Decodable quantum LDPC codes beyond the square root distance barrier using high dimensional expanders

Shai Evra
Institute for Advanced Studies
Princeton, USA
sevra@ias.edu

Tali Kaufman
Dept. of Computer Science
Bar-Ilan University
Israel
kaufmant@mit.edu

Gilles Zémor
Institut de Mathématiques de Bordeaux
UMR 5251, université de Bordeaux
Bordeaux, France
zemor@math.u-bordeaux.fr

***Abstract*—Constructing quantum LDPC codes with a minimum distance that grows faster than a square root of the length has been a major challenge of the field. With this challenge in mind, we investigate constructions that come from high-dimensional expanders, in particular Ramanujan complexes. These naturally give rise to very unbalanced quantum error correcting codes that have a large X-distance but a much smaller Z-distance. However, together with a classical expander LDPC code and a tensoring method that generalises a construction of Hastings and also the Tillich-Zemor construction of quantum codes, we obtain quantum LDPC codes whose minimum distance exceeds the square root of the code length and whose dimension comes close to a square root of the code length. When the ingredient is a 3-dimensional Ramanujan complex, we show that its 2-systole behaves like a square of the log of the complex size, which results in an overall quantum code of minimum distance $n^{1/2}\log n$, and sets a new record for quantum LDPC codes. When we use a 2-dimensional Ramanujan complex, or the 2-skeleton of a 3-dimensional Ramanujan complex, we obtain a quantum LDPC code of minimum distance $n^{1/2}\log^{1/2} n$. We then exploit the expansion properties of the complex to devise the first polynomial time algorithm that decodes above the square root barrier for quantum LDPC codes.**

***Keywords*-Quantum code, Ramanujan Complex, expander**

I. Introduction

A quantum CSS code [5], [28] of length n is defined by two binary matrices H_X and H_Z, each with n columns, and such their row-spaces W_X and W_Z are orthogonal. The matrices H_X and H_Z can be thought of as the parity-check matrices of classical codes, $C_X = W_X^{\perp}$ and $C_Z = W_Z^{\perp}$ respectively. The dimension of the quantum code is given by $n - \dim W_X - \dim W_Z$, equivalently it is the dimension of either of the quotient spaces C_X/W_Z or C_Z/W_X. The Hamming distance d_X (respectively d_Z) is defined as the smallest weight of a vector of C_X not in W_Z (respectively C_Z not in W_X). The minimum distance d of the quantum code is defined as $d = \min(d_X, d_Z)$. A quantum CSS code is said to be Low Density Parity Check (LDPC) if both matrices H_X and H_Z have row and column weights bounded from above by a constant.

Quantum LDPC error correcting codes are the subject of a lot of ongoing research. One reason is that quantum computers will need some form of quantum error correction, and it is generally assumed that the relevant error correcting codes will be of LDPC type because the associated quantum states can then be constructed through local interaction between qubits. Other motivations come from quantum complexity theory: for example, the "no low-energy trivial state" conjecture [11], generally thought of as a milestone towards a quantum PCP theorem, involves quantum LDPC codes.

Constructing quantum LDPC codes with a minimum distance that grows with n has been something of a challenge: one major difference with classical LDPC codes is that choosing a sparse parity-check matrix at random gives with very high probability an asymptotically good classical code, i.e. with dimension and minimum distance that scale as linear functions of the blocklength n. For the very same reason, there are no known random constructions of quantum LDPC codes, because choosing a matrix H_X at random will forbid the existence of a sparse matrix H_Z in the dual space of the rowspace W_X of H_X. All known constructions of quantum LDPC codes are in contrast highly structured. It is a wide open problem as to whether there exist families of asymptotically good quantum LDPC codes. More specifically, known quantum LDPC codes do not surpass a $\sqrt{n}$ barrier for the quantum minimum distance. Families of quantum LDPC codes include the Kitaev code [17], the earliest and most studied LDPC construction, one version of which has parameters $[[n, 2, \sqrt{n}]]$, generalisations to surface codes [4], [30], where qubits are associated to the edges of a graph that tiles a surface: when the rate of these codes is constant the minimum distance grows at best like $\log n$ [7], hypergraph product codes [29] that have a constant rate and minimum distance scaling like $\sqrt{n}$, the cubic codes of [6], codes from 4-dimensional hyperbolic manifolds [10], [18] that have constant rate and minimum distance n^{α} with $0.1 \leq \alpha \leq 0.3$, and iterated tensor power constructions [2]. There has been just one construction, due to Freedman, Meyer and Luo [9], that managed to break through the square root barrier for the minimum distance, yielding a

2575-8454/20/$31.00 ©2020 IEEE
DOI 10.1109/FOCS46700.2020.00029

quantum code of dimension 2 and distance that scales like $n^{1/2}\log^{1/4} n$[1]. A construction of Hastings [12] has been conjectured to yield codes with minimum distance close to linear in n, but does not provably break through the $\sqrt{n}$ barrier. A construction of Bravyi and Hastings [3] does yield asymptotically good quantum CSS codes, but at the expense of relaxing the LDPC condition, namely the matrices H_X and H_Z have rows of Hamming weight $\sqrt{n}$.

It is arguably one of the most intriguing problems of the theory of quantum LDPC codes, as to whether there exist codes whose minimum distance significantly exceed the $\sqrt{n}$ barrier. In the present work we contribute to this question by exhibiting codes that go beyond the Freedman et al. lower bound, and set a new record for the minimum distance that scales as $n^{1/2}\log n$. The dimension of these codes comes close to $\sqrt{n}$. The way this is achieved is by calling upon some remarkable properties of *Ramanujan complexes*. Ramanujan complexes are simplicial complexes that generalise Ramanujan graphs and have higher-dimensional expansion properties. The 2-dimensional Ramanujan LSV complexes of [23] can be thought of as a graph every edge of which belongs to a fixed number of triangles. By associating qubits to edges and using for H_X and H_Z the vertex-edge incidence matrix and the triangle-edge incidence matrix, one defines a quantum LDPC code such that $d_X = \log n$ and $d_Z = \Omega(n)$. Strictly speaking, this only yields a minimum distance equal to $\log n$, however this code has the remarkable property that $d_X d_Z = \Omega(n\log n) \gg n$. A method of Hastings [13] allows one to make a new quantum code out of d_Z/d_X copies of the original one, yielding a code of length nd_Z/d_X, the same dimension as the original dimension (in this case a constant), and minimum distance equal to d_Z. This already yields a code of length n and of minimum distance $\Omega(\sqrt{n\log n})$. In the present paper we further investigate how LSV complexes can yield good quantum error-correcting codes. We improve the dimension of the resulting quantum LDPC code by replacing the Hastings construction with a more general tensoring operation of complexes which will boost the code dimension to something close to $\sqrt{n}$. This construction can be seen as generalisation of the construction of [29] where a component bipartite graph is replaced by a 2-dimensional chain complex. It can also be deduced from [31]. We will prove that starting from a 3-dimensional LSV complex, the tensoring construction yields the record minimum distance $\Omega(n^{1/2}\log n)$. This involves obtaining a new systolic lower bound of the form $\log^2 n$ for these complexes. We will also prove a systolic lower bound of the form $\log^{k-1} n$ for k-dimensional LSV complexes, potentially yielding quantum LDPC codes with minimum distance $\Omega(\sqrt{n\log^{k-1} n})$ for abitrary k, but the dimension of these codes is for now only conjecturally non-zero.

[1]The paper [9] advertises $n^{1/2}\log^{1/2} n$ but this is a minor miscomputation.

