $\mathbf{c}^T$ linearly independent from columns of A_{j-1}, we would get a contradiction with Lemma 5. □

Notice that parts (b) and (c) in Theorem 4 can be united if we take $d_0 = 1$. In the following, we assume this to be the case.

Theorem 6. *The left minimum distance $d_j' = d(B_j, B_{j+1}^T)$ of the CSS code with generators B_j and B_{j+1}^T satisfies the following lower bound: (i) if $\tilde\kappa = 0$, $d_j' \ge d_{j-1}\delta$. (ii) Otherwise, if $\tilde\kappa > 0$, $d_j' \ge \min(d_j, d_{j-1}\delta)$.*

The proof relies on the following Lemma, a generalization of a statement used in the proof of the minimum-distance bound for the hypergraph-product codes[4].

Lemma 7. *Consider the matrices B_1 and B_2, such that $B_1B_2 = 0$, constructed from the matrices $A_1^{(n_0\times n_1)}$, $A_2^{(n_1\times n_2)}$, and $P^{(r\times c)}$ as in Eq. (2). Let $I_1\subseteq\{1,2,\ldots,n_1\}$ and $I_2\subseteq\{1,2,\ldots,c\}$ denote two arbitrary index sets, and the support of each of the vectors $\mathbf{a}_i\in\mathbb{F}_2^{n_1}$, $i\le r$, and $\mathbf{b}_j\in\mathbb{F}_2^c$, $j\le n_0$, respectively, be contained inside of I_1 and I_2. Consider $\mathbf{e} = (\sum_{i=1}^r \mathbf{a}_i\otimes\mathbf{y}_i^{(r)}|\sum_{j=1}^{n_0}\mathbf{y}_j^{(n_0)}\otimes\mathbf{b}_j)$ where $\mathbf{y}_i^{(s)}\in\mathbb{F}_2^s$ is a vector with the only non-zero element at the position i, such that $B_1\mathbf{e}^T = 0$. Consider matrices B_1' and B_2' similarly constructed from A_1', A_2', and P', where A_1' and P' are constructed from A_1 and P by keeping only the columns in I_1 and I_2, respectively, and A_2' is a generator matrix of the code $\mathcal{C}_{A_2}$* shortened *to I_2 [That is, we take a subcode of $\mathcal{C}_{A_2}$ consisting of codewords with $c_i = 0$ outside of I_2, and* puncture *it at these positions.] Also, define vectors $\mathbf{a}_i'$ and $\mathbf{b}_j'$ by dropping the (all-zero) components outside of I_1 and I_2, respectively, and the corresponding vector $\mathbf{e}'$ which satisfies $G_x'(\mathbf{e}')^T = 0$. With these definitions, if $\mathbf{e}'$ is a linear combination of rows of B_2', then $\mathbf{e}$ is a linear combination of rows of B_2.*

Proof of Theorem 6. For the reference, we are looking at

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

Consider a two-block vector $\mathbf{e} = (\mathbf{e}_1|\mathbf{e}_2)$, with $\mathbf{e}_1\in\mathbb{F}_2^{n_jr}$, $\mathbf{e}_2\in\mathbb{F}_2^{n_{j-1}c}$, where $w_1\equiv\operatorname{wgt}(\mathbf{e}_1) < d_j$, and $w_2\equiv\operatorname{wgt}(\mathbf{e}_2) < d_{j-1}\delta$, and assume $B_j\mathbf{e}^T = 0$. We are going to show that $\mathbf{e}$ is a linear combination of rows of B_{j+1}^T by using Lemma 7 twice.

step 1: given $\mathbf{e}_1$, mark the columns in A_j which are incident on non-zero positions in $\mathbf{e}$. Denote the corresponding index set and the submatrix of A_j, respectively, as $I_1 \subset \{1, 2, \ldots, n_j\}$ and A'_j. As in Lemma 7, denote A'_{j+1} the generator matrix of the code $\mathcal{C}_{A_{j+1}}$ shortened at the positions outside of I_1. By assumption, I_1 is an erasable set in $\mathcal{Q}(A_j, A^T_{j+1})$; this implies that $\mathcal{Q}\big(A'_j, (A'_{j+1})^T\big)$ encodes no qubits. Take $P' = P$, and construct the corresponding matrices B'_1 and B'_2, the shortened vectors $\mathbf{a}'_i$, as well as the corresponding vector $\mathbf{e}' \equiv (\mathbf{e}'_1|\mathbf{e}_2)$ which satisfies $B'_1(\mathbf{e}'_1)^T = 0$. The point of the first reduction is that the code $\mathcal{Q}' = \mathcal{Q}(A'_j, (A'_{j+1})^T)$ encodes no qubits, so that the weight of the first block in $\mathbf{e}$ no longer matters.

