Balanced Product Quantum Codes

Nikolas P. Breuckmann and Jens N. Eberhardt

arXiv:2012.09271v2 [quant-ph] 22 Dec 2020

Abstract—This work provides the first explicit and non-random family of $[[N, K, D]]$ LDPC quantum codes which encode $K \in \Theta(N^{\frac{4}{5}})$ logical qubits with distance $D \in \Omega(N^{\frac{3}{5}})$. The family is constructed by amalgamating classical codes and Ramanujan graphs via an operation called *balanced product*.

Recently, Hastings–Haah–O'Donnell and Panteleev–Kalachev were the first to show that there exist families of LDPC quantum codes which break the $\text{polylog}(N)\sqrt{N}$ distance barrier. However, their constructions are based on probabilistic arguments which only guarantee the code parameters with high probability whereas our bounds hold unconditionally.

Index Terms—Quantum codes, quantum error-correction, quantum fault-tolerance.

I. INTRODUCTION

THE construction of low-density parity check (LDPC) quantum codes has some unique challenges in comparison to classical LDPC codes. While there are classical codes with constant encoding rate and linear distance, so-called *good codes*, no equivalent statement is known for LDPC quantum codes. Even more severely, no LDPC quantum codes with distance significantly larger than $\sqrt{N}$ were known to exist until recently.

For a long time, the best known distance was achieved by Freedman–Meyer–Luo in [1]. Their codes are derived from fiber bundles over the torus T^2. The fibers are hyperbolic surfaces twisted along geodesics, giving rise to a quantum code family with distance $\sqrt[4]{\log N}\sqrt{N}$. Evra–Kaufman–Zémor [2] and Kaufman–Tessler [3] further improved this to $\sqrt{\log N}\sqrt{N}$ and $\log^k(N)\sqrt{N}$, respectively.

Recently, the apparent $\text{polylog}(N)\sqrt{N}$ distance barrier was broken. Hastings–Haah–O'Donnell [4] introduced *fiber bundle codes* which have a random classical code as base and a cycle graph as fiber. They obtain $K \in \Theta(N^{\frac{3}{5}})$ and $D \in \Omega(N^{\frac{3}{5}}/\text{polylog}(N))$. Panteleev–Kalachev [5], [6] obtained codes with almost linear distance bounds using a similar construction called *lifted product*, where $K \in \Theta(N^{\alpha}\log(N))$ and $D \in \Omega(N^{1-\alpha/2}/\log(N))$ for $0 \leq \alpha < 1$. Both constructions are not explicit, in the sense that they make use of the properties of random graphs. Hence, they can only guarantee the bounds to hold with high probability.[1]

In this manuscript we explain how to construct families of quantum codes with exceptional asymptotic properties in a completely explicit and highly symmetrical way. To this end, we mimic the well-known *balanced product* $X \times_H Y$ of two

Nikolas P. Breuckmann, University College London, United Kingdom, n.breuckmann@ucl.ac.uk

Jens N. Eberhardt, University of Bonn, Germany, mail@jenseberhardt.com

[1]There is a nice explicit construction due to Bacon et. al. [7] which gives subsystem codes with distance $D \in \Omega(n^{1-\epsilon})$. It has sparse gauge operators but it is not LDPC. There are other interesting constructions using a mapping of quantum circuits to Hamiltonians [8] where the LDPC condition is slightly weakened, see [9].

topological spaces X and Y with an action of a group H [10]. Balanced products may be familiar to physicists as they appear in the construction of vector bundles associated to principal bundles. Here, we introduce the balanced product $C \otimes_H D$ of chain complexes and (quantum) codes by linearizing the topological notion. We apply this construction to classical codes C with good expansion properties and a cycle graph D, both sharing a common cyclic symmetry H.

We give two constructions of highly-symmetrical classical codes with good expansion properties. The first makes use of Ramanujan graphs which arise as Cayley graphs of the projective linear group $\text{PGL}(2, q)$ and were introduced by Lubotzky–Phillips–Sarnak [11]. The second, similar, construction uses tessellations and finite coverings of hyperbolic surfaces [12]. Both constructions admit a cyclic symmetry of known order. While we ultimately employ the Lubotzky–Phillips–Sarnak construction, we note that hyperbolic surfaces are extremely flexible and could be more suitable for practical applications.

By carefully choosing constants we obtain our main result.

Main Theorem (see Theorem 24)**.** *There is an explicit family of $[[N, K, D_X, D_Z]]$ LDPC quantum codes encoding $K \in \Theta(N^{\frac{2}{3}})$ logical qubits with X-distance $D_X \in \Omega(N^{\frac{1}{3}})$ and Z-distance $D_Z \in \Theta(N)$.*

Applying the distance balancing procedure of [13] and [2] we obtain the following corollary.

Corollary (see Corollary 25)**.** *There is an explicit family of $[[N, K, D]]$ LDPC quantum codes encoding $K \in \Theta(N^{\frac{4}{5}})$ logical qubits with distance $D \in \Omega(N^{\frac{3}{5}})$.*

We note that due to a technical condition some members of the constructed code family may turn out to be a subsystem codes. However, we stress that they are LDPC with respect to the stabilizer checks. Therefore, they do not share the same draw-backs as previously known subsystem codes such as [7].

We believe that our methods can be used to construct families of good LDPC quantum codes, see Section VI.

Remark—This manuscript arose with the intention of giving an explicit construction and a more conceptual understanding of the fiber bundle codes of Hastings–Haah–O'Donnell. By adapting their distance arguments we were able to explicitly construct balanced product codes with $K \in \Theta(N^{\frac{3}{5}})$ and $D \in \Omega(N^{\frac{3}{5}})$ improving their distance bounds by a factor of $\text{polylog}(N)$. However, shortly before we intended to publish, Panteleev–Kalachev showed that even better distance bounds are attainable. We make use of a result of theirs to further improve our bounds.

Summary

In Section II we give a homological perspective on (quantum) codes. This allows us to prove previous results more ele-

gantly by using known techniques from homological algebra. In Section III we review definitions, properties and explicit constructions of expander graphs. We discuss a construction of good classical codes due to Tanner/Sipser–Spielman using expander graphs. Moreover, we prove refined combinatorial properties which are important for the distance bounds of our codes. In Section IV we define and prove basic properties of balanced products. Here, the general construction of our code is given. Finally, in Section V we prove our main theorem by combining all of the above.

II. (QUANTUM) CODES AND CHAIN COMPLEXES

In this section we give a homological perspective on classical and quantum codes which puts them on equal footing and makes them ameanable to tools from homological algebra and topology. In particular, we explain how to construct quantum codes from cell complexes, double complexes and the fiber bundle construction of Hastings et al. [4]. For the latter we provide some new perspectives which allows for more streamlined proofs of some of their homological results.

Note that for the remainder of this manuscript we will only consider vector spaces over the field $\mathbb{F}_2$.

A. Complexes of Vector Spaces

A *chain complex* of vector spaces $C = (C_\bullet, \partial)$ is a set of vector spaces C_i equipped with linear maps, called *differentials*,

$$\partial_i : C_i \to C_{i-1}$$

that square to zero

$$\partial_{i-1}\partial_i = 0$$

In the following we will mostly drop the indices from the notation, so for example write $\partial^2 = 0$.

We denote by

$$Z_i(C) = \ker \partial_i \subset C_i$$
$$B_i(C) = \operatorname{im} \partial_{i+1} \subset C_i$$
$$H_i(C) = Z_i(C)/B_i(C)$$

the *i-cycles*, *i-boundaries* and the *i-th homology* of the complex C, respectively. Elements in C_i are called *i-chains*.

For most complexes we will considered, the spaces C_i are equipped with a canonical bases of so called *i-cells*. Hence, there is a natural scalar product

$$\langle v, w \rangle \in \mathbb{F}_2 \text{ for } v, w \in C_i.$$

In this case, we will take the freedom to write C^i for the linear dual of C_i and identify

$$C_i = C^i$$

using the scalar product. We refer to elements in C^i as cochains. We denote the transposed maps of the differential ∂ by

$$\delta^i = (\partial_{i-1})^{tr} : C^i \to C^{i+1}$$

and define by

$$Z^i(C) = \ker \delta^i \subset C^i$$
$$B^i(C) = \operatorname{im} \delta^{i-1} \subset C^i$$
$$H^i(C) = Z^i(C)/B^i(C)$$

the *i-cocycles*, *i-coboundaries* and the *i-th cohomology* of the complex C. The scalar product on C_i and C^i induces a well-defined and non-degenerate pairing of $H_i(C)$ and $H^i(C)$ since $B^i(C) = Z_i(C)^\perp$. The scalar product hence induces an isomorphism

$$H_i(C) \cong H^i(C).$$

B. (Quantum) Codes from Complexes

1) Classical codes: A classical, linear, binary code $\mathcal{C}$ is a subspace of $\mathbb{F}_2^n$. The number of encodable bits in $\mathcal{C}$ is its dimension $k = \dim \mathcal{C}$. The smallest Hamming weight of any non-trivial element of $\mathcal{C}$ is called the *distance* of $\mathcal{C}$ and denoted d. We call a classical code of size n, dimension k and distance d an $[n, k, d]$-code.

A linear code can be specified as the kernel of a *parity check matrix*. This allows us to write a classical code $\mathcal{C}$ in terms of a chain complex C as follows. Let

$$C = (C_1 \xrightarrow{\partial^C} C_0)$$

such that $C_1 = \mathbb{F}_2^n$ and ∂^C is the parity check matrix of the code $\mathcal{C}$. Then $\mathcal{C}$ is the space of 1-cycles $\mathcal{C} = H_1(X) = Z_1(C) = \ker \partial_1^C$. Furthermore, the space of checks acting on the code is the space of 0-chains.

Any code $\mathcal{C}$ gives rise to a chain complex C in this way. On the other hand, any chain complex $C = (C_\bullet, \partial)$ contains at least one classical code; we simply pick an index i and take $\mathcal{C} = Z_i^C = \ker \partial_i^C$.

From now on we will abuse notation and use the same symbol C for both the code as a subspace of $\mathbb{F}_2^n$ and the chain complex $(C_\bullet, \partial)$. It will always be clear from context which interpretation to choose.

Anyone with a sole interest in classical codes will not benefit from viewing them through the lens of homology. It is useful to us because it puts classical codes on equal footing with quantum codes as we will see below.

2) Stabilizer quantum codes: Stabilizer quantum codes are defined by their stabilizer group $\mathcal{S}$ which is an abelian subgroup of the Pauli group operating on n qubits that does not contain $-I$. The code space is the subspace of the Hilbert space of n qubits which is point-wise stabilized by $\mathcal{S}$. Pauli operators which stabilize the code space (as a whole) but are not in $\mathcal{S}$ are called *logical operators*.

A special class of stabilizer codes are those where the stabilizer group $\mathcal{S}$ has a set of generators which operate as all-X or all-Z. They are called *CSS quantum codes*. We note in passing that an arbitrary $[[n, k, d]]$ stabilizer code can be mapped onto an $[[4n, 2k, 2d]]$ CSS code [14]. If we are only interested in asymptotic scaling of the code parameters it is thus sufficient to only consider CSS codes.

CSS codes are in bijection with chain complexes of length two. This is because the X/Z-type generators can be mapped

onto matrices H_X/H_Z. The condition that stabilizers need to commute is equivalent to demanding $H_Z^T H_X = 0$. Hence, a CSS code is nothing but a chain complex

$$C_1 \xrightarrow{H_Z^T} C_0 \xrightarrow{H_X} C_{-1}$$

As we have seen previously for classical codes the reverse is also true: We can always obtain a quantum code from a chain complex. Let $C = (C_\bullet, \partial)$ be a chain complex of length ≥ 2 then we pick some index i and take

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

as a quantum code.

The parameters of a CSS code are given by

$$n = \dim C_i$$
$$k = \dim H_i$$

and the distance d is the minimum weight of a representative of a non-trivial element of H_i or H^i. See [15] for more details.

We call a family of stabilizer codes *low-density parity-check codes (LDPC)* if there exists some $w \in \mathbb{N}$ such that for each member of the family there exists a set of generators of the stabilizer group such that each generator has weight at most w and each qubit is only in the support of at most w checks.

3) Subsystem codes: Consider a CSS code where the qubits are identified with the i-cells of a chain complex C, as explained above. A *subsystem CSS code* is a CSS code in which we only utilize a subset of the logical qubits for information storage. The other logical degrees of freedom are being downgraded to so-called *gauge qubits*.

From the perspective of homology this corresponds to splitting the i-th homology of C into a direct sum $H_i = H_i^{\mathcal{L}} \oplus H_i^{\mathcal{G}}$ where $H_i^{\mathcal{L}} - \{0\}$ is in bijection to the logical Z-operators (up to stabilizers) and $H_i^{\mathcal{G}} - \{0\}$ is in bijection to the non-trivial gauge Z-operators (up to stabilizers). The pairing of the homology group H_i with the cohomology group H^i induces the compatible splitting $H^i = H_{\mathcal{L}}^i \oplus H_{\mathcal{G}}^i$.

We call the minimum weight of any representative of a class in $H_i^{\mathcal{L}}$ ($H_{\mathcal{L}}^i$) the *bare Z-distance* (*bare X-distance*). Note that it is generally possible to reduce the weight of the representatives of classes in $H_i^{\mathcal{L}}$ and $H_{\mathcal{L}}^i$ by adding representatives of $H_i^{\mathcal{G}}$ and $H_{\mathcal{G}}^i$. This makes it necessary to define another notion of distance: The *Z-distance d_Z* of a subsystem CSS code is the largest integer such that for all $[z] \in H_i$ with the property that the restriction to the logical part is non-zero $[z]|_{H_i^{\mathcal{L}}} \neq 0$ we have that $|z| \geq d_Z$. The *X-distance d_X* is defined equivalently. The *distance d* of a subsystem code is $d = \min\{d_X, d_Z\}$.[2]

A family of subsystem codes is called an *LDPC subsystem code* if there exists some $w \in \mathbb{N}$ such that for each member of the family there exists a set of generators of the *stabilizer group* such that each generator has weight at most w and each qubit is only in the support of at most w checks. We note that families of codes exists for which the stabilizer generators can be measured indirectly by measuring a generating set of the

---

[2]What we call the distance of a subsystem code is also sometimes called *dressed distance* in the literature.

gauge operators and there are cases where the latter all have bounded support and each qubit is acted upon by a bounded number of gauge operators. There exists a nice construction due to Bacon et. al. [7] which gives subsystem codes with dressed distance $d \in \Omega(n^{1-\epsilon})$ and which has sparse gauge operators but which is not LDPC. For more background on quantum codes see [16].

C. Complexes from Spaces

The origin of chain complexes and homology lie in algebraic topology. We briefly recall how to associate a chain complex to a cell complex.

Cell complexes are a discrete and combinatorial analogues of topological spaces and arise as cellulations thereof. A regular cell complex X is a finite union of cells σ which are glued in a nice way. An n-dimensional cell in X is called an *n-cell*. We denote by X^n the set of all n-cells in X and by $\partial\sigma$ the set of all $(n-1)$-cells in the boundary of the n-cell σ.

