COMMUTING PAULI HAMILTONIANS AS MAPS BETWEEN FREE MODULES

JEONGWAN HAAH

Abstract. We study unfrustrated spin Hamiltonians that consist of commuting tensor products of Pauli matrices. Assuming translation-invariance, we observe that the Hamiltonian is described by a map between modules over the translation group algebra, so homological methods are applicable. We show universal properties of topologically ordered phases in low spatial dimensions. Particularly, we prove that in three dimensions there exists a point-like charge that can be isolated with energy barrier at most logarithmic in the separation distance. The isolation is due to a fractal operator. We also develop tools to compute the ground state degeneracy and to handle local unitary transformations.

Contents

Commuting Pauli Hamiltonians form a small class of Hamiltonians that are consisted of products of Pauli matrices such that each term commutes with any other terms. Classical examples are the Ising models in one or two dimensions.

Date: 24 April 2012.

The author is supported in part by the Institute for Quantum Information and Matter, an NSF Physics Frontier Center, and the Korea Foundation for Advanced Studies.

Albeit its simplicity of the energy spectrum, there are many intriguing models in this class for which the long range entanglement of the ground state plays a very important role. Prototypical is the Kitaev toric code model [1], which has been a solid testbed of ideas for topologically ordered systems.

The topological ordered models exhibit, as the name suggests, many properties that are insensitive local changes or defects. They had been discussed for the states of the fractional quantum Hall effects and the spin liquids; see e.g. Wen [2]. Perhaps, the most well-defined characteristic of the topological order is the local indistinguishability of the degenerate ground states; two different ground states gives the same expectation value for any local observables. (Note that this characteristic is not directly applicable to e.g. the topological insulators [3], for which certain symmetry properties distinguish them from trivial phases.) Due to the local indistinguishability, the topologically ordered systems are thought to be candidate media on which quantum information processing is performed. As a special application, the topologically ordered system can be used as a quantum memory, just like the ferromagnetic system is used as a classical memory.

However, the quantum memories in the topologically ordered systems often suffer from thermal instability. For example, the toric code model has point-like excitations, which can freely propagate by external noise from the thermal bath. Although a local operator can never access to the ground space, their accumulation may be able to. Indeed, by the thermal fluctuation, a ground state is often mapped to a different state, and the anticipated protection of the stored quantum information is not viable. The excitations that affects the stability of the quantum memory may be called "topological charges". A charge is an excitation that cannot be created alone locally but can be created with some other excitations. Indeed, the 4D toric code [4] has no charge at all, and can be used as a quantum memory whose failure probability decreases exponentially with the system size at low enough temperatures [5, 6].

The situation in three dimensions is more subtle but interesting. Models like 3D toric code model have charges that can freely propagate across the system by the interaction with the thermal bath, thereby two different ground states become mixed. On the other hand, as in the cubic code [7, 8, 9], there can exist charges that cannot propagate by any means. This class of models provides modest reliability as a quantum memory at nonzero temperature. However, the scaling of the memory time, until which the system is reliable as a memory medium, is not as favorable as it is for the 4D toric code model; the memory time grows with the system size according to a power law whose exponent is proportional to the inverse temperature, provided that the system size does not exceed some critical value determined by the temperature.

The very existence of the charges seems to adversely affect the memory time. In order to have a quantum memory, one needs to devise a read-out procedure explicitly — a classical analog is the measurement of the average magnetization of 2D Ising model. Though the charges may not propagate, they can be separated arbitrary far from their partner charges at a modest energy cost [8]. It may sound contradictory, but crucial is that a set of charges can expand only in a highly restrictive way. No good read-out procedure (sometimes called decoder) is known for the configurations of far separated charges. This should be contrasted to the 4D toric code model, in which any excited state consists of several loops. The large loops are suppressed by the Boltzmann factor, and the small loops can be almost perfectly treated by the read-out procedure. In short, the large entropy due to the point-likeness of the charges would likely drag the ground state to a hard-to-decipher state. See the discussion in [9].

Apart from the issue of the thermal stability and the possibility of quantum memory, the cubic code model apparently necessitates new tools to analyze it. When defined on a finite system with periodic boundary conditions, it shows exotic dependence of the ground state degeneracy on the system size. The degeneracy is sensitive to the number theoretic property of the linear system size L. For example, when L is a power of 2, the degeneracy grows exponentially with L, but becomes a constant if $L = 2^p + 1$. This was a numerical observation, and was not rigorously treated [7].

Results

In this paper, we systematically study commuting Pauli Hamiltonians that are translation-invariant. We always assume that our Hamiltonians are frustration-free; every term in the Hamiltonian is minimized on the ground space.

The main observation is that there is a purely algebraic description of commuting Pauli Hamiltonians in terms of maps between free modules over a Laurent polynomial ring by exploiting the translation-invariance. A Pauli matrix can be written as two binary numbers if we ignore the phase factors. For example, $I = (00), \sigma_x = (10), \sigma_z = (01), \sigma_y = (11)$. We write these binary numbers in the coefficients of Laurent polynomials. The exponents of the Laurent polynomials will represent the positions at which the Pauli matrices act. If the Hamiltonian is translation-invariant, and there are finitely many distinct interaction types, then it follows that only a finite number of the Laurent polynomials convey all data of the Hamiltonian. We view this finite data as a map between two free modules over the translation group algebra. We will show that the physical phase is solely determined by the image of this associated map.

We provide a few tools to compute the transformations of the Hamiltonians by local unitary operators and coarse-graining. They come down to a well-defined set of elementary row operations on the matrices associated to the Hamiltonians. As we restrict our scope to the commuting Pauli Hamiltonians, the local unitary operators are also restricted to the Clifford operators. (Clifford operators maps a tensor product of Pauli operators to a tensor product of Pauli operators.)

We define the characteristic dimension d associated to the Hamiltonian. If a Hamiltonian gives rise to a map between free modules, it is natural to think of the determinantal ideal of this map. The characteristic dimension is the Krull dimension of the algebraic set defined by this ideal. It is always upper bounded by the spatial dimension D. Moreover, d is less than or equal to $D - 2$ if the Hamiltonian is locally topologically ordered.

The characteristic dimension d controls the rate at which the ground state degeneracy may increase. Roughly speaking, the logarithm of degeneracy can grow like L^d where L is the linear system size. Thus, $D = 3$ is the minimal spatial dimension such that the degeneracy of a topologically ordered system can be diverging. For instance, the toric code models in various dimensions all correspond to the characteristic dimension 0, while the 3D cubic code model has characteristic dimension 1. However, it should be pointed out that the actual degeneracy does not behave as smooth as the function L^d; it can depend very sensitively on the system size.

Indeed, it shall be shown that the degeneracy is related to the number of points in an algebraic set. The boundary condition imposes a global constraint on the relevancy of the points in the algebraic set. The numerically observed phenomena for the cubic code model shall be exactly calculated.

In one dimension, we completely classify translation-invariant commuting Pauli Hamiltonians. We algorithmically show how to transform an arbitrary Hamiltonian into several copies of the Ising models.

In two dimensions, we characterize how the charges behave for topologically ordered models. Specifically, we prove that any excited state is a configuration of finitely many kinds of the charges, and the charges can be moved to an arbitrary position by a string operator. The result is a refined formulation of that of Bombin et al [10, 11].

In three dimensions, we prove that there always exists a point-like charge for any locally topologically ordered translation-invariant commuting Pauli Hamiltonian. A charge can be separated arbitrarily far from its partners by a local process with energy cost at most logarithmic in the separation distance. Here, the local process means a sequence of Pauli operators that are obtained by successive applications of single qubit Pauli operators. This is a fundamental property of the three dimensions. It suggests that we might not be able to have a topologically ordered system in three dimensions where the excitations are all loop-like as in 4D toric code model.