Our main focus will then be to study in detail the decoding problem for codes that come from 2-dimensional LSV complexes and achieve minimum distance $\Omega(\sqrt{n\log n})$. This involves using an auxiliary classical expander code to reduce the decoding problem to that of the unbalanced quantum code associated to the component simplicial LSV complex. We then use the coboundary expansion properties of the LSV complex to solve the remaining decoding problem. We also give an alternative decoding procedure when the 2-dimensional LSV complex is replaced by the 2-skeleton of a 3-dimensional complex.

The long version of the present paper may be found at https://arxiv.org/abs/2004.07935

II. Overview

A. CSS codes from simplicial complexes and from LSV complexes

A quantum CSS code is defined by two binary matrices H_X and H_Z such that $H_Z^T H_X = 0$. If we call X_0, X_1, X_2 the sets of rows of H_X, columns of H_X (or of H_Z), rows of H_Z, then H_Z^T and H_X are the matrices of two linear maps ∂_2 and ∂_1

$$\mathbb{F}_2^{X_2} \xrightarrow{\partial_2} \mathbb{F}_2^{X_1} \xrightarrow{\partial_1} \mathbb{F}_2^{X_0}$$

such that $\partial_1\partial_2 = 0$. More generally, a *chain complex* (of binary vector spaces) $\mathbf{X} = (X_0, X_1, \ldots, X_d)$ of dimension d, describes a collection of vector spaces of the form $\mathbb{F}_2^{X_p}$ together with linear maps $\partial_p : \mathbb{F}_2^{X_p} \to \mathbb{F}_2^{X_{p-1}}$, $p = 1 \ldots d$, such that $\partial_{p-1}\partial_p = 0$ for $p = 2 \ldots d$. The maps ∂_p are called differential or boundary operators. We can therefore extract a CSS code from any two consecutive differential operators of a chain complex. This of course does not tell us very much about which chain complexes are likely to give us interesting quantum codes, but it is natural to focus on *simplicial* complexes. A complex is simplicial when elements of X_p describe $(p+1)$-subsets S of X_0 (p-simplices) and the map ∂_p takes the vector supported by S to the vector supported by the union of all p-subsets of S. The sets X_0 and X_1 describe therefore respectively the vertex and edge set of a graph, the set X_2 describes a set of triangles in the graph, and so on. When extracting the subcomplex X_{p-1}, X_p, X_{p+1} of a simplicial complex, the rows of the matrix H_X describing ∂_p^T have weight $p+1$, implying that the matrix H_X is LDPC for fixed p. The associated quantum code is therefore LDPC when the complex is of *bounded degree*, meaning that every p-simplex is incident to at most a bounded number of $(p+1)$-simplices.

The simplicial complexes that we shall use come from the recent theory of high dimensional expanders and Ramanujan complexes. Ramanujan complexes generalise Ramanujan graphs in sophisticated ways and we will not define in all generality what they actually are, referring the interested reader to the excellent surveys [19] and [20]. We will

however mention some of their remarkable properties, which are most relevant to us in the present work. First of all, they can be explicitly constructed as clique complexes of Cayley or Schreier graphs associated to the finite groups $PGL_{d+1}(\mathbb{F}_{q^e})$ (d the dimension of the complex, q a prime power), as was done in [23], and in fact we shall focus only on these constructions, henceforth called LSV complexes. Secondly, their local structure displays excellent expansion properties, notably if $\mathbf{X} = (V, E, T)$ is a 2-dimensional LSV complex, and $L(v)$ its link around the vertex $v \in V$, which is a graph whose vertex set is made up of the neighbours of v and such that vertices u, w are connected in $L(v)$ if $(u, v, w) \in T$, then for any v the link $L(v)$ is isomorphic to the points versus lines incidence graph of a projective plane of order q. Third, as was shown in [16], for some of these 2-dimensional LSV complexes, their homology space $H_1 = \ker \partial_1 / \mathrm{Im}\, \partial_2$, whose dimension is exactly equal to the associated quantum code dimension, is non-zero, and similarly the second homology of 3-dimensional LSV complexes can be made to be non-zero. Fourth, following [16] and [8], these LSV complexes have cosystoles which grow linearly in the size of the complex. Fifth, we can construct LSV complexes (with non-trivial homology) whose injectivity radius grows logarithmically in the size of the complex, and note that the injectivity radius bounds from below the 1-systoles. From the above we can record the following result which follows essentially from the work of [16].

Theorem II.1. *There exists a family of bounded degree 2-dimensional LSV complexes $\mathbf{X} = (V, E, T)$, such that the quantum code associated to it is non-zero and satisfies*

$$\begin{aligned} n &= |E|, \quad k = \dim H^1(\mathbf{X}) > 0, \\ d_X &= S_1(\mathbf{X}) = \Omega(\log n), \\ d_Z &= S^1(\mathbf{X}) = \Omega(n) \end{aligned}$$

where S_1 and S^1 are the 1-systole and the 1-cosystole of the complex and are exactly equal to the minimum distances d_X and d_Z of the associated quantum code.

The 1-systolic distance (or X-distance) of the quantum code associated to a 2-dimensional simplicial complex is usually constrained by a $\log n$ upper bound. This is reminiscent of the girth of a regular graph (of degree ≥ 3) being bounded from above by $\log |V|$. However, when switching to the (X_{p-1}, X_p, X_{p-1}) subcomplex of a simplicial complex of dimension larger than 2, we may expect to achieve larger distances d_X. 3-dimensional LSV complexes $\mathbf{X} = (V, E, T, P)$, that on top of triangles have 4-cliques (tetrahedra or Pyramids) in the underlying graph were also studied in [16], where it was shown that their homology space $H_2 = \ker \partial_2 / \mathrm{Im}\, \partial_3$ is non-zero, and that their 2-cosystole behaves as $S^2(\mathbf{X}) = \Omega(|T|)$. This translates into the quantum code associated to the subcomplex (E, T, Q) having non-zero dimension and Z-distance $d_Z = \Omega(n)$ where $n = |T|$ is the code length. The behaviour of the 2-systole $S_2(\mathbf{X})$ was left unexplored. We prove a lower bound on the 2-systole, and also on higher-dimensional systoles: together with results from [16] and [8], this gives:

Theorem II.2.

(i) *For d-dimensional LSV complexes $\mathbf{X} = (X_0, \ldots, X_d)$, we have*

$$\begin{aligned} &\forall p = 1, \ldots, d-1, \\ &S_p(\mathbf{X}) = \Omega(\log^p |X_p|), \quad S^p(\mathbf{X}) = \Omega(|X_p|). \end{aligned}$$

(ii) *If $d = 3$, then there are LSV complexes for which $H^2(\mathbf{X}) \neq 0$, hence, the associated quantum code has parameters*

$$\begin{aligned} n &= |X_3|, \quad k = \dim H^2(\mathbf{X}) > 0, \\ d_X &= \Omega(\log^2 n), \\ d_Z &= \Omega(n). \end{aligned}$$

To prove part (i) of the Theorem, we invoke an injectivity radius argument, together with arguments from building theory and algebraic topology to claim that a non-trivial p-cycle must contain more p-faces than in the intersection of an apartment and a ball of radius $\log |X_p|$. An apartment is isomorphic to a tiling of d-dimensional Euclidean space and Euclidean geometry arguments enable us to conclude.

Part (i) of Theorem II.2 is quite general, and can in principle yield quantum LDPC codes with $d_X = \Omega(\log^j n)$ and $d_Z = \Omega(n)$ for $j > 2$. However, the dimension of these quantum code candidates is only conjectured to be non-zero.

