Quantum Codes from High-Dimensional Manifolds

Matthew B. Hastings

Station Q, Microsoft Research, Santa Barbara and Quantum Architectures and Computation Group, Microsoft Research, Redmond, USA
`mahastin@microsoft.com`

── **Abstract** ──────────────

We construct toric codes on various high-dimensional manifolds. Assuming a conjecture in geometry we find families of quantum CSS stabilizer codes on N qubits with logarithmic weight stabilizers and distance $N^{1-\epsilon}$ for any $\epsilon > 0$. The conjecture is that there is a constant $C > 0$ such that for any n-dimensional torus $\mathbb{T}^n = \mathbb{R}^n/\Lambda$, where Λ is a lattice, the least volume unoriented $n/2$-dimensional cycle (using the Euclidean metric) representing nontrivial homology has volume at least C^n times the volume of the least volume $n/2$-dimensional hyperplane representing nontrivial homology; in fact, it would suffice to have this result for Λ an integral lattice with the cycle restricted to faces of a cubulation by unit hypercubes. The main technical result is an estimate of Rankin invariants[24] for certain random lattices, showing that in a certain sense they are optimal. Additionally, we construct codes with square-root distance, logarithmic weight stabilizers, and inverse polylogarithmic soundness factor (considered as quantum locally testable codes[1]). We also provide an short, alternative proof that the shortest vector in the exterior power of a lattice may be non-split[8].

1998 ACM Subject Classification E.4 Coding and Information Theory

Keywords and phrases quantum codes, random lattices, Rankin invariants

Digital Object Identifier 10.4230/LIPIcs.ITCS.2017.25

1 Introduction

Quantum CSS stabilizer codes[6] can be understood in terms of homology[18, 13, 4], and different manifolds provide a rich source of different codes. The two-dimensional toric code[18, 13] and four-dimensional toric code[9] are commonly considered examples; they are code families based on families of cellulations of a two and four dimensional tori. Other manifolds[14] provide other interesting properties, such as greater distance, discussed below. In this paper, we consider families of codes based on high dimensional manifolds.

We begin by considering some parameters that quantify a CSS code. The elementary degrees of freedom of a CSS codes are qubits (or, more generally, qudits, for some $d \geq 2$). Let there be N such qudits so that the Hilbert space has dimension d^N. CSS codes can be parametrized by several parameters, which we write as $[[N, K, D, W]]$. Here N is the number of qudits. K is the number of encoded qudits, so that the code has a code space which is a subspace of dimension d^K. D is the "distance" of the code, defined below, while W is the "weight" of the stabilizers, defined also below. Generally speaking, larger K and D is desirable, while smaller W is also desirable (this discussion of desirability of certain values of the parameters ignores other questions like the ability to efficiently decode or encode states, which is a completely separate discussion that we do not consider in this paper).

The best families of quantum codes obtained thus far have significantly worse scaling than the corresponding scaling for classical linear codes. Families of classical codes exist with $K = \Theta(N), D = \Theta(N), W = \mathcal{O}(1)$ (so-called low density parity check codes provide

such an example[15, 20]). If we set $W = \mathcal{O}(1)$, then the largest known distance for a quantum code family is $\Theta(\sqrt{N \log(N)})$ as in Ref. [14], while if we want $D = \Theta(N)$, then the lowest known weight is $W = \Theta(\sqrt{N})$ as in Ref. [5]. These parameters refer to stabilizer codes; if one allows subsystem codes[23], then it is possible to achieve $D = \Theta(N^{1-\epsilon}), W = \mathcal{O}(1)$ for $\epsilon = \mathcal{O}(1/\sqrt{\log(N)})$ as in Ref. [3], but now the parameter W does not refer to the weight of a set of commuting stabilizers but rather the to weight of a set of generators of the "gauge group" and these generators need not commute with each other. If one requires that the stabilizer group be generated by local commuting operators, then currently no advantage is known for a subsystem code. Another notable stabilizer code family achieves $K = \Theta(N), D = \Theta(\sqrt{N}), W = \mathcal{O}(1)$ and has efficient an efficient local decoding algorithm[26].

In this paper, we construct code families that, assuming a conjecture in geometry, have almost linear distance and logarithmic weight generators. We review various concepts before giving an overview of the paper.

1.1   Review of CSS Codes and Relation to Homology

The code subspace is the subspace of the d^N-dimensional Hilbert space which is in the $+1$ eigenspace of several "stabilizers". These stabilizers are of two types, called "X-type" and "Z-type". The Z operator on the d-dimensional Hilbert space of a single qudit is the operator

$$
Z = \begin{pmatrix} 1 & & & \\ & \exp(\frac{2\pi i}{d}) & & \\ & & \exp(\frac{4\pi i}{d}) & \\ & & & \ldots \end{pmatrix},
\tag{1}
$$

while the X operator is the operator

$$
X = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & 1 & \\ & & & \ldots & \\ 1 & 0\ldots & & & \end{pmatrix}.
\tag{2}
$$

We write Z_i or X_i to indicate the operator Z or X acting on qudit i, tensored with the identity on all other qudits. Then, a Z-type stabilizer is the tensor product of Z operators on some qubits, possibly raised to integer powers. Such a Z-type stabilizer might be written, for example, $Z_1 Z_3^2$ to indicate that it is the tensor product of Z on qubit 1 with the square of Z on qubit 3. These exponents all can be taken in the range $1, 2, ..., d-1$; if an operator on a given qubit is raised to power 0, we simply do not write it when writing the Z stabilzer. The X-type stabilizers are similar, with Z replaced by X.

We encode the Z-type stabilizers in a matrix that we denote ∂_2. This matrix has N rows and has one column per Z-type stabilizer. The entries of the matrix are over the field $\mathbb{F}_d$. The entry in the i-th row and j-th column indicates which power of Z_i appears in the j-th stabilizer; thus, for example, for the stabilizer $Z_1 Z_3^2$, the first row in the corresponding column would have a 1 and the third row would have a 2 and all other rows would be zero. We encode the X-type stabilizers also in a matrix, denoted by ∂_1. This matrix has N columns and one row per X-type stabilizer, again with the entries over the field $\mathbb{F}_d$. The entry in the i-th row and j-th column indicates which power of X_j appears in the i-th stabilizer

A final requirement on CSS codes is that the stabilizers commute with each other. Any pair of Z-type stabilizers trivially commute, as do any pair of X-type stabilizers. The re-

quirement that the Z-type stabilizer commute with the X-type stabilizers can be simply expressed in terms of ∂_2, ∂_1 as

$$\partial_1 \partial_2 = 0. \tag{3}$$

This requirement is equivalent to saying that there is a chain complex

$$\mathcal{C}_2 \xrightarrow{\partial_2} \mathcal{C}_1 \xrightarrow{\partial_1} \mathcal{C}_0,$$

where $\mathcal{C}_2, \mathcal{C}_1, \mathcal{C}_0$ are vector spaces over $\mathbb{F}_d$, with basis elements in one-to-one correspondence with Z-type stabilizers, qudits, and X-type stabilizers, respectively. We have $\dim(C_1) = N$.

The number of encoded qudits K is given by the first Betti number, which is equal to $N - \dim(\mathcal{C}_2) - \dim(\mathcal{C}_0)$ assuming that all stabilizers are independent of each other (i.e., that the columns of ∂_2 are linearly independent, as are the rows of ∂_1).

The distance D is defined as follows. Let us say that an operator O is a Z-type logical operator if it is a tensor product of Z operators on qudits which commutes with all X-type stabilizers and which is not itself a product of Z-type stabilizers. In the language of homology, such an operator is a representative of a nontrivial first homology class; write

$$O = \prod_i Z_i^{a_i},$$

where the product ranges over all qudits and a_i are in $\mathbb{F}_d$. Define an N-component vector v with entries a_i, so that the requirement that O commutes with all X-type stabilizers is that $\partial_1 v = 0$, while the requirement that O not be a product of Z-type stabilizers is that v is not in the image of ∂_2. An X-type logical operator is defined similarly, with Z and X integerchanged everywhere in the definition. The weight of a Z-type (or X-type) logical operator O is defined to be the number of qudits i such that Z_i (or X_i)appears in O raised to a nonvanishing power mod d; we say that that Z_i or X_i is in the support of the logical operator. We define D_Z to be the minimum weight of a Z-type logical operator and D_X to be the minimum weight of an X-type logical operator and define the distance D by

$$D = \min(D_X, D_Z). \tag{4}$$

We define the weight W of a code to be the least integer W such that every row and every column of ∂_2 has at most W nonvanishing entries and also every row and every column of ∂_1 has at most W nonvanishing entries. Note that this means that not only does every stabilizer act on at most W different qudits, also every qudit is acted on by at most W different Z-type stabilizers and W different X-type stabilizers.

We define the weight of an operator which is a product of Z and X operators to be the number of qudits on which the operator acts nontrivially; for example, the operator $X_1 X_3$ has weight 2. Thus, every stabilizer has weight at most W.

A vector v in a vector space $\mathcal{C}_k$ is called a k-chain (or simply, a "chain"). If $\partial_k v = 0$, then v is called a k-cycle. The weight of a vector is defined to be the number of nonzero entries in the vector.

1.2 CSS Codes from Manifolds and Systolic Freedom

Conversely, just as one can define a chain complex from a CSS code, one can use a chain complex to define a CSS code. Given any chain complex over some field $\mathbb{F}_d$, one can define a qudit CSS code: choose any vector space in the chain complex to correspond to the qudits,

and then the vector spaces of one higher and one lower dimension correspond to the Z-type and X-type stabilizers. For example, given a triangulation (or cubulation or other discretization) of a four dimensional manifold one can define a chain complex

$$\mathcal{C}_4 \overset{\partial_4}{\to} \mathcal{C}_3 \overset{\partial_3}{\to} \mathcal{C}_2 \overset{\partial_2}{\to} \mathcal{C}_1 \overset{\partial_1}{\to} \mathcal{C}_0,$$

where the basis elements of $\mathcal{C}_k$ correspond to k-cells. Then, one can choose any integer q and let the qudits correspond to the q-cells and the Z-type stabilizers correspond to $(q+1)$-cells and the X-type stabilizers correspond to $(q-1)$-cells. The case $q = 2$ is the familiar four-dimensional toric code of Ref. [9], while the cases $q = 0, 4$ are classical repetition codes (Ising models) in the Z or X basis, respectively.

Defining CSS codes from manifolds has several nice advantages. For one, often the distance of the code can be translated into geometric properties of the manifold and (up to some technical details that we discuss below) it can be geometrically interpreted as the least possible volume of a q-dimensional cycle in a nontrivial homology class. Similarly, if the triangulation has a bounded local geometry, then this gives a bound on W.

Naively, it might seem that such constructions will not be able to obtain a better-than-square-root distance, i.e. $D = \Omega(\sqrt{N})$. We now give some intution for this naive belief, and give a more detailed discussion of the relation between volume and number of qudits in one particular example, as it will be useful later. Consider an n-dimensional torus constructed from a hypercube of length ℓ on each side for some integer ℓ by gluing the opposite faces together. Introduce coordinates $(x_1, \ldots, x_n)$. Discretize the torus by hypercubes of unit length in the obvious way, so that the 0-cells are at integer values of the coordinates. In this case, the volume of the torus equals the number of hypercubes in the discretization, which equals ℓ^n. The number of qudits is given by

$$N = \ell^n \binom{n}{q},$$

while

$$D_Z = \ell^q, \quad D_X = \ell^{n-q}.$$

To see that $D_Z \leq \ell^q$, one can pick any q-dimensional plane where q of the coordinates assume arbitrary values and the other coordinates are held fixed at integer values; then, the product of Z over the q-cells in this plane give a logical operator. We omit the proof that this upper bound for D is tight in this case. The value of D_X is given by picking any $(n-q)$-dimensional plane on the dual lattice and then taking the product of X over the the q-cells that intersects this plane also gives a logical operator.

Choosing the optimal value, $q = n/2$ still leads only to $D = \Theta(\sqrt{N})$. Varying the geometry of the torus by changing the aspect ratio (i.e., keeping the sides of the torus orthogonal to each other but changing the relative lengths) does not lead to any improvement.