Step 2: Consider the representation of the vector

$$\mathbf{e}_2 = \sum_{\ell=1}^{c} \mathbf{f}_\ell^{(n_{j-1})} \otimes \mathbf{y}_\ell^{(c)}, \tag{10}$$

where the assumed identity $B_j(\mathbf{e}')^T = 0$ implies $A_{j-1}\mathbf{f}_\ell^T = 0$ for any $1 \le \ell \le c$. For those ℓ where $\mathbf{f}_\ell$ is linearly dependent with the rows of A_j^T, $\mathbf{f}_\ell = \alpha_\ell A_j^T$, render this vector to zero by the linear transformation

$$\mathbf{e}' \to \mathbf{e}' + (0|\alpha_\ell \otimes \mathbf{y}_\ell^{(c)}) \cdot (B'_{j+1})^T.$$

Such a transformation only affects one vector $\mathbf{f}_\ell$. The resulting vector $\bar{\mathbf{e}}' = (\mathbf{e}'_1|\mathbf{e}'_2)$ has the second block of weight $\operatorname{wgt}(\mathbf{e}'_2) \le \operatorname{wgt}(\mathbf{e}_2) < d_{j-1}\delta$, it satisfies $B'_j(\bar{\mathbf{e}}')^T = 0$, and in the corresponding block representation (10) the remaining non-zero vectors $\mathbf{f}_\ell^{(n_{j-1})}$ all have weights d_{j-1} or larger.

This means that, for sure, there remains fewer than δ of these non-zero vectors $\mathbf{f}_\ell$. Therefore, in the representation $\mathbf{e}'_2 = \sum_{j=1}^{n_0} \mathbf{y}_j^{(n_0)} \otimes \mathbf{b}'_j$ compatible with Lemma 7, the union of supports of vectors $\mathbf{b}'_j$, I'_2, has cardinality $|I'_2| < \delta$. Indeed, I'_2 is just the set of the indices ℓ corresponding to the remaining non-zero vectors $\mathbf{f}_\ell^{(n_{j-1})}$.

Finally, in step 3, trim the columns of P, keeping only the positions inside I'_2. Since there are fewer then δ columns left, $c' = |I'_2| < \delta$, the resulting classical code contains no non-zero vectors, $c' = \operatorname{rank} P'$. Now, after we trimmed the columns of both A_j and of P, according to Eq. (6), $\mathcal{Q}\big(B''_j, \check{(}B_{j+1})^T\big)$ encodes no qubits; thus the corresponding vector $\mathbf{e}''$ which satisfies $B''_j(\mathbf{e}'')^T = 0$, is a linear combination of the rows of $(B''_{j+1})^T$.

We can now use Lemma 7 to show that the vector $\bar{\mathbf{e}}'$ is a linear combination of the rows of $(B'_{j+1})^T$; this remains true for the vector $\mathbf{e}'$. Using Lemma 7 again we see that the original two-block vector $\mathbf{e}$ with the block weights $w_1 < d_j$ and $w_2 < d_{j-1}\delta$ which satisfies $B_j\mathbf{e}^T = 0$ is necessarily a linear combination of the rows of B^T_{j+1}. This guarantees $d'_j \ge \min(d_j, d_{j-1}\delta)$.

To complete the proof, consider the case $\tilde{\kappa} = 0$ separately. Here, step 1 can be omitted; the code resulting from steps 2 and 3 alone would encode no qubits, regardless of the weight $\operatorname{wgt}(\mathbf{e}_1)$ of the first block. Thus, in this case we get the more generous lower bound $d'_j \ge d_{j-1}\delta$. □

V. EXPLICIT CODE PARAMETES

Consider the special case of a four-dimensional construction, from four matrices P_j, $j \in \{1, 2, 3, 4\}$, of dimension $r_j \times c_j$, with rank $u_j > 0$, so that the binary codes with the check