Our language is not completely new. A similar one appears in the error correcting code theory of computer science in the topic of multi-dimensional cyclic codes; see e.g. [12] and references therein. Also, there is an algebraic-geometry based design like Goppa codes [13]. However, the focus is different: We are interested in a fixed set of generators and exact sequences of modules describing the topological order. The fact that the commuting Pauli operators are represented as matrix, is very well-known in the theory of quantum error correcting codes. Our treatment is different in that the entries are not the binary values but the Laurent polynomials.

Only the system of qubits, or spin-1/2, will be discussed, but all of our results and argument straight-forwardly generalize to the system of qudits of prime dimensions. Technically, the ground field $\mathbb{F}_2$ for the qubit should be replaced by $\mathbb{F}_p$ for a prime integer p. Only important is that the ground field is finite. Some numerical value 2 should be replace by the characteristic p of the field. With this generalization in mind, we keep necessary minus $(-)$ signs in the statements, which should be ignored for qubits. Examples in this direction can be found in [14].

We start by deriving the matrix representation of commuting Pauli Hamiltonian, and explain in detail how the translation-invariance is exploited. The notion of modules over the translation-group algebra shall naturally emerge. Then, the operations on modules are induced by those on physical Hilbert space. They will define an equivalence relation between Hamiltonians. We move on to the topological orders and translate the conditions into those on a complex of modules. Consequences of the topological order condition in two and three spatial dimensions will be derived. Explicit calculations and more examples are presented in the last section. All ring in the current paper shall be commutative with 1.

$\mathbb{F}_2$	binary field $\{0,1\}$
D	spatial dimension
R	$\mathbb{F}_2[x_1, x_1^{-1}, \ldots, x_D, x_D^{-1}]$
$\mathfrak{b}_L$	ideal $(x_1^L - 1, \ldots, x_D^L - 1)$
q	number of qubits per site
t	number of interaction types
G	free R-module of the interaction labels (rank t)
P	free R-module of Pauli operators (rank $2q$)
E	free R-module of excitations (rank t)
σ	$G \to P$, generating matrix or map for the stabilizer module
ϵ	$P \to E$, generating matrix or map for excitations
$r \mapsto \bar{r}$	antipode map of the group algebra R.
$\dagger$	transpose followed by antipode map
λ_q	anti-symmetric $2q \times 2q$ matrix $\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$

TABLE 1. Reserved symbols. Any ring in this paper is commutative with 1.

1. ALGEBRAIC STRUCTURE OF COMMUTING PAULI HAMILTONIANS

1.1. **Pauli group as a vector space.** The Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

satisfy

$$\sigma_a \sigma_b = i\varepsilon_{abc}\sigma_c, \quad \{\sigma_a, \sigma_b\} = 2\delta_{ab}.$$

Thus, the Pauli matrices together with scalars $\pm 1, \pm i$ form a group under multiplication. Given a system of qubits, the set of all possible tensor products of the Pauli matrices form a group, where the group operation is the multiplication of operators. If the system is infinite, physically meaningful operators are those of finite support, i.e., acting on all but finitely many qubits by the identity. We shall only consider this Pauli group of finite support, and call it simply the *Pauli group*. An element of the Pauli group is called a *Pauli operator*.

Since any two elements of the Pauli group either commute or anti-commute, ignoring the phase factor altogether, one obtains an *abelian* group. Moreover, since any element O of the Pauli group satisfies $O^2 = \pm I$, An action of $\mathbb{Z}/2\mathbb{Z}$ on Pauli group modulo phase factors $P/\{\pm 1, \pm i\}$ is well-defined, by the rule $n \cdot O = O^n$ where $n \in \mathbb{Z}/2\mathbb{Z}$. For $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ being a field, $P/\{\pm 1, \pm i\}$ becomes a vector space over $\mathbb{F}_2$. The group of single qubit Pauli operators up to phase factors is identified with the two dimensional $\mathbb{F}_2$-vector space. If Λ is the index set of all qubits in the system, the whole Pauli group up to phase factors is the direct sum $\bigoplus_{i \in \Lambda} V_i$ where V_i is the vector space of the Pauli operators for the qubit at i. Explicitly, $I = (00), \sigma_x = (10), \sigma_z = (01), \sigma_y = (11)$. A multi-qubit Pauli operator is written as a finite product of the single qubit Pauli operators, and hence is written as a binary string in which all but finitely many entries are zero. A pair of entries of the binary string describes a single qubit component in the tensor product expression. The multiplication of two Pauli operators corresponds to entry-wise addition of the two binary strings modulo 2.

The commutation relation may seem at first lost, but one can recover it by introducing a symplectic form [15]. Let $\lambda_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ be a symplectic form on the vector space $(\mathbb{F}_2)^2$ of a single qubit Pauli operators. [1] One can easily check that the commutation relation of two Pauli matrices O_1, O_2 is precisely the value of this symplectic form evaluated on the pair of vectors representing O_1, O_2, respectively. Two multi-qubit Pauli operator (anti-)commutes if and only if there are (odd)even number of pairs of the anti-commuting single qubit Pauli operators in their tensor product expression. So, the two Pauli operator (anti-)commutes precisely when the value of the direct sum of symplectic form $\bigoplus_{q\in\Lambda} \lambda_1$ is (non-)zero. (Λ could be infinite but the form is well-defined since any vector representing a Pauli operator is of finite support.) We shall call the value of the symplectic form the *commutation value*.

1.2. **Pauli space on a group.** Let Λ be the index set of all qubits, and suppose now that Λ itself is an abelian group. There is a natural action of Λ on the Pauli group modulo phase factors induced from the group action of Λ on itself by multiplication. For example, if $\Lambda = \mathbb{Z}$, the action of Λ is the translation on the one dimensional chain of qubits. If $R = \mathbb{F}_2[\Lambda]$ is the group algebra with multiplicative identity denoted by 1, the Pauli group modulo phase factors acquires a structure of an R-module. We shall call it the *Pauli module*. The Pauli module is free and has rank 2.

Let $r \mapsto \bar{r}$ be the antipode map of R, i.e., the $\mathbb{F}_2$-linear map into itself such that each group element is mapped to its inverse. Since Λ is abelian, the antipode map is an algebra-automorphism. Let the coefficient of $a \in R$ at $g \in \Lambda$ be denoted by a_g. Hence, $a = \sum_{g\in\Lambda} a_g g$ for any $a \in R$. One may write $a_g = (a\bar{g})_1$.

Define

$$\mathrm{tr}(a) = a_1$$

for any $a \in R$.

Proposition 1.1. *Let $(a, b), (c, d) \in R^2$ be two vectors representing Pauli operators O_1, O_2 up to phase factors:*

$$O_1 = \left(\bigotimes_{g\in\Lambda} (\sigma_x^{(g)})^{a_g} \right) \left(\bigotimes_{g\in\Lambda} (\sigma_z^{(g)})^{b_g} \right),$$

$$O_2 = \left(\bigotimes_{g\in\Lambda} (\sigma_x^{(g)})^{c_g} \right) \left(\bigotimes_{g\in\Lambda} (\sigma_z^{(g)})^{d_g} \right)$$

where $\sigma^{(g)}$ denotes the single qubit Pauli operator at $g \in \Lambda$. Then, O_1 and O_2 commute if and only if

$$\mathrm{tr}\left(\begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} \right) = 0.$$

[1] The minus sign is not necessary for qubits, but is for qudits of prime dimensions

Proof. The commutation value of $(\sigma_x^{(g)})^n(\sigma_z^{(g)})^m$ and $(\sigma_x^{(g)})^{n'}(\sigma_z^{(g)})^{m'}$ is $nm' - mn' \in \mathbb{F}_2$. Viewed as pairs of group algebra elements, $(\sigma_x^{(g)})^n(\sigma_z^{(g)})^m$ and $(\sigma_x^{(g)})^{n'}(\sigma_z^{(g)})^{m'}$ are (ng, mg) and $(n'g, m'g)$, respectively. We see that

$$nm' - mn' = \operatorname{tr}\left(\begin{pmatrix} ng^{-1} & mg^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} n'g \\ m'g \end{pmatrix} \right).$$