However, this naive belief is false. "Systolic freedom" is the term for a concept due to Gromov[2], that one may have manifolds for which the product of the q-systole (the least volume cycle representing a nontrivial element of q-th homology) times the $(n-q)$-systole may be arbitrarily larger than the volume of the manifold. This phenomenon was originally observed for integer homology (corresponding to qudit quantum codes with large d), while only later in Ref. [14] was it constructed for $\mathbb{Z}_2$ homology.

1.3   Overview of Paper

In the original construction of systolic freedom[2], the topology of the manifold was held fixed and the metric was varied to obtain a diverging ratio between the product of the q-

systole and the $(n-q)$-systole to the volume of the manifold (for some given pairs $q, n-q$), while in the $\mathbb{Z}_2$ case[14], the topology of the manifold was varied to obtain a diverging ratio. In this paper, we consider instead a family of manifolds with different dimension. Most of the paper is devoted to considering tori $\mathbb{R}^n/\Lambda$ for certain random lattices Λ. In section 2 we make various definitions of the random lattices and define Rankin invariants. In section 3 we give an overview of the construction and present a geometric conjecture 1 and state theorem 5 that, assuming the conjecture, there exist quantum CSS codes with logarithmic weight and almost linear distance. In section 4 we prove lower bounds on the Rankin invariant of certain random lattices, which is the main step in proving theorem 5. In section 5 we discuss some obstacles to proving even a weaker form of conjecture 1 (involving cycles with integer coefficients) and we consider shortest vectors in the exterior product of a lattice. Finally, in section 6 we give some alternative constructions which have only square-root distance but which have inverse polylogarithmic soundness parameters as quantum locally testable codes[1].

To give some motivation to our lattice construction, consider the two-dimensional toric code. On a square lattice with length ℓ on each side, there are $2\ell^2$ qubits and the distance ℓ. Suppose we ignore the details of the cellulation and take an arbitrary torus $\mathbb{R}^2/\Lambda$, pretending that the number of qubits is equal to the area (ℓ^2) and the distance is equal to the shortest vector in the lattice Λ. Then, a slightly better geometry than the square lattice would be to take the hexagonal lattice, as the ratio of the square of the length of the shortest vector to the area of the torus is equal to $2/\sqrt{3}$ rather than 1. This is only a slight constant improvement over the square lattice. However, in higher dimensions, the shortest vector in lattice Λ can be roughly $\sqrt{n}$ longer than the $1/n$ power of the volume of the torus $\mathbb{R}^n/\Lambda$. Further, if we consider least volume cycles representing nontrivial homology for $q > 1$, then larger improvements are possible (at least for cycles which are hyperplanes). This motivates our construction and the consideration of so-called "Rankin invariants"[24].

In this paper, we will consider codes based on cellulations of such tori (in higher dimensions) where the sides of the torus are not orthogonal. These tori will be $\mathbb{R}^n/L$ for some lattice L, where the lattice does not have a basis of orthogonal vectors. However, L will be an integral lattice, so that it is still possible to cellulate $\mathbb{R}^n/L$ by unit hypercubes. This is done by taking the obvious cellulation of $\mathbb{R}^n$ by unit hypercubes (i.e., every unit hypercube whose vertices are at integer points is a cell in the cellulation) and then identifying cells that differ by translation by a lattice vector. Fig. 1 gives a simple example in the case $n = 2$.

2 Random Lattices and Definitions

Consider a so-called LDA lattice[7, 10] as follows. We pick a prime p. We will construct a lattice which is a subset of $\mathbb{Z}^n$ for some even n. We first construct a linear code over field $\mathbb{F}_p^n$. We define this code by a "code generator matrix" G which is an n-by-k matrix such that the *column* vectors are a basis for the codewords. (We explicitly call it a "code generator matrix" rather than just a "generator matrix", as we will also consider lattice generator matrices later.) Usually in coding theory, it is instead conventional to let the *rows* of a code generator matrix be the basis for a code, but to maintain consistency with notation we use later, we instead use the *columns* as the basis. We choose the entries of G independently and uniformly from $\mathbb{F}_p$.

We will be interested in taking n large at fixed ratio $k/n < 1$. With high probability (i.e., with probability tending to 1 as $n \to \infty$ with k/n fixed), G is non-degenerate (see next paragraph). Assuming that G is indeed non-degenerate, one can find a permutation of the
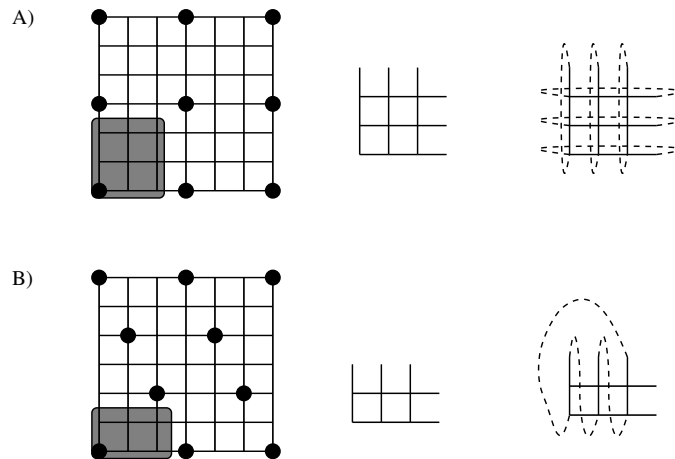
■ **Figure 1** Leftmost part of A) shows part of a cellulation of $\mathbb{R}^2$ by unit squares, as well as showing a lattice L with basis vectors $(3,0)$ and $(0,3)$. Solid circles represent points of L. The shaded region contains a maximal set of points in $\mathbb{Z}^2$ which do not differ by translation by L. Middle part of A) shows 0-cells of the shaded region, as well as 1- and 2-cells attached to them. Rightmost part of A) shows how the 1-cells in the middle part are attached: the dashed lines indicate that the top of a given 1-cell on the top of the figure is attached to a 0-cell at the bottom. Similarly for attaching cells on the right to those on the left. Figure B) is similar, but now L has basis vectors $(3,0)$ and $(2,2)$. Now the dashed lines indicate that a 1-cell on the top of the figure is attached to a 0-cell on the bottom, but that 0-cell is translated horizontally (horizontal dashed lines are not shown in B; they are the same as in A). For both A,B, the code has distance 3, but B has smaller volume.

rows such that G is in the form

$$G = \begin{pmatrix} A \\ B \end{pmatrix}$$

where A, B are k-by-k and $(n-k)$-by-k matrices with A non-degenerate. Then, since A is non-degenerate there exists a sequence of elementary column operations that brings A to the identity matrix, where for a matrix over $\mathbb{F}_p^n$ an elementary column operation is one of: adding one column to another, multiplying a column by any nonzero element of the field, or interchanging two columns. These column operations bring G to the form

$$G = \begin{pmatrix} I \\ C \end{pmatrix},$$

where I is the k-by-k identity matrix and C is some $(n-k)$-by-k matrix. Since the entries of C are obtained by applying these column operations to the entries of B, the entries of C are chosen independently of each other and uniformly from $\mathbb{F}_p$, i.e., applying any elementary column operation to an ensemble of matrices with entries chosen uniformly and independently leaves this ensemble invariant. This is the form of G that we work with in the rest of this section.

▶ **Definition 1.** Let the lattice L_0 be the set of points $x_1, ..., x_n$ in $\mathbb{Z}^n$ such that the vector $(x_1 \mod p, ..., x_n \mod p)$ is in the linear code defined by G.

We now show that with high probability, G is non-degenerate. With probability $1 - (1/p)^n$, the first column of G has a nonzero entry. By elementary column operations, adding a multiple of the first column to other columns, we can set all other columns equal to zero

in the first row for which the first column has a nonzero entry. Then, with probability $1 - (1/p)^{n-1}$, the second column has a nonzero entry in some other row. Add a multiple of the second column to the third, fourth,... column to set them equal to zero in the first row for which the second column has a nonzero entry. Continuing in this fashion, the probability that G is non-degenerate is $(1 - (1/p)^n)(1 - (1/p)^{n-1}) \ldots (1 - (1/p)^{n-k+1})$ which indeed is $1 - o(1)$.

The lattice L_0 is the set of integer linear combinations of the columns of G (interpreted as vectors of integers, rather than as vectors of elements of $\mathbb{F}_p$) and of the n vectors with a p in one coordinate and zeroes elsewhere. Then, the lattice L_0 is the set of integer linear combinations of the columns of the matrix

$$\begin{pmatrix} I & pI & 0 \\ C & 0 & pI \end{pmatrix},$$

where the row blocks have sizes k and $n - k$ respectively, while the column blocks have sizes k, k, $n - k$, and respectively, and where I is the identity matrix of appropriate size. However, any integer linear combination of column vectors of $\begin{pmatrix} pI \\ 0 \end{pmatrix}$ is also an integer linear combination of column vectors of

$$\begin{pmatrix} I & 0 \\ C & pI \end{pmatrix}.$$

To see this, consider any vector of integers $\vec{y} = (y_1, ..., y_k)$. Then,

$$\begin{pmatrix} pI \\ 0 \end{pmatrix} \vec{y} = \begin{pmatrix} I \\ C \end{pmatrix} p\vec{y} - \begin{pmatrix} 0 \\ pI \end{pmatrix} C\vec{y}. \tag{5}$$

Thus, L_0 is the set of integer linear combinations of columns of the matrix

$$B_0 = \begin{pmatrix} I & 0 \\ C & pI \end{pmatrix}.$$

A matrix B such that the lattice is the set of integer combinations of columns of B is called a generating matrix for the lattice. Two different generating matrices B_1, B_2 define the same lattice if and only if $B_1 = B_2 T$ where T is an integer matrix such that T^{-1} also is an integer matrix. In this case, the matrix B_1 can be turned into the matrix B_2 by a sequence of elementary column operations where an elementary column operations is one of: adding one column to another, changing the signs of all entries in a column, or interchanging two columns.

Given a lattice L with generating matrix B which is an n-by-k matrix, such that B has rank k, we define the volume of the lattice to equal $\mathrm{vol}(L) = \det(B^\dagger B)^{1/2}$. If $k = n$, then $\mathrm{vol}(L) = |\det(B)|$.

▶ **Definition 2.** Given any linearly independent set of vectors $x_1, ..., x_k$ in $\mathbb{Z}^n$ (or more generally in $\mathbb{R}^n$) we define their volume $\mathrm{vol}(x_1, ..., x_k)$ to be the volume of the lattice generated by the n-by-k matrix with columns $x_1, ..., x_k$.

This matrix B_0 is lower triangular and so $\det(B_0)$ is easily computed:

$$\mathrm{vol}(L_0) = |\det(B_0)| = p^{n-k}. \tag{6}$$

▶ **Definition 3.** An "integral lattice" is defined to be a lattice whose generating matrix has integer entries. A "primitive lattice" is defined to be an integral lattice such that there is no

other integral lattice of the same rank properly containing it, where the rank of a lattice is defined to be the dimension of the subspace spanned by points in the lattice. Equivalently, a primitive lattice is an integral lattice such that there is no integral lattice which spans the same subspace and properly contains it.

Example: in two dimensions, the lattice generated by the vector $(2, 1)$ is primitive, while that generated by $(4, 2)$ is not.

Unless specified, all lattices will be in n dimensions. We use $|\ldots|$ to denote the ℓ_2 norm of a vector.

Finally, we define the Rankin invariant.

▶ **Definition 4.** The Rankin invariant $\gamma_{n,m}(L)$ for a lattice L with rank n is defined to be

$$\gamma_{n,m}(L) = \min_{\substack{v_1,\ldots,v_m \in L \\ \mathrm{vol}(v_1,\ldots,v_m) \neq 0}} \left(\frac{\mathrm{vol}(v_1,\ldots,v_m)}{\mathrm{vol}(L)^{m/n}} \right)^2. \tag{7}$$

The square in the above definition is included for historical reasons. The factor m/n in the exponent of $\mathrm{vol}(L)$ is such that the invariant is unchanged under rescaling the lattice L by any constant factor. In the case $m = 1$, the Rankin invariants $\gamma_{n,1}(L)$ is related to the length of the shortest vector: $\gamma_{n,1}(L) = \min_{x \in L, x \neq 0} \frac{|x|^2}{\mathrm{vol}(L)^{2/n}}$. Clearly, $\gamma_{n,n}(L) = 1$ for all L.