Next, we transform the quantum codes we have just discussed into quantum LDPC codes with minimum distance larger than $\sqrt{n}$.

B. Balancing distances d_X and d_Z of a quantum code

We introduce the following construction of a quantum code. it takes as input:

- A quantum code $\mathcal{Q} = \mathcal{Q}(\mathbf{X})$ defined by two low-density parity-check matrices H_X and H_Z. We can think of it as coming from an abstract chain complex $\mathbf{X} = (X_0, X_1, X_2)$ where X_0 and X_2 index the set of rows of H_X and the set of rows of H_Z respectively, and X_1 indexes both the set of columns of H_X and the set of of columns of H_Z. The matrices H_X and H_Z define incidence relations between elements of X_0 and X_1 and between elements of X_1 and X_2. We denote by $d_X(\mathcal{Q})$ and $d_Z(\mathcal{Q})$ its X and Z-distances.
- A classical LDPC code $C = C(\mathbf{Y})$ defined by a low-density parity-check matrix H. We can think of it as coming from a 1-dimensional chain complex $\mathbf{Y} = (A, B)$, which just means that we index the columns of H by a set A and its rows by a set B. The matrix H defines an incidence relation between elements of A and B. It is important that the matrix H

has no redundant rows, i.e. $\mathrm{rank}(H) = |B|$. We denote by $d(C)$ its minimum distance.

The construction outputs a new quantum code $\mathcal{Q}(\mathcal{X})$ by defining a 2-dimensional chain complex $\mathcal{X} = (\mathcal{X}_0, \mathcal{X}_1, \mathcal{X}_2)$, where

$$\mathcal{X}_0 = (X_0 \times A) \cup (X_1 \times B)$$
$$\mathcal{X}_1 = (X_1 \times A) \cup (X_2 \times B)$$
$$\mathcal{X}_2 = X_2 \times A.$$

To define incidence between elements of $\mathcal{X}_0$ and elements of $\mathcal{X}_1$, we declare any $(x_1, a) \in X_1 \times A$ to be incident to (x_0, a) for all $x_0 \in X_0$ incident to x_1 in $\mathbf{X}$, and to be incident to (x_1, b) for all $b \in B$ incident to a in $\mathbf{Y}$. We also declare any $(x_2, b) \in X_2 \times B$ to be incident to (x_1, b) for all $x_1 \in X_1$ incident to x_2 in $\mathbf{X}$. To define incidence between elements of $\mathcal{X}_2$ and elements of $\mathcal{X}_1$, we declare $(x_2, a) \in X_2 \times A$ to be incident to (x_1, a) for all $x_1 \in X_1$ incident to x_2 in $\mathbf{X}$, and to be incident to (x_2, b) for all $b \in B$ incident to a in $\mathbf{Y}$. The factor graph representation of the quantum is depicted on Figure 1.

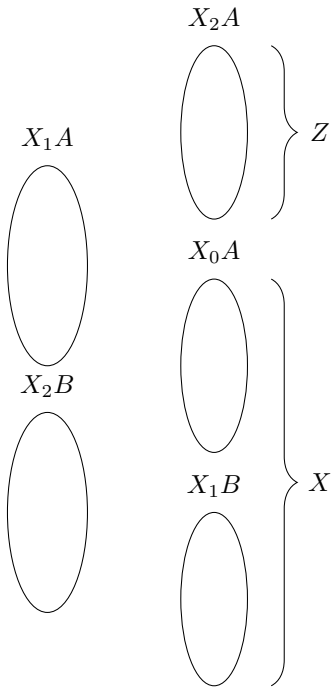

Figure 1. The factor graph structure of the quantum code $\mathcal{Q}(\mathcal{X})$. The code length is $N = |X_1||A| + |X_2||B|$.

From the definitions, we have that: If w_X^R, w_Z^R, w_Z^C are upper bounds respectively on the row weights of H_X, the row weights of H_Z and the column weights of H_Z, and if w^R, w^C are upper bounds respectively on the row weights and the column weights of H, then $\mathcal{Q}(\mathcal{X})$ is LDPC with its Z-row weights W_Z and X-row weights W_X being bounded from above by

$$W_Z \leq w_Z^R + w^C$$
$$W_X \leq \max(w_X^R, w^R + w_Z^C).$$

Similar relations hold for Z and X column weights of the new code.

We prove:

Theorem II.3. *The resulting quantum LDPC code $\mathcal{Q}(\mathcal{X})$ has length, dimension, X-distance and Z-distance equal to, respectively:*

$$N = |X_1||A| + |X_2||B|$$
$$K = \dim \mathcal{Q} \dim C$$
$$D_X = d_X(\mathcal{Q}) d(C)$$
$$D_Z = d_Z(\mathcal{Q}).$$

Theorem II.3 can also be derived from Theorem 1 of [31]. Theorem II.3 generalises a construction of Hastings [13] that corresponds to the special case when the complex $\mathbf{Y} = (A, B)$ is simplicial and when the underlying graph is a simple path. In coding theory terms, it is the case when the classical code C has dimension 1 and is the repetition code. The construction [29] of quantum LDPC codes is also a special instance of it, corresponding to the case when $X_0 = \emptyset$, meaning that there is no parity-check matrix H_X and that $d_X = 1$: in other words $\mathcal{Q}(\mathbf{X})$ is reduced to a classical LDPC code.

Theorem II.3 tells us therefore that if we have a quantum code $\mathcal{Q}$ such that $d_Z \gg d_X$, we can apply to it the $\mathcal{X}$-construction using a classical code C with minimum distance $d \approx d_Z/d_X$, and obtain a new quantum code with $D_X \approx D_Z$.

Specifically, starting with the "Ramanujan" quantum codes of the previous section, and using for the classical code C an asymptotically good LDPC code, i.e. with dimension and minimum distance that are linear in its blocklenth, (such a code being known to exist, either through the random methods that go back to Gallager, or through the expander code construction of Sipser and Spielman [27]), we obtain:

Corollary II.4.

(i) *2-dimensional Ramanujan complexes yield a family of quantum LDPC codes of length N, dimension K, and minimum distance D, with*

$$K = \Omega\left(\sqrt{\frac{N}{\log N}}\right), \qquad D = \Omega(\sqrt{N \log N}).$$

(ii) *3-dimensional Ramanujan complexes yield a family of quantum LDPC codes of length N, dimension K, and minimum distance D, with*

$$K = \Omega\left(\frac{\sqrt{N}}{\log N}\right), \qquad D = \Omega(N^{1/2} \log N).$$

C. The decoding problem

We now address the decoding problem for the codes of Corollary II.4. The objective is to correct any pattern of errors up to a constant fraction of the distance. We do not know how to do it for the codes of (ii) in Corollary II.4, but we achieve it for the codes of (i).

A CSS code of length n comes with two syndrome maps, namely

$$\begin{aligned} \sigma_X \ &: \mathbb{F}_2^{X_1} \to \mathbb{F}_2^{X_0} & \qquad \sigma_Z \ &: \mathbb{F}_2^{X_1} \to \mathbb{F}_2^{X_2} \\ \mathbf{x} \ &\mapsto H_X \mathbf{x}^T & \qquad \mathbf{x} \ &\mapsto H_Z \mathbf{x}^T \end{aligned}$$

where (X_0, X_1, X_2) is the associated complex. The syndrome maps σ_X and σ_Z are also the boundary and coboundary operators of the complex Let $\mathbf{e} = (\mathbf{e}_X, \mathbf{e}_Z)$ be a couple of vectors of $\mathbb{F}_2^n$, each of weight at most t. The *decoding problem* for a CSS code is, given $\sigma_X(\mathbf{e}_X)$ and $\sigma_Z(\mathbf{e}_Z)$, to recover an *equivalent* version of $\mathbf{e}$, namely a vector $\mathbf{e}' = (\mathbf{e}'_X, \mathbf{e}'_Z)$ such that $\mathbf{e}_X + \mathbf{e}'_X \in C_Z^\perp$ and $\mathbf{e}_Z + \mathbf{e}'_Z \in C_X^\perp$.