Since any Pauli operator is a finite product of these, the result follows by linearity. □

We wish to characterize a $\mathbb{F}_2$-subspace S of the Pauli module invariant under the action of Λ, i.e., a submodule, on which the commutation value is always zero. As we will see in the next subsection, this particular subspace yields a local Hamiltonian whose energy spectrum is exactly solvable, which is the main object of this paper. Let (a, b) be an element of $S \subseteq R^2 = (\mathbb{F}_2[\Lambda])^2$. For any $r \in R$, (ra, rb) must be a member of S. Demanding that the symplectic form on S vanish, by Proposition 1.1 we have

$$\operatorname{tr}(ra\bar{b} - rb\bar{a}) = 0.$$

Since r was arbitrary, we must have $a\bar{b} - b\bar{a} = 0$. [2] Let us denote $\begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix}$ as $\begin{pmatrix} a \\ b \end{pmatrix}^\dagger$, and write any element of R^2 as a 2×1 matrix. We conclude that S is a submodule of R^2 over R generated by $s_1, \ldots, s_t$ such that any commutation value always vanishes, if and only if

$$s_i^\dagger \lambda_1 s_j = 0$$

for all $i, j = 1, \ldots, t$.

The requirement that Λ be a group might be too restrictive. One may have a coarse group structure on Λ, the index set of all qubits. We consider the case that the index set is a product of a finite set and a group. By abuse of notation, we still write Λ to denote the group part, and insist that to each group element are associated q qubits ($q \geq 1$). Thus obtained Pauli module should now be identified with R^{2q}, where $R = \mathbb{F}_2[\Lambda]$ is the group algebra that encodes the notion of translation. We write an element v of R^{2q} by a $2q \times 1$ matrix, and denote by $v^\dagger$ the transpose matrix of v whose each entry is applied by the antipode map. We always order the entries of v such that the upper q entries describes the σ_x-part and the lower the σ_z-part. Since the commutation value on R^{2q} is the sum of commutation values on R^2, we have the following: If S is a submodule of R^{2q} over R generated by $s_1, \ldots, s_t$, the commutation value always vanishes on S, if and only if for all $i, j = 1, \ldots, t$

$$s_i^\dagger \lambda_q s_j = 0$$

where $\lambda_q = \begin{pmatrix} 0 & \mathrm{id}_q \\ -\mathrm{id}_q & 0 \end{pmatrix}$ is a $2q \times 2q$ matrix.

Let us summarize our discussion so far.

Proposition 1.2. *On a set of qubits $\Lambda \times \{1, \ldots, q\}$ where Λ is an abelian group, the group of all Pauli operators of finite support up to phase factors, form a free module $P = R^{2q}$ over the group algebra $R = \mathbb{F}_2[\Lambda]$. The commutation value*

$$\langle a, b \rangle = \operatorname{tr}(a^\dagger \lambda_q b)$$

[2] A symmetric bilinear form $\langle r, s \rangle = \operatorname{tr}(r\bar{s})$ on R is non-degenerate.

for $a, b \in P$ is zero if and only if the Pauli operators corresponding to a and b commute. If σ is a $2q \times t$ matrix whose columns generate a submodule $S \subseteq P$, then the commutation value on S always vanishes if and only if

$$\sigma^\dagger \lambda_q \sigma = 0.$$

1.3. **Local Hamiltonians on groups.** Recall that we place q qubits on each *site* of Λ. The total system of the qubits is $\Lambda \times \{1, \ldots, q\}$.

Definition 1. Let

$$H = -\sum_{g \in \Lambda} h_{1,g} + \cdots + h_{t,g}$$

be a local Hamiltonian consisted of Pauli operators that is (i)commuting, (ii) translation-invariant up to signs, and (iii) frustration-free. We call H a *code Hamiltonian* (also known as *stabilizer Hamiltonian*). The *stabilizer module* of H is the submodule of the Pauli module P generated by the images of $h_1, \ldots, h_t$ in P. The number of *interaction types* is t.

The energy spectrum of the code Hamiltonian is trivial; it is discrete and equally spaced.

Example 1. One dimensional Ising model is the Hamiltonian

$$H = -\sum_{i \in \mathbb{Z}} \sigma_z^{(i)} \otimes \sigma_z^{(i+1)}.$$

The lattice is the additive group $\mathbb{Z}$, and the group algebra is $R = \mathbb{F}_2[x, \bar{x}]$. The Pauli module is R^2 and the stabilizer module S is generated by

$$\begin{pmatrix} 0 \\ 1+x \end{pmatrix}.$$

One can view this as the matrix σ of Proposition 1.2. H is commuting; $\sigma^\dagger \lambda_1 \sigma = 0$.

1.4. **Excitations.** For a code Hamiltonian H, an excited state is described by the terms in the Hamiltonian that have eigenvalues -1. Each of the flipped terms is interpreted as an *excitation*. Although the actual set of all possible configurations of excitations that are obtained by applying some operator to a ground state, may be quite restricted, it shall be convenient to think of a larger set. Let E be the set of configurations of all finite number of excitations without asking physical relevance. Since an excitation is by definition a flipped term in H, the set E is equal to the collection of all finite sets consisted of the terms in H.

If Pauli operators U_1, U_2 acting on a ground state creates excitations $e_1, e_2 \in E$, their product $U_1 U_2$ creates excitations $(e_1 \cup e_2) \setminus (e_1 \cap e_2)$. Here, we had to remove the intersection because each excitation is its own annihilator; any term in the H squares to the identity. Exploiting this fact, we make E into a vector space over $\mathbb{F}_2$. Namely, we take formal linear combinations of terms in H with the coefficient $1 \in \mathbb{F}_2$ when the terms has -1 eigenvalue, and the coefficient $0 \in \mathbb{F}_2$ when the term has $+1$ eigenvalue. The symmetric difference is now expressed as the sum of two vectors $e_1 + e_2$ over $\mathbb{F}_2$. In view of Pauli group as a vector space, $U_1 U_2$ is the sum of the two vectors $v_1 + v_2$ that respectively represents U_1, U_2. Therefore, the association $U_i \mapsto e_i$ induces a linear map from the Pauli space to the space of excitations E.

The set of all excited states obeys the translation-invariance as the code Hamiltonian H does. So, E is a module over the group algebra $R = \mathbb{F}_2[\Lambda]$. The association $U_i \mapsto e_i$ clearly respects this translation structure. Our discussion is summarized by saying that the excitations are described by an R-linear map

$$\epsilon : P \to E$$

from the Pauli module P to the *module of excitations* E.

As the excitation module is the collection of all finite sets of the terms in H, we can speak of the *module of generator labels* G, which is equal to E as an R-module. G is a free module of rank t if there are t types of interaction. The matrix σ introduced in Section 1.2 can be viewed as

$$\sigma : G \to P$$

from the module of generator labels to the Pauli module.

Proposition 1.3. *If σ is the generating map for the stabilizer module of a code Hamiltonian, then*

$$\epsilon = \sigma^\dagger \lambda_q .$$

Proof. This is a simple corollary of Proposition 1.2. Let $h_{i,g}$ be the terms in the Hamiltonian where $i = 1, \ldots, t$, and $g \in \Lambda$. In the Pauli module, they are expressed as gh_i where h_i is the i-th column of σ. For any $u \in P$, let $\epsilon(u)_i$ be the i-th component of $\epsilon(u)$. By definition,

$$\epsilon(u)_i = \sum_{g \in \Lambda} g \ \operatorname{tr}\left((gh_i)^\dagger \lambda_q u \right) = \sum_{g \in \Lambda} g \ \operatorname{tr}\left(\bar{g} h_i^\dagger \lambda_q u \right) = h_i^\dagger \lambda_q u$$

Thus, $h_i^\dagger \lambda_q$ is the i-th row of ϵ. □

Remark 1. The commutativity condition in Proposition 1.2 of the code Hamiltonian is recast into the condition that

$$G \xrightarrow{\sigma} P \xrightarrow{\epsilon} E$$

be a complex, i.e., $\epsilon \circ \sigma = 0$. Equivalently,

$$\operatorname{im} \sigma \subseteq (\operatorname{im} \sigma)^\perp = \ker \epsilon$$

where $\perp$ is with respect to the symplectic form.