The Rankin invariant $\gamma_{n,1}(L)$ is related to the length of the shortest vector in the lattice. To understand the higher Rankin invariants, consider a set of vectors $v_1,\ldots,v_m \in L$ with $\mathrm{vol}(v_1,\ldots,v_m) \neq 0$. Consider the torus $\mathbb{R}^n/L$. The m-dimensional hyperplane spanned by $v_1,\ldots,v_m$ represents a nontrivial integer homology class and has an m-dimensional volume (using the Euclidean metric) equal to $\mathrm{vol}(v_1,\ldots,v_m)$.

One can also understand the higher Rankin invariants in another way. A choice of vectors $v_1,\ldots,v_m \in L$ with $\mathrm{vol}(v_1,\ldots,v_m) \neq 0$ corresponds to a basis for a rank-m sublattice of L. Thus, the Rankin invariants are a lower bound on the volume of rank-m sublattices. This interpretation will be used later, in section 4.

3   Overview of Construction: Conjectures and Main Result on Distance

We will consider a family of CSS codes obtained by choosing a fixed $p > 1$ and taking LDA lattices with $k = n/2$ from the random ensemble above, for all (even) values of n. With high probability, this lattice has rank n. Given the integral lattice L_0, we take a cellulation of the torus $\mathbb{R}^n/L_0$ by hypercubes of length 1 on each side. Then, we consider a qubit toric code on this cellulation with degrees of freedom on q-cells for $q = n/2$. Then, the number of q-cells is equal to

$$N = \binom{n}{n/2} p^{n/2}. \tag{8}$$

The distance of the code is equal to the weight of the least weight logical X or Z operator. The vector corresponding to such an operator represents nontrivial homology or cohomology with $\mathbb{Z}_2$ coefficients. We conjecture that:

▶ **Conjecture 1.** *There exists a constant $C > 0$, such that for any n-dimensional integral lattice L, for the toric code obtained by the cellulation using integer hypercubes and degrees of freedom on q-cells for $q = n/2$, the distance is lower bounded by*

$$C^n \min_{\substack{v_1,\ldots,v_q \in L \\ \mathrm{vol}(v_1,\ldots,v_q) \neq 0}} \mathrm{vol}(v_1,\ldots,v_q) = C^n \mathrm{vol}(L)^{q/n} \gamma_{n,q}(L)^{1/2}$$

.

Let us motivate this conjecture. The least volume hyperplane representing nontrivial homology has volume equal to the Rankin invariant. This hyperplane need not lie on the q-cells that we have chosen. We can deform the hyperplane to get a cycle that lies on the q-cells using the Federer-Fleming deformation theorem[11]: this theorem is based on deforming the cycle to lie on the $(n-1)$-skeleton (i.e., the $(n-1)$-dimensional faces of the hypercubes of unit size), then on the $(n-2)$-skeleton, and so on, iteratively, until the cycle lies on the q-skeleton. The deformation to move cycle from the m-skeleton to the $(m-1)$-skeleton is done by choosing a point randomly in an m-dimensional hypercube and then projecting the cycle outwards from that point to the boundary. This deformation may increase the volume, but that is fine: what we are considered with is lower bounding the volume.

However, it is not clear that the optimal operator is obtained by such a deformation procedure starting from a hyperplane. There may be, for example, unoriented chains which are not hyperplanes but which represent nontrivial homology and have much smaller volume than the least volume hyperplane. The conjecture is that such cycles can have at most exponentially smaller (i.e., smaller by a factor C^n) volume.

Conjecture 1 considers the distance of the code, which is equal to the least volume of a $\mathbb{Z}_2$ cycle representing nontrivial homology. The cycles are in the chain complex obtained from the cellulation using hypercubes. One may be tempted to make a (possibly stronger) conjecture that a similar inequality holds for more general chains, such as smooth chains. This conjecture has a purely geometrical statement:

▶ **Conjecture 2.** *There exists a constant $C > 0$, such that for any n-dimensional lattice L, the $n/2$-systole with $\mathbb{Z}_2$ coefficients of the torus $\mathbb{R}^n/L$ is lower bounded by*

$$C^n \min_{\substack{v_1,...,v_q \in L \\ \mathrm{vol}(v_1,...,v_q) \neq 0}} \mathrm{vol}(v_1,...,v_q) = C^n \mathrm{vol}(L)^{q/n} \gamma_{n,q}(L)^{1/2} \ .$$

Conjecture 1 would follow from conjecture 2 since the systole is defined by taking the infimum over smooth cycles, while in conjecture 1 we restrict to cycles which lie on the cellulation by unit hypercubes. In this regard, we remark that the possible increase in volume from the Federer-Fleming deformation theorem may be superexponentially large: the upper bound is at most $2n^{n/2}\binom{n}{n/2}$ (see Ref. [12]).

In this paper, we prove that:

▶ **Theorem 5.** *Assume that conjecture 1 holds. Then, for any $\epsilon > 0$, there exists a family of quantum CSS codes on N qubits with distance $D = \Omega(N^{1-\epsilon})$ and weight $w = \mathcal{O}(\log(N))$ and with $\Theta(N^\delta)$ encoded qubits, where $\delta > 0$ (δ depends on ϵ).*

This theorem will follow from a corollary of theorem 23, which implies that for any constant $c < 1/\sqrt{2\pi e}$, with high probability we have $\min_{\substack{v_1,...,v_q \in L \\ \mathrm{vol}(v_1,...,v_q) \neq 0}} \mathrm{vol}(v_1,...,v_q) \geq (cp)^{n/2}$. Hence, with high probability, $D \geq (cC^2 p)^{n/2}$. Since $N = \binom{n}{n/2} p^{n/2} \leq (4p)^{n/2}$, with high probability we have

$$D \geq (cC^2 p)^{\log_{4p}(N)} = N^{\frac{\log(cC^2 p)}{\log(4p)}} \ .$$

Fixing c to be any constant slightly smaller than $1/\sqrt{2\pi e}$, we find that for any $\epsilon > 0$ that for all sufficiently large p we have

$$1 - \epsilon \leq \frac{\log(cC^2 p)}{\log(4p)}$$

so that $D \geq N^{1-\epsilon}$.

We have $w = \mathcal{O}(d) = \mathcal{O}(\log(N))$.

The number of encoded qubits is equal to $\binom{n}{k} = 2^{(1-o(1))n} = 2^{2(1-(o(1))\log_{4p}(N)} = N^{2(1-o(1))/\log(4p)} \equiv N^\delta$.

The main work will be theorem 23, to lower bound the Rankin invariant for this class of lattices. The reader may wonder why we introduce this class of lattices, instead of re-using previous results which show that there exist random lattices with a large Rankin invariant, $\gamma_{n,n/2}(L) \geq (\frac{k}{12})^{n/4}$. See theorem 3 in Ref. [16]. The reason is that the random lattices constructed there need not be integral lattices and so we do not have such an obvious cell decomposition to place on the lattices. We comment later on the relationship between the Rankin invariant for our lattice (which depends on n, p) and the invariant in Ref. [16]; this requires considering how large n needs to be compared to p in our construction.

Note that we choose p large so that the exponentially growing factor, $\approx 2^n$, arising from the factor $\binom{n}{n/2}$ in the number of cells will be polynomially smaller than the volume $p^{n/2}$. We have $2^n = (p^n)^{1/\log_2(p)}$.

We remark that similar code constructions can be made by choosing degrees of freedom on q-cells for $q \neq n/2$, taking n large at a fixed ratio q/n. In this case, a natural generalization of conjecture 1 is to assume that there is a constant C such that $d_Z \geq C^n \mathrm{vol}(L)^{q/n} \gamma_{n,q}(L)^{1/2}$ and $d_X \geq C^n \mathrm{vol}(L)^{(n-q)/n} \gamma_{n,n-q}(L)^{1/2}$. Assuming this conjecture, our construction would give a code with $d_X d_Z$ polynomially larger than N.

4   Rankin Invariants

In this section, we will prove lower bounds on the Rankin invariants[24] $\gamma_{n,m}(L_0)$ of L_0. The proof uses the probabilistic method; in particular, we use the first moment method. To motivate the proof, let us first sketch a proof method for $\gamma_{n,1}(L_0)$; then, we give a sketch a possible extension of the proof method to $\gamma_{n,m}(L_0)$ and explain some difficulties with this extension; finally, we outline the approach we use which is a modification of that. First, suppose we just want to lower bound $\gamma_{n,1}(L_0)$; i.e., we wish to lower bound the shortest vector in the lattice. This can be done by a first moment method: estimate the number of integer vectors with length less than some given length ℓ; then, compute the probability that any given integer vector is in the lattice (this probability is $p^{-(n-k)}$ for a randomly chosen code assuming G is non-degenerate); so, for sufficiently small ℓ, the average number of integer vectors with length less than ℓ in the lattice is small so it is unlikely that any integer vectors with length less than ℓ will be in the lattice. One might attempt to do something similar for the Rankin invariants: estimate the number of rank m integral lattices in n dimensions with volume at most V and then compute the probability that an integral lattice is in a randomly chosen linear code, i.e., that this integral lattice is a sublattice of L_0. Call this rank-m lattice K and call its generating matrix M_K. In fact, Ref. [25] provides asymptotic estimates (large V) for the number of such lattices K, so it might seem that one could directly use the results there in a first moment method. Indeed, this approach might work, but since the results of Ref. [25] hold in the asymptotic limit (large V), some additional estimates would be needed (we do use many results in Ref. [25]). However, the results we need are in some ways simpler than that of Ref. [25] because we do not care about an exact estimate of the number of such lattices, only an upper bound. Further, rather than applying the first moment method by estimating the number of lattices K with some given volume and estimating the probability that such a lattice is in the code and then showing that the product is small for small V, we will apply the first moment method to each column of the generating matrix M_K *separately* (with M_K written in Hermite normal form). That is, we

first estimate (this step is exactly analogous to the discussion at the start of this paragraph regarding how to lower bound $\gamma_{n,1}(L_0)$) the probability that there is a choice for the first column which has small length and which is in the code. Then, we estimate the probability that there is a choice for the second column which is also in the code such that the ratio of the volume of the lattice generated by the first two columns of M_K to the volume of the lattice generated by the first column of M_K is small. To do this calculation, we need the concept of "factor lattice" [25], reviewed below. We continue in this fashion over the other columns, showing that the ratio of the volume of the lattice generated by the first a rows of M_K to the volume of the lattice generated by the first $a-1$ rows of a is likely to be large, for each $a = 2, 3, \ldots$.

4.1 Counting Points

Let $V_d(r)$ denote the volume of a ball of radius r in d dimensions:

$$V_d(r) = \frac{\pi^{d/2}}{\Gamma(\frac{d}{2}+1)} r^d. \tag{9}$$

Given a rank-l lattice L which spans some space E, we define the Voronoi cell to be the set of points y in E such that $|y| \leq |y - v|$ for all lattice points $v \neq 0$. The l-dimensional volume of the Voronoi cell is equal to $\text{vol}(L)$.

▶ **Definition 6.** Given a lattice L, let $N(L, z, r)$ denote the number of points in lattice L within distance r of some given point z.

▶ **Lemma 7.** *Let L be a rank-l lattice in d dimensions which spans some space E. Suppose the diameter of the Voronoi cell of L is bounded by some given D. Then, for any z, r,*

$$N(L, z, r) \leq \frac{1}{\text{vol}(L)} V_l(r + D). \tag{10}$$

Proof. For every point $x \in L$ within distance r of z, let T_x be the set of points $y \in E$ such that $y - x$ is in the interior of the Voronoi cell. The sets T_x are non-overlapping and each has l-dimensional volume $\text{vol}(L)$. So, the volume of $\cup_{x,|x-z|\leq r} T_x$ is equal to $N(L, z, r)\text{vol}(L)$. Every x is within distance r of z and so every point in $\cup_{x,|x-z|\leq r} T_x$ is within distance $r + D$ of z, so $N(L, z, r)\text{vol}(L) \leq V_k(r + D)$. ◄

We make some more definitions.