For example, consider the cell complex $X = C_\ell$ with 1-cells $\sigma_1, \ldots, \sigma_\ell$ and 0-cells $\tau_1, \ldots, \tau_\ell$ such that the boundary of σ_i is $\partial\sigma_i = \{\tau_i, \tau_{i+1}\}$, where we take indices modulo ℓ. Then C_ℓ corresponds to a celluation of a circle S^1 into ℓ pieces. Equivalently, C_ℓ can be viewed as a cycle graph, where 1-cells and 0-cells correspond to edges and vertices, respectively.

To a cell complex X one can associate a chain complex $C(X) = (C_\bullet(X), \partial)$ via

$$C_i(X) = \bigoplus_{\sigma \in X_i} \mathbb{F}_2 \sigma \text{ and } \partial(\sigma) = \sum_{\tau \in \partial\sigma} \tau.$$

With this, we can define the *homology* of a cell complex X via

$$H_i(X) = H_i(C(X)).$$

In our previous example it is easy to see that $\dim H_1(C_\ell) = 1$. Furthermore, interpreting the complex C as a classical code as described in Section II-B yields the repetition code. Another example is the $\ell \times \ell$-torus T_ℓ which is a cell complex of dimension 2. Here $\dim H_1(T_\ell) = 2$ and the quantum code associated to the chain complex $C(T_\ell)$ yields the famous toric code with parameters $[[2\ell^2, 2, \ell]]$.

D. Double Complexes and Total Complexes

In a wide variety of situations, chain complexes arise as the *total complex* of a *double complex*. A double complex $E = (E_{\bullet,\bullet}, \partial^v, \partial^h)$ is an array of vector spaces $E_{p,q}$ equipped with vertical and horizontal maps

$$\partial_{p,q}^v : E_{p,q} \to E_{p,q-1} \text{ and}$$
$$\partial_{p,q}^h : E_{p,q} \to E_{p-1,q}$$

such that ∂^v and ∂^h are commuting differentials

$$(\partial^v)^2 = (\partial^h)^2 = 0 \text{ and } \partial^v \partial^h = \partial^h \partial^v.$$

Here, and in the following, we will mostly drop the indices of differentials from the notation.

It is often useful to interpret a double complex as a "complex of complexes". Namely, each column of C forms

$$\begin{array}{ccc}
E_{p,q} & \xrightarrow{\ \partial^h_{p,q}\ } & E_{p-1,q} \\
{\scriptstyle \partial^v_{p,q}}\Big\downarrow & & \Big\downarrow{\scriptstyle \partial^v_{p-1,q}} \\
E_{p,q-1} & \xrightarrow[\ \partial^h_{p,q-1}\ ]{} & E_{p-1,q-1}
\end{array}$$

Fig. 1. A square in a double complex E which is required to commute.

$$\begin{array}{ccc}
C_p \otimes D_q & \xrightarrow{\ \partial^C_{p-1}\otimes\mathrm{id}\ } & C_{p-1} \otimes D_q \\
{\scriptstyle \mathrm{id}\,\otimes\partial^D_q}\Big\downarrow & & \Big\downarrow{\scriptstyle \mathrm{id}\,\otimes\partial^D_{q-1}} \\
C_p \otimes D_{q-1} & \xrightarrow[\ \partial^C_{p-1}\otimes\mathrm{id}\ ]{} & C_{p-1} \otimes D_{q-1}
\end{array}$$

Fig. 2. A square in the tensor product double complex $C \boxtimes D$.

a vertical complex using the vertical differential ∂^v whereas the horizontal differentials ∂^h define a horizontal complex of these vertical complexes.

1) Total Complex: A double complex E can be collapsed into a complex by "summing over the diagonals". The resulting *total complex* $\mathrm{Tot}(E)$ is the complex defined via

$$\mathrm{Tot}(E)_n = \bigoplus_{p+q=n} E_{p,q}$$

and the differential is given by $\partial = \partial^v + \partial^h$. In fact

$$\begin{aligned}
\partial^2 &= (\partial^v + \partial^h)^2 \\
&= (\partial^v)^2 + (\partial^v\partial^h + \partial^h\partial^v) + (\partial^h)^2 = 0
\end{aligned}$$

using that E is a double complex.

2) Tensor Product and Hypergraph Product: A fundamental example of a double complex is obtained by forming a tensor product of two complexes. Let $C = (C_\bullet, \partial^C)$ and $D = (D_\bullet, \partial^D)$ be two complexes. Then the *tensor product double complex* $C \boxtimes D$ of C and D is defined via

$$\begin{aligned}
(C \boxtimes D)_{p,q} &= C_p \otimes D_q, \\
\partial^v = \partial^C \otimes \mathrm{id}_D \ &\text{and}\ \partial^h = \mathrm{id}_C \otimes\partial^D.
\end{aligned}$$

The *tensor product complex* of two complexes C and D

$$C \otimes D = \mathrm{Tot}(C \boxtimes D)$$

is the total complex of their tensor product double complex.

The special case where where C and D are 1-complexes are also known as *hypergraph products* which were introduced in [17]. This was generalized for C being a complex of arbitrary finite length in [18].

3) Homology of Total Complexes: In general, the computation of the homology of a total complex $\mathrm{Tot}(E)$ can be quite subtle and subject of the powerful mathematical formalism of *spectral sequences*, which we briefly review in Appendix A. However, there are certain situations, in which the homology of a double complex can be computed from the homology of its vertical and horizontal complexes.

The homology of the complex $C \otimes D$ is subject of the *Künneth formula*.

$$\begin{array}{ccc}
E_{1,1} & & E_{0,1} \\
{\scriptstyle \partial^v}\Big\downarrow & & \Big\downarrow{\scriptstyle \partial^v} \\
E_{1,0} & & E_{0,0}
\end{array}$$

Fig. 3. The vertical differential in the double complex $E_{p,q}$

$$H_1(E_{1,\bullet}, \partial^v) \xrightarrow{\ \partial^h\ } H_1(E_{0,\bullet}, \partial^v)$$

$$H_0(E_{1,\bullet}, \partial^v) \xrightarrow[\ \partial^h\ ]{} H_0(E_{0,\bullet}, \partial^v)$$

Fig. 4. The induced horizontal differential on the vertical homology groups $H_q(E_{p,\bullet}, \partial^v)$.

Theorem 1 (Künneth formula). *There is a natural isomorphism*

$$H_n(C \otimes D) \cong \bigoplus_{p+q=n} H_p(C) \otimes H_q(D).$$

Another simple example, which will be of interest for us, is the situtations in which E is a 2×2 complex, that is, $E_{p,q} = 0$ for all $p, q \neq \{0,1\}$. In this case, the homology of $\mathrm{Tot}(E)$ can be computed by first taking homology in the vertical and then horizontal direction.

First, one takes homology along the differentials ∂^v, see Figure 3. The horizontal differential ∂^h induces a differential on resulting homology groups $H_q(E_{p,\bullet}, \partial^v)$, see Figure 4. Secondly, one takes homology along these induced horizontal differentials to obtain homology groups

$$H_p(H_q(E_{\bullet,\bullet}, \partial^v), \partial^h).$$

The homology of the total complex is comprised of these groups and one obtains an analogue of the Künneth formula.

Theorem 2. *If E is a 2×2-complex there is a natural isomorphism*

$$H_n(\mathrm{Tot}(E)) \cong \bigoplus_{p+q=n} H_p(H_q(E_{\bullet,\bullet}, \partial^v), \partial^h).$$

Proof. All differentials on the second page of the spectral sequence of the double complex E vanish since either their domain or codomain is zero. See Appendix A. □

E. Fiber Bundle Codes

Fiber bundle codes where introduced by Hastings et al. in [4] to demonstrate a construction of quantum codes breaking the $\sqrt{N}\,\mathrm{polylog}(N)$ distance bounds for the first time. The idea behind fiber bundle codes is to introduce a *twist* in the (horizontal) differentials in the tensor product double complex, in order to increase the distance of the resulting code.

For simplicity, let us consider two 1-complexes

$$\begin{aligned}
B &= (B_1 \xrightarrow{\partial^B} B_0)\ \text{and} \\
F &= (F_1 \xrightarrow{\partial^F} F_0),
\end{aligned}$$

we refer to as *base* and *fiber* respectively. Denote by $\mathrm{Aut}(F)$ the finite group of linear automorphisms of the complex F, that is, linear automorphisms of F_1 and F_0 that commute with the differential ∂^F. Further, denote basis vectors of B_i by b^i and write $b^0 \in \partial^B b^1$ if b^0 appears with a nonzero coefficient in $\partial^B b^1$.

The idea is to twist the horizontal differentials in the tensor product double complex $B \boxtimes F$ by a *connection* or *twist* φ which is a choice of an automorphism $\varphi(b^1, b^0) \in \mathrm{Aut}(F)$ to every pair (b^1, b^0) such that $b^0 \in \partial^B b^1$. Intuitively, the connection φ describes how the fiber F varies over the base B, hence its name.

The *fiber bundle double complex* $B \boxtimes_\varphi F$ is

$$
\begin{array}{ccc}
B_1 \otimes F_1 & \xrightarrow{\partial_\varphi} & B_0 \otimes F_1 \\
{\scriptstyle \mathrm{id} \otimes \partial^F} \downarrow & & \downarrow {\scriptstyle \mathrm{id} \otimes \partial^F} \\
B_1 \otimes F_0 & \xrightarrow[\partial_\varphi]{} & B_0 \otimes F_0
\end{array}
$$

where

$$
\partial_\varphi(b^1 \otimes f) = \sum_{b^0 \in \partial^B b^1} b^0 \otimes \varphi(b^1, b^0)(f).
$$

Chains in $B_1 \otimes F_0$, resp. $B_0 \otimes F_1$, are referred to as *horizontal*, resp. *vertical*, where we think of the base and fiber stretching out in the horizontal, resp. vertical, direction.

The *fiber bundle code* given by the total complex

$$
B \otimes_\varphi F = \mathrm{Tot}(B \boxtimes_\varphi F).
$$

It is easy to see that $B \otimes_\varphi F$ is really a double complex; ∂_φ and $\mathrm{id} \otimes \partial^F$ commute since $\varphi(b^1, b^0)$ commutes with ∂^F. Note that when $\varphi = 1$ then $\partial_\varphi = \partial^B \otimes \mathrm{id}$ and $B \otimes_\varphi F = B \otimes F$ is the usual tensor product complex.

Under mild conditions, the homology of the fiber bundle complex $B \otimes_\varphi F$ fulfills a Künneth formula.

Theorem 3. *Assume that the connection φ acts as the identity on the homology of F. Then there is an isomorphism.*

$$
H_n(B \otimes_\varphi F) \cong \bigoplus_{p+q=n} H_p(B) \otimes H_q(F).
$$

Proof. By Theorem 2 there is an isomorphism

$$
H_n(B \otimes_\varphi F) \cong \bigoplus_{p+q=n} H_p(H_q(B_\bullet \otimes F_\bullet, \mathrm{id} \otimes \partial), \partial_\varphi).
$$

Since the vertical differential $\mathrm{id} \otimes \partial$ acts trivially on the base B we get

$$
H_q(B_p \otimes F_\bullet, \mathrm{id} \otimes \partial) = B_p \otimes H_q(F).
$$

Since by assumption φ acts as the identity on the homology of F, the induced horizontal differential

$$
\partial_\varphi : B_p \otimes H_q(F) \to B_{p-1} \otimes H_q(F)
$$

is equal to $\partial \otimes \mathrm{id}$ and we obtain

$$
H_p(H_q(B_\bullet \otimes F_\bullet, \mathrm{id} \otimes \partial), \partial_\phi) = H_p(B) \otimes H_q(F).
$$

$\square$

We say that the complex F be *augmented* if there is a map $\epsilon : F_0 \to \mathbb{F}_2$, such that $\epsilon \partial^F = 0$. For example, if $F = C(Y)$

is the chain complex of a space Y a natural augmentation is induced by the projection $Y \to \{pt\}$ to a point. In this case, there is a natural map of chain complexes $\pi : F \to \mathbb{F}_2$ given by

$$
\begin{array}{ccc}
F_1 & \longrightarrow & F_0 \\
\downarrow {\scriptstyle 0} & & \downarrow {\scriptstyle \epsilon} \\
0 & \longrightarrow & \mathbb{F}_2
\end{array}
$$

which induces projection and restriction maps

$$
\pi_* : B \otimes_\varphi F \to B, \; b \otimes f \mapsto \pi(f)b \text{ and}
$$
$$
\pi^* : B^* \to (B \otimes_\varphi F)^*, \; b \mapsto b \otimes \pi^{tr}(1).
$$

Hastings et al. in [4] consider a special situation, in which these maps induce isomorphisms on the first (co-)homology group.

Theorem 4. *Under the assumptions that*

1) *the connection φ acts as the identity on the homology of F,*
2) *the augmentation induces an isomorphism $\epsilon : H_0(F) \to \mathbb{F}_2$ and*
3) $H_0(B) = 0$

the maps π_* and π^* induce isomorphism

$$
\pi_* : H_1(B \otimes_\varphi F) \to H_1(B) \text{ and}
$$
$$
\pi^* : H^1(B) \to H^1(B \otimes_\varphi F).
$$

Proof. Follows from Theorem 3. $\square$

This is a slight generalization of Lemma 2.5. in Hastings et al. where a similar result is obtained by elementary methods.

Hastings et al. focus on a special choice of B, F and ϕ and estimate the distance of the resulting code. We will not repeat their arguments here, as we will use different techniques to bound the distance of our codes.

III. EXPANDER CODES

In this section we will discuss a class of classical, linear, binary codes have number of bits k and distance d both scaling linearly in n. They are called *expander codes* and were defined by Sipser and Spielman [19].

A. Local Systems

It was shown by Tanner [20] that a large (global) code X can be improved if its parity checks are replaced by the parity checks of a small (local) code L.[3] In order to be able to do this we need that the parity checks of the global code X are all of weight s and the local code has block length s. We will restrict ourselves to the case where the global code X is a graph code with variables given by edges X^1 and checks by vertices X^0.

Let X be a finite s-regular graph. For a vertex $v \in X^0$, denote by $\delta v \subset X^1$ the set of incident edges. Further, let

$$
L = (L_1 \xrightarrow{\partial^L} L_0)
$$

[3]Tanner calls the local codes "subcodes" in [20].

denote a $[s,k,d]$-code called the *local code*. Denote by $\mathcal{B}$ the distinguished basis of L_1 given by the 1-cells (bits) of the code L. Furthermore, fix for any $v \in X^0$ a bijection

$$\Lambda_v : \delta v \to \mathcal{B}$$

and let $\Lambda = \{\Lambda_v\}_{v \in X^0}$. Each Λ_v is simply a labelling of the edges around the vertex v.

The global code associated to the graph X and local code L is given by the complex

$$C(X, L, \Lambda) = (C_1(X) \xrightarrow{\partial} C_0(X) \otimes L_0)$$

and the differential is defined via

$$\partial e = v \otimes \partial^L \Lambda_v(e) + w \otimes \partial^L \Lambda_w(e)$$

where $e \in X^1$ is an edge connecting vertices $v, w \in X^0$. We refer to these codes as *Tanner codes*.

We mention in passing that it was observed in [21] that Tanner codes can also be understood in terms of *twisted homology*, where the boundary operator defined in Equation (1) takes values in the L_0-valued functions over X^0 instead of the $\mathbb{F}_2$-vector space $C_0(X) \otimes L_0$. Both definitions are clearly equivalent, but the one given here is more convenient for our purposes.