2. Equivalent Hamiltonians

The stabilizer module entirely determines the physical phase of the code Hamiltonian in the following sense.

Proposition 2.1. *Let H and H' be code Hamiltonians on a system of qubits, and suppose their stabilizer modules are the same. Then, there exists a unitary*

$$U = \bigotimes_{g \in \Lambda} U_g$$

mapping the ground space of H onto that of H'. Moreover, there exist a continuous one-parameter family of gapped Hamiltonians connecting $UHU^\dagger$ and H'.

Proof. Let $\{p_\alpha\}$ be a maximal set of $\mathbb{F}_2$-linearly independent Pauli operators of finite support that generates the common stabilizer module S. $\{p_\alpha\}$ is not necessarily translation-invariant. Any ground state $|\psi\rangle$ of H is a common eigenspace of $\{p_\alpha\}$ with eigenvalues $p_\alpha |\psi\rangle = e_\alpha |\psi\rangle$, $e_\alpha = \pm 1$. Similarly, the ground space of H' gives the eigenvalues $e'_\alpha = \pm 1$ for each p_α.

The abelian group generated by $\{p_\alpha\}$ is precisely the vector space S, and the assignment $p_\alpha \mapsto e_\alpha$ defines a dual vector on S. If U is a Pauli operator of possibly infinite support, then $p_\alpha U |\psi\rangle = e''_\alpha e_\alpha U |\psi\rangle$ for some $e''_\alpha = \pm 1$, where e''_α is determined by the commutation relation between U and p_α. Thus, the first statement follows if we can find U such that the commutation value between U and p_α is precisely e''_α. This is always possible since the dual space of the vector space P is isomorphic to the direct product $\prod_{\Lambda \times \{1,\ldots,q\}} \mathbb{F}_2^2$, which is vector-space-isomorphic to the Pauli group of arbitrary support up to phase factors. [3]

Now, $UHU^\dagger$ and H' have the same eigenspaces, and in particular, the same ground space. Consider a continuous family of Hamiltonians

$$H(u, u') = uUHU^\dagger + u'H'$$

where $u, u' \in \mathbb{R}$. It is clear that

$$H = H(1,0) \to H(1,1) \to H(0,1) = H'$$

is a desired path. □

The criterion of Proposition 2.1 to classify the physical phases is too narrow. Physically meaningful universal properties should be invariant under simple and local changes of the system. More concretely,

Definition 2. Two code Hamiltonians H and H' are *equivalent* if their stabilizer modules become the same under a finite composition of symplectic transformations, coarse-graining, and tensoring ancillas.

We shall define the symplectic transformations, the coarse-graining, and the tensoring ancillas shortly.

2.1. Symplectic transformations.

Definition 3. A *symplectic transformation* T is an automorphism of the Pauli module induced by a unitary operator on the system of qubits such that

$$T^\dagger \lambda_q T = \lambda_q$$

where † is the transposition followed by the entry-wise antipode map.

Only the unitary operator on the physical Hilbert space that respects the translation can induce a symplectic transformation. By definition, a symplectic transformation maps each local Pauli operator to a local Pauli operator, and preserves the commutation value for any pair of Pauli operators.

Proposition 2.2. *Any two unitary operators U_1, U_2 that induces the same symplectic transformation differ by a Pauli operator (of possibly infinite support).*

[3] If V is a finite dimensional vector space over some field, the dual vector space of $\bigoplus_I V$ is isomorphic to $\prod_I V$ where I is an arbitrary index set.

Proof. The symplectic transformation induced by $U = U_1^\dagger U_2$ is the identity. Hence, U maps each single qubit Pauli operator $\sigma_{x,z}^{(g,i)}$ to $\pm\sigma_{x,z}^{(g,i)}$. By the argument as in the proof of Proposition 2.1, there exists a Pauli operator O of possibly infinite support that acts the same as U on the system of qubits. Since Pauli operators form a basis of the operator algebra of qubits, we have $O = U$. □

The effect of a symplectic transformation on the generating map σ is a matrix multiplication on the left.

$$\sigma \to U\sigma$$

For example, the following is induced by uniform Hadamard, controlled-Phase, and controlled-NOT gates. For notational clarity, let $E_{i,j}(a)$ be the row-addition elementary $2q \times 2q$ matrix

$$[E_{i,j}(a)]_{\mu\nu} = \delta_{\mu\nu} + \delta_{\mu i}\delta_{\nu j} a$$

where $\delta_{\mu\nu}$ is the Kronecker delta, and $a \in R = \mathbb{F}_2[\Lambda]$ and $i \neq j$. Recall that we order the components of P such that the first half components are for σ_x-part, and the second half components are for σ_z-part.

Definition 4. The following are *elementary symplectic transformations*:

- (Hadamard) $E_{i,i+q}(-1)E_{i+q,i}(1)E_{i,i+q}(-1)$ where $1 \le i \le q$,
- (controlled-Phase) $E_{i+q,i}(f)$ where $f = \bar{f}$ and $1 \le i \le q$,
- (controlled-NOT) $E_{i,j}(a)E_{j+q,i+q}(-\bar{a})$ where $1 \le i \neq j \le q$.

Recall that the Hadamard gate is a unitary transformation on a qubit given by

$$U_H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

with respect to basis $\{|0\rangle, |1\rangle\}$. At operator level,

$$U_H X U_H^\dagger = Z, \quad U_H Z U_H^\dagger = X$$

where X and Z are the Pauli matrices σ_x and σ_z, respectively. Thus, the application of Hadamard gate on every i-th qubit of each site of Λ swaps the corresponding X and Z components of P.

The controlled phase gate is a two-qubit unitary operator whose matrix is

$$U_P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

with respect to basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. At operator level,

$$U_P(X \otimes I)U_P^\dagger = X \otimes Z, \qquad U_P(Z \otimes I)U_P^\dagger = Z \otimes I,$$
$$U_P(I \otimes X)U_P^\dagger = Z \otimes X, \qquad U_P(I \otimes Z)U_P^\dagger = I \otimes Z.$$

Note that since U_P is diagonal any two U_P on different pairs of qubits commute. Let (g, i) denote the i-th qubit at $g \in \Lambda$. The uniform application

$$U_g^{(i)} = \prod_{h \in \Lambda} U_P((h,i),(h+g,i))$$

of U_P throughout the lattice Λ such that each $U_P((h,i),(h+g,i))$ acts on the pair of qubits (h,i) and $(h+g,i)$ is well-defined. From the operator level calculation of U_P, we see that $U_g^{(i)}$ induces

$$P \ni (\dots, x_i, \dots, z_i, \dots) \mapsto (\dots, x_i, \dots, z_i + (g+\bar{g})x_i, \dots) \in P$$

on the Pauli module, which is represented as $E_{i+q,i}(g+\bar{g})$. The composition

$$U_{g_1}^{(i)} U_{g_2}^{(i)} \cdots U_{g_n}^{(i)}$$

of finitely many controlled-Phase gates $U_g^{(i)}$ with different g is represented as $E_{i,i+q}(f)$ where $f = \bar{f} = \sum_{k=1}^n g_k + \bar{g}_k$. The single qubit phase gate

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

maps $X \leftrightarrow Y$ and $Z \mapsto Z$. On the Pauli module P, it is

$$P \ni (\dots, x_i, \dots, z_i, \dots)^T \mapsto (\dots, x_i, \dots, z_i + x_i, \dots)^T \in P.$$

which is $E_{i+q,i}(1)$. Note that any $f \in R$ such that $f = \bar{f}$ is always of form $f = \sum g_k + \bar{g}_k$ or $f = 1 + \sum g_k + \bar{g}_k$ where g_k are monomials. Thus, the Phase gate and the controlled-Phase gate induce transformations $E_{i+q,i}(f)$ where $f = \bar{f}$.