▶ **Definition 8.** Given a rank-l lattice L spanning a subspace E, the polar lattice L^P is the lattice of all vectors in E which have integral inner products with all vectors in L. The polar lattice also has rank l and $\text{vol}(L^P)\text{vol}(L) = 1$.

▶ **Definition 9.** Let Γ_0^n be the rank-n lattice in n dimensions consisting of all vectors for which all coordinates are integral.

▶ **Definition 10.** Given a primitive lattice L spanning subspace E, the orthogonal lattice $L^\perp$ consists of all vectors in Γ_0^n with vanishing inner product with all vectors in L.

▶ **Definition 11.** Let L be a rank-l primitive sublattice of Γ_0^n and let E be the subspace spanned by L. Let π project onto the orthogonal complement of E, which we write $E^\perp$. Let $\pi(\Gamma_0^n) \equiv \Gamma_0^n/L$. Then, Γ_0^n/L is also a lattice, called the factor lattice. It has rank $n - l$

We have[25]

$$\mathrm{vol}(L)\mathrm{vol}(\Gamma_0^n/L) = 1. \tag{11}$$

This equation follows from this lemma:

▶ **Lemma 12.**

$$\Gamma_0^n/L = ((L)^\perp)^P. \tag{12}$$

Proof. See Ref. [25]. ◀

▶ **Lemma 13.** *Let L be a rank-l primitive sublattice of Γ_0^n. Let π and Γ_0^n/L be as above. Then, the diameter of the Voronoi cell of Γ_0^n/L is bounded by $\sqrt{n-l}$.*

Proof. Since L has rank $l < n$, there must be some vector w_1 which has a 1 in one coordinate and zeroes in all other coordinates (i.e., w_1 is of the form $(0,\ldots,0,1,0,\ldots,0)$) which is not in E. Then, since the span of E and w_1 has dimension $l+1$, if $k < n-1$, there must be some other vector w_2 of the same form which is not in the span of E and l_1. Proceeding in this fashion, we construct vectors $w_1,\ldots,w_{n-l}$, all of which have zeroes in all but one coordinate and a 1 in that coordinate. The vectors $\pi(w_i)$ span $E^\perp$. So, every point y in $E^\perp$ can be written as a linear combination $y = \pi(\sum_i a_i w_i)$. If the a_i are integer, then y is a lattice point in $\pi(\Gamma_0^n)$. Every linear combination $\sum_i a_i w_i$ is within distance $(1/2)\sqrt{n-l}$ of some linear combination $\sum_i b_i w_i$ with integer b_i (to see this, simply round all a_i to the nearest integer). Since the norm does not increase under projection, every $\pi(\sum_i a_i w_i)$ is also within distance $(1/2)\sqrt{n-l}$ of some $\pi(\sum_i b_i w_i)$ for integer b_i and hence every point in E is within distance $(1/2)\sqrt{n-l}$ of a lattice point. ◀

We remark that the lattice with basis vectors $\pi(w_i)$ may not include all points in $\pi(\Gamma_0^n)$; as an example, consider $l = 1$ and $n = 2$ and let L be the lattice with basis vector $(2,1)$ and let $w_1 = (0,1)$. The vector $\pi((1,0))$ is then not included in the lattice with basis vector $\pi(w_1)$.

▶ **Lemma 14.** *Let L be a rank-l primitive sublattice of Γ_0^n. Let π and Γ_0^n/L be as above. The number of points in Γ_0^n/L within distance r of the origin is bounded by*

$$N(\Gamma_0^n/L, 0, r) \leq \mathrm{vol}(L)V_l(r + \sqrt{n-l}). \tag{13}$$

Proof. This follows from lemmas 7,13 and Eq. (11). ◀

4.2 Hermite Normal Form For Lattices

Consider a rank-m integral lattice K in n dimensions. If this lattice has basis vectors $v_1,\ldots,v_m$, we write an n-by-m matrix M_K whose columns are these basis vectors. We label the rows of the matrix by integers $1,\ldots,n$ and label the columns by integers $1,\ldots,m$. Such a matrix is called a lattice generator matrix for the lattice. Then, the set of points in the integral lattice is the image under M_K of Γ_0^m. By a sequence of column operations (adding one column of M_K to another column, which does not change the image, or changing the sign of a column, which also does not change the image), we can bring always bring the matrix M_K to so-called "Hermite normal form"; further, there is a unique matrix M_K in Hermite normal form which generates K.

Our definition of Hermite normal form differs from that of other authors because we will *reverse* the order of columns and *reverse* the order of rows compared to the usual order. This is because we will be doing induction later and with the reversed order of columns, the notation will be much more natural later. See Eq. (17) for an example of Hermite normal form below.

▶ **Definition 15.** A matrix M_K is said to be in Hermite normal form if for every column j there is a row i_j with $1 \leq i_1 < i_2 < \ldots < i_m \leq n$ such that the entries of M_K obey:

$$i > i_j \quad \rightarrow \quad (M_K)_{i,j} = 0 \tag{14}$$

and

$$(M_K)_{i_j,j} > 0, \tag{15}$$

and

$$l > j \quad \rightarrow \quad 0 \leq (M_K)_{i_j,l} < (M_K)_{i_j,j}. \tag{16}$$

We say that "the first a columns of M_K are in Hermite normal form" if the submatrix of M_K consisting of the first a columns is in Hermite normal form. In this case, for every column j with $j \leq a$ there is a row i_j with $1 \leq i_1 < i_2 < \ldots < i_a \leq n$ such that Eqs. (14,15,16) hold when restricted to the case that $j \leq a$ and $l \leq a$.

We introduce some notation. This notation defines various vector spaces and vectors in terms of the matrix M_K; we do not explicitly write M_K in the definition, but rather the particular choice of M_K should be clear in context. The last nonzero entry in the j-th column occurs in the i_j-th row. Define a sequence of lattices $K_1, K_2, \ldots, K_m$, where K_j has rank j and K_j is defined to be the lattice generated by the submatrix of M_K containing the first j rows and the first i_j columns. Note that $K_m = K$. Note also that if K_a is primitive then K_b is primitive for all $b < a$.

We let $\vec{v}_j$ be the vector given by the first i_j rows of the j-th column.

This notation can be clarified with an example of $n = 5, m = 3$, with $i_1 = 2, i_2 = 4, i_3 = 5$, where we write

$$M_K = \begin{pmatrix} (\vec{v}_1)_1 & (\vec{v}_2)_1 & (\vec{v}_3)_1 \\ (\vec{v}_1)_2 & (\vec{v}_2)_2 & (\vec{v}_3)_2 \\ 0 & (\vec{v}_2)_3 & (\vec{v}_3)_3 \\ 0 & (\vec{v}_2)_4 & (\vec{v}_3)_4 \\ 0 & 0 & (\vec{v}_3)_5 \end{pmatrix}, \tag{17}$$

with $(\vec{v}_j)_i$ denoting the i-th entry of vector $\vec{v}_j$. For this matrix to be in Hermite normal form, we have $0 \leq (\vec{v}_2)_2, (\vec{v}_3)_2 < (\vec{v}_1)_2$ and $0 \leq (\vec{v}_3)_4 < (\vec{v}_2)_4$.

The lattice K_j is a sublattice of $\Gamma_0^{i_j}$. We let M_{K_j} be the submatrix of M_K consisting of the first j rows and the first i_j columns so that M_{K_j} generates K_j. We also define a lattice $\tilde{K}_j$ which is a sublattice of $\Gamma_0^{i_{j+1}}$. The lattice $\tilde{K}_j$ will be the sublattice generated by the submatrix of M_K consisting of the first j rows and the first i_{j+1} columns. We let $M_{\tilde{K}_j}$ be the submatrix of M_K consisting of the first j rows and the first i_{j+1} columns. Hence, the last $i_{j+1} - i_j$ entries of every vector in $\tilde{K}_j$ are equal to 0.

Let π_j project onto the orthogonal complement of the span of $\tilde{K}_j$.

▶ **Lemma 16.** *Let K be a rank-m lattice in n dimensions with generating matrix M_K in Hermite normal form. Then, there exist an n-by-m integer matrix M_{K^P} which is a lattice generating matrix in Hermite normal form (with the same i_j as M_K) for a primitive lattice, and an m-by-m integer matrix F which is upper triangular with positive diagonal entries such that we have*

$$M_K = M_{K^P} F. \tag{18}$$

Further, F, M_{K^P} are unique.

Proof. Let K^P be a primitive lattice spanning the same space as K and containing the lattice K. (Note that such a primitive K^P must exist and is unique: it is the lattice consisting of all integer points which are in the space spanned by K). Let K^P be generated by M_{K^P} with M_{K^P} in Hermite normal form; note that since K^P is unique, M_{K^P} is uniquely determined by K. Then, since K is contained in K^P, every column of M_K is an integer linear combination of columns of M_{K^P}. So, $M_K = M_{K^P} F$ for some integer matrix F.

M_K, M_{K^P} must have the same i_j or their columns would not span the same space.

Since M_K, M_{K^P} have the same i_j, it follows that F is upper triangular with positive diagonal entries: restrict M_K, M_{K^P} to the rows $i_1, i_2, \ldots, i_m$, giving upper triangular matrices of size m-by-m. Call these matrices A, B respectively. Then $A = BF$, so $F = B^{-1}A$. Since B is upper triangular, so is B^{-1} and so is F. ◄

4.3   Counting Column Choices

▶ **Definition 17.** A lattice L is *consistent* with a code generator matrix G if every point $(x_1, ..., x_n)$ in the lattice has the property that $(x_1 \mod p, \ldots, x_n \mod p)$ is in the code defined by G. A lattice generator matrix M_L is consistent with a code generator matrix G if the lattice generated by M_L is consistent with G.

We will use a to label a column choice, $1 \le a \le m$. We will construct lattices K_a in terms of K_{a-1} and $\vec{v}_a$.

▶ **Lemma 18.** *Let M_K be in Hermite normal form. Then,*

$$\text{vol}(K_a) = \text{vol}(K_{a-1})|\pi_{a-1}(\vec{v}_a)|. \tag{19}$$

Proof. Immediate from the definition of volume. ◄

Assume K_{a-1} is primitve. Then, the next lemma gives a one-to-one correspondence between vectors $\vec{v}_a$ obeying *one* of the conditions needed for Hermite normal form (the condition Eq. (16)) and vectors in a certain factor lattice. In lemma 20 we consider the case that K_{a-1} is not primitive. Note that there is an additional condition on v_a, namely that its first entry be positive, in order for the matrix M_{K_a} to be in Hermite normal form.

▶ **Lemma 19.** *Let the first $a-1$ columns of M_K be given and assume that the first $a-1$ columns of M_K are in Hermite normal form and assume that K_{a-1} is a primitive sublattice of Γ_0^n. Then, there is a one-to-one correspondence between vectors $\vec{v}_a$ such that*

$$j < a \quad \rightarrow \quad 0 \le (M_K)_{i_j,a} < (M_K)_{i_j,j} \tag{20}$$

and points $\vec{x}$ of the lattice $\Gamma_0^{i_a}/\tilde{K}_{a-1}$, such that if $\vec{x}$ corresponds to $\vec{v}_a$ then $\pi_{a-1}(\vec{v}_a) = \vec{x}$.

Proof. We will show that for every $\vec{x} \in \Gamma_0^{i_a}/\tilde{K}_{a-1}$, there exists a unique $\vec{v}_a$ obeying Eq. (20) such that $\pi_{a-1}(\vec{v}_a) = \vec{x}$. This gives a map $\mathcal{F}$ from $\Gamma_0^{i_a}/\tilde{K}_{a-1}$ to vectors obeying Eq. (20). This map is one-to-one since distinct vectors $\vec{x}_1 \ne \vec{x}_2$ cannot both be the image of the same vector $\vec{v}_a$ under the map π_{a-1}. This map $\mathcal{F}$ is onto since any vector $\vec{v}_a$ obeying Eq. (20) is the image of $\pi_{a-1}(\vec{v}_a)$ under this map.