Not every choice of graph X will give interesting codes. In the following section we will discuss infinite families of graphs $\{X_i\}_{i \in \mathbb{N}}$ called expander graphs which combined with a suitable local code L will yield families of good classical codes. In this case we will refer to the Tanner codes as *expander codes*.

Let us also note already here that the choice of local labels Λ will not affect any of the bounds proved later. Hence, we will often simply omit Λ and write $C(X, L)$, although the exact properties of the global code will in fact depend on Λ.

B. Expander Graphs

Expander graphs can be understood intuitively as graphs which are strongly connected. Strong connectivity by itself is nothing special as the complete graph is clearly as connected as a graph can be. However, it is non-trivial that infinite families of graphs exist which are strongly connected despite being s-regular, i.e. every vertex has constant degree s.

1) Basic definitions: The connectivity of a graph X can be quantified by the *Cheeger constant*

$$h(X) = \min_{\substack{S \subset V \\ 0 < |S| < \frac{|X^0|}{2}}} \frac{|\delta S|}{|S|}$$

where $\delta S = \{\{u, v\} \in X^1 \mid u \in S, v \in X^0 - S\}$ is the set of edges connecting S with its complement.[4] When $h(X)$ is small it means that we can disconnect a relatively large number of vertices (those in S) from the rest of the graph by removing a relatively small number of edges (those in δS).

There are other measures equivalent to the Cheeger constant. In particular, *spectral expansion* will be useful to us here. From

---

[4]We may equivalently think of S as a 0-chain in $C_0(X)$, δ as the coboundary operator and $|\cdot|$ as the Hamming weight.

now on we will assume that X is a connected, s-regular graph. Let A be the adjacency matrix of the graph X. The largest eigenvalue of A will always be s. Let λ_2 be the second largest eigenvalue of A. The *Cheeger inequalities* relate the Cheeger constant with λ_2:

$$\frac{1}{2}(s - \lambda_2) \leq h(X) \leq \sqrt{2s(s - \lambda_2)}$$

The lower the second eigenvalue λ_2 the better of an expander the graph X is. There exists a slight variation of the lower bound.

Lemma 5. *Let X be an s-regular graph with second largest eigenvalue λ_2 and let $S \subset X^0$ with $|S| < \alpha|X^0|$. Then it holds that*

$$(1 - \alpha)(s - \lambda_2) \leq \frac{|\delta S|}{|S|}. \tag{1}$$

Proof. The proof is a trivial extension of the standard proof of the Cheeger inequalities. $\square$

Naturally, we might ask what is the largest expansion rate that we can hope for. This is answered in terms of spectral expansion by the following theorem.

Theorem 6 (Alon–Boppana bound)**.** *Let X be an s-regular graph with second largest eigenvalue λ_2 then*

$$\lambda_2 \geq 2\sqrt{s-1} - \frac{2\sqrt{s-1}-1}{\lfloor \mathrm{diam}(X)/2 \rfloor}.$$

In particular, for a family of s-regular graphs $\{X_i\}$ such that $|X_i| \to \infty$ for $i \to \infty$ we have the lower bound $2\sqrt{s-1}$ on all of their second largest eigenvalues. Graphs which saturate this bound are called *Ramanujan graphs*.

It is a classic result that random graphs are expanders with high probability. Furthermore, in [22] it is shown that random graphs are very close to being Ramanujan. More concretely, let $\epsilon > 0$ and take a random s-regular graph X then the second largest eigenvalue of X is $\lambda_2 < 2\sqrt{s-1} + \epsilon$ with high probability (depending on ϵ and $|X|$). In Section III-D we will discuss explicit constructions of expander graphs.

2) Properties of expanders: We will now discuss some results on expander graphs.

Theorem 7 (Alon–Chung [23])**.** *Let X be an s-regular graph with second largest eigenvalue λ_2 and $S \subset X^0$ of size $|S| = \gamma|X^0|$ with $0 < \gamma < 1$. Let $X(S)$ be the subgraph of X induced by S. Let*

$$\alpha = \gamma^2 + \frac{\lambda_2}{s}\gamma(1 - \gamma). \tag{2}$$

It holds that the number of edges of the subgraph $X(S)^1$ is upper bounded as

$$|X(S)^1| \leq \alpha|X^1|.$$

By negation we obtain the following useful corollary.

Corollary 8. *Any set of edges $E \subset X^1$ of size $\alpha|X^1|$ is incident to more than $\gamma|X^0|$ vertices.*

We also have an explicit lower bound for the number of vertices incident to a set of edges $E \subset X^1$.

Lemma 9 (Edge-to-vertex expansion)**.** *Let $E \subset X^1$ with $|E| \leq \alpha|X^1|$. Let $\Gamma(E) \subset X^0$ denote the set of vertices incident to the edges in E. We then have*

$$|\Gamma(E)| \geq \beta|E|$$

where

$$\beta = \frac{\sqrt{\lambda_2^2 + 4s(s - \lambda_2)\alpha} - \lambda_2}{s(s - \lambda_2)\alpha}. \tag{3}$$

Proof. We can solve Equation (2) for γ and obtain

$$\gamma(\tilde{\alpha}) = \frac{\sqrt{\lambda_2^2 + 4s(s - \lambda_2)\tilde{\alpha}} - \lambda_2}{2(s - \lambda_2)}.$$

Since $\gamma(\tilde{\alpha})$ is a convex function we can lower bound it for $\tilde{\alpha}$ between 0 and α by a linear function with slope $\gamma(\alpha)/\alpha$. Combined with Corollary 8 we obtain

$$|\Gamma(E)| \geq \gamma|X^0| \geq \frac{2\gamma(\alpha)}{s\alpha}\alpha|X^1| = \beta|E|$$

as claimed. $\qquad\square$

The basic property of spectral expanders given in Lemma 5—sets of vertices S have large boundary with their complement—can be refined. The following lemma estimates how many vertices in S have many edges connecting them with the complement of S.

Lemma 10. *Let $S \subset X^0$ be a subset of vertices with $|S| \leq \alpha|X^0|$. Let $0 \leq b \leq s$ and denote*

$$A = \{v \in S \mid |(\delta S)_v| \geq s - b\}$$

where for $v \in S$ we define $(\delta S)_v = \delta S \cap \delta v$. Let

$$\beta = ((b - \lambda_2) - \alpha(s - \lambda_2))b^{-1}$$

then there is a lower bound

$$|A| \geq \beta|S|.$$

Proof. Let $B = S - A$. We partition the boundary δS accordingly into

$$(\delta S)_A = \bigcup_{v \in A}(\delta S)_v \text{ and } (\delta S)_B = \bigcup_{v \in B}(\delta S)_v.$$

Since $|(\delta S)_v| \leq s$ for all $v \in S$ and $|(\delta S)_v| < s - b$ for all $v \in B$ we get

$$(\delta S)_A \leq s|A| \text{ and}$$
$$(\delta S)_B \leq (s - b)|B|.$$

These inequalities together with Lemma 5 give

$$s|A| + (s - b)|B| \geq (1 - \alpha)(s - \lambda_2)|S|.$$

Since S is the disjoint union of A and B we can cancel the term $|B|$ to obtain

$$|A| \geq \frac{(b - \lambda_2) - \alpha(s - \lambda_2)}{b}|S| = \beta|S|$$

which is what we wanted to show. $\qquad\square$

C. Properties of Expander Codes

1) Parameters: What is the number of encoded bits of the expander code? — The local code L is defined by $s - k_L$ linear constraints. Each vertex of the expander graph X thus contributes $(1 - k_L/s)s$ constraints to the (global) code $C(X, L)$. As some constraints may be linearly dependent[5] and using $2|X^1| = s|X^0|$ we obtain the bound

$$k_{C(X,L)} \geq (2k_L/s - 1)|X^1|. \tag{4}$$

Theorem 11 (Sipser–Spielman [19])**.** *Let s be the block length of the local code L and d_L its distance. Further, let λ_2 the second-largest eigenvalue of the s-regular expander graph X. Then the distance $d_{C(X,L)}$ of the expander code $C(X,L)$ is lower bounded as follows:*

$$d_{C(X,L)} \geq \frac{(d_L - \lambda_2)d_L}{(s - \lambda_2)s}|X^1| \tag{5}$$

Proof. Consider a set of variables (edges) $E \subset X^1$ of size

$$|E| = \frac{s|X^0|}{2}\left(\gamma^2 + \frac{\lambda_2}{s}\gamma(1 - \gamma)\right). \tag{6}$$

By Corollary 8 we have that these edges are incident to more than $\gamma|X^0|$ vertices. Let $X(E)$ be the subgraph induced by E. The average number of edges incident to each vertex in $X(E)$ is

$$\frac{2|E|}{X(E)^0} \leq \frac{2|E|}{\gamma|X^0|} = s\left(\gamma + \frac{\lambda_2}{s}(1 - \gamma)\right).$$

We can now consider a simple probabilistic argument to constrain the weight of code words: If the average number of edges per vertex is smaller than the code distance of the local code d_L then E can not be a code word of the global code (the expander code). This means we must have

$$s\left(\gamma + \frac{\lambda_2}{s}(1 - \gamma)\right) < d_L$$

which is equivalent to

$$\gamma < \frac{d_L - \lambda_2}{s - \lambda_2}.$$

The above reasoning implies that for E to be a code word we must have $\gamma \geq (d_L - \lambda_2)/(s - \lambda_2)$ and substituting this into Equation (6) gives the result. $\qquad\square$

For the bound to be non-trivial we need that the distance of the local code must be strictly larger than the second eigenvalue of X:

$$d_L > \lambda_2 \tag{7}$$

We note that the bound actually given in [19, Lemma 15] is $d_{C(X,L)} \geq n(d_L - \lambda_2)^2/(s - \lambda_2)^2$ which is slightly worse than Equation (5). It is obtained by dropping the second term in Equation (6) which implicitly assumes that Equation (7) holds.

---

[5]This happens for example when the all-ones vector is a parity check of the local code L.

2) Expansion properties of Tanner codes: A matrix $A \in \mathbb{F}_2^{m \times n}$ is called (α, β)-*expanding* if for any $x \in \mathbb{F}_2^n$ with $|x| \leq \alpha n$ we have that $|Ax| \geq \beta |x|$. In this section we will analyse the expansion properties of the Tanner code

$$C(X, L, \Lambda) = (C_1(X) \xrightarrow{\partial} C_0(X) \otimes L_0)$$

given the spectral expansion λ_2 of the graph X and the distances $d_L, d_{L^\perp}$ of the local code L and its dual $L^\perp$. The following theorem shows that small errors will violate a large amount of checks.

Theorem 12. *For $\alpha > 0$ let $x \in C_1(X)$ such that $|x| \leq \alpha |X^1|$. Then $|\partial(x)| \geq \beta |x|$ where $\beta = \beta' \beta''$ and*

$$\beta' = \frac{\sqrt{\lambda_2^2 + 4s(s - \lambda_2)\alpha} - \lambda_2}{s(s - \lambda_2)\alpha}$$

$$\beta'' = \frac{(d_L - \lambda_2) - \frac{4\alpha}{s}(s - \lambda_2)}{d_L}$$

Proof. Denote by $E \subset X^1$ the subset of edges corresponding to the 1-chain x. Then $|E| = |x|$. Denote by $S = \Gamma(E) \subset X^0$ the set of vertices incident to E. In the notation of Lemma 10, let

$$A = \{v \in S \mid |(\delta S)_v| \geq s - d_L\}.$$

Since δS and E are disjoint, for all $v \in A$ we have

$$1 \leq |\delta v \cap E| < d_L.$$

Hence, at least one check at every vertex in A is violated and

$$|\partial(x)| \geq |A|.$$

Using the bounds for the edge-to-vertex vertex expansion of X, see Lemma 9 we get $S \geq \beta' |E|$. Now

$$|S| \leq 2|E| \leq 2\alpha |X^1| = \frac{4\alpha}{s}|X^0|$$

Then Lemma 10 yields $|A| \geq \beta'' |S|$. So, in total, we obtain the desired inequality. $\square$

Dually, the following theorem estimates the number of bits involved in any set of checks.

Theorem 13. *For $\alpha > 0$ let $y \in C_0(X) \otimes L_0$ such that $|y| \leq \alpha |X^0|(s - k_L)$. Then $|\delta(y)| \geq \beta y$ where*

$$\beta = \frac{(d_{L^\perp} - \lambda_2) - \alpha(s - k_L)(s - \lambda_2)}{(s - k_L)d_{L^\perp}}$$

Proof. Let S be the subset of vertices appearing non-trivially in y. Hence

$$y = \sum_{v \in S} v \otimes c_v$$

for appropriate $0 \neq c_v \in L_0$. Hence, clearly

$$(s - k_L)^{-1}|y| \leq |S| \leq |y|. \tag{8}$$

In the notation of Lemma 10, let

$$A = \{v \in S \mid |(\delta S)_v| \geq s - d_{L^\perp}\}.$$

By definition of the differential in the Tanner code, we have $|\delta(v \otimes c_v)| = |\delta_L(c_v)| \geq d_{L^\perp}$. Hence for each vertex $v \in A$, there is at least one edge $e \in (\delta S)_v$ such that e appears

in $\delta(v \otimes c_v)$. Since $e \in (\delta S)_v$ it appears in no other term $\delta(v' \otimes c_{v'})$ for $v \neq v' \in S$. Hence

$$|\delta(y)| \geq |A|.$$

Now the statement follows using Lemma 10 and Equation (8). $\square$

D. Explicit Constructions of Expander Graphs

In order to be able to apply the construction outlined in Section IV we need to have full control over the automorphism group of the expander graphs. This excludes in particular any randomized constructions of expanders. It turns out that projective linear groups give rise to several families of expanders and we outline two approaches below.

1) LPS-expander: The first construction we discuss is in fact the first explicit construction of Ramanujan expanders, which satisfy the optimal bound $\lambda_2 < 2\sqrt{s-1}$. It was achieved by Lubotzky, Phillips and Sarnak (LPS) in [11] by defining certain Cayley graphs which we will now discuss.

Consider a group G with generating set S. We assume that S is symmetric, i.e. if $s \in S$ then $s^{-1} \in S$. The *(undirected) Cayley graph* $\mathrm{Cay}(G, S)$ consists of the vertex-set G and any two vertices $g, g' \in G$ are connected by an edge if and only if there exists an $s \in S$ such that $g' = sg$. We stress that (among many other properties) the expansion of Cayley graphs $\mathrm{Cay}(G, S)$ depends on the choice of the generating set S.