The controlled-NOT gate is a two-qubit unitary operator whose matrix is

$$U_N = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

with respect to basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. That is, it flips the *target* qubit conditioned on the *control* qubit. At operator level,

$$\begin{aligned} U_N(X \otimes I)U_N^\dagger &= X \otimes X, & U_N(Z \otimes I)U_N^\dagger &= Z \otimes I, \\ U_N(I \otimes X)U_N^\dagger &= I \otimes X, & U_N(I \otimes Z)U_N^\dagger &= Z \otimes Z. \end{aligned}$$

If $i < j$, the uniform application

$$U_g^{(i,j)} = \bigotimes_{h \in \Lambda} U_P((h,i),(h+g,j))$$

such that each $U_N((h,i),(h+g,j))$ acts on the pair of qubits (h,i) and $(h+g,j)$ with one at (h,i) being the control induces

$$\begin{aligned} P \ni &(\dots, x_i, \dots, x_j, \dots, z_i, \dots, z_j, \dots)^T \\ &\mapsto (\dots, x_i, \dots, x_j + g x_i, \dots, z_i + \bar{g} z_j, \dots, z_j, \dots)^T \in P. \end{aligned}$$

Thus, any finite composition of controlled-NOT gates with various g is of form $E_{i,j}(a)E_{j+q,i+q}(\bar{a})$. It might be useful to note that the controlled-NOT and the Hadamard combined, induces a symplectic transformation

- (controlled-NOT-Hadamard) $E_{i+q,j}(a)E_{j+q,i}(\bar{a})$ where $a \in R$ and $1 \le i \ne j \le q$.

Remark that an arbitrary row operation on the upper q components can be compensated by a suitable row operation on the lower q components so as to be a symplectic transformation.

2.2. **Coarse-graining.** Not all unitary operators conform with the lattice translation. In Example 1 the lattice translation has period 1. Then, for example, the Hadamard gate on every second qubit does not respect this translation structure; it only respects a coarse version of the original translation. We need to shrink the translation group to treat such a unitary operators.

Let Λ be the original translation group of the lattice with q qubits per site, and Λ' be its subgroup of finite index: $|\Lambda/\Lambda'| = c < \infty$. The total set of qubits $\Lambda \times \{1,\dots,q\}$ is set-theoretically the same as $\Lambda' \times \{1,\dots,c\} \times \{1,\dots,q\} = \Lambda' \times \{1,\dots,cq\}$. We take Λ' as our new translation group under *coarse-graining*. The Pauli group modulo phase factors remains the same as a $\mathbb{F}_2$-vector space for it depends only on the total index set of qubits. We shall say that the system is *coarse-grained by* $R' = \mathbb{F}_2[\Lambda']$. It does not change the original Hamiltonian. However, the modules, G, P, E, etc., should be considered as R'-modules after the coarse-graining.

For example, suppose $\Lambda = \mathbb{Z}^2$, so the original base ring is $R = \mathbb{F}_2[x, y, \bar{x}, \bar{y}]$. If we coarse-grain by $R' = \mathbb{F}_2[x', y', \bar{x}', \bar{y}']$ where $x' = x^2, y' = y^2$, we are taking the sites $1, x, y, xy$ of the original lattice as a single new site.

2.3. **Tensoring ancillas.** We have considered possible transformations on the stabilizer modules of code Hamiltonians, and kept the underlying index set of qubits invariant. It is quite natural to allow tensoring ancilla qubits in trivial states. In terms of the stabilizer module $S \subseteq P = R^{2q}$, it amounts to embed S into the larger module $R^{2q'}$ where $q' > q$. Concretely, let $\sigma = \begin{pmatrix} \sigma_X \\ \sigma_Z \end{pmatrix}$ be the generating matrix of S as in Proposition 1.2. By *tensoring ancilla*, we embed S as

$$\begin{pmatrix} \sigma_X \\ \sigma_Z \end{pmatrix} \to \begin{pmatrix} \sigma_X & 0 \\ 0 & 0 \\ \sigma_Z & 0 \\ 0 & 1 \end{pmatrix}.$$

This amounts to taking the direct sum of the original complex

$$G \xrightarrow{\sigma} P \xrightarrow{\epsilon} E$$

and the trivial complex

$$0 \to R \xrightarrow{\begin{pmatrix} 0 \\ 1 \end{pmatrix}} R^2 \xrightarrow{\begin{pmatrix} 1 & 0 \end{pmatrix}} R \to 0$$

to form

$$G \oplus R \to P \oplus R^2 \to E \oplus R.$$

3. Topological order

From now on we assume that Λ is isomorphic to $\mathbb{Z}^D$ as an additive group. D shall be called the *spatial dimension* of Λ.

Definition 5. Let $\sigma : G \to P$ be the generating map for the stabilizer module of a code Hamiltonian H. We say H is *exact* if $(\operatorname{im}\sigma)^\perp = \operatorname{im}\sigma$, or equivalently

$$G \xrightarrow{\sigma} P \xrightarrow{\epsilon = \sigma^\dagger \lambda_q} E$$

is exact, i.e., $\ker \epsilon = \operatorname{im} \sigma$.

It follows from definition that the exactness condition is a property of the equivalence class of code Hamiltonians as defined in Definition 2.

By imposing periodic boundary conditions, a translation-invariant Hamiltonian yields a family of Hamiltonians $\{H(L)\}$ defined on a finite system consisted of L^D sites. One might be concerned that some $H(L)$ would be frustrated. We intentionally exclude such a situation. The frustration might indeed occur, but it can easily be resolved by choosing the signs of terms in the Hamiltonian. In this way, one might loose the translation-invariance in a strict sense. However, we retain the physical phase regardless of the sign choice because different sign choices are related by a Pauli operator acting on the whole system which is a product unitary operator. Hence, the entanglement property of the ground state and the all properties of excitations do not change.

Definition 6. Let $H(L)$ be Hamiltonians on a finite system of linear size L in D dimensional physical space, and Π be the corresponding ground space projector. $H(L)$ is called *topologically ordered* if for any O supported inside a hypercube of size $(L/2)^D$ one has

$$\Pi_L O \Pi_L \propto \Pi_L. \tag{1}$$

This means that no local operator is capable of distinguishing different ground states. This condition is trivially satisfied if $H(L)$ has a unique ground state. A technical condition that is used in the proof of the stability of topological order against small perturbations is the following 'local topological order' condition [16, 17, 18]. We use a simplified version. We say *pyramid region $A(r)$ of linear size r* for the set

$$A(r) = \left\{ (i_1, \ldots, i_D) \in \mathbb{Z}^D \;\middle|\; i_\mu \ge 0,\ \sum_\mu i_\mu \le r \right\}$$

or its translation. The *apex* will be referred to the point of the smallest coordinates.