First we show existence of somer vector $\vec{v}_a$. Every vector $\vec{x}$ in $\Gamma_0^{i_a}/\tilde{K}_{a-1}$ is given by $\vec{x} = \pi_{a-1}(\vec{y})$ for some $\vec{y} \in \Gamma_0^{i_a}$. For any such vector $\vec{y}$, we can add lattice vectors in $\tilde{K}_{a-1}$ so that Eq. (20) (i.e., set $\vec{v}_a$ equal to $\vec{y}$ plus some sum of lattice vectors; this can be done iteratively, so that it holds first for $j = a - 1$, then $j = a - 2$, and so on). Adding these lattice vectors does not change the image of the result under π_{a-1}.

Now uniqueness. Suppose that $\pi_{a-1}(\vec{y}) = \pi_{a-1}(\vec{z})$ for $\vec{y}, \vec{z}$ being two possible choices of $\vec{v}_a$ such that Eq. (20) is obeyed. Then, $\pi_{a-1}(\vec{y} - \vec{z}) = 0$, so $\vec{y} - \vec{z}$ is in the span of $\tilde{K}_{a-1}$. Since K_{a-1} is primitive so is $\tilde{K}_{a-1}$ and so $\vec{y} - \vec{z}$ is in $\tilde{K}_{a-1}$. Let $M_K(i, j)$ denote the submatrix of M_K containing the first i rows and the first j columns, so that $M_K(i_a, a - 1)$ is a lattice generating matrix for $\tilde{K}_{a-1}$. So, $\vec{y} - \vec{z} = M_K(i_a, a - 1)\vec{u}$, where $\vec{u} \in \Gamma_0^{a-1}$. Then, Eq. (20) requires that $\vec{u} = 0$. This follows inductively: if the last entry of $\vec{u}$ is nonzero, then it is not possible for both $\vec{y}$ and $\vec{z}$ to obey Eq. (20) for $j = a - 1$; to see this, note that then the $(a - 1)$-th entries of $\vec{y}, \vec{z}$ must differ by a positive integer multiple of $(M_K)_{i_j, j}$ and so they cannot both fall in the range $0, 1, \ldots, (M_K)_{i_j, j} - 1$. So, $\vec{y} - \vec{z}$ differs by an elements of the lattice generated by $M_K(i_a, a - 2)$ and so $\vec{y} - \vec{z} = M_K(i_a, a - 2)\vec{u}'$ for $\vec{u}' \in \Gamma_0^{a-2}$. Again, the last entry of $\vec{u}'$ must equal zero so that Eq. (20) will be obeyed for $j = a - 2$. We continue inductively for $j = a - 3, \ldots$.   ◀

The next lemma is similar to the previous except that we no longer assume that K_{a-1} is primitive.

▶ **Lemma 20.** *Let the first $a - 1$ columns of M_K be given and assume that the first $a - 1$ columns of M_K are in Hermite normal form.*

Let $M_K(i, j)$ denote the submatrix of M_K containing the first i rows and the first j columns, so that $M_{\tilde{K}_{a-1}} = M_K(i_a, a - 1)$ is a lattice generating matrix for $\tilde{K}_{a-1}$. Use lemma 16 to write

$$M_{\tilde{K}_{a-1}} = M_{\tilde{K}_{a-1}^P} F.$$

Then, the possible choices of $\vec{v}_a$ such that

$$j < a \quad \rightarrow \quad 0 \le (M_K)_{i_j, a} < (M_K)_{i_j, j} \tag{21}$$

are in one-to-one correspondence with choices of tuples $(\vec{x}, f_1, \ldots, f_{a-1})$, where $\vec{x}$ is a point in $\Gamma_0^{i_a}/\tilde{K}_{a-1}$ and $f_1, \ldots, f_{a-1}$ are integers obeying $0 \le f_i < F_{i,i}$, such that if $(\vec{x}, f_1, \ldots, f_{a-1})$ corresponds to $\vec{v}_a$ then $\pi_{a-1}(\vec{v}_a) = \vec{x}$. Thus, there are $\det(F)$ distinct vectors $\vec{v}_a$ corresponding to $\vec{x}$.

Proof. We will show that for every $\vec{x} \in \Gamma_0^{i_a}/\tilde{K}_{a-1}$, there exist $\det(F)$ distinct vectors $\vec{v}_a$ obeying Eq. (21) such that $\pi_{a-1}(\vec{v}_a) = \vec{x}$. These $\det(F)$ vectors will be labelled by $f_1, \ldots, f_{a-1}$.

First we show existence. Every vector $\vec{x}$ in $\Gamma_0^{i_a}/\tilde{K}_{a-1}$ is given by $\vec{x} = \pi_{a-1}(\vec{y})$ for some $\vec{y} \in \Gamma_0^{i_a}$. For any such vector $\vec{y}$, we can add lattice vectors in $\tilde{K}_{a-1}$ so that Eq. (21) will hold (this can be done iteratively, so that it holds first for $j = a - 1$, then $j = a - 2$, and so on). Adding these lattice vectors does not change the image of the result under π_{a-1}.

Now, for each $\vec{x}$, let $\vec{z}$ be some fixed vector such that Eq. (21) holds for $\vec{v}_a = \vec{z}$ and such that $\vec{x} = \pi_{a-1}(\vec{z})$. Suppose that $\pi_{a-1}(\vec{y}) = \pi_{a-1}(\vec{z})$ for $\vec{y}$ some other possible choice of $\vec{v}_a$ such that Eq. (21) is obeyed. We count the number of possible choices of $\vec{y}$. Then, $\pi_{a-1}(\vec{y} - \vec{z}) = 0$, so $\vec{y} - \vec{z}$ is in the span of $\tilde{K}_{a-1}$. Since $\tilde{K}_{a-1}^P$ is primitive, $\vec{y} - \vec{z} = M_{\tilde{K}_{a-1}^P}\vec{u}$, where $\vec{u} \in \Gamma_0^{a-1}$. There are $F_{a-1,a-1}$ possible choices for the $(a - 1)$-th entry of $\vec{u}$. To see this, note that $\vec{y}$ and $\vec{z}$ both obey Eq. (21) for $j = a - 1$. For $j = a - 1$, this equation gives a constraint that the $(a - 1)$-th entry of $\vec{y}$ must fall in the range $0, \ldots, (M_K)_{i_{a-1}, a-1} - 1$. The $(a - 1)$-th entry of $\vec{y}$ is determined by the $(a - 1)$-th entry of $\vec{u}$ and shifting that entry of $\vec{u}$ by one shifts the $(a - 1)$-th entry of $\vec{y}$ by $(M_{\tilde{K}_{a-1}^P})_{i_{a-1}, a-1}$. We have $(M_K)_{i_{a-1}, a-1} = (M_{\tilde{K}_{a-1}^P})_{i_{a-1}, a-1} F_{a-1, a-1}$ so that there are $F_{a-1, a-1}$ possible choices. Then, given this choice of the $(a - 1)$-th entry of $\vec{u}$, there are $F_{a-2, a-2}$ possible choices for the $(a - 2)$-th entry of $\vec{u}$, and so on.   ◀

▶ **Lemma 21.** *Let M_K be a matrix in Hermite normal form which is a lattice generating matrix for a rank-m integral lattice K in n dimensions. Let K_{a-1} be given and let r be a real number. Let $C(r, K_{a-1})$ denote the number of choices of K_a such that*

$$\text{vol}(K_a) \leq r K_{a-1}. \tag{22}$$

Then,

$$C(r, K_{a-1}) \leq \text{vol}(K_{a-1}) V_{i_a-a+1}(r + \sqrt{i_a - a + 1}). \tag{23}$$

If $r < 1$ then $C(r, K_{a-1}) = 0$.

Proof. Let $\vec{v}_a$ be as defined above. By lemma 18

$$\text{vol}(K_a) = \text{vol}(K_{a-1})|\pi_{a-1}(\vec{v}_a)|. \tag{24}$$

so $|\pi_{a-1}(v_a)| \leq r$. By Eq. (15), the first entry of $\vec{v}_a$ is ≥ 1, and since all vectors in K_{a-1} vanish in the first entry, we have $|\pi_{a-1}(\vec{v}_a)| \geq 1$, so indeed $C(r, K_{k-1}) = 0$ for $r < 1$.

By lemma 20, the vector $\vec{v}_a$ is in one-to-one correspondence with a tuple $(\vec{x}, f_1, \ldots, f_{a-1})$ where $\vec{x}$ is a vector in lattice $\Gamma_0^{i_a}/\tilde{K}_{a-1}^P$. By lemma 13, the lattice $\Gamma_0^{i_a}/\tilde{K}_{a-1}^P$ has the diameter of its Voronoi cells bounded by $\sqrt{i_a - a + 1}$. So, for given $\Gamma_0^{i_a}/\tilde{K}_{a-1}^P$ and given r, the number of possible choices of $\vec{x}$ such $|\pi_{a-1}(\vec{v}_a)| \leq r$ is bounded by

$$N(\Gamma_0^{i_a}/\tilde{K}_{a-1}^P, 0, r) \leq \frac{1}{\text{vol}(\Gamma_0^{i_a}/\tilde{K}_{a-1}^P)} V_{i_a-a+1}(r + \sqrt{i_a - a + 1}). \tag{25}$$

So, by Eq. (11),

$$N(\Gamma_0^{i_a}/\tilde{K}_{a-1}^P, 0, r) \leq \text{vol}(K_{a-1}^P) V_{i_a-a+1}(r + \sqrt{i_a - a + 1}). \tag{26}$$

Factorize $M_K(i_a, a-1) = M_{\tilde{K}_{a-1}^P} F$, as in lemma 20.

The number of possible choices of $f_1, \ldots, f_{a-1}$ is equal to $\det(F) = \text{vol}(K_{a-1})/\text{vol}(K_{a-1}^P)$. So, the total number of choices of K_a is bounded by

$$\det(F)\text{vol}(K_{a-1}^P) V_{i_a-a+1}(r + \sqrt{i_a - a + 1}) = \text{vol}(K_{a-1}) V_{i_a-a+1}(r + \sqrt{i_a - a + 1}), \tag{27}$$

as claimed. ◀

4.4 First Moment Bound

▶ **Lemma 22.** *Let G be an n-by-k code generator matrix for a code, chosen from the ensemble defined previously (entries chosen independently and uniformly from $\mathbb{F}_p$). Let M_K be an n-by-k lattice generator matrix. Let K_{a-1} be given and assume the first $a-1$ columns of M_K are in Hermite normal form. Let $Pr(K_{a-1}, r)$ denote the probability that, conditioned on K_{a-1} being consistent with G, there exists a choice of v_a such that K_a is consistent with G and such that the first a columns of M_K are in Hermite normal form and such that*

$$\text{vol}(K_a) \leq r K_{a-1}. \tag{28}$$

Then, for $r < 1$, $Pr(K_{a-1}, r) = 0$, and for $r < p$,

$$Pr(K_{a-1}, r) \leq p^{-(n-k)}\text{vol}(K_{a-1}) V_{i_a-a+1}(r + \sqrt{i_a - a + 1}). \tag{29}$$

Proof. By lemma 21, indeed there are no choices of v_a such that $r < 1$. If $r < p$, then $0 < (\vec{v}_a)_1 < p$ so $(\vec{v}_a)_1 \neq 0 \mod p$. So, the a-th column of M_K is not in the span of the first $a - 1$ columns of M_K modulo p. So, even though we have conditioned on K_{a-1} being consistent with G, the probability that a given choice of $\vec{v}_a$ is consistent with G is bounded by $p^{-(n-k)}$. (The probability is $p^{-(n-k)}$ if we condition on G being non-degenerate and smaller if G may be degenerate.)

So, by lemma 21, the average number of choices of $\vec{v}_k$ consistent with G is bounded by $p^{-(n-k)}\mathrm{vol}(K_{a-1})V_{i_a-a+1}(r + \sqrt{i_a - a + 1})$. ◄

The next theorem estimates the probability that, for a randomly chosen code generator matrix, there is a rank-m lattice K of small volume which is consistent with that matrix. The bounds becomes effective for volume smaller than $(cp)^{\min(m,n-k)}$ with $c < 1/\sqrt{2\pi e}$.