LPS-expanders are Cayley graphs with respect to the groups $\mathrm{PGL}(2, q)$ or $\mathrm{PSL}(2, q)$ which we wil now define. Let $\mathbb{F}_q$ be the finite field of order q and let $\mathrm{GL}(2, q)$ be the group of invertible matrices in $\mathbb{F}_q^{2 \times 2}$. The *projective general linear group* $\mathrm{PGL}(2, q)$ is defined as

$$\mathrm{PGL}(2, q) = \mathrm{GL}(2, q)/\mathbb{F}_q^\times.$$

The *special linear group* $\mathrm{SL}(2, q)$ is the kernel of the determinant $\det : \mathrm{GL}(2, q) \to \mathbb{F}_q^\times$. The *projective special linear group* $\mathrm{PSL}(2, q)$ is $\mathrm{SL}(2, q)$ up to signs

$$\mathrm{PSL}(2, q) = \mathrm{SL}(2, q)/\{\pm 1\}.$$

We wil now define the generating sets of the LPS-expanders. Let p be a prime and let

$$\tilde{S}_p = \{(a, b, c, d) \in \mathbb{Z}^4 \mid a^2 + b^2 + c^2 + d^2 = p\}.$$

A classical theorem by Jacobi implies that $|\tilde{S}_p| = 8(p + 1)$. We have two cases:

1) $p \equiv 1 \mod 4$: For any $(a, b, c, d) \in \tilde{S}_p$ we have that exactly one element is odd and the rest are even. Define $S_p \subset \tilde{S}_p$ be the subset where a is positive and odd.

2) $p \equiv 3 \mod 4$: For any $(a, b, c, d) \in \tilde{S}_p$ we have that exactly one element of $\{a, b, c, d\}$ is even and the rest are odd. Define $S_p \subset \tilde{S}_p$ be the subset where a is even and the first non-zero element is positive.

It can be shown that either way $|S_p| = p + 1$. Now let q be prime and $x, y \in \mathbb{F}_q$ such that $x^2 + y^2 + 1 = 0$ then we define the following set of matrices:

$$S_{p,q} = \left\{ \begin{bmatrix} a + bx + dy & -by + c + dx \\ -by - c + dx & a - bx - dy \end{bmatrix} \mid (a, b, c, d) \in S_p \right\}$$

where the product between integers and elements of $\mathbb{F}_q$ is defined in the obvious way.

For $a \in \mathbb{Z}$ and p an odd prime we define the *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a \\ 1, & \text{if } p \nmid a \text{ and } a \text{ is a square modulo } p \\ -1, & \text{if } p \nmid a \text{ and } a \text{ is not a square modulo } p. \end{cases}$$

Theorem 14 (Lubotzky–Phillips–Sarnak [11]). *Assume that p and q are distinct, odd primes such that $q > 2\sqrt{p}$. If*

$$\left(\frac{p}{q}\right) = 1$$

then the set $S_{p,q}$ is a symmetric generating set of $\mathrm{PSL}(2,q)$ and we define $X_{p,q} = \mathrm{Cay}(\mathrm{PSL}(2,q), S_{p,q})$.

Otherwise we must have

$$\left(\frac{p}{q}\right) = -1$$

and the set $S_{p,q}$ is a symmetric generating set of $\mathrm{PGL}(2,q)$ and we define $X_{p,q} = \mathrm{Cay}(\mathrm{PGL}(2,q), S_{p,q})$.

In both cases the graphs $X_{p,q}$ are connected, $p+1$–regular expanders with $\lambda_2 < 2\sqrt{p}$.

For more information on LPS-expanders see [24].

2) Hyperbolic tessellations: Expander graphs can also be generated by purely geometric means, namely by considering regular tessellations of hyperbolic space. In particular, there exist infinitely many regular tessellations of the hyperbolic plane $\mathbb{H}^2$. A regular tessellation is an edge-to-edge covering of the plane by regular polygons. They are completely specified by the number of sides of the polygon r and the number of polygons meeting at each vertex s. This data is captured in the *Schläfli symbol* $\{r, s\}$.

It is possible, using the symmetry group $G_{r,s}$ of a regular tessellation $\{r, s\}$, to construct families of closed hyperbolic surfaces of increasing size. From this we can obtain infinite families of graphs $\{X_i\}$ by ignoring the faces or, in mathematical terms, by taking their the 1-skeleton $X_i^{\leq 1}$. This is done by factoring out normal subgroups N of the symmetry group $G_{r,s}$. The details of this procedure are outlined in Appendix B.

It was proven in [25] (using results from [26]) that all hyperbolic regular tessellations $\{r, s\}$ give families of s-regular expander graphs. Unfortunately, we are not aware of any explicit bounds on λ_2.

One method of obtaining normal subgroups is by taking a matrix representation of $G_{r,s}$ and reducing the matrix coefficients modulo a prime number. This induces a group homomorphism π_p. Since the kernel of any group homomorphism is normal we can consider $N_p = \ker \pi_p$ as candidates. In the context of quantum codes this procedure was used in [12], [27] in order to construct codes based on compact four-dimensional hyperbolic manifolds.

The group of orientation preserving symmetries of a regular tessellation $G_{r,s}^+ = \langle \rho, \sigma \mid \rho^r, \sigma^s, (\rho\sigma)^2 \rangle$ is generated by the order-r rotation around a face and the order-s rotation around a vertex. It naturally embeds into the real projective linear
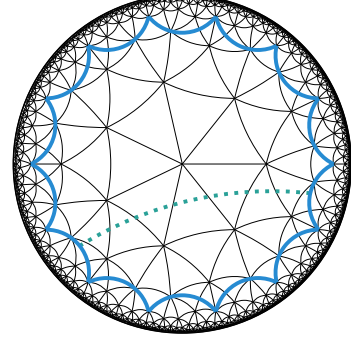

Fig. 5. A hyperbolic genus 3 surface supporting the $\{3, 7\}$ tessellation. It is called the Klein quartic. The dotted line indicates the translation $\tau = (\rho\sigma^{-2})^4$ under which points are being identified. The symmetry group of the surface is $\mathrm{Isom}(\mathbb{H}^2/N_\tau) = \mathrm{PSL}(2,7) \rtimes \mathbb{Z}_2$.

group (cf. Equation (16) in Appendix B). One representation of $G_{r,s}^+$ in $\mathrm{SL}(2,\mathbb{R})$ is due to Magnus [28]. It is obtained by mapping

$$\rho \mapsto R = \frac{i}{\sin(\pi/s)} \begin{bmatrix} \cos(\pi/r)\, e^{i\pi/s} & \xi\, e^{-i\pi/s} \\ -\xi\, e^{i\pi/s} & -\cos(\pi/r)\, e^{-i\pi/s} \end{bmatrix}$$

where $\xi = \sqrt{\cos(\pi/r)^2 - \sin(\pi/s)^2}$ and

$$\sigma \mapsto S = \begin{bmatrix} e^{i\pi/s} & 0 \\ 0 & e^{-i\pi/s} \end{bmatrix}.$$

The corresponding elements $\bar{R}$ and $\bar{S}$ in $\mathrm{PSL}(2,\mathbb{R})$ fulfill exactly the same relations as ρ and σ so that $G_{r,s}^+ \simeq \langle \bar{R}, \bar{S} \rangle$.

We now observe that for certain choices of $\{r, s\}$ the entries of R and S are algebraic integers, i.e. they are roots of normed polynomials with integer coefficients.[6] In that case we can adjoin the missing roots to $\mathbb{Z}$ giving a ring A and obtain $G_{r,s}^+ \leq \mathrm{PSL}(2, A)$. Reducing A modulo a prime p via π_p maps the matrix coefficients into a finite field $\mathbb{F}_{p^m}$. Hence, we obtain a subgroup of $\mathrm{PSL}(2, p^m)$.

It turns out that there are cases where this mapping $\pi_p : G_{r,s}^+ \to \mathrm{PSL}(2, p^\nu)$ is an epimorphism so that in fact $\mathrm{im}\,\pi_p \simeq \mathrm{PSL}(2, p^\nu)$. Additionally, in order for $\mathrm{PSL}(2, p^\nu)$ to be the symmetry group of a compactified surface we need that the corresponding $\ker \pi_p$ is torsion-free. The epimorphic images of $G_{r,s}^+$ onto $\mathrm{PSL}(2,q)$ with torsion-free kernel are classified by the following theorem.[7] It is in fact more general, as it also covers cases where there are epimorphic images of $G_{r,s}^+$ onto $\mathrm{PGL}(2,q)$ with torsion-free kernel.

We define $\mu(p, n)$ to be the smallest $\nu \in \mathbb{N}$ such that

$$p^\nu \equiv \pm 1 \begin{cases} \mathrm{mod}\, n, & \text{if } 2 \nmid n \\ \mathrm{mod}\, 2n, & \text{if } 2 \mid n. \end{cases}$$

We extend this definition to any sequence of integers $n_1, \ldots, n_w \in \mathbb{N}$ either equal or coprime to p by defining $\mu(p, n_1, \ldots, n_w)$ as the least common multiple

---

[6]For example, for the Magnus representation this is the case whenever the ratio $\cos(\pi/r)/\sin(\pi/s)$ is an algebraic integer.

[7]The results of Langer–Rosenberger in [29] are more general, we only quote the part which is relevant for us here.
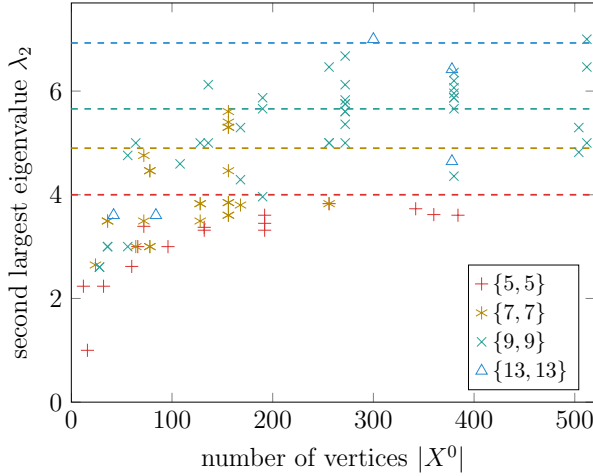
Fig. 6. The second largest eigenvalues of hyperbolic surfaces of small size labeled by their Schläfli symbol $\{r, s\}$. The dashed lines indicate the asymptotic lower bound $2\sqrt{s-1}$ of Theorem 6.

of $\mu(p, n_1), \ldots, \mu(p, n_w)$. For some tuple $(n', m', l') \in \mathbb{N}^3$ define the following two conditions:

(A) $m' = 2$, l' and $\nu = \mu(p, n', l')$ are even, $\mu(p, m')$ and $\mu(p, l')$ do not divide $\nu/2$, $\mu(p, n')$ divides $\nu/2$ and $p^{\frac{\nu}{2}} \equiv \pm 1 \mod l'$.

(B) m', l' and $\nu = \mu(p, n', m', l')$ are even, $\mu(p, m')$ and $\mu(p, l')$ do not divide $\nu/2$, $\mu(p, n')$ divides $\nu/2$, $p^{\frac{\nu}{2}} \equiv \pm 1 \mod m'$ and $p^{\frac{\nu}{2}} \equiv \pm 1 \mod l'$.

Theorem 15 (Langer–Rosenberger [29])**.** *Let $\{r, s\}$ be the Schläfli symbol of a hyperbolic tessellation and $p \geq 3$ a prime with either a) $p \nmid rs$, or b) $r = p$ and $p \nmid s$, or c) $s = p$ and $p \nmid r$.*

The group $\mathrm{PSL}(2, p^\nu)$, where $\nu = \mu(p, 2, r, s)$, is the epimorphic image of $G_{r,s}^+$ with torsion-free kernel if either

1) r *and* s *are odd, or*
2) r *or* s *(or both) are even and there exists no permutation* (n', m', l') *of* $(2, r, s)$ *such that condition (A) or (B) are fulfilled.*

The group $\mathrm{PGL}(2, p^\nu)$, where $\nu = \mu(p, 2, r, s)/2$, is the epimorphic image of $G_{r,s}^+$ with torsion-free kernel if r or s (or both) are even and there exists a permutation (n', m', l') of $(2, r, s)$ such that condition (A) or (B) is fulfilled.

A famous example is the *Klein quartic* shown in Figure 5. It is a hyperbolic surface of genus 3 which is tessellated by $\{3, 7\}$ and whose orientation-preserving symmetries form the group $\mathrm{PSL}(2, 7)$. The kernel of the reduction is isomorphic to $N_\tau^+ \leq G_{3,7}^+$ which is generated by all conjugates of the translation $\tau = (\rho\,\sigma^{-2})^4$ (cf. Equation (17)).

The discussion above indicates that hyperbolic expanders are related to Cayley graphs $\mathrm{Cay}\left(\mathrm{PSL}(2, \mathrm{q}), \{\bar{R}, \bar{S}, \bar{R}^{-1}, \bar{S}^{-1}\}\right)$. This relation is made precise in [25] by defining a quasi-isometry between them.

E. Local Codes

In order to construct good expander codes it suffices for the local codes to satisfy the constraints given by Equation (4)

and Equation (7), namely that it has to have rate $k_L/2 > 1/2$ and distance larger than the second eigenvalue of the graph $d_L > \lambda_2$.

1) Goppa Codes: A large family of codes which provides suitable candidates for the local codes L are *Goppa codes*. We consider their binary version here: Let m be a positive integer and let $g \in \mathbb{F}_{2^m}[x]$ be a polynomial of degree t. Furthermore, let $\gamma_1, \ldots, \gamma_s \in \mathbb{F}_{2^m}$ be chosen such that $g(\gamma_i) \neq 0$ for all i. A vector $c = (c_1, \ldots, c_s) \in \mathbb{F}_2^s$ is a code word of the Goppa code $\mathrm{GC}(g, \{\gamma_i\})$ if and only if

$$\sum_{i=1}^s \frac{c_i}{x - \gamma_i} \equiv 0 \mod g.$$

Note that we restricted the code to be over $\mathbb{F}_2$ which naturally embeds into $\mathbb{F}_{2^m}$. It can be shown that these codes come with the following bounds.

Theorem 16. *The (binary) Goppa code $\mathrm{GC}(g, \{\gamma_i\})$ defined above encodes $k_{\mathrm{GC}} \geq s - mt$ many bits and has distance $d_{\mathrm{GC}} \geq 2t + 1$.*

Hence, in order to satisfy the constraints Equation (4) and Equation (7) we only have to find a suitable polynomial g and elements $\gamma_1, \ldots, \gamma_s \in \mathbb{F}_{2^m}$.

It turns out that, using some deep results on exponential sums, it is possible to also bound the distance of the dual code of a Goppa code.

Theorem 17 (Moreno–Moreno [30])**.** *Assume the polynomial g has degree t and all roots of g are distinct. Let Z be the set of roots of g and let $\{\gamma_i\}$ be the set $\mathbb{F}_{2^m} - Z$. Then the distance $d_{\mathrm{GC}^\perp}$ of the dual code $\mathrm{GC}(g, \{\gamma_i\})^\perp$ is bounded from below by*

$$d_{\mathrm{GC}^\perp} \geq 2^{m-1} - \frac{|Z| - 1}{2} - (t - 1)\,2^{m/2}.$$

2) Cyclic codes and canonical labelings: To define the expander code $C(X, L, \Lambda)$ we need to fix a labeling Λ of the edges around each vertex. As the bounds do not depend on this labeling it can be chosen arbitrarily. However, it would be desirable if the labeling is compatible with some symmetries of the graph around each vertex.

In Figure 7 we show an example of an expander code $C(X, L)$ where X is obtained from a $\{3, 7\}$ tessellation of a genus-3 surface and the local code L is the $[7, 4, 3]$ Hamming code which is cyclic. Here there is a canonical choice for the labeling which respects the rotational symmetry around each vertex and of the cyclic symmetry of the local code. With this labeling the automorphism group acts transitively on the checks. Hence all checks are given by the orbit of a single check. Such codes are called *single-orbit symmetric codes*, a notion first introduced by Kaufman–Wigderson in [31].