In [24], which is a particular instance of the product $\mathcal{X}$ construction just discussed, a decoding algorithm was devised that relied on expansion of the two underlying complexes (simply graphs in this case). In the present case, we cannot hope for such an approach to be completely transposed because though the underlying component simplicial complex $\mathbf{X}$ exhibits remarkable coboundary expansion, it does not have boundary expansion. However, the product quantum code $\mathcal{Q}(\mathcal{X})$ has a property that the codes of [24] do not have: if the component quantum code $\mathcal{Q}(\mathbf{X})$ can be decoded both from X-errors and from Z-errors, (which does not happen for the codes of [24] since the component "quantum code" is really a classical code and corrects zero X-errors), and if the classical code C also decodes a linear fraction of errors, then the overall code $\mathcal{Q}(\mathcal{X})$ can be decoded from both X-errors and Z-errors.

So we need a component quantum code that we can correct from both types of errors. For 2-dimensional simplicial complexes, boundary decoding (from X-errors) comes naturally, because it can be handled by complete decoding of cycle codes of graphs, which is known to be achievable in polynomial time through minimal weight matching in graphs. Focusing on 2-dimensional simplicial complexes $\mathbf{X}$, we prove the reduction:

Theorem II.5.

(i) *Suppose the classical LDPC code C comes with a polynomial-time decoding algorithm that corrects any pattern of less than $\alpha|A|$ errors. Then there is a polynomial time algorithm for $\mathcal{Q}(\mathcal{X})$ that corrects all X-errors of weight smaller than $\alpha|A|d_X/2$ where d_X is the 1-systole or X-distance for the component code $\mathcal{Q}(\mathbf{X})$.*

(ii) *Suppose there is a polynomial time decoding algorithm for the component quantum code $\mathcal{Q}(\mathbf{X})$ that corrects any pattern of Z-errors of weight smaller than w. Then there exists a polynomial time algorithm for $\mathcal{Q}(\mathcal{X})$ that corrects any pattern of Z-errors of weight smaller than w.*

To have a solution to the decoding problem for the product code $\mathcal{Q}(\mathcal{X})$, it remains to find a decoding algorithm for coboundary decoding (from Z-errors) of the component quantum code $\mathcal{Q}(\mathbf{X})$. We achieve this using coboundary expansion of LSV complexes in two different ways. For a 2-dimensional complex $\mathbf{X} = (V, E, T)$ the algorithm takes the following form:

Decoding algorithm:

Input: the coboundary or Z-syndrome $\mathbf{f}_0 = \sigma_Z(\mathbf{e})$ for a Z-error $\mathbf{e}$.

Procedure: for $k \geq 1$, look for a vertex v, and a vector $\mathbf{y}_k \in \mathbb{F}_2^E$, whose support is entirely in the edge-neighbourhood of v, such that $|\sigma_Z(\mathbf{y}_k) + \mathbf{f}_{k-1}| < |\mathbf{f}_{k-1}|$. Set $\mathbf{f}_k = \mathbf{f}_{k-1} + \sigma_Z(\mathbf{y}_k)$. Repeat until $\mathbf{f}_k = 0$ and output $\mathbf{e}' = \mathbf{y}_1 + \mathbf{y}_2 + \cdots \mathbf{y}_k$.

We prove:

Theorem II.6. *There exist constants c, q_0, such that when $\mathbf{X}$ is any 2-dimensional LSV complex of local parameter $q > q_0$, any Z-error vector $\mathbf{e} \in \mathbb{F}_2^E$ of weight $|\mathbf{e}| \leq c|E|$ is always correctly decoded by the decoding algorithm.*

The algorithm of Theorem II.6 is linear-time in the code length $|E|$, but with a constant that is exponential in the local parameter q. We can remove the constant when we replace the 2-dimensional LSV complex by the 2-skeleton $\mathbf{X} = (V, E, T)$ of a 3-dimensional LSV complex (V, E, T, P). Note that this differs from taking its (E, T, P) subcomplex which is used to create the codes of Corollary II.4 (ii). The associated product quantum code $\mathcal{Q}(\mathcal{X})$ will again have parameters equivalent to those of Corollary II.4 (i), though with looser constants. But in return we prove:

Theorem II.7. *For q fixed and large enough, there exists a constant c', such that when $\mathbf{X}$ is the 2-skeleton of any 3-dimensional LSV complex of local parameter q, any Z-error vector $\mathbf{e} \in \mathbb{F}_2^E$ of weight $|\mathbf{e}| \leq c'|E|$ is always correctly decoded by the decoding algorithm using local vectors $\mathbf{y}_k \in \mathbb{F}_2^E$ of weight 1.*

Note that the constant c' in Theorem II.7 depends on q, as opposed to the constant c in Theorem II.6 which is universal.

D. Comments and open questions

- The "expander" quantum LDPC codes of [24] can be seen as having been constructed through a co-complex tensoring operation with two 1-dimensional chain complexes, i.e. two bipartite graphs that are taken to be expanding graphs. The present quantum codes are obtained by replacing one of the components by a coboundary expanding simplicial complex. In both

cases expansion is crucial to decoding, even though we rely on different decoding strategies. We have focused on using Ramanujan LSV complexes, but good quantum codes are also liable to come from more general families of higher-dimensional expanders. What is needed is a simplicial complex with sufficiently good local expansion in its links: from this global expansion properties can be derived [26] and the required coboundary expansion follows. To obtain a quantum code of non-zero dimension one furthermore needs non-zero homology, and to obtain systolic bounds one requires the existence of a covering complex with zero homology and a growing injectivity radius.

- Reasonable values can be given for the constants in Theorem II.1: for large enough q, we have that $d_Z = S^1(\mathbf{X})$ is at least a quantity arbitrarily close to $n/4$ and $d_X \geq \frac{1}{32}\log_q n - 3$. The number of Z-errors correctable by the algorithm in Theorem II.6 can be made arbitrarily close to a $1/144$ fraction of the distance d_Z. The constants in Theorem II.2 and Theorem II.7 are much looser.
- It is possible to show that the logarithmic behaviour of the systolic distance d_X in Theorem II.1 cannot be improved. However it is very much open as to whether the $\log^2 n$ lower bound on d_X in Theorem II.2 is best possible or not. Any improvement would of course mean an improvement over the minimum distance of the quantum code of Corollary II.4 (ii).
- Coboundary decoding of 2-dimensional LSV complexes and of 2-skeletons of 3-dimensional complexes $\mathbf{X}$ is linear in their length $|E|$, which translates into linear-time decoding from Z-errors for the quantum code $\mathcal{Q}(\mathcal{X})$. However for X-errors we need to rely on complete decoding of the cycle code associated to the 1-skeleton of the complex $\mathbf{X}$ which is not linear in $|E|$ and we do not obtain a linear-time decoding algorithm for $\mathcal{Q}(\mathcal{X})$. It would of course be interesting to find an alternative strategy that would result in linear-time decoding from X-errors.
- The distance record-breaking higher-dimensional code of Corollary II.4 (ii) can be decoded from Z-errors by the same strategy as that used to prove Theorem II.7 if we replace the component (E, T, P) 2-complex of a 3-dimensional LSV complex by the (E, T, P) component of a 4-*dimensional* LSV complex. How to decode the corresponding quantum code from X-errors has eluded us however.
- We have focused on decoding worst-case errors. It would be interesting to address the decoding problem for random errors. The X-error decoding algorithm for the quantum code $\mathcal{Q}(\mathcal{X})$ is easily seen to work just as well for random errors up to a positive fraction of the code length. However, our Z-error correcting strategy fails for linear weight random errors and a different approach needs to be devised.