▶ **Theorem 23.** *Let $P_{lat}(H, p, n, m)$ denote the probability that for a random code generator matrix G for a code over $\mathbb{F}_p^n$ there is a rank-m lattice K consistent with a code generator matrix such that $\mathrm{vol}(K) \leq H$.*

For any p, for any real number $x > \sqrt{2\pi e}$, for sufficiently large $n - m$,

$$P_{lat}((cp)^{\min(m,n-k)}, p, n, m) \leq mc^m x^{n-m+1}. \tag{30}$$

The required $n - m$ is quadratic in $p(x - \sqrt{2\pi e})^{-1}$.

Proof. Note that if there is a lattice K of rank-m consistent with the code generator matrix, then the lattices $K_1, \ldots, K_{m-1}$ constructed above have ranks $1, \ldots, m - 1$ respectively and are also consistent with the code generator matrix and have $\mathrm{vol}(K_a) \leq \mathrm{vol}(K)$. So, it suffices to consider the case $m \leq n - k$ (if $m > n - k$, then consider the lattice K_{n-k} instead).

For M_K in Hermite normal form, since $i_1 < i_2 < \ldots < i_m < n$, we have $i_a \leq n - m + a$ and so $i_a - a + 1 \leq n - m + 1$. We use the bound (the inequality on the second line holds for all sufficiently large $n - m$)

$$
\begin{aligned}
V_{n-m+1}(r + \sqrt{n-m+1}) &= \frac{\pi^{\frac{n-m+1}{2}}}{\Gamma(\frac{n-m+1}{2})}(r + \sqrt{n-m+1})^{n-m+1} \\
&\leq \left(\frac{2\pi e}{n-m+1}\right)^{\frac{n-m+1}{2}}(r + \sqrt{n-m+1})^{n-m+1} \\
&= \left(\frac{r\sqrt{2\pi e}}{\sqrt{n-m+1}} + \sqrt{2\pi e}\right)^{n-m+1},
\end{aligned}
\tag{31}
$$

Let c be a real number, $0 < c < 1$. We will make a choice of c below.

By lemma 22 and Eq. (31), given K_{a-1}, if $\mathrm{vol}(K_{a-1}) \leq (cp)^m$, we have

$$
\begin{aligned}
Pr(K_{a-1}, r) &\leq c^m p^{m-(n-k)}\left(\frac{r\sqrt{2\pi e}}{\sqrt{n-m+1}} + \sqrt{2\pi e}\right)^{n-m+1} \\
&\leq c^m \left(\frac{r\sqrt{2\pi e}}{\sqrt{n-m+1}} + \sqrt{2\pi e}\right)^{n-m+1}.
\end{aligned}
\tag{32}
$$

For $r < p$, this is bounded by $c^m\left(\frac{p\sqrt{2\pi e}}{\sqrt{n-m+1}} + \sqrt{2\pi e}\right)^{n-m+1}$. For any p, for any real number $x > \sqrt{2\pi e}$, for sufficiently large $n - m$, this is bounded by $c^m x^{n-m+1}$. (The required $n - m$ is quadratic in $p(x - \sqrt{2\pi e})^{-1}$.)

Suppose that $\mathrm{vol}(K) \leq (cp)^m$ for some $c < 1$. Then, $\mathrm{vol}(K_a) \leq (cp)^m$ for all a and for some a we have $\mathrm{vol}(K_a)/\mathrm{vol}(K_{a-1}) < p$. However, for $\mathrm{vol}(K_a) \leq (cp)^m$, the above calculation bounds the probability for given a that there is a choice of K_a such that

$\text{vol}(K_a)/\text{vol}(K_{a-1}) < p$ by $c^m x^{n-m+1}$ for all sufficiently large $n - m$. By a union bound, the probability that for some a there is a choice of K_a such that $\text{vol}(K_a)/\text{vol}(K_{a-1}) < p$ is bounded by $mc^m x^{n-m+1}$ for all sufficiently large $n - m$. So, $P_{lat}((cp)^m, p, n, m) \leq mc^m x^{n-m+1}$ for all sufficiently large $n - m$. ◀

This implies the following corollary for the Rankin invariant:

▶ **Corollary 24.** *For any p, k, for all sufficiently large n at fixed ratio m/n, for any $c < 1/\sqrt{2\pi e}$, with high probability we have*

$$\gamma_{n,m}(L_0) \geq (cp)^{2\min(m,n-k)} p^{-2m(n-k)/n}. \tag{33}$$

(Recall that with high probability G is non-degenerate so L_0 is rank n.)

We remark that it might be possible to tighten the bounds of theorem 23 to bound P_{lat} even for some range of x smaller than $\sqrt{2\pi e}$, especially for small m. One possible way to tighten the bounds is to use the fact that if there $\text{vol}(K) < p^{m-z}$ for some integer $z > 0$ then there must be at least z different a such that $\text{vol}(K_a)/\text{vol}(K_{a-1}) < p$; in the proof above we only used that there was at least one such a.

We remark also that, up to the constant c, the value of the Rankin invariant at $m = k = n/2$ is optimal for an integral lattice; i.e., the dependence on p is optimal. The reason is that it implies that an $n/2$-dimensional sublattice of L_0 has the same volume (again, up to factors of c^m) as L_0 does.

It is also worth comparing the value of the Rankin invariant that we find to the Rankin invariant for random lattices (from a different ensemble) in Ref. [16]. The Rankin constant $\gamma_{n,m}$ is defined to be the maximum of $\gamma_{n,m}(L)$ over all lattices L. Those random lattices in Ref. [16] were used to lower bound the Rankin constant $\gamma_{n,n/2}$ by $\gamma_{n,n/2} \geq (\frac{k}{12})^{n/4}$. Since we need to take $n \sim p^2$ for the bounds of theorem 23 to be effective, if we choose $m = k = n/2$ and $p \sim \sqrt{n}$ we find that with high probability $\gamma_{n,n/2}(L_0) \geq (\text{const.} \times n)^{n/4}$. Thus, we find the same leading behavior $n^{n/4}$, with the Rankin invariants differing only by factors const.^{n}.

5   Volume of Oriented Systole

In this section, we consider a weaker conjecture than 1. Throughout this section, we consider the case of homology using integer coefficients, rather than $\mathbb{Z}_2$ coefficients. In this setting, there is a general method, called "calibration" [17] for lower bounding weights. We will show that this method gives an effective lower bound for homology classes which have a particular form, which we call "split", but we will show that it does not give a useful lower bound in general. The reason for this is related to the existence of short vectors in the exterior q-th power of L_0.

Given an rank-n lattice L, we write its m-th exterior power as $\wedge^m L$. This exterior power is a lattice of vectors in $\binom{n}{m}$ dimensions; the vectors in this lattice are linear combinations (with integer coefficients) of vectors $v_1 \wedge v_2 \wedge \ldots \wedge v_m$, where $v_i \in L$ and the exterior product is anti-symmetric under interchange: $v_1 \wedge v_2 = -v_2 \wedge v_1$.

▶ **Definition 25.** A vector v in $\wedge^m L$ is called "split" if $v = x_1 \wedge \ldots \wedge x_m$ for $x_1, \ldots x_m \in L$.

The q-th homology classes of the torus T^n are in one-to-one correspondence with vectors in $\wedge^q \mathbb{Z}^n$. For the torus $\mathbb{R}^n/L_0$ that we consider, it will be more convenient to regard the classes as being in one-to-one correspondence with vectors in $\wedge^q L_0$. That is, the k-th homology class represented by a hyperplane which is a span of k basis vectors will correspond to the vector which is the exterior product of these k basis vectors.

The lattice $\wedge^m L$ inherits an inner product:

$$(x_1 \wedge \ldots \wedge x_m) \cdot (y_1 \wedge \ldots \wedge y_m) = \det(S),$$

where S has matrix elements $S_{i,j} = x_i \cdot y_j$. We write this norm $|X|$, where $X \in \wedge^m L_0$. Calibration allows one to lower bound the volume of a representative of a homology class in $\wedge^q L_0$ using this inner product.

We first explain this lower bound in the split case. The arguments are not new.

▶ **Lemma 26.** *Let* $\mathrm{vol}(v_1, \ldots, v_q) \neq 0$. *Then, the minimum volume of any closed chain (either a sum of faces of q-faces of the unit hypercubes used in the cubulation or more generally an arbitrary sum of simplices) representing homology class $X = v_1 \wedge \ldots \wedge v_q$ is greater than or equal to $|v_1 \wedge \ldots \wedge v_q|$.*

Proof. Let us write $v \cdot d\vec{x}$ to denote a differential 1-form $\sum_i (v)_i dx^i$, where $i = 1, \ldots, n$ are orthogonal basis directions in Euclidean space and $(v)_i$ are components of i. Consider the differerential q-form $\omega = (v_1 \cdot d\vec{x}) \wedge (v_2 \cdot d\vec{x}) \wedge \ldots \wedge (v_q \cdot d\vec{x})$. Let S denote the hyperplane spanned by vectors $v_1, \ldots, v_q$ (the hyperplane is oriented, so the order of vectors matters). We have $\int_S \omega = |X|^2$. Further, for any chain C in the same homology class as S, we have $\int_C \omega = \int_S \omega = |X|^2$, where the integral over C is given by writing C as a sum of q-faces of the unit hypercubes and integrating ω over each face. (Indeed, one can also consider more general C, such as sums of arbitrary simplices, and the same result holds). For a q-face (or indeed any sum of q-dimensional simplices), the integral of ω over that face is bounded by $|X|$ times the volume of the face. Hence, the volume of C must be at least equal to $(\int_C \omega)/|X| = |X|$. ◀

Now we consider the nonsplit case. In contrast to the split case where we were able to "calibrate" the hyperplane S (find a differential form assuming maximum value on that hyperplane), we might not be able to calibrate nonsplit homology classes. However, we can still obtain a lower bound.

▶ **Lemma 27.** *Let* $X \in \wedge^q L$, $X \neq 0$. *Then, the minimum volume of any closed chain representing homology class X is lower bounded by $|X|$.*

Proof. Write $X = \sum_a X_a$, where X_a are split vectors. For each $X_a = v_1^a \wedge \ldots \wedge v_q^a$, define a differential q-form $\omega_a = (v_1^a \cdot d\vec{x}) \wedge \ldots \wedge (v_q^a \cdot d\vec{x})$. Let $\omega = \sum_a \omega_a$.

Let S_a denote the hyperplane spanned by vectors $v_1^a, \ldots, v_q^a$. Let S denote the union of hyperplanes S_a. We have $\int_{S_a} \omega_b = (X_a, X_b)$. Hence, $\int_S \omega = |X|^2$.

We now consider the maximum of the integral of C over a q-face or q-dimensional simplex of unit volume. This is equal to

$$\max_{V \text{ split}, |V|=1}(V, X),$$

where we take the maximum over all split vectors $V \in \wedge^q \mathbb{R}^n$, with V not necessarily in $\wedge^q L$; i.e., $V = v_1 \wedge \ldots \wedge v_q$ for *arbitrary* $v_1, \ldots v_q$, with $v_1, \ldots, v_q$ not necessarily in the lattice L (i.e., we are upper bounding the integral over a unit volume square in the hyperplane spanned by $v_1, \ldots v_q$). If we relax the requirement that V be split, we have $\max_V (V, X) = |X|$. The restriction to split V can only reduce the maximum, so the maximum over split V is at most $|X|$. So, as in lemma 26, since the integral over ω over any chain representing the same homology class as X must be equal to the $\int_S \omega = |X|$, the volume of such a chain must be at least $|X|$. ◀

One may wonder whether the bound in lemma 27 can be significantly improved if we do not relax the requirement that V be split. Of course, if X is split, then

$$\max_{V \text{ split, } |V|=1}(V, X) \geq |X|/\sqrt{\binom{n}{q}} = |X|$$

and the maximum is achieved for $V = X$. However, for X not split, the maximum might be smaller and so the lower bound on the volume would be correspondingly: we can lower bound the volume of a closed chain representing homology class X by $|X|^2/\max_{V \text{ split, } |V|=1}(V, X)$. Unfortunately, this at best only leads to a small improvement in the bound. We claim that

$$\max_{V \text{ split, } |V|=1}(V, X) \geq |X|/\sqrt{\binom{n}{q}}, \tag{34}$$

so that at best we would lower bound the volume by $\sqrt{\binom{n}{q}}|X|$, and since $\sqrt{\binom{n}{q}} < 2^{n/2}$, this leads to only a small improvement (recall that there are $N = p^{n/2}$ qubits and we choose $p >> 1$). To see Eq. 34, consider the orthogonal basis for $\wedge^q \mathbb{R}^n$ of vectors $x_1 \wedge \ldots \wedge x_q$ where $x_1, \ldots, x_q$ are chosen from the n different coordinate directions. These basis vectors are all split. Since $\wedge^q \mathbb{R}^n$ is $\binom{n}{q}$-dimensional, there must be some basis vector V such that $|(V, X)| \geq |X|/\sqrt{\binom{n}{q}}$. Using this vector V (or its negation if the inner product (V, X) is negative) in the maximum gives Eq. (34).