It would be desirable if we could construct a family of codes which has this property. This is achieved by Kaufman–Lubotzky in the context of edge-transitive Ramanujan graphs [32]. In this work, it is shown that using the construction of LPS-expanders they can achieve a cyclic symmetry around each vertex. Moreover they construct suitable cyclic codes with good properties and show that the resulting Tanner
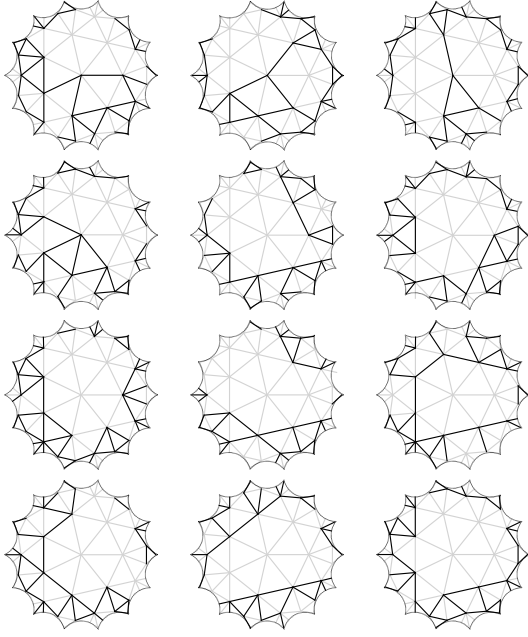
Fig. 7. Basis of a $[84, 12, 19]$ hyperbolic expander code $C(X, L)$. The graph X is derived from the $\{3, 7\}$ tessellation of the Klein quartic. The local code L is the $[7, 4, 3]$ Hamming code which is cyclic. Edges correspond to variables which are colored in black if their value is 1 and grey if their value is 0. Around each vertex is a code word of the Hamming code.

codes are single-orbit symmetry codes with linear number of encoded bits and linear distance.

A convinient choice are *BCH codes* which are a subclass of cyclic Goppa codes. The polynomial g is chosen to be x^t and the γ_i are the i-th powers of a primitive s-th root of unity, see [33, Example 8.2.6].

However, there is a subtlety when combining BCH codes with LPS-expanders, namely that the degree of LPS-expanders is even but the number of bits in BCH codes is odd. In order to overcome this the authors of [32] apply the doubling process of [34] to appropriately chosen BCH codes. For hyperbolic expanders this problem disappears as there is no restriction on the degree and thus there is more flexibility in the choice of the cyclic code.

3) Existence of good local codes: We can give stronger bounds on the properties of the local codes if we do not have to give an explicit construction. The following result, which extends the Gilbert-Varshamov bound by a bound for the distance of the dual code, was given in [6] without a formal proof. Here we spell out the argument in full detail. Let

$$H_2(\delta) = -\delta \log_2(\delta) - (1 - \delta) \log_2(1 - \delta)$$

be the binary entropy function.[8]

Theorem 18 (Gilbert–Varshamov+)**.** *Choose* $\delta \in (0, 0.11)$. *Then for all* $n > 2/(1/2 - H_2(\delta))$ *there exists a binary, linear code* C *with number of encoded bits* $k_C > n/2$, *distance* $d_C \geq \delta n$ *and dual code* $C^\perp$ *with distance* $d_{C^\perp} \geq \delta n$.

[8]The binary entropy function H_2 and the variable δ should not be confused with the second homology class and the coboundary operator. We will only use the former in the context of Theorem 18.

Proof. Fix $\delta \in (0, 0.11)$. Let A be the fraction of matrices G in $\mathbb{F}_2^{k \times n}$ such that there exists an $m \in \mathbb{F}_2^k - \{0\}$ with $|mG| < \delta n$. For fixed m let A_m be the fraction of matrices G in $\mathbb{F}_2^{k \times n}$ such that $|mG| < \delta n$. Clearly, we have

$$A \leq \sum_{m \in \mathbb{F}_2^k - \{0\}} A_m.$$

Equivalently, A_m can be defined as

$$\sum_{\substack{y \in \mathbb{F}_2^n \\ |y| \leq \delta n - 1}} A_{m,y}$$

where $A_{m,y}$ of all fractions of matrices G in $\mathbb{F}_2^{k \times n}$ with the property that $mG = y$. Clearly $A_{m,y} = 2^{-n}$ independently of m and y. Hence

$$A_m = \frac{|\operatorname{B}_0(\delta n - 1)|}{2^n}$$

where $\operatorname{B}_0(\delta n - 1)$ denotes the set of all $y \in \mathbb{F}_2^n$ with $|y| \leq \delta n - 1$. We can bound

$$|\operatorname{B}_0(\delta n - 1)| \leq 2^{H_2(\delta)n}$$

and obtain

$$A \leq 2^{k - (1 - H_2(\delta))n}.$$

Now, let us consider the fraction A' of *full-rank* matrices in $G \in \mathbb{F}_2^{k \times n}$ such that there exists an $m \in \mathbb{F}_2^k - \{0\}$ with $|mG| < \delta n$. Since any matrix which is not of full rank contributes to A, we have

$$A' \leq A \leq 2^{k - (1 - H_2(\delta))n}.$$

The group of invertible $\mathbb{F}_2^{k \times k}$-matrices $\operatorname{GL}(k, 2)$ operates *freely* from the left on the matrices G of full rank, so that all of the orbits have the same size. The orbits actually correspond to the different k-dimensional subspaces of $\mathbb{F}_2^n$, so the set of orbits is in fact the set of all codes of block length n. In particular, each representative of an orbit has the same distance. Hence, the fraction of codes with distance smaller than δn is equal to A'.

Similarly, denote by B' the fraction of subspaces of dimension $n - k$ of maximum distance smaller than δn. By the same arguments as before we can show that

$$B' \leq 2^{(n-k) - (1 - H_2(\delta))n}.$$

Since duality $C \mapsto C^\perp$ is a bijection between codes with k, respectively $n - k$ encoded bits B' is also the fraction of codes C with k encoded bits for which $d_{C^\perp} < \delta n$. Now, let D' be the fraction of codes C with k encoded bits such that their distance $d_C < \delta n$ or their dual distance $d_{C^\perp} < \delta n$. Then $D' \leq A' + B'$. We are interested in the case $k > n/2$ which implies $k > n - k$ so that $D' \leq 2^{k - (1 - H_2(\delta))n + 1}$. If the right hand side is smaller than 1 we are done since then we know there must exist a code with the desired properties. This condition is equivalent to $k - (1 - H_2(\delta))n + 1 < 0$. Since we are looking for k to be an integer between $n/2$ and $(1 - H_2(\delta))n - 1$, such k exists if $(1/2 - H_2(\delta))n > 2$. Now a direct calculation shows that $1/2 > H_2(\delta)$ if $\delta \in (0, 0.11)$ and the statement follows. $\square$

IV. Quantum Codes from Balanced Products

In this section we describe how chain/cell complexes with compatible symmetries can be turned into a new chain/cell complex. In special cases this is equivalent to the fiber bundle construction of Hastings–Haah–O'Donnell [4] or the lifted product construction of Panteleev–Kalachev [6].

A. Motiviation from Topolology

Our construction of codes is strongly motivated by principal bundles and associated fiber bundles, which we briefly recap now. Let X be a topological space with a *free* right action of a group H. Assuming some technical conditions, the quotient map

$$\pi : X \to X/H$$

is a principal H-bundle and in particular a fiber bundle with base X/H and fiber H.

1) Balanced Products: From the bundle (X, π) and any space Y with a left action of H one can construct a new fiber bundle over X/H and with fiber Y in the following way. Let H act anti-diagonally on the cartesian product $X \times Y$ via

$$(x, y) \cdot h = (x \cdot h^{-1}, \, h \cdot y).$$

The *balanced product* is the set of equivalence classes (H-orbits) under the action above:

$$X \times_H Y = (X \times Y)/H$$

We denote the elements of $X \times_H Y$ with square brackets $[x, y]$ to highlight that they are not tuples but equivalence classes under the action of H. Note that we can move a group element $h \in H$ from one side to the other $[x \cdot h, y] = [x, h \cdot y]$.

By projection we obtain a map

$$\pi_Y : X \times_H Y \to X/H, [x, y] \mapsto xH$$

which is the desired fiber bundle with fiber Y.

2) Example: Klein Bottle: For example, let $X = S^1$ be a circle and $H = \mathbb{Z}_2$ act via rotation by half a turn. Then $X/H = S^1$ is also a circle and $\pi : X \to X/H$ a 2-fold covering. Let H act on the circle $Y = S^1$ by the antipodal map. Then the associated balanced product $S^1 \times_{\mathbb{Z}_2} S^1$ is a *Klein bottle* which is a fiber bundle over the circle

$$\pi_{S^1} : S^1 \times_{\mathbb{Z}_2} S^1 \to S^1$$

with fiber S^1.

3) Trivialisations of Bundles: There is another, coordinatized, perspective on principal bundles and associated bundles which resembles the construction of fiber bundle codes by Hastings et al. more closely, see Section II-E.

For this, choose a *trivialisation* of the bundle $\pi : X \to X/H$, that is, a covering $\{U_i\}$ of X/H by open subsets and homeomorphisms

$$\psi_i : \pi^{-1}(U_i) \to U_i \times H$$

which are compatible with the action of H. If two sets U_i and U_j intersect non-trivially, the trivialisation induces transition maps

$$\varphi_{i,j} : U_i \cap U_j \to H.$$

These are the continuous version of the *connection* or *twist* φ used in definition of fiber bundle codes by Hastings et al. (see Section II-E).

The bundle $\pi : X \to X/H$ can be completely recovered from the data $\{U_i, \varphi_{i,j}\}$ by glueing the spaces $U_i \times H$ along the intersections $(U_i \cap U_j) \times H$ using the transition maps $\varphi_{i,j}$.

Similarly, if Y is a space with a left H-action, the data $\{U_i, \varphi_{i,j}\}$ allows to construct a fiber bundle with fiber Y by glueing the spaces $U_i \times Y$ using the action of $\varphi_{i,j}(x)$ on Y. In fact, this construction agrees with the balanced product $X \times_H Y$ described above.

B. Balanced Products of Vector Spaces

The balanced product in topology has an analogue in linear algebra. For vector spaces V, W with a linear right, respectively left action, of H the *balanced product* of V and W is defined as the quotient

$$V \otimes_H W = V \otimes W / \langle vh \otimes w - v \otimes hw \rangle.$$

To differentiate tensors in $V \otimes W$ and $V \otimes_H W$ we denote the former by $v \otimes w$ and the latter by $[v \otimes w]$. Note that $[vh \otimes w] = [v \otimes hw]$.

The balanced product can be understood as the tensor product

$$V \otimes_H W = V \otimes_{\mathbb{F}_2[H]} W$$

over the group algebra

$$\mathbb{F}_2 H = \left\{ \sum_{h \in H} a_h \, h \mid a_h \in \mathbb{F}_2 \right\}.$$

If H is finite and of odd order, then averaging over all group elements defines an isomorphism

$$V \otimes_H W \xrightarrow{\sim} (V \otimes W)^H, \, [v \otimes w] \mapsto \sum_{h \in H} vh^{-1} \otimes hw$$

with $(V \otimes W)^H$ being the set of elements in $V \otimes W$ that are invariant under the antidiagonal action $h \cdot (v \otimes w) = vh^{-1} \otimes hw$.

If $W = \mathbb{F}_2$ is equipped with the trivial action of H, then

$$V \otimes_H \mathbb{F}_2 = V / \langle vh - v \rangle = V_H$$

is the space of *coinvariants* of V under the action of H.

C. Balanced Products of Chain Complexes

1) Definition: We can extend the definition from vector spaces to chain complexes. Let C, D be chain complexes with a linear right, respectively left, action of H. By definition, this means that the action of H commutes with the differentials. Similarly, as for the double complexes discussed in Section II-D we can form the *balanced product double complex* $C \boxtimes_H D$ via

$$(C \boxtimes_H D)_{p,q} = C_p \otimes_H D_q,$$
$$\partial^v = \partial^C \otimes \mathrm{id}_D \text{ and } \partial^h = \mathrm{id}_C \otimes \partial^D.$$

Here, by abusing notation we denote ∂^v and ∂^h the induced differential on the quotients $C_p \otimes_H D_q$ of $C_p \otimes D_q$.

The *balanced product complex* is the total complex of the balanced product double complex

$$C \otimes_H D = \text{Tot}(C \boxtimes_H D).$$

If H is the trivial group, the balanced product is just the tensor product. Hence, balanced product complexes (codes) yield a generalization of the tensor (or hypergraph) product.

Assuming that H is a finite group of odd order we obtain the following version of the Künneth formula.

Lemma 19. *Let H be a finite group of odd order acting on C and D from the left and right, respectively. There is an isomorphism*

$$H_n(C \otimes_H D) \cong \bigoplus_{p+q=n} H_p(C) \otimes_H H_q(D).$$

Proof. To see this, note that the complex $C \otimes_H D$ is obtained from the complex $C \otimes D$ by passing to the coinvariants under the anti-diagonal action of H. Since H is finite and of odd order, taking coinvariants is naturally equivalent with taking invariants. Since taking invariants commutes with taking kernels and taking coinvariants commutes with taking cokernels, they commute with passing to homology. The statement follows from the Künneth formula for tensor products. $\square$

2) Relation to fiber bundle codes: In special cases the balanced product complex is an instance of a fiber bundle complex introduced by Hastings et al., see Section II-E. Namely, if C is a two-term complex and the action H restricts to a free action on the bases of each C_i, then there is a connection φ such that

$$C \otimes_H D = B \otimes_\varphi F$$

where $B_i = C_i/\langle ch - c \rangle$ and $F = D$. We skip the details here and will elaborate on this in a special case later on.

3) Relation to lifted product codes: If the complex D also fulfills the conditions of C from the last paragraph then the balanced product specializes to a so called *lifted product* (LP) or *generalized hypergraph product* (GHP)

$$C \otimes_H D = \text{LP}(\partial^C, \partial^D)$$

introduced by Panteleev–Kalachev in [5], [6]. Since we will make use of some of their results, let us elaborate on this. Denote by $R = \mathbb{F}_2 H$ the group algebra of H. Using the free action of H on the bases of C_i and D_i one can write the complexes C and D in the form

$$C = (R^n \xrightarrow{\partial^C} R^m)$$

$$D = (R^k \xrightarrow{\partial^D} R^l)$$

for suitable n, m, k and l. Hence, $\partial^C \in R^{n \times m}$ and $\partial^D \in R^{k \times l}$ can be identified with matrices with entries in the algebra R. The lifted product code is defined in terms of the matrices

$$M_1 = [\partial_C \otimes I_k, I_n \otimes \partial_D] \text{ and } M_2 = \begin{bmatrix} I_m \otimes \partial_D \\ \partial_C \otimes I_l \end{bmatrix}$$

where $\otimes$ denotes the Kronecker product of matrices over R. The matrices M_i have entries in the algebra R.

The action of R on itself by left multiplication (*regular representation*) defines an embedding $R \subset \mathbb{F}_2^{|H| \times |H|}$. In the case that $H = \mathbb{Z}_\ell$ is the cyclic group, the matrices in the image of this embedding are called *circulant matrices*.