Definition 7. Let $H(L)$ be code Hamiltonians on a finite system of linear size L in D dimensional physical space. For any pyramid region $A = A(r)$ of linear size r, let Π_A be the projector onto the common eigenspace of the smallest eigenvalue of terms in the Hamiltonian $H(L)$ that are supported on A. For $b > 0$, denote by A^b the distance b neighborhood of A. $H(L)$ is called *locally topologically ordered* if there exists a constant $b > 0$ such that for any operator O supported on a pyramid region A of linear size $r < L/2$ one has

$$\Pi_{A^b} O \Pi_{A^b} \propto \Pi_{A^b}. \tag{2}$$

Since any operator is a $\mathbb{C}$-linear combination of Pauli operators, if Eq. (1),(2) are satisfied for Pauli operators, then (local) topological order condition follows. If a Pauli operator O is anti-commuting with a term in a code Hamiltonian $H(L)$, The left-hand side of Eq. (1),(2) are identically zero. In this case, there is nothing to be checked. If O acting on A is commuting with every term in $H(L)$ supported inside A^b, Eq. (1) demands that it act as identity on the ground space, i.e., O must be a product of terms in $H(L)$ up to $\pm i, \pm 1$. Eq. (2) further demands that O must be a product of terms in $H(L)$ supported inside A^b up to $\pm i, \pm 1$.

Lemma 3.1. *A code Hamiltonian H is exact if and only if $H(L)$ is locally topologically ordered for all sufficiently large L.*

It shall be important to use *Laurent polynomials* to express elements of the group algebra $R = \mathbb{F}_2[\mathbb{Z}^D] \cong \mathbb{F}_2[x_1, x_1^{-1}, \dots, x_D, x_D^{-1}]$. For example,

$$xy^2z^2 + xy^{-1} \quad \iff \quad 1(1,2,2) + 1(1,-1,0).$$

The sum of the absolute values of exponents of a monomial will be referred to as *absolute degree*. The absolute degree of a Laurent polynomial is defined to be the maximum absolute degree of its terms. The degree measures the distance or size in the lattice.

Proof. ("only if") Without loss of generality, assume that σ is expressed in polynomials with non-negative exponents. Let w be the maximum of all absolute degree of entries of σ; it is the interaction range. Let O be a Pauli operator supported on a pyramid region of linear size r. Choose the origin of the lattice $\mathbb{Z}^D$ such that the pyramid region has its apex at $(w, w, \dots, w) \in \mathbb{Z}^D$. Then O as an element of the Pauli module is expressed as a $2q \times 1$ matrix v whose entries are polynomials in D variables with positive exponents of absolute degree at most $r + w$.

We have to show that for any such v, if $v \in \ker \epsilon$, then v can be expressed as a linear combination

$$v = \sum_i c_i \sigma_i$$

of the columns σ_i of σ such that the coefficients $c_i \in R$ have absolute degree not exceeding $w + r$. (The constant b in the definition of the local topological order will be $O(w)$.)

By the exactness assumption, $\ker \epsilon = \operatorname{im} \sigma$. Since all of our Laurent polynomials have non-negative exponents, we can use a tool for modules over polynomial rings: Gröbner basis. (See Chapter 15 of Eisenbud [19].) Buchberger's algorithm to calculate Gröbner basis of $\operatorname{im} \sigma$ with respect to the homogeneous degree monomial order produces Gröbner basis of degree not exceeding w. The standard division algorithm can then be used to compute the coefficients c_i. Thus obtained c_i have non-negative exponents that are bounded above by $r + w$. [4]

("if") Suppose $v \in \ker \epsilon$. We have to show $v \in \operatorname{im} \sigma$. Choose so large L that the Pauli operator O representing v is contained in a pyramid region far from the boundary. The local topological order condition implies that O is a product of terms near the pyramid region. Since this product expression is independent of the boundary, we see $v \in \operatorname{im} \sigma$. □

3.1. **Characterization of exact sequences.** The quoted theorem below characterizes an exact sequence from the properties of connecting maps. A few notions should be recalled. Let $\mathbf{M}$ be a matrix, not necessarily square, over a ring. A minor is the determinant of square submatrix of $\mathbf{M}$. *k-th determinantal ideal* $I_k(\mathbf{M})$ is the ideal generated by all $k \times k$ minors of $\mathbf{M}$. It is not hard to see that the determinantal ideal is invariant under any invertible matrix multiplication on either

[4] This part can be adapted to an error correcting procedure or a decoder. The bottleneck of the universal decoder presented in [9] is the routine that tests whether a given cluster of excitations can be created by a Pauli operator supported in the box that envelops the cluster. The Gröbner basis for $\operatorname{im} \epsilon$ in the homogeneous degree monomial order provides a fast algorithm for it: The division algorithm yields zero remainder with respect to the Gröbner basis, if and only if the given cluster is in $\operatorname{im} \epsilon$. One minor modification is that one has to consider an enveloping pyramid in place of the enveloping box. Note also that this argument proves that the topological order condition as defined in [9] is always satisfied if the code Hamiltonian is exact.

side. The *rank* of $\mathbf{M}$ is the largest k such that k-th determinantal ideal is nonzero. (Sometimes 0-th determinantal ideal is taken to be the unit ideal by convention.) For a map ϕ between free modules, we write $I(\phi)$ to denote the k-th determinantal ideal of the matrix of ϕ where k is the rank of that matrix. Fitting Lemma (Eisenbud Corollary-Definition 20.4 [19]) states that determinantal ideals only depend on $\operatorname{coker}\phi$.

The *(Krull) dimension* of a ring is the supremum of lengths of chains of prime ideals. Here, the length of a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

is defined to be n. In particular, in a dimension zero ring every prime ideal is maximal. The *codimension* or *height* of a prime ideal $\mathfrak{p}$ is the supremum of the lengths of chains of prime ideals contained in $\mathfrak{p}$. That is, the codimension of $\mathfrak{p}$ is the Krull dimension of the local ring $R_{\mathfrak{p}}$. The codimension of an arbitrary ideal I is the minimum of codimensions of primes that contain I. The *dimension* of an ideal $I \subseteq R$ is the Krull dimension of R/I. If S is an affine domain, i.e., a homomorphic image of a polynomial ring over a field with finitely many variables such that S has no zero-divisors, it holds that $\operatorname{codim} I + \dim I = \dim S$. See Chapter 13 of Eisenbud [19].

We shall be dealing with three different kinds of 'dimensions': The first one is the spatial dimension D, which has an obvious physical meaning. The second one is the Krull dimension of a ring, just introduced. The Krull dimension is upper bounded by the spatial dimension in any case. The last one is the dimension of some module as a vector space. Recall that all of our base ring contains a field – $\mathbb{F}_2$ for qubits. The vector space dimension arises naturally when we actually count the number of orthogonal ground states. The dimension as a vector space will always be denoted with a subscript like $\dim_{\mathbb{F}_2}$.

Proposition 3.2 (Eisenbud [19] Theorem 20.9, Proposition 18.2; Northcott [20] Chapter 6 Theorem 15)**.** *If a complex of free modules over a ring*

$$0 \to F_n \xrightarrow{\phi_n} F_{n-1} \to \cdots \to F_1 \xrightarrow{\phi_1} F_0$$

is exact, then

- $\operatorname{rank} F_k = \operatorname{rank}\phi_k + \operatorname{rank}\phi_{k+1}$ *for* $k = 1, \ldots, n-1$
- $\operatorname{rank} F_n = \operatorname{rank}\phi_n$.
- $I(\phi_k) = (1)$ *or else* $\operatorname{codim} I(\phi_k) \geq k$ *for* $k = 1, \ldots, n$.

Remark 2. For exact code Hamiltonian, we have a exact sequence $G \xrightarrow{\sigma} P \xrightarrow{\epsilon=\sigma^\dagger\lambda} E$. As we will see in Lemma 6.1, $\operatorname{coker}\sigma$ has a finite free resolution, and we may apply the Proposition 3.2. Since $\overline{I_k(\sigma)} = I_k(\epsilon)$ for any $k \geq 1$, we have

$$2q = \operatorname{rank} P = \operatorname{rank}\sigma + \operatorname{rank}\epsilon = 2\ \operatorname{rank}\sigma.$$

The size $2q \times t$ of the matrix σ satisfies $t \geq q$. If $I_q(\sigma) \neq R$, then $\operatorname{codim} I_q(\sigma) \geq 2$.