III. Decoding product complexes

We now focus on decoding the tensor product of a 2-dimensional simplicial complex $\mathbf{X}$ with a 1-dimensional complex $\mathbf{Y}$. We shall write $V = X_0$ for the set of vertices of $\mathbf{X}$, $E = X_1$ for its edge set, $T = X_2$ for its triangle set. We can think of (V, E, T) and (A, B) as incidence structures, in particular (A, B) is defined by a bipartite graph between A and B. We recall that what we require of (A, B) is that :

- the coboundary map $\delta_{B\to A} : \mathbb{F}_2^B \to \mathbb{F}_2^A$ has zero kernel, in other words the $|B| \times |A|$ incidence matrix H_{AB} of the bipartite graph (A, B) has rank $|B|$.
- the matrix H_{AB} is the parity-check matrix of a classical LDPC code C_{AB} of minimum distance $d_{AB} \geq c|A|$ for some constant c.

We will also require that the classical code C_{AB} comes with a decoding algorithm that is guaranteed to correct all errors of weight up to a fraction of its minimum distance. The expander codes of [27] are known to achieve this.

The quantum code $\mathcal{Q} = \mathcal{Q}(\mathcal{X})$ associated to the product complex has the factor graph representation depicted on Figure 1.

The quantum code now has coordinate (variable) set $\mathcal{N} = (E \times A) \cup (T \times B)$ that we abbreviate to $\mathcal{N} = EA \cup TB$. We have two syndrome functions

$$\begin{aligned}\sigma_Z &: \mathbb{F}_2^{\mathcal{N}} \to \mathbb{F}_2^{TA}\\ \sigma_X &: \mathbb{F}_2^{\mathcal{N}} \to \mathbb{F}_2^{VA\cup EB} = \mathbb{F}_2^{VA} \oplus \mathbb{F}_2^{EB}.\end{aligned}$$

We view σ_X as a boundary map and σ_Z as a coboundary map. This point of view is helpful since these maps inherit properties of the coboundary and boundary maps of the simplicial complex $\mathbf{X}$.

We adopt the following convention: we refer to the 1-cycles of the 2-complex $\mathbf{X}$, i.e. the cycles of the underlying graph (V, E), simply as *cycles.* We shall call the elements of $C_X = \ker \sigma_X$ in the product complex $\mathcal{X}$ as *Cycles* (capital C). By *trivial Cycle* (or Boundary) we shall mean an element of $\operatorname{Im} \sigma_Z^*$. Similarly, we will talk about cocycles in $\mathbf{X}$ (1-cocycles) and coCycles in the product complex $\mathcal{X}$, i.e. elements of $C_Z = \ker \sigma_Z$. To identify easily the 1-boundary maps ∂_1 in their respectives complexes $\mathbf{X}$ and $\mathbf{Y}$ we will write $\partial_{E\to V}$ and $\partial_{A\to B}$. Finally we will typically denote a vector (in $\mathbb{F}_2^A$, $\mathbb{F}_2^{EA}$, etc.) by bold letters, but also will regularly identify vectors with their supports to lighten notation. For example an element $a \in A$ will regularly also denote the vector of $\mathbb{F}_2^A$ whose support is $\{a\}$. Hopefully this abuse will not introduce confusion.

For the quantum code $\mathcal{Q}(\mathcal{X})$ we examine separately the cases of decoding X-errors and Z-errors since the situation is quite asymetrical. In both cases the goal is to correct a constant fraction of the minimum distance of $\mathcal{Q}(\mathcal{X})$.

A. Decoding X-errors

Theorem III.1. *Suppose the classical LDPC code C_{AB} comes with a polynomial-time decoding algorithm that corrects any pattern of less than $\alpha|A|$ errors. Then there is a polynomial time algorithm that given $\sigma_X(\mathbf{x})$ for $\mathbf{x} \in \mathbb{F}_2^{\mathcal{N}}$ of weight smaller than $\alpha|A|S_1(X)/2$, returns $\mathbf{x}+\mathbf{u}$ where $\mathbf{u} \in \mathrm{Im}\,(\sigma_Z^*)$.*

Note that the algorithm of Theorem III.1 returns precisely a solution to the decoding problem.

We now describe the decoding strategy.

• *EA representation.* Let $\mathbf{x} \in \mathbb{F}_2^{\mathcal{N}}$ be a arbitrary chain. We claim that there is a trivial Cycle $\mathbf{v} \in \mathrm{Im}\,\sigma_X^*$ such that $\mathbf{x}+\mathbf{v}$ has all its non-zero coordinates in EA. This is because the map $\partial_{A\to B}$ is surjective, meaning that for every $b \in B$ there is a set $A_b \subset A$, such that $b = \partial_{A\to B}(A_b)$. So for every coordinate $tb \in TB$ that is in the support of $\mathbf{x}$ we can add (this is not an algorithmic procedure, just an existence result) the σ_Z^*-image of the set $t \times A_b$. We shall call such a sum $\mathbf{x}+\mathbf{v}$ an *EA-representation* of $\mathbf{x}$ (it is not unique). Decoding from $\sigma_X(\mathbf{x})$ will consist of looking for an EA-representation of $\mathbf{x}$.

• *First decoding step: decoding from the VA part of $\sigma_X(\mathbf{x})$.* We focus on the VA-component of the X-syndrome and notice that it is the disjoint union, for $a \in A$, of the syndromes of all the Ea-components of $\mathbf{x}$. In other words, if we write:

$$\mathbf{x} = \sum_{a\in A} \mathbf{x}_a \otimes a + \mathbf{x}_{TB}$$

where $\mathbf{x}_a \in \mathbb{F}_2^E$ and $\mathbf{x}_{TB}$ has its support inside TB, then:

$$\sigma_X(\mathbf{x})_{|_{\mathrm{VA}}} = \sum_{a\in A} \partial_{E\to V}(\mathbf{x}_a) \otimes a.$$

The boundaries $\partial_{E\to V}(\mathbf{x}_a) \otimes a$ are in Va and disjoint, and the first decoding step consists simply of decoding from every V_a-component of the X-syndrome $\partial_{E\to V}(\mathbf{x}_a)$ to obtain a candidate for $\mathbf{x}_a$. This decoding procedure occurs, as just mentioned, inside the (V, E) graph, so we may apply the polynomial-time complete decoding procedure known to exist for cycle codes of graphs [25]. This returns the smallest weight vector $\mathbf{x}'_a$ to $\mathbf{x}_a$ such that $\mathbf{x}_a + \mathbf{x}'_a$ is a cycle. Whenever $\mathbf{x}_a$ has smaller weight than half the 1-systole $S_1(\mathbf{X})/2$ we have, since $|\mathbf{x}'_a| \le |\mathbf{x}_a|$, that $\mathbf{x}_a + \mathbf{x}'_a$ must be a trivial cycle.

For the purpose of clarity, we first describe the rest of the decoding procedure in a simple case which will help to follow the general situation.