On can replace the entries of the matrices in M_i by the corresponding matrices in $\mathbb{F}_2^{|H| \times |H|}$. The resulting matrices form a chain complex over $\mathbb{F}_2$ denoted by $\text{LP}(\partial^C, \partial^D)$. It is easy to see that this complex agrees with the balanced product complex $C \otimes_H D$.

D. Balanced Product and Bundles on Graphs

We now turn to a discrete version of the topological motivation from Section IV-A. For simplicity, we only consider one-dimensional cell complexes, i.e. graphs. However, the same ideas apply for cell complexes of arbitrary dimension.

1) Quotient graph and trivialisation: Let X be a graph with a free action of a finite group H, that is, H acts freely on vertices and edges. Further, we assume that there is no edge connecting two vertices of the form v and vh. We refer to this as the *quotient condition* (see [12]). For convenience, we choose an H-invariant orientation of the graph X and write $e = (v, v')$ for an oriented edge from v to v'. Such a choice is possible since H acts freely on the edges of X.

The *quotient graph* X/H is obtained in the following way. The vertices in X/H are the H-orbits $\mathcal{V}$ of vertices in X

$$(X/H)^0 = \{\mathcal{V}\}.$$

The edges in X/H are the H-orbits of $\mathcal{E}$ of edges in X

$$(X/H)^1 = \{\mathcal{E}\}.$$

Hence, two vertices $\mathcal{V}, \mathcal{V}'$ are adjacent in X/H if there are $v \in \mathcal{V}$ and $v' \in \mathcal{V}$ such that v and v' are adjacent in X. The orientation on X induces an orientation of X/H.

By the assumptions on the action of H on X, the quotient map

$$\pi : X \to X/H, v \mapsto vH$$

is a principal bundle and in particular an $|H|$-fold covering of X/H. If X is s-regular, so is X/H.

A *trivialisation* of $\pi : X \to X/H$ is a choice of representative $R = \{v \in \mathcal{V}\}$ for each orbit. It induces a *connection* ϕ_R

$$\phi_R : (X/H)^1 \to H, \mathcal{E} = (\mathcal{V}, \mathcal{V}') \mapsto \phi_R(\mathcal{E}).$$

Here, $\phi_R(\mathcal{E})$ is defined as follows. Denote by $v, v' \in R$ the representatives of $\mathcal{V}, \mathcal{V}'$. Then $\phi_R(\mathcal{E})$ denotes the unique element in H such that $(v, v'\phi_R(\mathcal{E}))$ is an edge in X.
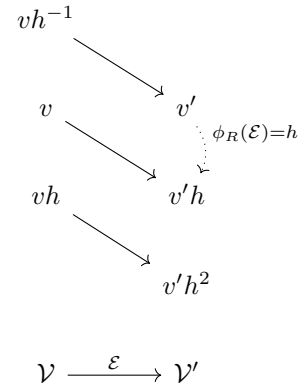
By choosing an approriate trivialisation R it is always possible to *locally* simplify ϕ_R such that, for example, $\phi_R(\mathcal{E}) = 1$ for all edges incident to a single fixed vertex. However, if X is connected, it is not possible to find a tivialisation R such that *globally* $\phi_R = 1$.

It is straightforward to see that one can recover the bundle $\pi : X \to X/H$ from X/H and ϕ_R and we will make use of both perspectives.

2) Balanced Products of Graphs: From the fiber bundle $\pi : X \to X/H$ and another graph Y with a left action of H we can form the balanced product $X \times_H Y = (X \times Y)/H$ which is the quotient of the cartesian product complex $X \times Y$ by the antidiagonal action of H. The map

$$\pi_Y : X \times_H Y \to X/H$$

has fibers Y and can be reconstructed from X/H, the transition maps ϕ_R and Y.

E. General Construction of Quantum Codes

Now, we combine the ideas of Tanner codes and balanced products. Keeping the notation from the last section, additionally assume that the graph X is s-regular. Furthermore, let L be a local $[s, k, d]$-code and $\Lambda = \{\Lambda_v\}_{v \in X^0}$ a labeling. We choose Λ in an H-invariant way, that is, we assume that

$$\Lambda_{vh}(eh) = \Lambda_v(e). \tag{9}$$

1) Definition in terms of the balanced product: We will consider the balanced product double complex $C(X, L) \boxtimes_H C(Y)$

$$
\begin{array}{ccc}
C_1(X) \otimes_H C_1(Y) & \xrightarrow{\partial \otimes \mathrm{id}} & (C_0(X) \otimes L_0) \otimes_H C_1(Y) \\
{\scriptstyle \mathrm{id} \otimes \partial} \downarrow & & \downarrow {\scriptstyle \mathrm{id} \otimes \mathrm{id} \otimes \partial} \\
C_1(X) \otimes_H C_0(Y) & \xrightarrow[\partial \otimes \mathrm{id}]{} & (C_0(X) \otimes L_0) \otimes_H C_0(Y)
\end{array}
$$

and the associated balanced product complex

$$C(X, L) \otimes_H C(Y).$$

Here $C(X, L) = C(X, L, \Lambda)$ denotes the Tanner code as defined in Section III-A. Our construction of quantum codes is based on this definition, using special choices of H, X, L and Y later on.

The construction above is a special case of the balanced product of two complexes, see Section IV-C. There are many interesting variants of this definitions, as for example the balanced product of two Tanner codes, which we will not discuss here.

2) Definition in terms of fiber bundles: As in the previous section, there is also a coordinatized definition of $C(X, L) \boxtimes_H C(Y)$ and $C(X, L) \otimes_H C(Y)$. For this, note that X/H is still an s-regular graph and by Equation (9) the labeling Λ descends to X/H. We can hence also consider the Tanner code

$$C(X/H, L) = (C_1(X/H) \xrightarrow{\partial} C_0(X/H) \otimes L_0)$$

and *fiber bundle double complex* $C(X/H, L) \boxtimes_{\phi_R} C(Y)$

$$
\begin{array}{ccc}
C_1(X/H) \otimes C_1(Y) & \xrightarrow{\partial_{\phi_R}} & C_0(X/H) \otimes L_0 \otimes C_1(Y) \\
{\scriptstyle \mathrm{id} \otimes \partial} \downarrow & & \downarrow {\scriptstyle \mathrm{id} \otimes \mathrm{id} \otimes \partial} \\
C_1(X/H) \otimes C_0(Y) & \xrightarrow[\partial_{\phi_R}]{} & C_0(X/H) \otimes L_0 \otimes C_0(Y)
\end{array}
$$

where

$$
\partial_{\phi_R}(\mathcal{E} \otimes y) = \\
\mathcal{V} \otimes \partial^L \Lambda_{\mathcal{V}}(\mathcal{E}) \otimes y + \mathcal{V}' \otimes \partial^L \Lambda_{\mathcal{V}'}(\mathcal{E}) \otimes \phi_R(\mathcal{E}) y
$$

for an oriented edge $\mathcal{E} = (\mathcal{V}, \mathcal{V}')$. The associated *fiber bundle complex* is obtained as the total complex

$$C(X/H, L) \otimes_{\phi_R} C(Y) = \mathrm{Tot}(C(X/H, L) \boxtimes_{\phi_R} C(Y)).$$

Again, it is straighforward to see that one can equate

$$C(X, L) \boxtimes_H C(Y) = C(X/H, L) \boxtimes_{\phi_R} C(Y) \text{ and}$$
$$C(X, L) \otimes_H C(Y) = C(X/H, L) \otimes_{\phi_R} C(Y).$$

Moreover, one can also interpret $C(X, L, \Lambda) \otimes_H C(Y)$ as a lifted product code, see Section IV-C3. It is helpful to have all perspectives in mind.

3) (Co-)Homology: The (co-)homology groups of the balanced product complex $C(X, L) \otimes_H C(Y)$ can be calculated using the Künneth formula for balanced products, see Lemma 19.

We will make this explicit here. We denote elements in $H_1(C(X, L) \otimes_H C(Y))$ by $[(u, v)]$ where

$$u \in C_1(X, L) \otimes_H C_0(Y) \text{ and } v \in C_0(X, L) \otimes_H C_1(Y)$$

and refer to u as the *horizontal* and v as the *vertical* part. The Künneth formula implies that $H_1(C(X, L) \otimes_H C(Y))$ is generated by the complementary subspaces of *horizontal* homology classes

$$H_1^h(C(X, L) \otimes_H C(Y)),$$

which admit a representative of the form $(u, 0)$ and *vertical* homology classes

$$H_1^v(C(X, L) \otimes_H C(Y)),$$

which admit a representative of the form $(0, v)$. We denote the corresponding projection maps by

$$p^h : H_1(C(X, L) \otimes_H C(Y)) \to H_1^h(C(X, L) \otimes_H C(Y))$$
$$p^v : H_1(C(X, L) \otimes_H C(Y)) \to H_1^v(C(X, L) \otimes_H C(Y)).$$

The maps can be computed as

$$p^h([(u, v)]) = [u] \text{ and } p^v([(u, v)]) = [v]$$

if $[u]$ and $[v]$ are homology classes. To evaluate the projection maps given a general representative (u, v), note that the Künneth formula ensures that one can always find a homologous representative (u', v') where $[u']$ and $[v']$ *are* homology classes.

Note that if $H_0(C(X, L)) = 0$, or equivalently, the checks of the Tanner code $C(X, L)$ are linearly independent, we have

$$H_1(C(X, L) \otimes_H C(Y)) = H_1^h(C(X, L) \otimes_H C(Y))$$

and there are no non-trivial vertical homology classes.

The obvious dual definitions and statements apply to co-homology. For example, the space of *horizontal cohomology* classes denoted by

$$H_h^1(C(X,L) \otimes_H C(Y)) \subseteq H^1(C(X,L) \otimes_H C(Y))$$

consists of cohomology classes with have a representative of the form $(u,0)$ for

$$u \in C^1(X,L) \otimes_H C^0(Y) = C_1(X,L) \otimes_H C_0(Y).$$

The corresponding projections are denoted by p_h and p_v.

F. Balanced Product with a Circle

We are interested in a special situation. Namely, let $H = \mathbb{Z}_\ell$ be the cyclic group and $Y = C_\ell$ the cycle graph of size ℓ, with ℓ odd. Then the natural action of $\mathbb{Z}_\ell$ on C_ℓ by translation induces a trivial action on the homology groups $H_0(C_\ell) = H_1(C_\ell) = \mathbb{F}_2$. Fix some vertex y_0 and edge y_1 in C_ℓ. Then the maps

$$\mathbb{F}_2[\mathbb{Z}_\ell] \to C_i(C_\ell), \sum_h a_h h \mapsto \sum_h a_h y_i h$$

are isomorphisms for $i = 1, 2$. Similarly, for every vector space V with a linear right action the maps

$$V \to V \otimes_{\mathbb{Z}_\ell} C_i(C_\ell), v \mapsto [v \otimes y_i].$$

are isomorphism for $i = 1, 2$.

Consider the linear maps

$$\iota : H_1(C(X/H,L)) \to H_1^h(C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell)),$$

$$\left[\sum_{\mathcal{E}} a_{\mathcal{E}} \mathcal{E}\right] \mapsto \left[\sum_{\mathcal{E}} a_{\mathcal{E}} \sum_{e \in \mathcal{E}} [e \otimes y_0], 0\right]$$

taking a code word of the Tanner code $H_1(C(X/H,L))$ to a code word in the balanced product code $H_1^h(C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell))$. Conversely we define the linear map

$$\pi : H_1^h(C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell)) \to H_1(C(X/H,L))$$

$$\left[\left[\sum_e a_e e \otimes y_0\right], 0\right] \mapsto \left[\sum_e a_e eH\right]$$

which projects a code word of the balanced product code $H_1^h(C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell))$ onto a code word of the Tanner code $H_1(C(X/H,L))$.

The composition $\pi \circ \iota$ is the multiplication with $|\mathbb{Z}_\ell| = 1 \mod 2$ and hence the identity. Note that by the Künneth formula there is an isomorphism

$$H_1^h(C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell)) \cong H_1(C(X,L)) \otimes_{\mathbb{Z}_\ell} H_0(C_\ell)$$
$$= H_1(C(X,L))/\langle vh - v \rangle$$

and the latter can naturally identified with $H_1(C(X/H,L))$. Hence π and ι are indeed isomorphisms by a dimension argument.

For $Y = C_\ell$ the projection map p^h takes a particularly nice form when composed with π. Independently of finding a nice representative (u,v) where $[u]$ is a homology class, one has

$$\pi \circ p^h \left[\left[\sum_e a_e e \otimes y_0\right], v\right] = \left[\sum_e a_e eH\right].$$

This follows easily by checking that the definition is invariant under adding boundaries. Dually, the transposed of the maps π and ι define an isomorphism

$$H_h^1(C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell)) \cong H^1(C(X/H,L)).$$

We subsume the result in the following theorem.

Theorem 20. *The number of logical bits that can be encoded in the horizontal part of the balanced product code*

$$\dim H_1^h(C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell)) = \dim H_1(C(X/H,L)) \quad (10)$$

agrees with the number of logical bits in the Tanner code $C(X/H,L)$.

We note that these results can also be obtained by using the definition by fiber bundles outlined in Section IV-E2 and the discussion in Section II-E.

G. Balanced Product Subsystem Codes

For later applications we are only interested in the horizontal part of the homology. This is because we will obtain superior distance bounds for these elements. To achieve this we make use of the formalism of subsystem codes which we introduced in Section II-B. We refer to this as the *horizontal subsystem balanced product code*.

We define the logical operators of Z-type to correspond to the non-trivial elements of

$$H_1^{\mathcal{L}} = H_1^h(C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell))$$

and the gauge qubits of Z-type, which we disregard, to be the non-trivial elements of

$$H_1^{\mathcal{G}} = H_1^v(C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell)).$$

This induces the splitting in the cohomology

$$H_{\mathcal{L}}^1 = H_h^1(C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell))$$

and

$$H_{\mathcal{G}}^1 = H_v^1(C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell)).$$

Note, that if the checks in the Tanner code $C(X/H,L)$ are independent then the vertical (co)homology classes vanish. In this case this procedure is unnecesary as $H_1^{\mathcal{G}} = 0$.

H. Distance Theorems

Using the ingenious distance bounds for lifted product codes by Panteleev–Kalachev in [6], we are able to bound the (co-)homological distance of the balanced products between Tanner codes and cycles $C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell)$ in terms of expansion properties of the Tanner code $C(X,L)$.

Theorem 21 (Panteleev–Kalachev [6])**.** *Assume that the boundary map of the Tanner code* $C(X,L)$

$$C_1(X) \xrightarrow{\partial} C_0(X) \otimes L_0$$

is $(\alpha_{\mathrm{ho}}, \beta_{\mathrm{ho}})$-*expanding. Let* $x = (u,v)$ *be a representative of a non-trivial homology class* $[x] \in H_1(C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell))$.