The Rankin invariant is the minimal value of the norm $|X|$ over nonzero split vectors. Thus, the results on the Rankin invariant give a lower bound on the volume of representatives of split homology classes. However, in Ref. [8], it was shown that for certain lattices L the shortest nonzero vector in $\wedge^m L$ may be shorter than the Rankin invariant. Interestingly, the lattices we consider here provide another example where this occurs; in fact this occurs for any lattice with sufficiently large Rankin invariant.

▶ **Lemma 28.** *Let L be a rank-n lattice. Then, the shortest nonzero vector in $\wedge^m L$ has norm at most $\sqrt{\gamma_{\binom{n}{m}}}\text{vol}(L)^{m/n}$, where $\gamma_{\binom{n}{m}}$ denotes Hermite's constant in dimension $\binom{n}{m}$.*

Hence, if $\gamma_{n,m}(L) \geq \gamma_{\binom{n}{m}}$, then the shortest vector is not split.

Proof. We have $\text{vol}(\wedge^m L) = \text{vol}(L)^{\binom{n-1}{m-1}}$ by Proposition 1.10.4 of Ref. [21]. The lattice $\wedge^m L$ has rank $r = \binom{n}{m}$, and so the shortest nonzero vector in $\wedge^m L$ has length at most $\sqrt{\gamma_r}\text{vol}(\wedge^m L)^{1/r}$, where γ_r is Hermite's constant. So, the shortest nonzero vector in $\wedge^m L$ has length at most

$$\sqrt{\gamma_r}\text{vol}(L)^{\binom{n-1}{m-1}/\binom{n}{m}} = \sqrt{\gamma_r}\text{vol}(L)^{m/n}. \tag{35}$$

◀

For all r, we have $\gamma_r \leq 1 + r/4$, with an asymptotic behavior $\gamma_r \lesssim \frac{2r}{\pi e}$[22]. So, $\sqrt{\gamma_{\binom{n}{m}}} \leq \sqrt{1 + \binom{n}{m}/4}$. So, lemma 28 has an interesting interpretation for the application to quantum codes. If the bound in lemma 27 is saturated so that the least volume cycle representing a homology class has volume $|X|$, then we find that the code has roughly square-root distance. Thus, conjecture 1 implies that for some homology classes, the bound of lemma 27 is far from saturated. The possible improvement of Eq. (34) leads to only a small improvement here (though, it is possible that if the possible improvement of Eq. (34) holds for the homology classes with smallest $|X|$ and if the bound of lemma 28 is saturated then one might be able to prove a slightly above square-root distance for integer homology).

6   Quantum Locally Testable Codes from High-Dimensional Constructions

In this section, we give a construction of quantum codes which are "locally testable" [1] using high-dimensional constructions. The construction uses a different topology than above; the similarity in the constructions is simply that in both cases we consider a family of codes derived from manifolds of varying dimension, with the number of qubits in the code depending exponentially on the dimension of the manifold.

Let us write $\mathrm{wt}(O)$ to indicate the weight of an operator O. Similarly, given a vector v (in one of the vector spaces defining the chain complexes), we let $\mathrm{wt}(v)$ denote the number of nonzero entries in v.

Given a CSS stabilizer code defined from a chain complex $\ldots \mathcal{C}_{q+1} \overset{\partial_{q+1}}{\to} \mathcal{C}_q \overset{\partial_q}{\to} \mathcal{C}_{q-1} \ldots$, with the qudits associated with q-cells and the Z-type and X-type stabilizers associated with $(q+1)$-cells and $(q-1)$-cells, respectively, we define soundness parameters $\epsilon_X(w), \epsilon_Z(w)$ as follows:

▶ **Definition 29.** Define

$$\epsilon_Z(w) = \min_{v \in \mathcal{C}_q, \mathrm{wt}(v)=w, \partial_q v \neq 0} \Big(\max_{u \in \mathcal{C}_q, \partial_q u = 0} \frac{\mathrm{wt}(\partial v)}{\mathrm{wt}(v+u)} \Big). \tag{36}$$

Define $\epsilon_X(w)$ similarly, with ∂_q replaced with ∂_{q+1}^T, where the superscript T denotes transpose.

Equivalently, consider the minimum over all Z-type operators O, such that O has weight w and such that O does not commute with at least one stabilizer, of the following quantity: take the maximum, over all Z-type operators P which commute with all stabilizers, of the ratio of the number of stabilizers which do not commute with O to the weight of $O + P$. This minimum is ϵ_Z.

The codes of Ref. [26] have distance $\Theta(\sqrt{N})$, stabilizer weight $\mathcal{O}(1)$ and have $\epsilon_{X,Z}(w)$ bounded away from zero for $w \lesssim \sqrt{N}$, as shown in Ref. [19]. It is unclear whether or not families of codes exist which have distance which is $\Omega(\sqrt{N})$ and stabilizer weight $\mathcal{O}(1)$ and which have $\epsilon_{X,Z}(w)$ bounded away from zero for *all* w.

Here we give a simple construction of a family of qubit codes with 2 encoded qubits and with distance $\Theta(\sqrt{N})$, $\epsilon_{X,Z}(w)$ only polylogarithmically small for all w, and with *logarithmic* weight stabilizers. We warm up with a construction of a qubit code family with no encoded qubits (and hence the notion of distance is meaningless for this code) but with $\epsilon_{X,Z}(w)$ bounded away from zero for all w and with logarithmic weight stabilizers; we call this the "simplex code". We then give the full construction, which is based on a product of hyperspheres.

6.1   Simplex Code

Of course, with no encoded qubits, there are some fairly trivial constructions of code with $\epsilon_{X,Z}$ strictly bounded away from zero. For example, one can take a code with N qubits and stabilizers $Z_1, Z_2, \ldots, Z_N$. Thus, every product of Z operators commutes with all stabilizers (and so $\epsilon_Z(w)$ is a minimum over an empty set), while clearly $\epsilon_X(w) = 1$ for all w. However, the simplex code construction that we give obeys Poincare duality and has an entangled ground state.

The code we consider is obtained by taking a toric code on a n-dimensional sphere, with the degrees of freedom on q-cells for $q = n/2$. The exact value of q is not very important;

the important thing is that q/n is neither close to 0 nor close to 1 so that the number of q-cells will be exponential in n. However, the case $q = n/2$ is the self-dual case so this makes the proofs slightly simpler as we need to consider only one type of stabilizer.

The cellulation of the n-sphere that we use is to take the boundary of a $n+1$-dimensional simplex. We label the 0-cells by integers $1, \ldots, n+2$. For $0 \leq r \leq n$, there are $\binom{n+2}{r+1}$ distinct r-cells, labelled by subsets of $\Lambda \equiv \{1, \ldots, n+2\}$ with $r+1$ elements. We use qubits so the vector spaces are all over $\mathbb{F}_2$.

For $1 \leq r \leq n$, the boundary operator ∂_r acting on an r-cell labelled by some $(r+1)$-element set $S \subset \Lambda$ gives the sum of $r+1$ different $(r-1)$-cells, labelled by the distinct r-element subsets of S. For example, for $n \geq 2$, $\partial_2\{1,2,3\} = \{1,2\} + \{1,3\} + \{2,3\}$. We set $\partial_0 = 0$. One may verify that $\partial_{r-1}\partial_r = 0$ for all r.

For $q = n/2$, there are $N = \binom{n+2}{n/2+1}$ qubits, so N is exponentially large in n. Remark: in previous sections, the number of qubits we also had an exponential factor p^{n-k} which, for large p, was the dominant exponential scaling; in this subsection, we do not have such a factor.

Each qubit is acted on by $q+1$ stabilizers (as each q-cell has $q+1$ cells in its boundary) and each stabilizer acts on $q+2$ different qubits (as each $(q+1)$-cell has $q+2$ cells in its boundary and each $(q-1)$-cell has $q+2$ cells in its coboundary). Hence, the weight is indeed logarithmic in N, $w = (1/2 + o(1)) \cdot \log_2(N)$.

Finally, we show soundness. First, let us introduce notation.

▶ **Definition 30.** Given an r-cell σ labelled by some set S and a set $T \subset \Lambda$, we define $r \cup T$ to equal 0 if $S \cap T \neq \emptyset$ and otherwise $r \cup T$ is the $r + |T|$-cell labelled by $S \cup T$.

Given a vector $v \in \mathcal{C}_r$, we define $v \cup T$ by linearity. $v \cup T \in \mathcal{C}_{r+|T|}$ and the coefficient of $v \cup S$ corresponding to an $r + |T|$-cell labelled by a set U is equal to the coefficient of v corresponding to the r-cell labelled by $U \setminus T$ if $T \subset U$ and is equal to 0 is $T \not\subset U$.

▶ **Lemma 31.** *For the simplex code, for all w, $\epsilon_X(w) = \epsilon_Z(w) \geq 1$.*

Proof. Consider any $v \in \mathcal{C}_q$ with $\partial_q v \neq 0$. Set $w = (\partial_q v) \cup \{1\}$. Then, one may verify that $\partial_q x = \partial_q v$ (and hence, setting $w = x - v$, $\partial_q w = 0$) and that $\text{wt}(x) \leq \text{wt}(\partial_q v)$.   ◀

The proof of soundness above has a very simple geometric interpretation. We take the boundary $\partial_q v$ and shrink it to a point (arbitrarily choosing the vertex $\{1\}$ as the point that we shrink it to).

6.2   Hypersphere Product Code

The above construction had constant soundness, but had no encoded qubits. We now give a different construction with 2 encoded qubits and distance $\sqrt{N}$ and inverse polylogarithmic soundness. We now consider the toric code on a product of spheres, $S^n \times S^n$.

We pick an integer $p \geq 1$ (p need not be prime); p will be chosen to equal $\log(N)$ below in order to achieve square-root distance. We choose a cellulation of S^n as follows: consider an $(n+1)$-dimensional hypercube of side length p on each side (we call this the "large" hyercube). Cellulate that large hypercube using hypercubes of side length 1 on each side; we call these the "small" hypercubes) (so that there are p^{n+1} small hypercubes in the cellulation). Then, take the boundary of the hypercube to get a cellulation of S^n.

A small $(n+1)$-dimensional hypercube has $\binom{n+1}{r}2^{n+1-r}$ different r-cells in its boundary (each r-cell is a product of 1-cells in r out of the $n+1$ directions and then for each of the remaining directions there are 2 possible choices of 0-cells). The number of r-cells in the

cellulation of the large hypercube is $\binom{n+1}{r}(p+1)^{n+1-r}p^r$. To see this, assign coordinates $[0,p]$ for each side of the large hypercube. Then, each r-cell is a product of 1-cells in r out of the $n+1$ directions with 0-cells in the remaining directions. The midpoints of the 1-cells are at half-integer coordinate in the interval $[0,p]$ and so there are p possible choices for each cell. There are $p+1$ possible choices for the coordinates of each 0-cell as these cells are at integer coordinates in the interval $[0,p]$. To determine the number of r-cells in the boundary of the large hypercube, restrict to the case that in at least one of the directions, the coordinate must be 0 or p. This gives the number equal to

$$\binom{n+1}{r}(p+1)^{n+1-r}p^r\left(1 - (\frac{p+1-2}{p+1})^{n+1-r}\right),$$

where the ratio in parenthesis $\frac{p+1-2}{p+1}$ is the probability that for a random integer coordinate in the range $[0,p]$, the coordinate is not on the boundary 0 or p. Thus, there are at most $2^{(1-o(1))\cdot n}p^n$ cells (if $n >> p$) and at least $2^{1-o(1))\cdot n}p^{n-1}$ cells (if $n << p$).