• *Case when (A, B) is a path.* Let us suppose the graph (A, B) describes the edge-vertex incidence structure of a path, as in (1). The associated classical code C_{AB} is the repetition code, i.e. the code of dimension 1 generated by the all-one vector.

$$a_1 \overset{b_1}{\text{———}} a_2 \overset{b_2}{\text{———}} a_3 \text{ - - - - - - } a_{m-1} \overset{b_{m-1}}{\text{———}} a_m \qquad (1)$$

We have in this case $d_X(\mathcal{Q}) = mS_1(\mathbf{X})$ where $m = |A|$. If we use the simple majority decoder for the repetition code, we can correct any pattern of errors of weight $< |A|/2$ and the hypothesis on the weight of the error vector $\mathbf{x}$ in Theorem III.1 translates into $|\mathbf{x}| < mS_1(\mathbf{X})/4$. Under this hypothesis, we have that the number of $a \in A$ such that $\mathbf{x}_a$ is closer to a non-trivial cycle than to 0, is less than $|A|/2$.

• *Situation after the first decoding step.* The first decoding step yields a vector $\mathbf{y} = \sum_{a\in A} \mathbf{y}_a \otimes a$ such that

$$\sigma_X(\mathbf{y}))_{|_{\mathrm{VA}}} = \sigma_X(\mathbf{x})_{|_{\mathrm{VA}}}.$$

The vector $\mathbf{x}+\mathbf{y}$ is therefore such that each of its a-components $\mathbf{x}_a + \mathbf{y}_a$, for all $a \in A$, is a cycle, and from the discussion just above we have that a strict minority of them are non-trivial.

• *Second (and final) decoding step.* The decoder computes $\sigma_X(\mathbf{x}) + \sigma_X(\mathbf{y}) = \sigma_X(\mathbf{x}+\mathbf{y})$ and tries to recover an EA-representation of $\mathbf{z} = \mathbf{x}+\mathbf{y}$. Without loss of generality we suppose that $\mathbf{z}$ is equal to one of its EA-representations. Switching from $\mathbf{z}$ to one of its EA-representations changes its weight but does not change the nature of its a-components $\mathbf{z}_a$ which remain either trivial cycles or non-trivial cycles: in particular the fact that a minority of a-components of $\mathbf{z}$ are non-trivial is unchanged and this is the only feature used in the coming decoding argument.

We now have to deal with an X-syndrome whose VA-component is zero, and we are left with an EB-component from which to decode. We have

$$\mathbf{s} = \sigma_X(\mathbf{z}) = \sigma_X(\mathbf{z})_{|_{\mathrm{EB}}} = \sum_{a\in A} \sigma_X(\mathbf{z}_a \otimes a).$$

We may decompose $\mathbf{s}$ into b-components, $b \in B$,

$$\mathbf{s} = \sum_{b\in B} \mathbf{s}_b \otimes b$$

and using the path structure (1) of $A - B$ we have, for $i = 1, \dots m-1$,

$$\mathbf{s}_i = \mathbf{s}_{b_i} = \mathbf{z}_{a_i} + \mathbf{z}_{a_{i+1}}.$$

Rewrite $\mathbf{z}_i = \mathbf{z}_{a_i}$ to lighten notation. Given $\mathbf{s}$ and starting from a_1, the decoder may therefore construct the vector $\mathbf{z}' \in \mathbb{F}_2^{EA}$, $\mathbf{z}' = (\mathbf{z}'_1, \dots, \mathbf{z}'_n)$, $\mathbf{z}'_i \in \mathbb{F}_2^E$, setting

$$\begin{aligned}
\mathbf{z}'_1 &= 0 \\
\mathbf{z}'_2 &= \mathbf{z}_1 + \mathbf{z}_2 \\
\mathbf{z}'_3 &= (\mathbf{z}_2 + \mathbf{z}_3) + \mathbf{z}'_2 \\
&\vdots \\
\mathbf{z}'_i &= (\mathbf{z}_{i-1} + \mathbf{z}_i) + \mathbf{z}'_{i-1} \\
&\vdots
\end{aligned}$$

so that $\sigma_X(\mathbf{z}') = \sigma_X(\mathbf{z})$. We see that we have

$$\mathbf{z}' = (\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_n) + (\mathbf{z}_1, \mathbf{z}_1, \ldots, \mathbf{z}_1).$$

Similarly, the decoder can construct the alternative candidate vectors for $\mathbf{z}'$,

$$\mathbf{z}' = (\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_n) + (\mathbf{z}_i, \mathbf{z}_i, \ldots, \mathbf{z}_i) \tag{2}$$

for all values $i = 1, \ldots, n$.

We see that $\mathbf{z}'$ is equal to $\mathbf{z}$ up to addition of a trivial Cycle if and only if $\mathbf{z}_i$ is a trivial cycle in the complex $\mathbf{X}$. When $\mathbf{z}_i$ is non-trivial, then every trivial component of $\mathbf{z}$ becomes non-trivial in $\mathbf{z}'$. Therefore, the decoder may differentiate between the two cases $\mathbf{z}_i$ trivial/non-trivial in (2) by computing, for every component of $\mathbf{z}'$, whether it is a trivial cycle or not. Note that this test is obviously polynomial-time since it just involves testing whether a vector z_i belongs to a well-identified vector space or not and is achieved with elementary linear algebra. When it finds a majority of trivial components, it knows it is in the case "$\mathbf{z}_i$ trivial", and outputs $\mathbf{z}'$. We have that $\mathbf{y} + \mathbf{z}'$ is equal to the original error vector $\mathbf{x}$ up to addition of a trivial Cycle. This concludes the decoding algorithm in the case when (A, B) is a path.

• *Case of general bipartite graphs* (A, B).

As before, we try to recover an EA-representation of $\mathbf{z} = \mathbf{x}+\mathbf{y}$. Without loss of generality we assume $\mathbf{z}$ is one of those EA-representations. The chain $\mathbf{z}$ therefore has a syndrome $\sigma_X(\mathbf{z})$ with zero VA-component.

We first recover an arbitrary chain $\mathbf{z}'$ from the syndrome $\sigma_X(\mathbf{z})$ by picking any solution to the linear system. We obtain therefore $\mathbf{z}'$ such that $\sigma_X(\mathbf{z}') = \sigma_X(\mathbf{z})$. Now we define the subcode $\mathcal{C}$ of C_X with zero TB-component, i.e. the code in $\mathbb{F}_2^{EA}$ made up of those vectors with zero σ_X syndrome. This is exactly the tensor code

$$\begin{aligned}\mathcal{C} &= \ker \partial_{E\to V} \otimes \ker \partial_{A\to B} \\ &= \ker \partial_{E\to V} \otimes C_{AB} \\ &= Z_1(\mathbf{X}) \otimes Z_1(\mathbf{Y})\end{aligned}$$

so that we can write $\mathbf{z}' = \mathbf{z} + \mathbf{c}$, with $\mathbf{c} \in \mathcal{C}$. We also have that both $\mathbf{z}$ and $\mathbf{z}'$ live naturally in the tensor product space

$$\ker \partial_{E\to V} \otimes \mathbb{F}_2^A = Z_1(\mathbf{X}) \otimes C_1(\mathbf{Y})$$

(as opposed to the initial $\mathbb{F}_2^E \otimes \mathbb{F}_2^A$). We can therefore use a basis $\mathcal{Z}$ of cycles of $\ker \partial_{E\to V}$ and express $\mathbf{z}'$ in the basis of elementary tensors $z \otimes a$, $z \in \mathcal{Z}$, $a \in A$. Finally, we also have that the subcode $\mathcal{C}'$ of $\mathcal{C}$

$$\operatorname{Im} \partial_{T\to E} \otimes \ker \partial_{A\to B} = B_1(\mathbf{X}) \otimes Z_1(\mathbf{Y}) \tag{3}$$

is exactly the set of EA-representations of $\sigma_Z^*(\mathbb{F}_2^{TA})$. Therefore, we only need to recover $\mathbf{z}$ up to an element of $\mathcal{C}'$.