1) *If the horizontal part*

$$0 \neq p^h(x) \in H_1^h(C(X,L) \otimes_{\mathbb{Z}_\ell} C(C_\ell))$$

of x is non-trivial, then

$$|x| = |u| + |v| \geq |X^1| \min \{\alpha_{\mathrm{ho}}/2, \alpha_{\mathrm{ho}}\beta_{\mathrm{ho}}/4\}.$$

2) *Else, if $p^h(x) = 0$, then*

$$|x| = |u| + |v| \geq \ell \min \{\alpha_{\mathrm{ho}}/(4s), \alpha_{\mathrm{ho}}\beta_{\mathrm{ho}}/(4s)\}.$$

Proof. The code $C(X, L) \otimes_{\mathbb{Z}_\ell} C(C_\ell)$ agrees with the a lifted product code $\mathrm{LP}(A, 1 + x)$ in the notation of Panteleev–Kalachev [6] where $A = \partial$ is the matrix representing the differential ∂ of the Tanner code $C(X, L)$.

The two cases in the theorem correspond to Case 1 and 2 in the proof of [6, Proposition 2]. The homology class $\pi(p^h(x))$ corresponds to $u(1)$, and $|X^1|$ to $n\ell$ in the notation of [6]. $\square$

There is the following dual distance bound for the cohomology.

Theorem 22 (Panteleev–Kalachev [6])**.** *Assume that the coboundary map of the Tanner code $C(X, L)$*

$$C_1(X) \xleftarrow{\ \delta\ } C_0(X) \otimes L_0$$

is $(\alpha_{\mathrm{co}}, \beta_{\mathrm{co}})$-expanding. Let $x = (u, v)$ be a representative of a non-trivial cohomology class $[x] \in H^1(C(X, L) \otimes_{\mathbb{Z}_\ell} C(C_\ell))$.

1) *If the vertical part*

$$0 \neq p_v(x) \in H_v^1(C(X, L) \otimes_{\mathbb{Z}_\ell} C(C_\ell))$$

of x is non-trivial, then

$$|x| = |u| + |v| \geq |X^0| s \min \{\alpha_{\mathrm{co}}/2, \alpha_{\mathrm{co}}\beta_{\mathrm{co}}/4\}.$$

2) *Else, if $p_v(x) = 0$, then*

$$|x| = |u| + |v| \geq \ell \min \{\alpha_{\mathrm{co}}/(4s), \alpha_{\mathrm{co}}\beta_{\mathrm{co}}/(4s)\}.$$

To subsume, we obtain the following corollary.

Corollary 23. *The stabilizer/subsystem code of $C(X, L) \otimes_{\mathbb{Z}_\ell} C(C_\ell)$ defined by $H_1^{\mathcal{L}} = H_1^h(C(X, L) \otimes_{\mathbb{Z}_\ell} C(C_\ell))$, see Section IV-G, is an $[[N, K, D_X, D_Z]]$ code where*

$$N = 3|X^1|$$
$$K = \dim H_1(C(X/\mathbb{Z}_\ell, L)) \geq (2k_L/s - 1)|X^1|/\ell$$
$$D_Z \geq |X^1| \min \{\alpha_{\mathrm{ho}}/2, \alpha_{\mathrm{ho}}\beta_{\mathrm{ho}}/4\}$$
$$D_X \geq \min \{\alpha_{\mathrm{co}}|X^1|, \alpha_{\mathrm{co}}|X^1|/2, \ell\alpha_{\mathrm{co}}/(4s), \ell\alpha_{\mathrm{co}}\beta_{\mathrm{co}}/(4s)\}$$

in the notation of Theorem 21 and Theorem 22.

Proof. The number of physical qubits N is given by

$$\dim (C(X, L) \otimes_{\mathbb{Z}_\ell} C(C_\ell))_1 = |X^1| + s|X^0| = 3|X^1|.$$

The number of logical qubits encoded in the horizontal subsystem is the number of bits encoded in the Tanner code $C(X/\mathbb{Z}_\ell, L)$, see Theorem 20, which is bounded below by

$$k_{C(X/\mathbb{Z}_\ell, L)} \geq (2k_L/s - 1) |(X/\mathbb{Z}_\ell)^1|$$

via Equation (4). Now $\mathbb{Z}_\ell$ acts freely on X by assumption and hence $|(X/\mathbb{Z}_\ell)^1| = |X^1|/\ell$.

The bound for the homological distance D_Z follows from Case 1 of Theorem 21, since the homological distance of the subsystem code is the minimum distance of representatives of

homology classes which do not vanish when projected onto $H_1^{\mathcal{L}} = H_1^h(C(X, L) \otimes_{\mathbb{Z}_\ell} C(C_\ell))$.

The bound for D_X follows from combining Case 1 and 2 in Theorem 22. $\square$

V. EXPLICIT EXAMPLES

The goal of this section is to prove the following theorem.

Theorem 24. *There exists an explicit construction of a family of $[[N, K, D_X, D_Z]]$ LDPC quantum codes which encode $K \in \Theta(N^{\frac{2}{3}})$ logical qubits, with X-distance $D_X \in \Omega(N^{\frac{1}{3}})$ and Z-distance $D_Z \in \Theta(N)$.*

The distance balancing of [13] and [2] respects the splitting of the homology group described in Section IV-G. Applying the distance balancing procedure of [2] using classical $[N^{\frac{2}{3}}, \Theta(N^{\frac{2}{3}}), \Theta(N^{\frac{2}{3}})]$-codes we obtain the following corollary.

Corollary 25. *There exists an explicit construction of a family of $[[N, K, D]]$ LDPC quantum codes which encode $K \in \Theta(N^{\frac{4}{5}})$ logical qubits with distance $D \in \Omega(N^{\frac{3}{5}})$.*

1) Expander graphs X: The graphs X will be LPS-expanders defined in Section III-D. Choose primes p and q such that

$$\left(\frac{p}{q}\right) = -1$$

so that the graphs $X = X_{p,q}$ are Cayley graphs of the group $\mathrm{PGL}(2, q)$. Hence we have

$$|X^0| = |\mathrm{PGL}(2, q)| = q(q^2 - 1),$$

their degree is $s = p + 1$ and their second largest eigenvalues satisfy the bound $\lambda_2 \leq 2\sqrt{s-1}$.

2) Subgroups H: The subgroups H for the balanced product need to be cyclic subgroups which act freely on the graphs X. Furthermore, to obtain regular quotient graphs, we need to show that there is no edge connecting vertices g and gh for $h \in H$. Since all edges in X are of the form (g, sg) for $s \in S_{p,q}$ this is equivalent to the quotient condition (see Section IV-D)

$$S_{p,q} \cap gHg^{-1} = \emptyset \text{ for all } g \in \mathrm{PGL}(2, q). \quad (11)$$

The quotient condition implies that we act freely on the edges X^1.

We claim that these properties are fulfilled by the subgroup of unipotent upper-triangular matrices

$$H = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \mid x \in \mathbb{F}_q \right\} \subset \mathrm{PGL}(2, q).$$

First H is isomorphic to the additive group of $\mathbb{F}_q$ and hence a cyclic group of order q. Since X is a Cayley graph H acts freely on the vertices X^0.

To show that no element in H is conjugate to an element in $S_{p,q}$, see the quotient condition Equation (11), we argue via determinants. Note that the determinant of an element $g \in \mathrm{PGL}(2, q)$ is defined up to multiplication with a square, so $\det(g) \in \mathbb{F}_q^\times / (\mathbb{F}_q^\times)^2$. We have

$$\det(ghg^{-1}) = 1 \in \mathbb{F}_q^\times / (\mathbb{F}_q^\times)^2 \text{ and } \det(s) = p \in \mathbb{F}_q^\times / (\mathbb{F}_q^\times)^2$$

for all $h \in H$, $g \in \mathrm{PGL}(2,q)$ and $s \in S_{p,q}$. However, by assumption p is not a square modulo q and hence $1 \neq p$ in $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$.

3) Local codes L: In order for the Tanner code $C(X,L)$ to be a code with a linear number of encoded bits and linear distance we need it to satisfy the constraints given by Equation (4) and Equation (7), namely that it has to have rate $k_L/2 > 1/2$ and distance larger than the second eigenvalue of the graph $d_L > \lambda_2$. Furthermore, in order to be able to apply Theorem 13 we need that the dual code $L^\perp$ has distance larger than the second eigenvalue of the graph $d_L > \lambda_2$ as well.

Theorem 18 guarantees the existence of such a local code L with the lower bound $d_L, d_{L^\perp} \geq \delta s$ for some $\delta \in (0, 0.11)$. Although Theorem 18 does not give a construction of this code L, we can find it by brute force in $O(1)$ time with respect to the size of X.

Proof of Theorem 24. With the discussion above, choose $p = 401$, $\delta = 0.1$, $\alpha_{\mathrm{ho}} = 10^{-3}$, $\alpha_{\mathrm{co}} = 10^{-5}$. Then using Theorem 12 and Theorem 13 we get that β_{ho} and β_{co} are bounded below by positive constants. The family of codes are the horizontal subsystem balanced product codes. Using Corollary 23 and letting $q \to \infty$ we obtain a code family with the desired properties. We note that in our construction we essentially took Kronecker products of sparse matrices so that the resulting parity check matrices are sparse as well which in turn implies that the family is LDPC. $\qquad\square$

VI. Conclusion

We have demonstrated that balanced products of classical codes give rise to explicit families of LDPC quantum codes with exceptional asymptotic properties.

In this manuscript we focused on balanced products with cycle graphs. This prevents the number of logical qubits K and cohomological distance D_X from being linear. We conjecture that *good* LDPC quantum codes with linear number of logical qubits and distance can obtained by replacing cycle graphs by good classical codes.

Conjecture. *The horizontal subsystem codes associated to the balanced products $C(X_{p,q}, L) \otimes_{\mathrm{PGL}(2,q)} C(X_{p,q}, L)^*$ form a family of* good *LDPC quantum codes.*

We were able to show that these codes have constant encoding rate. We leave the question if they also attain linear distance as an open problem.

A further line of research is finding efficient decoding algorithms for our codes. There are a number of interesting and efficient decoding algorithms for expander codes. It seems reasonable that they can be adapted to our setting as done in [35].

Appendix A
Spectral Sequences

In general, the computation of the homology of a total complex $\mathrm{Tot}(E)$ can be quite subtle and subject of the powerful mathematical formalism of *spectral sequences*, which we want to very briefly explore. For a nice reference, see [36, Section III.7.3]. Simply stated, the formalism is an iterative

$$\begin{array}{ccc}
E_{p,q} & & E_{p-1,q} \\
{\scriptstyle \partial^v = \partial^0}\downarrow & & \downarrow{\scriptstyle \partial^v = \partial^0} \\
E_{p,q-1} & & E_{p-1,q-1}
\end{array}$$

Fig. 8. A part of the 0-th page of the spectral sequence $E_{p,q}^r \Rightarrow H^n(\mathrm{Tot}(E))$.

procedure to obtain better and better approximations of the homology of $\mathrm{Tot}(E)$. Precisely, the spectral sequence of the double complex E consists of so called *pages* of arrays of vector spaces $E_{p,q}^r$ labeled by a non-negative integer r, such that

$$\bigoplus_{p+q=n} E_{p,q}^r \text{ "converges to" } H_n(\mathrm{Tot}(E))$$

as $r \to \infty$ and one suggestively writes

$$E_{p,q}^r \Rightarrow H_n(\mathrm{Tot}(E)), \text{ for } p + q = n.$$

Furthermore, there is an iterative procedure to go from one page to the next. Namely, the r-th page of a spectral sequence is equipped with differentials

$$\partial_{r,p,q} : E_{p,q}^r \to E_{p-r,q+r-1}^r$$

such that the next page $E_{p,q}^{r+1}$ is obtained by taking homology along those differentials.

Spectral sequences can be very intricate. However, in many circumstances one can show that all differentials on a certain page r_0, where r_0 is hopefully very small, vanish. In this case, one says that the spectral sequence *degenerates on page r_0*. Then, all following pages will be the same and there are isomorphisms

$$\bigoplus_{p+q=n} E_{p,q}^r \cong H_n(\mathrm{Tot}(E))$$

for all $r \geq r_0$.

1) The First Pages: Let us briefly discuss the first three pages of the spectral sequence of the double complex E. The 0-th page of is simply given by E itself

$$E_{p,q}^0 = E_{p,q}.$$

Its differential

$$\partial_0 = \partial^v : E_{p,q}^0 = E_{p,q} \to E_{p,q-1} = E_{p,q-1}^0.$$

is the vertical differential of E. The first page is given by the homology of this differential

$$E_{p,q}^1 = H_q(E_{p,\bullet}, \partial^v).$$

Since ∂^v and ∂^h commute, the horizontal differential ∂^h induces maps

$$\begin{aligned}
\partial_1 = \partial^h : E_{p,q}^1 &= H_q(E_{p,\bullet}, \partial^v) \\
&\to E_{p-1,q}^1 = H_q(E_{p-1,\bullet}, \partial^v)
\end{aligned}$$

which constitute the differential on the first page. Iterating once more, the second page is obtained by taking homology along this differential

$$E_{p,q}^2 = H_p(H_q(E_{\bullet,\bullet}, \partial^v), \partial^h).$$

$$H_q(E_{p,\bullet}, \partial^v) \xrightarrow{\ \partial^h\ } H_q(E_{p-1,\bullet}, \partial^v)$$

$$H_{q-1}(E_{p,\bullet}, \partial^v) \xrightarrow[\partial^h_{p,q-1}]{} H_{q-1}(E_{p-1,\bullet}, \partial^v)$$

Fig. 9. A part of the first page of the spectral sequence $E^r_{p,q} \Rightarrow H^n(\mathrm{Tot}(E))$.

In other words, the second page is obtained by first taking vertical and then horizontal homology of the double complex. It is already quite involved to write down the differential on the second page.

APPENDIX B
HYPERBOLIC SURFACES AND THEIR SYMMETRIES

1) Hyperbolic geometry: The geometry of space with constant negative curvature is called hyperbolic. This geometry can be realized in different models consisting of a set of points and a hyperbolic distance function. We will consider the *Poincaré disc model* in which the set of points is given by the interior of a disc of unit radius

$$\mathbb{H}^2 = \{z \in \mathbb{C} \mid \|z\| < 1\}.$$

and the distance between two points $x, y \in \mathbb{H}^2_d$ is given by

$$\mathrm{dist}(x, y) = \cosh^{-1}\left(1 + \frac{2\|x-y\|^2}{(1-\|x\|^2)(1-\|y\|^2)}\right).$$

Lengths are highly distorted but the angles in which lines intersect are faithfully represented. Shortest lines (geodesics) connecting two points are given by circular arcs which intersect the unit circle in right angles.

A fact of hyperbolic trigonometry which we will use later is the following: Consider a triangle in $\mathbb{H}^2$ with internal angles α, β, γ. It must hold that

$$\alpha + \beta + \gamma < \pi. \tag{12}$$

A proof of this fact and more background on hyperbolic geometry can be found in [37].

2) Isometry group: Bijective maps $\iota : \mathbb{H}^2 \to \mathbb{H}^2$ which leave the distance between any two points invariant, i.e.

$$\mathrm{dist}(\iota(x), \iota(y)) = \mathrm{dist}(x, y) \tag{13}$$

for all $x, y \in \mathbb{H}^2$, are called *hyperbolic isometries*. Just as for the euclidean plane $\mathbb{E}^2$, they can be reflections, rotations, translations or combinations thereof. The set of all isometries forms a group under composition called the isometry group $\mathrm{Isom}(\mathbb{H}^2)$.