m	n_0	n_1	n_2	n_3	n_4
1	r_1	c_1			
2	$r_1 r_2$	$r_1 c_2 + c_1 r_2$	$c_1 c_2$		
3	$r_1 r_2 r_3$	$r_1 r_2 c_3 + r_1 c_2 r_3 + c_1 r_2 r_3$	$r_1 c_2 c_3 + c_1 r_2 c_3 + c_1 c_2 r_3$	$c_1 c_2 c_3$	
4	$r_1 r_2 r_3 r_4$	$r_1 r_2 r_3 c_4 + r_1 r_2 c_3 r_4$ $r_1 c_2 r_3 r_4 + c_1 r_2 r_3 r_4$	$c_1 r_2 r_3 c_4 + c_1 r_2 c_3 r_4 + c_1 c_2 r_3 r_4$ $r_1 c_2 r_3 c_4 + r_1 c_2 c_3 r_4 + r_1 r_2 c_3 c_4$	$r_1 c_2 c_3 c_4 + c_1 r_2 c_3 c_4$ $+ c_1 c_2 r_3 c_4 + c_1 c_2 c_3 r_4$	$c_1 c_2 c_3 c_4$
m	k_0	k_1	k_2	k_3	k_4
1	$\tilde\kappa_1$	κ_1			
2	$\tilde\kappa_1 \tilde\kappa_2$	$\tilde\kappa_1 \kappa_2 + \kappa_1 \tilde\kappa_2$	$\kappa_1 \kappa_2$		
3	$\tilde\kappa_1 \tilde\kappa_2 \tilde\kappa_3$	$\kappa_1 \tilde\kappa_2 \tilde\kappa_3 + \tilde\kappa_1 \kappa_2 \tilde\kappa_3 + \tilde\kappa_1 \tilde\kappa_2 \kappa_3$	$\kappa_1 \kappa_2 \tilde\kappa_3 + \kappa_1 \tilde\kappa_2 \kappa_3 + \tilde\kappa_1 \kappa_2 \kappa_3$	$\kappa_1 \kappa_2 \kappa_3$	
4	$\tilde\kappa_1 \tilde\kappa_2 \tilde\kappa_3 \tilde\kappa_4$	$\kappa_1 \tilde\kappa_2 \tilde\kappa_3 \tilde\kappa_4 + \tilde\kappa_1 \kappa_2 \tilde\kappa_3 \tilde\kappa_4$ $+ \tilde\kappa_1 \tilde\kappa_2 \kappa_3 \tilde\kappa_4 + \tilde\kappa_1 \tilde\kappa_2 \tilde\kappa_3 \kappa_4$	$\kappa_1 \kappa_2 \tilde\kappa_3 \tilde\kappa_4 + \kappa_1 \tilde\kappa_2 \kappa_3 \tilde\kappa_4 + \kappa_1 \tilde\kappa_2 \tilde\kappa_3 \kappa_4$ $+ \tilde\kappa_1 \kappa_2 \kappa_3 \tilde\kappa_4 + \tilde\kappa_1 \kappa_2 \tilde\kappa_3 \kappa_4 + \tilde\kappa_1 \tilde\kappa_2 \kappa_3 \kappa_4$	$\kappa_1 \kappa_2 \kappa_3 \tilde\kappa_4 + \kappa_1 \kappa_2 \tilde\kappa_3 \kappa_4$ $+ \kappa_1 \tilde\kappa_2 \kappa_3 \kappa_4 + \tilde\kappa_1 \kappa_2 \kappa_3 \kappa_4$	$\kappa_1 \kappa_2 \kappa_3 \kappa_4$
	d_0	d_1	d_2	d_3	d_4
1	1 (?)	δ_1			
2	1(?)	$\tilde\kappa_1 \tilde\kappa_2 > 0:\ \min(\delta_1, \delta_2)$ $\tilde\kappa_1 = 0:\ \delta_2$ $\tilde\kappa_2 = 0:\ \delta_1$	$\delta_1 \delta_2$		
3	1 (?)	$\tilde\kappa_3 > 0:\ \min(d_1^{(m=2)}, \delta_3)$ $\tilde\kappa_3 = 0:\ \delta_3$	$\tilde\kappa_3 > 0:\ \min(d_2^{(m=2)}, d_1^{(m=2)} \delta_3)$ $\tilde\kappa_3 = 0:\ d_1^{(m=2)} \delta_3$	$\delta_1 \delta_2 \delta_3$	
4	1(?)	$\tilde\kappa_4 > 0:\ \min(d_1^{(m=3)}, \delta_4)$ $\tilde\kappa_4 = 0:\ \delta_4$	...	...	$\delta_1 \delta_2 \delta_3 \delta_4$

TABLE I. Parameters of the first four chain complexes. The distance is minimized over all non-zero combinations of the products of δ_j and $\tilde\delta_j$ corresponding to the products of κ_j and $\tilde\kappa_j$ that actually contribute to the total k.

matrices P_j and P_j' have distances δ_j and $\tilde\delta_j$, respectively. The parameters of thus constructed codes are given in the Table I on page 8 (assuming all matrices have non-zero rank).

---

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

[2] 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).

[3] Earl T. Campbell, "A theory of single-shot error correction for adversarial noise," (2018), unpublished, 1805.09271.

[4] 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.