So we use a cycle basis $\mathcal{Z}$ of the form $\mathcal{Z} = \mathcal{Z}_0 \cup \mathcal{Z}_1$ where $\mathcal{Z}_0$ is a basis of the boundary space $\operatorname{Im} \partial_{T\to E}$. We now identify the chain $\mathbf{z}'$ as an element of $\mathbb{F}_2^{\mathcal{Z}} \otimes \mathbb{F}_2^A$: in concrete terms, this means we have identified $\mathbf{z}'$ with a $|\mathcal{Z}| \times |A|$ array that we obtain by elementary linear algebra. This array is partitioned into the union of a $|\mathcal{Z}_0| \times |A|$ subarray and a $|\mathcal{Z}_1| \times |A|$ subarray corresponding to the spaces $\mathbb{F}_2^{\mathcal{Z}_0} \otimes \mathbb{F}_2^A$ and $\mathbb{F}_2^{\mathcal{Z}_1} \otimes \mathbb{F}_2^A$. Now suppose first that at the first decoding step, the cycle code decoder that decodes every Ea component has made no error, meaning it recovers for every a the original Ea-component $\mathbf{x}_a$ of the error up to a trivial cycle. This translates into $\mathbf{z} = \mathbf{x} + \mathbf{y}$ being entirely inside $\mathbb{F}_2^{\mathcal{Z}_0} \otimes \mathbb{F}_2^A$, and having a zero component inside the $|\mathcal{Z}_1| \times |A|$ subarray. In this case the $\mathbb{F}_2^{\mathcal{Z}_1} \otimes \mathbb{F}_2^A$ component of $\mathbf{z}'$, viewed as a $|\mathcal{Z}_1| \times |A|$ array, has rows that are all codewords of C_{AB}, and to obtain $\mathbf{z}$ up to an element of $\mathcal{C}'$, we simply need to remove these codewords and put the $\mathbb{F}_2^{\mathcal{Z}_1} \otimes \mathbb{F}_2^A$ component at zero. Of course, we can't expect that there will be no errors during the first decoding step: but our hypothesis on the weight of the error vector, namely $|\mathbf{x}| < \alpha|A|S_1(\mathbf{X})/2$, implies that the cycle code decoder will add a non-trivial cycle to $\mathbf{x}_a$, for less than $\alpha|A|$ values of a. This translates into the number of non-zero columns of $\mathbf{z}$ in its $|\mathcal{Z}_1| \times |A|$ subarray component being less than $\alpha|A|$. This means in particular that every one of the rows of the subarray has weight less than $\alpha|A|$. Now on each of these rows $\mathbf{z}'$ is equal to $\mathbf{z}$ plus a codeword of C_{AB}, that we need to remove to recover $\mathbf{z}$ from $\mathbf{z}'$ up to a vector of $\mathcal{C}'$. Identifying and removing this codeword is always possible by applying the decoding procedure for C_{AB} that corrects up to $\alpha|A|$ errors. Once we have $\mathbf{z}$ up to a vector of $\mathcal{C}'$ we add it to $\mathbf{y}$ to obtain an equivalent version of the original error vector $\mathbf{x}$ and we are done.

B. Decoding Z-errors

Let us say that the 2-dimensional complex (V, E, T) *corrects w Z-errors* if there is a polynomial-time algorithm that: given the 2-coboundary $\delta_{E\to T}(\mathbf{e})$ of a cochain $\mathbf{e} \in \mathbb{F}_2^E$ of Hamming weight at most w, outputs $\mathbf{e} + \mathbf{c}$ where $\mathbf{c} \in \operatorname{Im} \delta_{V\to E}$ is a 1-coboundary. Note that this means exactly that the quantum code associated to the 2-complex corrects w Z-errors, hence the terminology.

Turning once more to the quantum code $\mathcal{Q}$ associated to the product of complexes $\mathbf{X}$ and $\mathbf{Y}$ associated to (V, E, T) and (A, B) we have the result:

Theorem III.2. *Suppose the 2-dimensional complex (V, E, T) corrects w Z-errors. Then there exists a polynomial-time algorithm that given $\sigma_Z(\mathbf{x})$ for $\mathbf{x} \in \mathbb{F}_2^N$ of weight at most w returns $\mathbf{x} + \mathbf{u}$ where $\mathbf{u} \in \operatorname{Im} \sigma_X^*$.*

In other words Theorem III.2 says that if the quantum code associated to the component 2-complex (V, E, T) can correct w Z-errors, then so can the product quantum code $\mathcal{Q}(\mathcal{X})$.

Again, it is natural to look at the decomposition of the error vector:

$$\mathbf{x} = \mathbf{x}_{EA} + \mathbf{x}_{TB}$$

with $\mathbf{x}_{EA} = \sum_{a\in A} \mathbf{x}_a \otimes a$. If we suppose that the error vector $\mathbf{x}$ is entirely supported in EA, then we have

$$\sigma_Z(\mathbf{x}) = \sum_{a\in A} \sigma_Z(\mathbf{x})_{|\text{Ta}}$$

with

$$\sigma_Z(\mathbf{x})_{|\text{Ta}} = \delta_{E\to T}(\mathbf{x}_a) \otimes a$$

Decoding would then consist of recovering in parallel $\mathbf{x}_a$ or an equivalent cochain from $\delta(\mathbf{x}_a)$ for every a. Obviously if $|\mathbf{x}| \leq t$ then $|\mathbf{x}_a| \leq w$ for every a and we can apply the decoding algorithm for the 2-dimensional simplicial complex $\mathbf{X}$.

However, when $\mathbf{x}_{TB} \neq 0$, this straightforward approach breaks down because every $\sigma_Z(\mathbf{x})_{|\text{Ta}}$ need not be a copy of a 2-coboundary anymore. To bypass this problem we look for a special equivalent form of $\mathbf{x}$.

Recall that the map $\delta_{B\to A} : \mathbb{F}_2^B \to \mathbb{F}_2^A$ has zero kernel. This implies that there exists $A' \subset A$, $|A'| = |B|$, such that the restricted linear map

$$\delta_{B\to A'} : \mathbb{F}_2^B \to \mathbb{F}_2^{A'},$$

defined by restricting the support of every vector of $\operatorname{Im}\delta$ to A', is one-to-one. Define $A'' = A \setminus A'$. Recall that two Z-error vectors are said to be equivalent if they differ by a vector of σ_X^*.