Note that any translation (in hyperbolic or euclidean space) can be written in terms of two reflections along suitably chosen parallel lines. The same holds for rotations where the two lines intersect at the fixed-point of the rotation. In fact $\mathrm{Isom}(\mathbb{E}^2)$ and $\mathrm{Isom}(\mathbb{H}^2)$ are both generated by reflections. We call an isometry *orientation-preserving* if it consists of an even number of reflections. Orientation-preserving isometries form a subgroup of index 2 which we denote $\mathrm{Isom}^+(\mathbb{H}^2)$.

In the Poincaré model isometries can be realized in terms of a matrix group.[9] We define the action of matrices on $\mathbb{H}^2$ via fractional linear transformations

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z = \frac{az+b}{cz+d}. \tag{14}$$

These transformations are also called *Möbius tranformations*. By enforcing Equation (13) we see that real 2×2-matrices with determinant $+1$ leave the distance function dist_h invariant. They therefore describe isometries of $\mathbb{H}^2$. Furthermore, it is easy to see that multiplying a matrix with -1 defines the same isometry.

Let $\mathrm{SL}(2, \mathbb{R})$ be the group of real 2×2-matrices with determinant $+1$, called the *special linear group*. As the overall sign does not affect the transformation in Equation (14) we consider the *projective special linear group* $\mathrm{PSL}(2, \mathbb{R}) = \mathrm{SL}(2, \mathbb{R})/\{\pm 1\}$. A classic result of hyperbolic geometry is that the fractional linear transformations of $\mathrm{PSL}(2, \mathbb{R})$ are in fact exactly the orientation preserving isometries, i.e. we have

$$\mathrm{Isom}^+(\mathbb{H}^2) \simeq \mathrm{PSL}(2, \mathbb{R}).$$

Finally, we note that a subgroup H of $\mathrm{Isom}^+(\mathbb{H}^2)$ operates fixed-point free if and only if H is torsion-free, i.e. if it contains no elements of finite order.

3) Hyperbolic tessellations: Just as we can tessellate the euclidean plane $\mathbb{E}^2$ with polygonal shapes, we can tessellate the hyperbolic plane $\mathbb{H}^2$ with polygons as well. A particular class of tessellations are *regular tessellations* which are edge-to-edge coverings by copies of a regular polygon with the same number of polygons meeting at a vertex. We will call the polygons of the tessellation *faces*. Regular tessellations are completely determined by the number of edges of each face r (r-gons) and the number of faces incident to each vertex s. This information is summarized in the *Schläfli symbol* $\{r, s\}$. Not every pair of numbers r and s is a valid tessellation due to geometric constraints. This can be seen as follows: subdivide a face into $2r$ triangles by cutting along all lines of symmetry. Each triangle has internal angles $\pi/2$, π/r and π/s. In $\mathbb{E}^2$ the sum of these angles has to be π, so that the only possible regular tessellations of $\mathbb{E}^2$ are tessellations by squares $\{4, 4\}$, hexagons $\{6, 3\}$ and triangles $\{3, 6\}$. In the hyperbolic plane the restriction due to Equation (12) allows for an infinite number of regular tessellations, namely all $\{r, s\}$ such that

$$\frac{1}{r} + \frac{1}{s} < \frac{1}{2}. \tag{15}$$

4) Symmetries of regular tessellations: Regular tessellations are highly symmetric. The group of symmetries of a regular tessellation is generated by reflections along lines of symmetry. These lines of symmetry subdivide the tessellation into identical triangles with internal angles $\pi/2$, π/r and π/s. The symmetry group acts freely and transitively on the triangles, meaning that no triangle is stabilized by the group action and every triangle can be mapped onto any other. By fixing one arbitrary triangle and assigning it the identity element of

---

[9]It is more common to use the so-called upper-half plane model to define these isometries. However, the half-plane model is equivalent to the Poincaré disc model via the Cayley transformation.
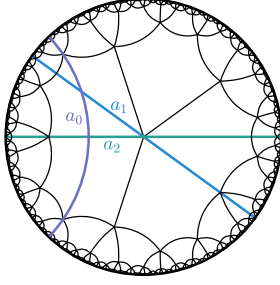
Fig. 10. Picture of a regular $\{5, 5\}$ tessellation in in the Poincaré disc model. All line segments are geodesics with respect to the hyperbolic geometry.

the group, we have a one-to-one correspondence between the triangles and the group elements. Each triangle is uniquely determined by a triple consisting of a vertex, an edge and a face of the tessellation (all adjacent to one another). Such triples are also known as *flags*. Two triangles are adjacent if and only if their corresponding flags differ in exactly one of their entries.

All symmetries of the tessellation must preserve the distance which makes them isometries. Let $G_{r,s}$ denote the symmetry group of a hyperbolic tessellation with Schläfli symbol $\{r, s\}$, then we have that $G_{r,s} \leq \mathrm{Isom}(\mathbb{H}^2)$.

The symmetry group of a regular tessellation $\{r, s\}$ can be defined as a finitely presented group in terms of the generators and their relations. There are three generators: a_0, a_1 and a_2, each a reflection on one of the sides of a triangle. The generator a_0 reflects on the side of the triangle opposed to the vertex of the tessellation, a_1 reflects on the side of the triangle opposed to the edge of the tessellation and a_2 reflects on the side of the triangle opposed to the middle of the face of the tessellation.

We can define $G_{r,s}$ as a finitely presented group in terms of its generators and the relations they obey. As the generators are reflections we must have that a_i^2 is equal to the neutral element of the group. Furthermore, the product of two generators forms a rotation. For example, $a_0 a_1$ is a rotation around the center of a face which has order r. Similarly, $a_1 a_2$ and $a_0 a_2$ are rotations around a vertex and an edge so that their orders are s and 2, respectively. These are in fact all relations so that the symmetry group of a $\{r, s\}$ tessellation is

$$G_{r,s} = \left\langle a_0, a_1, a_2 \mid a_0^2, a_1^2, a_2^2, (a_0 \, a_1)^r, (a_1 a_2)^s, (a_0 a_2)^2 \right\rangle.$$

There exists a index 2 subgroup in $G_{r,s}$ which is generated by the rotations $\rho = a_0 a_1$ and $\sigma = a_1 a_2$. The group is the subgroup of orientation preserving symmetries and denoted

$$G_{r,s}^+ = \left\langle \rho, \sigma \mid \rho^r, \sigma^s, (\rho\sigma)^2 \right\rangle.$$

The groups $G_{r,s}^+$ are a special case of Fuchsian triangle groups, which are also denoted $\Delta(2, r, s)$ in the literature. Note that from the discussion in Section B-2 it follows that

$$G_{r,s}^+ \leq \mathrm{Isom}^+(\mathbb{H}^2) \simeq \mathrm{PSL}(2, \mathbb{R}). \qquad (16)$$

5) Compact hyperbolic surfaces: We can use the identification between the fundamental triangles and the group elements to obtain tessellations of closed surfaces. The idea is

to consider finite quotients of the infinite group, which leave the local structure of the group invariant. Geometrically, the procedure essentially consists of finding translations and identifying points which differ by these translations. For example, on the 2D euclidean plane we can take an arbitrary translation and by identifying all points differing by this translation we obtain a cylinder of infinite length. Taking a second translation, which is not co-linear with the first one, we obtain a torus.

In euclidean space all translation commute, but this is not true any longer in curved spaces, in particular in $\mathbb{H}^2$. Therefore we have to find a set of translations which, as a whole, commutes with all other elements of the symmetry group $G_{r,s}$. In the language of group theory; we are looking for a normal subgroup N of $G_{r,s}$ which operates without fixed-points on $\mathbb{H}^2$. In the simplest case we consider a single translation τ and take the normal closure of the group generated by τ with respect to either $G_{r,s}$ or $G_{r,s}^+$ depending on whether we want to restrict ourselves to orientation preserving isometries:

$$N_\tau^{(+)} = \langle \tau \rangle^{G_{r,s}^{(+)}} = \{ g^{-1} t g \mid g \in G_{r,s}^{(+)}, \, t \in \langle \tau \rangle \} \qquad (17)$$

If N_τ has finite index in $G_{r,s}^{(+)}$ then $\mathbb{H}^2 / N_\tau^{(+)}$ is a closed surface with finite area.

Such surfaces give rise to quantum codes with a linear encoding rate [38].

References

[1] M. H. Freedman, D. A. Meyer, and F. Luo, "$\mathbb{Z}_2$-Systolic Freedom and Quantum Codes," *Mathematics of quantum computation, Chapman & Hall/CRC*, pp. 287–320, 2002.

[2] S. Evra, T. Kaufman, and G. Zémor, "Decodable quantum ldpc codes beyond the $\sqrt{n}$ distance barrier using high dimensional expanders," 2020.

[3] T. Kaufman and R. J. Tessler, "New cosystolic expanders from tensors imply explicit quantum ldpc codes with $\omega(\sqrt{n} \log^k n)$ distance," 2020.

[4] M. B. Hastings, J. Haah, and R. O'Donnell, "Fiber bundle codes," *arXiv preprint arXiv:2009.03921*, 2020.

[5] P. Panteleev and G. Kalachev, "Degenerate quantum ldpc codes with good finite length performance," *arXiv preprint arXiv:1904.02703*, 2019.

[6] ——, "Quantum ldpc codes with almost linear minimum distance," 2020.

[7] D. Bacon, S. T. Flammia, A. W. Harrow, and J. Shi, "Sparse quantum codes from quantum circuits," *IEEE Transactions on Information Theory*, vol. 63, no. 4, pp. 2464–2479, 2017.

[8] N. P. Breuckmann and B. M. Terhal, "Space-time circuit-to-hamiltonian construction and its applications," *Journal of Physics A: Mathematical and Theoretical*, vol. 47, no. 19, p. 195304, 2014.

[9] T. C. Bohdanowicz, E. Crosson, C. Nirkhe, and H. Yuen, "Good approximate quantum LDPC codes from spacetime circuit hamiltonians," in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, 2019, pp. 481–490.

[10] I. M. James, *General topology and homotopy theory*. Springer Science & Business Media, 2012.

[11] A. Lubotzky, R. Phillips, and P. Sarnak, "Ramanujan graphs," *Combinatorica*, vol. 8, no. 3, pp. 261–277, 1988.

[12] N. P. Breuckmann and V. Londe, "Single-shot decoding of linear rate ldpc quantum codes with high performance," *arXiv preprint arXiv:2001.03568*, 2020.

[13] M. B. Hastings, "Weight reduction for quantum codes," *arXiv preprint arXiv:1611.03790*, 2016.

[14] S. Bravyi, B. M. Terhal, and B. Leemhuis, "Majorana fermion codes," *New Journal of Physics*, vol. 12, no. 8, p. 083039, 2010.

[15] N. P. Breuckmann, "Homological quantum codes beyond the toric code," Ph.D. dissertation, RWTH Aachen University, 2017.

[16] B. M. Terhal, "Quantum error correction for quantum memories," *Reviews of Modern Physics*, vol. 87, no. 2, p. 307, 2015.

[17] 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*, vol. 60, no. 2, pp. 1193–1202, 2013.

[18] W. Zeng and L. P. Pryadko, "Higher-dimensional quantum hypergraph-product codes with finite rates," *Physical review letters*, vol. 122, no. 23, p. 230501, 2019.

[19] M. Sipser and D. A. Spielman, "Expander Codes," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 1710–1722, 1996.

[20] R. Tanner, "A recursive approach to low complexity codes," *IEEE Transactions on Information Theory*, vol. 27, no. 5, pp. 533–547, 1981.

[21] R. Meshulam, "Graph codes and local systems," *arXiv preprint arXiv:1803.05643*, 2018.

[22] J. Friedman, "Relative expanders or weakly relatively ramanujan graphs," *Duke Mathematical Journal*, vol. 118, no. 1, pp. 19–35, 2003.

[23] N. Alon and F. R. Chung, "Explicit construction of linear sized tolerant networks," *Discrete Mathematics*, vol. 72, no. 1-3, pp. 15–19, 1988.

[24] G. Davidoff, P. Sarnak, and A. Valette, *Elementary number theory, group theory and Ramanujan graphs*. Cambridge University Press, 2003, vol. 55.

[25] M. Conder, A. Lubotzky, J. Schillewaert, and F. Thilmany, "Constructing highly regular expanders from hyperbolic coxeter groups," *arXiv preprint arXiv:2009.08548*, 2020.

[26] A. Salehi Golsefidy, "Super-approximation, I: p-adic semisimple case," *International Mathematics Research Notices*, vol. 2017, no. 23, pp. 7190–7263, 2017.

[27] L. Guth and A. Lubotzky, "Quantum error correcting codes and 4-dimensional arithmetic hyperbolic manifolds," *Journal of Mathematical Physics*, vol. 55, no. 8, p. 082202, 2014.

[28] W. Magnus, *Noneuclidean tesselations and their groups*. Academic Press, 1974.

[29] U. Langer and G. Rosenberger, "Erzeugende endlicher projektiver linearer Gruppen," *Results in Mathematics*, vol. 15, no. 1-2, pp. 119–148, 1989.

[30] C. J. Moreno and O. Moreno, "Exponential sums and goppa codes. i," *Proceedings of the American Mathematical Society*, vol. 111, no. 2, pp. 523–531, 1991.

[31] T. Kaufman and A. Wigderson, "Symmetric ldpc codes and local testing," in *Property testing*. Springer, 2010, pp. 312–319.

[32] T. Kaufman and A. Lubotzky, "Edge transitive ramanujan graphs and highly symmetric ldpc good codes," 2011.

[33] J. Van Lint and G. Van der Geer, *Introduction to coding theory and algebraic geometry*. Birkhäuser, 2012, vol. 12.

[34] J. H. van Lint, "Repeated-root cyclic codes," *IEEE Transactions on Information Theory*, vol. 37, no. 2, pp. 343–345, 1991.

[35] O. Fawzi, A. Grospellier, and A. Leverrier, "Constant overhead quantum fault-tolerance with quantum expander codes," in *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 2018, pp. 743–754.

[36] S. I. Gelfand and Y. I. Manin, *Methods of Homological Algebra*, ser. Springer Monographs in Mathematics. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003. [Online]. Available: http://link.springer.com/10.1007/978-3-662-12492-5

[37] J. G. Ratcliffe, S. Axler, and K. Ribet, *Foundations of Hyperbolic Manifolds*. Springer, 2006, vol. 149.

[38] N. P. Breuckmann and B. M. Terhal, "Constructions and noise threshold of hyperbolic surface codes," *IEEE transactions on Information Theory*, vol. 62, no. 6, pp. 3731–3744, 2016.

Jens N. Eberhardt is a postdoctoral fellow at the University of Bonn. He is interested in geometric representation theory and its applications. He obtained his PhD at the University of Freiburg working with Prof. Wolfgang Soergel. His previous stations include RWTH Aachen University, UCLA and the Max Planck Institute for Mathematics in Bonn.

Nikolas P. Breuckmann holds a UCLQ Research Fellowship at University College London. He is interested in quantum information and related fields. He obtained his PhD at RWTH Aachen University working with Prof. Barbara Terhal on quantum fault-tolerance and quantum complexity theory. He has worked in industry at PsiQuantum, a Bay Area based start-up building a silicon-photonics based quantum computer.