4. Ground state degeneracy

Let $H(L)$ be the Hamiltonians on finite systems obtained by imposing periodic boundary conditions as in Section 3. A symmetry operator of $H(L)$ is a linear combination of Pauli operator that commutes with $H(L)$. In order for a Pauli symmetry operator to have a nontrivial action on the ground space, it must not be a product of terms in $H(L)$. In addition, since $H(L)$ is a sum of Pauli operators, a symmetry Pauli operator must commute with each term in $H(L)$. Hence, a symmetry Pauli operator O with nontrivial action on the ground space must have image v in the Pauli module such that

$$v(O) \in \ker \epsilon_L \setminus \operatorname{im} \sigma_L$$

where

$$G/\mathfrak{b}_L G \xrightarrow{\sigma_L} P/\mathfrak{b}_L P \xrightarrow{\epsilon_L} E/\mathfrak{b}_L E$$

and

$$\mathfrak{b}_L = (x_1^L - 1, \ldots, x_D^L - 1) \subseteq R,$$

which effectively imposes the periodic boundary conditions. Since each term in $H(L)$ acts as an identity on the ground space, if O' is a term in $H(L)$, the symmetry operator O and the product OO' has the same action on the ground space. OO' is expressed in the Pauli module as $v(O) + v'(O')$ for some $v' \in \operatorname{im} \sigma_L$. Therefore, the set of Pauli operators of distinct actions on the ground space is in one-to-one correspondence with the factor module

$$K(L) = \ker \epsilon_L \ / \ \operatorname{im} \sigma_L .$$

The vector space dimension $\dim_{\mathbb{F}_2} K(L)$ is precisely the number of independent Pauli operators that have nontrivial action on the ground space. Since $\ker \epsilon_L = (\operatorname{im} \sigma_L)^\perp$ by definition of ϵ, and $\operatorname{im} \sigma_L$ as an $\mathbb{F}_2$-vector space is a null space of the symplectic vector space $P/\mathfrak{b}_L P$, it follows that $(\operatorname{im} \sigma_L)^\perp = \operatorname{im} \sigma_L \oplus W$ for some hyperbolic subspace W. The quotient space $K(L) \cong W$ is thus hyperbolic and has even vector space dimension $2k$. Choosing a symplectic basis for $K(L)$, it is clear that $K(L)$ represents the tensor product of k qubit-algebras. Therefore, the ground space degeneracy is exactly 2^k. In the theory of quantum error correcting codes, k is called the number of logical qubits, and the elements of $K(L)$ are called the logical operators. In this section, k will always denote $\frac{1}{2} \dim_{\mathbb{F}_2} K$.

4.1. **Condition for degenerate Hamiltonian.**

Definition 8. The *associated ideal* for a code Hamiltonian is the q-th determinantal ideal $I_q(\sigma) \subseteq R$ of the generating map σ. Here, q is the number of qubits per site. The *characteristic dimension* is the Krull dimension of $R/I_q(\sigma)$.

Lemma 4.1. *Let I be the associated ideal of an exact code Hamiltonian, and $\mathfrak{m}$ be a maximal ideal of R. Then, $I \not\subseteq \mathfrak{m}$ implies that the localized homology*

$$K(L)_\mathfrak{m} = \ker(\epsilon_L)_\mathfrak{m} \ / \ \operatorname{im}(\sigma_L)_\mathfrak{m}$$

is zero for all $L \geq 1$.

Proof. Recall that the localization and the factoring commute. By assumption, $(I_q(\epsilon))_\mathfrak{m} = \overline{(I_q(\sigma))_\mathfrak{m}} = (1) = R_\mathfrak{m} =: S$. For notational convenience in the proof, let us drop the subscript $\mathfrak{m}$ denoting the localization. Recall that the local ring S has the unique maximal ideal $\mathfrak{m}$, and any element outside the maximal ideal is a unit. If every entry of ϵ is in $\mathfrak{m}$, then $I_q(\epsilon) \subseteq \mathfrak{m} \neq S$. Therefore, there is a unit entry, and by column and row operations, ϵ is brought to

$$\epsilon \cong \begin{pmatrix} 1 & 0 \\ 0 & \epsilon' \end{pmatrix}$$

where ϵ' is the submatrix. It is clear that $I_{q-1}(\epsilon') \subseteq I_q(\epsilon)$ since any $q-1 \times q-1$ submatrix of ϵ' can be thought of as a $q \times q$ submatrix of ϵ where the first column and first row have the unique nonzero entry 1 at $(1,1)$. It is also clear that $I_{q-1}(\epsilon') \supseteq I_q(\epsilon)$ since any $q \times q$ submatrix of ϵ contains either zero row or column, or the $(1,1)$ entry 1 of ϵ. Hence, $I_{q-1}(\epsilon') = (1)$, and we can keep extracting unit elements into the diagonal by row and column operations. See also Chapter 1 Theorem 12 of Northcott [20]. After q steps, $t \times 2q$ matrix ϵ becomes precisely

$$\epsilon \cong \begin{pmatrix} \mathrm{id}_q & 0 \\ 0 & 0 \end{pmatrix}$$

where id_q is the $q \times q$ identity matrix. Since localization preserves the exact sequence $G \to P \to E$, σ maps to the lower q components of P with respect to the basis where ϵ is in the above form. Since $I_q(\sigma) = (1)$, we must have (after basis change)

$$\sigma \cong \begin{pmatrix} 0 & 0 \\ \mathrm{id}_q & 0 \end{pmatrix}.$$

Therefore, even after factoring by the proper ideal $\mathfrak{b}_L$, the homology $K(L) = \ker \epsilon_L \ / \ \mathrm{im}\, \sigma_L$ is still zero. □

Corollary 4.2. *The associated ideal of an exact code Hamiltonian is the unit ideal, i.e., $I_q(\sigma) = R$, if and only if*

$$K(L) = \ker \epsilon_L \ / \ \mathrm{im}\, \sigma_L = 0$$

for all $L \geq 1$.

Proof. If $I(\sigma) = R$, $I(\sigma)$ is not contained in any maximal ideal $\mathfrak{m}$. The above lemma says $K(L)_\mathfrak{m} = 0$. Since a module is zero if and only if its localization at every maximal ideal is zero, $K(L) = 0$ for all $L \geq 1$.

For the converse, observe that if $\mathbb{F}$ is any extension field of $\mathbb{F}_2$, for any $\mathbb{F}_2$-vector space W, we have $\dim_\mathbb{F} \mathbb{F} \otimes_{\mathbb{F}_2} W = \dim_{\mathbb{F}_2} W$. We replace the ground field $\mathbb{F}_2$ with its algebraic closure $\mathbb{F}^a$ to test whether $K(L) \neq 0$. If $I_q(\sigma)$ is not the unit ideal, then it is contained in a maximal ideal $\mathfrak{m} \subsetneq R$. By Nullstellensatz, $\mathfrak{m} = (x_1 - a_1, \ldots, x_D - a_D)$ for some $a_i \in \mathbb{F}^a$. Since in R any monomial is a unit, we have $a_i \neq 0$. Therefore, there exists $L \geq 1$ such that $a_i^L = 1$ and $2 \nmid L$. The equation $x^L - 1 = 0$ has no multiple root.