Lemma III.3. (Reduced cochain). *Let $\mathbf{x} \in \mathbb{F}_2^{\mathcal{N}}$. There exists an equivalent vector $\mathbf{x}'$ such that the EA-component of $\mathbf{x}'$ is entirely supported by EA'', in other words $\mathbf{x}'_a = 0$ for every $a \in A'$. Furthermore, we have that the weight of every Ea-component of $\mathbf{x}'$, for $a \in A''$, is upper bounded as: $|\mathbf{x}'_{Ea}| \leq |\mathbf{x}_{EA}|$. In particular, every Ea-component of $\mathbf{x}'$ is upper bounded by the total weight of $\mathbf{x}$.*

Proof: For every $a \in A'$, there exists a subset $B_a \subset B$, such that $\delta_{B\to A'}(B_a) = \{a\}$. Given the decomposition of $\mathbf{x}$

$$\mathbf{x} = \sum_{a\in A} \mathbf{x}_a \otimes a + \mathbf{x}_{TB}$$

we construct $\mathbf{x}'$ as:

$$\mathbf{x}' = \mathbf{x} + \sigma_X^* \left(\sum_{a\in A'} \sum_{b\in B_a} \mathbf{x}_a \otimes b \right).$$

which clearly deletes all EA' coordinates of $\mathbf{x}$. We also see that for any $a \in A''$, an e coordinate is added to the support of x_a, only if there is at least one $a \in A'$ such that x_a contains e in its support. This implies that the weight of $\mathbf{x}'_a$ cannot exceed the total weight of $\mathbf{x}$. ∎

When switching from $\mathbf{x}$ to its reduced form, we may obtain a cochain with larger weight but the EA component of the reduced chain has weight at most w. Since the weight of the EA component will turn out to be the only relevant one for the decoding argument, we may therefore assume that the error vector $\mathbf{x}$ is already in the reduced form given by Lemma III.3.

The decoding algorithm: We first recover the TB component $\mathbf{x}_{TB}$ of $\mathbf{x} = \mathbf{x}_{EA} + \mathbf{x}_{TB}$. The syndrome map σ_X, when applied to the TB component, is one-to-one when restricting its image to TA', since it is equal to $Id \otimes \delta_{B\to A'}$ and we have chosen A' such that $\delta_{B\to A'}$ is one-to-one. Therefore we can deduce the TB component $\mathbf{x}_{TB}$ of $\mathbf{x}$ from the TA' component of the $\sigma_Z(\mathbf{x})$. To find the EA component of $\mathbf{x}$, we only need to decode from $\sigma_Z(\mathbf{x}) + \sigma_Z(\mathbf{x}_{TB})$. This puts us back in the situation when the Z-error vector has no TB-component, and we can just apply the w-error-correcting algorithm to every Ta component of the syndrome. This concludes the proof of Theorem III.2.

ACKNOWLEDGMENTS

We wish to thank Anthony Leverrier for pointing out to us the relevance of reference [13] and setting us on the path leading to this paper. We are grateful to the Israeli Institute for Advanced Studies and the Simons Institute for the theory of Computing for hosting programmes on high-dimensional expanders that fostered this work.

SE is supported by NSF grant number DMS-1638352. TK Aknowledges support by ERC, and GZ is supported by ANR project ANR-18-CE47-0010 (QUDATA).

REFERENCES

[1] P. Abramenko and K. S. Brown. Buildings: theory and applications. Vol. 248. Springer Science & Business Media, 2008.

[2] B. Audoux, and A. Couvreur. On tensor products of CSS codes, *Annales de l'Institut Henri Poincaré (D)*, 2019, 6 (2), pp.239-287.

[3] S. Bravyi, and M. A. Hastings. Homological product codes, *Proceedings of the 46th annual ACM symposium on theory of computing, STOC '14*. New York, NY, USA, May 31– June 04, 2014, ACM, 2014, pp. 273–282.

[4] N. Breuckmann and B. Terhal. Constructions and Noise Threshold of Hyperbolic Surface Codes. *IEEE Trans. Inf. Theory*, 62 (6) 2016, pp. 3731–3744.

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

[6] A. Couvreur, N. Delfosse and G. Zémor. A construction of quantum LDPC codes from Cayley graphs, *IEEE Trans. Inform. Theory* 59 (9) 2013, pp. 6087—6098.

[7] N. Delfosse. Tradeoffs for reliable quantum information storage in surface codes and color codes, *IEEE International Symposium on Information Theory (ISIT)* 2013.

[8] S. Evra and T. Kaufman. Bounded degree cosystolic expanders of every dimension. *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*. 2016.

[9] M. H. Freedman, D. A. Meyer and F. Luo. Z_2-systolic freedom and quantum codes, *Mathematics of quantum computation*, Chapman & Hall/CRC, 287-320 (2002).

[10] L. Guth and A. Lubotzky. Quantum error-correcting codes and 4-dimensional arithmetic hyperbolic manifolds, *J. of Mathematical physics*, (2013).

[11] M. A. Hastings. Trivial low energy states for commuting Hamiltonians, and the quantum PCP conjecture. *Quantum Information & Computation*, 13(5-6):393–429, 2013.

[12] M. A. Hastings. Quantum Codes from High-Dimensional Manifolds. *ITCS* 2016.

[13] M. A. Hastings. Weight reduction for quantum codes. *Quantum Information & Computation*, 17(15-16):1307–1334, 2017.

[14] A. Hatcher. Algebraic Topology. Cambridge University Press, 2000.

[15] S. Hoory, N. Linial and A. Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc.* 43 (2006), pp. 439–561.

[16] T. Kaufman, D. Kazhdan and A. Lubotzky. Isoperimetric inequalities for Ramanujan complexes and topological expanders. *Geometric and Functional Analysis* 26.1 (2016): 250-287.

[17] A. Yu. Kitaev. Fault-tolerant quantum computation by anyons, *Ann. Physics* 303 (2003), no. 1, 2–30.

[18] V. Londe and A. Leverrier. Golden codes: quantum LDPC codes built from regular tessellations of hyperbolic 4-manifolds, *Quantum Information & Computation*, 19 (5-6) (2019).

[19] A. Lubotzky. Ramanujan complexes and high dimensional expanders, *Japanese Journal of Mathematics*, (2013).

[20] A. Lubotzky. High dimensional expanders, *Proceedings of the ICM* (2018): (1) 705–730.

[21] A. Lubotzky and R. Meshulam. A Moore bound for simplicial complexes, *Bulletin of the London Mathematical Society*, **39** (2007) 353-358.

[22] A. Lubotzky, B. Samuels and U. Vishne. Ramanujan complexes of type $\widetilde{A}_d$, *Israel Journal of Mathematics*, **149** (2005) pp. 267–300.

[23] A. Lubotzky, B. Samuels and U. Vishne. Explicit construction of Ramanujan complexes of type $\widetilde{A}_d$, *European Journal of Combinatorics*, **26(6)**(2005) 965-993.

[24] A. Leverrier, J.-P. Tillich, and G. Zémor. Quantum expander codes. In *Foundations of Computer Science (FOCS), 2015 IEEE 56th Annual Symposium on*, pages 810–824. IEEE, 2015.

[25] A. Ntafos and A. Hakimi. On the complexity of some coding problems, *IEEE Trans. Inf. Theory*, 27 (6) 1981, pp. 794–796.

[26] I. Oppenheim. Local Spectral Expansion Approach to High Dimensional Expanders Part I: Descent of Spectral Gaps. *Discrete & Computational Geometry* 59, pp. 293—330 (2018).

[27] M. Sipser, and D. A. Spielman. Expander codes, *IEEE Trans. Inf. Theory*, 42 (6) 1996, pp. 1710–1722.

[28] A. Steane. Multiple-particle interference and quantum error correction. *Proc. R. Soc. Lond. A*, 452(1954):2551–2577, 1996.

[29] J-P. Tillich, and G. Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength, *IEEE Trans. Inf. Theory*, 60 (2) 2014, pp. 1193–1202.

[30] 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*, LNCS 5557, Springer pp. 259-273.

[31] W. Zeng and L. Pryadko. Higher-Dimensional Quantum Hypergraph-Product Codes with Finite Rates. Phys. Rev. Lett. 122, 230501, 2019.