We take the product of this cellulation with itself to get a cellulation of $S^n \times S^n$. The degrees of freedom will be on the q-cells for $q = n$, so that N is again exponential in n. We have $\log_2(N) = 2(1 + \log_2(p) + o(1)) \cdot n$ for $n >> p$ and $\log_2(N) = 2(1 + \log_2(p) + o(1)) \cdot n - 2\log_2(p)$ for $n << p$. We will take $p = 1/\log(N), n = \Theta(\log(N)/\log(\log(N)))$.

Each qubit is acted on by $2n$ stabilizers and each stabilizer acts on $2(n+1)$ qubits. Hence, the weight is logarithmic in N, $w = \Theta(\log(N)/\log(\log(N)))$.

The number of encoded qubits is equal to 2, as can be computed from the homology of $S^n \times S^n$ (by the Künneth formula, $H_i(S^n \times S^n; \mathbb{Z}_2) = 2$ for $i = n$, $H_i(S^n \times S^n; \mathbb{Z}_2) = 1$ for $i = 0, 2n$, and $H_n(S^n \times S^n; \mathbb{Z}_2) = 0$ otherwise).

▶ **Lemma 32.** *For the hypersphere product code,*

$$d_X(w) = d_Z(w) = (p+1)^{n+1}\left(1 - (\frac{p+1-2}{p+1})^{n+1}\right) = \Theta(N^{\frac{p}{p+2}}). \tag{37}$$

For $p = \Omega(\log(N))$,

$$d_X(w) = d_Z(w) = \Theta(\sqrt{N}). \tag{38}$$

Proof. Let a be a 0-cell in the second S^n in the product $S^n \times S^n$. Let $Z(a,2)$ be the logical Z operator which is the product Z_i over all i which are the product of an n-cell in the first S^n with 0-cell a. Then, any logical X operator which anticommites with $Z(a,2)$ must have some support on some cell i which is a product of an n-cell in the first S^n with 0-cell a. However, since $Z(a,2)$ and $Z(b,2)$ are homologous for any two choices of 0-cells a,b in the second S^n ($Z(a,2), Z(b,2)$ differ by a product of stabilizers), that logical X operator must have some support on some cell i which is a product of an n-cell in the first S^n with 0-cell a for *all* 0-cells a in the second S^n. Hence, that logical X operator must have a number of cells in its support equal to the number of 0-cells in the second S^n. This number is equal to $(p+1)^{n+1}\left(1 - (\frac{p+1-2}{p+1})^{n+1}\right)$.

This number is also an upper bound to $d_X(w)$, since the product of X over all cells which are a product of a fixed n-cell in the first S^n with an arbitrary 0-cells in the second S^n is a logical operator.

We can similarly lower bound the number of cells in the support of any logical X operator which anticommutes with the operator $Z(a,1)$, defined to be the logical Z operator which is the product Z_i over all i which are the product of an n-cell in the *second* S^n with 0-cell a in the *first* S^n. ◀

We now show soundness. Again, the geometric interpretation is to shrink the boundary to a point.

▶ **Lemma 33.** *For the hypersphere product code, $\epsilon_X(w) = \epsilon_Z(w) \geq \Omega(1/\log(N)^2)$.*

Proof. Consider any $v \in \mathcal{C}_q$ with $\partial_q v \neq 0$.

We place coordinates $[0, p]^{n+1}$ on the first large hypercube. Call the face where the first coordinate is equal to p the "top face". Call the face where the first coordinate is equal to 0 the "bottom face". Let $v_0 = v$. We will construct a sequence $v_1, v_2, \ldots, v_f \in \mathcal{C}_q$ for some integer f where we bound $\mathrm{wt}(v_{i+1} - v_i)$ with the final vector $v_f = 0$. In this way, we will bound $\mathrm{wt}(v_0)$. We construct the sequence so that the boundaries $\partial_q v_i$ are first removed from the top face of the first hypercube, then moved from the top face to the bottom face of the first hypercube, and finally moved to a point on the bottom face of the first hypercube.

Throughout this proof, when we refer to coordinates, we refer to the first hypercube in the product. We regard an r-cell as being a product of 0-cells and 1-cells. That is, each cell in the product of hypercubes is product of cells in each hypercube. Then, each r-cell in a hypercube is a product of r 1-cells and $n + 1 - r$ 0-cells. The $n + 1$ different terms in the product correspond to different coordinates. When we say that a cell "is a 0-cell" in a given coordinate, we mean that the cell is a product of a 0-cell in that coordinate with some cells in other coordinates.

We first explain the middle step, moving from top face to bottom face. Suppose that some v_i has $\partial_q v_i$ vanishing on the top face. Indeed, suppose that $\partial_q v_i$ vanishes if the first coordinate is greater than x, for some integer x. Then, let $\pi_x(\partial_q v_i)$ be the projection of $\partial_q v_i$ onto cells with first coordinate equal to x. This projection consists only of cells which are 0-cells in the first coordinate. Let $v_{i+1} - v_i$ be defined by taking $\pi_x(\partial_q i)$ and replacing every 0-cell in the first coordinate at position x with a 1-cell at position $x - 1/2$. Then, $\pi_x(\partial_q v_{i+1}) = 0$. Iterating this procedure, decreasing x from p, to $p - 1$, to $p - 2$, and so on, we can construct a sequence $v_i, v_{i+1}, \ldots$ so that the final vector in the second has boundary only on the bottom face. There are at most p steps in the sequence. Note that because $\partial^2 = 0$, once we ensure that $\pi_x(\partial_q v_i) = 0$, then we know that $\partial_q v_i$ has not cells which are 1-cell in the first coordinate with midpoint as $x - 1/2$.

Now we explain the first step, moving the boundary off the top face. We apply above the above procedure to the *second* coordinate. We let $\pi_{p,x}(\partial_q v_i)$ be the projection $\partial_q v_i$ onto cells with first coordinate equal to p and second coordinate equal to x, for integer x. We then construct a sequence so that this projection vanishes for $x = p, p - 1, \ldots$, following the same procedure as in the above paragraph. There are at most p steps in this sequence. We then repeat this for the second coordinate, third coordinate, and so on; giving at most pn steps.

The final step is the same as the first step, with the top face replaced by the bottom face.

So, there are at most $\mathcal{O}(pn)$ steps in the sequence. We have $\mathrm{wt}(\partial_q v_i) \leq \mathrm{wt}(\partial_q v)$ for all vectors in the sequence, and there are at most $\mathcal{O}(pn)$ steps, so this gives $\epsilon_X(w) \geq \Omega(1/pn) = \Omega(1/\log(N)^2)$. ◀

In the above construction, we lost a factor of n due to having n steps in the sequence to move the boundary. Likely for this construction, this factor cannot be avoided since the diameter of the hypercube is pn. One might wonder whether other geometries (such as a geometry that more closely approximates a sphere) would improve on this factor; note however that since the volume of a sphere of radius r in n-dimensional Euclidean space scales roughly as $(r/n)^{n/2}$, one would need to take the radius proportional to n in order to obtain a large volume so again one would need to have a large diameter for the geometry.

7 Discussion

We have presented several different code constructions based on the toric code on families of higher-dimensional manifolds. Rather than varying the geometry or topology at fixed dimension, as is more commonly done, we have considered varying dimension. This leads to a scaling in which the number of qubits, N, scales exponentially with dimension, n, so that the weight of the stabilizers w is proportional $n \propto \log(N)$. Assuming conjecture 1, we have constructed a code family with almost linear distance and logarithmic weight.

References

1 Dorit Aharonov and Lior Eldar. Quantum locally testable codes. *SIAM Journal on Computing*, 44(5):1230–1262, 2015.

2 Ivan Babenko and Mikhail Katz. Systolic freedom of orientable manifolds. *Annales scientifiques de l'Ecole normale supérieure*, 31(6):787–809, 1998. `doi:10.1016/S0012-9593(99)80003-2`.

3 Dave Bacon, Steven T Flammia, Aram W Harrow, and Jonathan Shi. Sparse quantum codes from quantum circuits. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, pages 327–334. ACM, 2015.

4 H. Bombin and M. A. Martin-Delgado. Homological error correction: Classical and quantum codes. *Journal of Mathematical Physics*, 48(5):052105, may 2007. `doi:10.1063/1.2731356`.

5 Sergey Bravyi and Matthew B Hastings. Homological product codes. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 273–282. ACM, 2014.

6 A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105, aug 1996. `doi:10.1103/physreva.54.1098`.

7 John Horton Conway and Neil James Alexander Sloane. *Sphere packings, lattices and groups*, volume 290. Springer Science & Business Media, 2013.

8 Renaud Coulangeon. Minimal vectors in the second exterior power of a lattice. *Journal of algebra*, 194(2):467–476, 1997.

9 Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill. Topological quantum memory. *Journal of Mathematical Physics*, 43(9):4452–4505, 2002.

10 Uri Erez, Simon Litsyn, and Ram Zamir. Lattices which are good for (almost) everything. *IEEE Transactions on Information Theory*, 51(10):3401–3416, 2005.

11 Herbert Federer and Wendell H Fleming. Normal and integral currents. *Annals of Mathematics*, 72:458–520, 1960.

12 Federer-Fleming deformation theorem. Encyclopedia of Mathematics. URL: `http://www.encyclopediaofmath.org/index.php?title=Federer-Fleming_deformation_theorem&oldid=28190`.

13 Michael H. Freedman and David A. Meyer. Projective plane and planar quantum codes. *Foundations of Computational Mathematics*, 1(3):325–332, jul 2001. `doi:10.1007/s102080010013`.

14 Michael H Freedman, David A Meyer, and Feng Luo. Z2-systolic freedom and quantum codes. *Mathematics of quantum computation, Chapman & Hall/CRC*, pages 287–320, 2002.

15 Robert Gallager. Low-density parity-check codes. *IRE Transactions on information theory*, 8(1):21–28, 1962.

16   Nicolas Gama, Nick Howgrave-Graham, Henrik Koy, and Phong Q Nguyen. Rankin?s constant and blockwise lattice reduction. In *Annual International Cryptology Conference*, pages 112–130. Springer, 2006.

17   Reese Harvey and H Blaine Lawson. Calibrated geometries. *Acta Mathematica*, 148(1):47–157, 1982.

18   A.Yu. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2–30, jan 2003. `doi:10.1016/s0003-4916(02)00018-0`.

19   Anthony Leverrier, Jean-Pierre Tillich, and Gilles Zémor. Quantum expander codes. In *Foundations of Computer Science (FOCS), 2015 IEEE 56th Annual Symposium on*, pages 810–824. IEEE, 2015.

20   David JC MacKay. Good error-correcting codes based on very sparse matrices. *IEEE transactions on Information Theory*, 45(2):399–431, 1999.

21   Jacques Martinet. *Perfect lattices in Euclidean spaces*, volume 327. Springer Science & Business Media, 2013.

22   John Willard Milnor and Dale Husemoller. *Symmetric bilinear forms*, volume 60. Springer, 1973.

23   David Poulin. Stabilizer formalism for operator quantum error correction. *Physical review letters*, 95(23):230504, 2005.

24   Robert Alexander Rankin. On positive definite quadratic forms. *Journal of the London Mathematical Society*, 1(3):309–314, 1953.

25   Wolfgang M Schmidt et al. Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height. *Duke Mathematical Journal*, 35(2):327–339, 1968.

26   Jean-Pierre Tillich and Gilles Zémor. Quantum ldpc codes with positive rate and minimum distance proportional to $n^{1/2}$. *arXiv preprint arXiv:0903.0566*, 2009.