We claim that $K(L) \neq 0$. It is enough to verify this for the localization at $\mathfrak{m}$. Since anything outside $\mathfrak{m}$ is a unit in $R_\mathfrak{m}$, we see $(\mathfrak{b}_L)_\mathfrak{m} = \mathfrak{m}$ for each $x_i^L - 1$ contains exactly one $x_i - a_i$ factor. Therefore, $(\epsilon_L)_\mathfrak{m} = \epsilon_\mathfrak{m}/(\mathfrak{b}_L)_\mathfrak{m}$ and $(\sigma_L)_\mathfrak{m} = \sigma_\mathfrak{m}/(\mathfrak{b}_L)_\mathfrak{m}$ is a matrix over the field $R/\mathfrak{m} = \mathbb{F}^a$. Since $I_q(\sigma) \subseteq \mathfrak{m}$, we have $I_q(\sigma_L)_\mathfrak{m} = 0$. That is, $\mathrm{rank}_{\mathbb{F}^a} (\sigma_L)_\mathfrak{m} < q$ and $\mathrm{rank}_{\mathbb{F}^a} (\epsilon_L)_\mathfrak{m} < q$. It is clear that $\dim_{\mathbb{F}^a} K(L)_\mathfrak{m} = \dim_{\mathbb{F}^a} \ker(\epsilon_L)_\mathfrak{m} / \mathrm{im}(\sigma_L)_\mathfrak{m} \geq 2$. □

This corollary says that in order to have a *degenerate* Hamiltonian $H(L)$, one must have a proper associated ideal. We shall simply speak of a *degenerate* code Hamiltonian if its associated ideal is proper.

4.2. **Counting number of points in an algebraic set.** It is important that the factor ring

$$R/\mathfrak{b}_L = \mathbb{F}_2[x_1, \ldots, x_D] \ / \ (x_1^L - 1, \ldots, x_D^L - 1)$$

is finite dimensional as a vector space over $\mathbb{F}_2$, and hence is Artinian. In fact, $\dim_{\mathbb{F}_2} R/\mathfrak{b}_L = L^D$. Due to the following structure theorem of Artinian rings, $K(L)$ can be explicitly analyzed by the localizations.

Proposition 4.3 (Atiyah-MacDonald [21] Chap. 8, Eisenbud [19] Sec. 2.4)**.** *Let S be an Artinian ring. (For example, S is a homomorphic image of a polynomial ring over finitely many variables with coefficients in a field $\mathbb{F}$, and is finite dimensional as a vector space over $\mathbb{F}$.) Then, there are only finitely many maximal ideals of S, and*

$$S \cong \bigoplus_{\mathfrak{m}} S_{\mathfrak{m}}$$

where the sum is over all maximal ideals $\mathfrak{m}$ of S and $S_{\mathfrak{m}}$ is the localization of S at $\mathfrak{m}$.

The following calculation tool is sometimes useful. Recall that a group algebra is equipped with a non-degenerate scalar product $\langle v, w\rangle = \operatorname{tr}(v\bar{w})$. This scalar product naturally extends to a direct sum of group algebras.

Lemma 4.4. *Let $\mathbb{F}$ be a field, and $S = \mathbb{F}[\Lambda]$ be the group algebra of a finite abelian group Λ. Let v_i be elements of a free S-module S^n, and*

$$N = \left(\sum_i S v_i \right)^{\perp} = \{ v \in S^n | \langle v, v_i \rangle = 0 \textit{ for all } i \}.$$

Then, the dual vector space N^* of N is isomorphic as vector spaces to

$$N^* \cong S^n / \sum_i S v_i .$$

Proof. Consider $\phi : S^n \ni x \mapsto \langle \cdot, x \rangle \in N^*$. The map ϕ is surjective since the scalar product is non-degenerate and S^n is a finite dimensional vector space. The kernel of ϕ is precisely $N^{\perp}$. □

Corollary 4.5. *Put $2k = \dim_{\mathbb{F}_2} K(L)$. Then,*

$$k = qL^D - \dim_{\mathbb{F}_2} \operatorname{im} \sigma_L = \dim_{\mathbb{F}_2} \ker \epsilon_L - qL^D .$$

Further, if $q = t$, then

$$k = \dim_{\mathbb{F}_2} \operatorname{coker} \epsilon_L .$$

Proof. Put $S = R/\mathfrak{b}_L$. If $v_1, \ldots, v_t$ denote the columns of σ_L, we have

$$\ker \sigma_L^\dagger = \lambda_q \ker \epsilon_L = \bigcap_i v_i^{\perp} = \left(\sum_i S v_i \right)^{\perp} = (\operatorname{im} \sigma_L)^{\perp} . \tag{3}$$

Hence, $\dim_{\mathbb{F}_2} \ker \epsilon_L = \dim_{\mathbb{F}_2} S^{2q} - \dim_{\mathbb{F}_2} \operatorname{im} \sigma_L$. Since $\dim_{\mathbb{F}_2} S = L^D$ and $K(L) = \ker \epsilon_L / \operatorname{im} \sigma_L$, the first claim follows.

Since $\operatorname{im} \sigma_L \cong S^t / \ker \sigma_L$, if $t = q$, we have $k = \dim_{\mathbb{F}_2} \ker \sigma_L$ by the first claim. From Eq. (3), we conclude that $k = \dim_{\mathbb{F}_2} S^t / \operatorname{im} \sigma_L^\dagger = \dim_{\mathbb{F}_2} \operatorname{coker} \epsilon_L$. □

We will apply these results in Section 8.

The characteristic dimension is related to the rate at which the degeneracy increases as the system size increases in the following sense. Recall that $2k = \dim_{\mathbb{F}_2} K(L)$ and the ground state degeneracy is 2^k.

Lemma 4.6. *Suppose $2 \nmid L$. Let $\mathbb{F}^a$ be the algebraic closure of $\mathbb{F}_2$. If N is the number of maximal ideals in $\mathbb{F}^a \otimes_{\mathbb{F}_2} R$ that contains $\mathfrak{b}_L + I_q(\sigma)$, then*

$$2N \le \dim_{\mathbb{F}_2} K(L) \le 2qN.$$

Proof. We replace the ground field F_2 with $\mathbb{F}^a$. Any maximal ideal of an Artinian ring $\mathbb{F}^a[x_i^{\pm 1}]/\mathfrak{b}_L$ is of form $\mathfrak{m} = (x_1 - a_1, \ldots, x_D - a_D)$ where $a_i^L = 1$ by Nullstellensatz. Since $2 \nmid L$, we see that $(\mathfrak{b}_L)_\mathfrak{m} = \mathfrak{m}$ and that $(R/\mathfrak{b}_L)_\mathfrak{m} \cong \mathbb{F}^a$ is the ground field. (See the proof of Corollary 4.2.)

Now, $I_q(\sigma) + \mathfrak{b}_L \subseteq \mathfrak{m}$ iff $I_q(\sigma)_\mathfrak{m} + (\mathfrak{b}_L)_\mathfrak{m} \subseteq \mathfrak{m}_\mathfrak{m} = (\mathfrak{b}_L)_\mathfrak{m}$ iff $I_q(\sigma)$ becomes zero over $R_\mathfrak{m}/(\mathfrak{b}_L)_\mathfrak{m} \cong \mathbb{F}^a$ iff $2 \le \dim_{\mathbb{F}^a} K(L)_\mathfrak{m} \le 2q$. Since by Proposition 4.3, $\dim_{\mathbb{F}^a} K(L)$ is a finite direct sum of localized ones, we are done. □

Lemma 4.7. *Let I be an ideal such that $\dim R/I = d$. We have*

$$\dim_{\mathbb{F}_2} R/(I + \mathfrak{b}_L) \le cL^d$$

for all $L \ge 1$ and some constant c independent of L.

Proof. We replace the ground field with its algebraic closure $\mathbb{F}^a$. Write $\tilde{x}_i$ for the image of x_i in R/I. By Noether normalization theorem, there exist $y_1, \ldots, y_d \in R/I$ such that R/I is a finitely generated module over $\mathbb{F}^a[y_1, \ldots, y_d]$. Moreover, one can choose $y_i = \sum_{j=1}^D M_{ij} \tilde{x}_j$ for some rank d matrix M whose entries are in $\mathbb{F}^a$. (See Theorem 13.3 of Eisenbud [19]) Making M into a reduced row echelon form, we may assume $y_i = \tilde{x}_i + \sum_{j>d} a_{ij} \tilde{x}_j$ for each $1 \le i \le d$.

Let $S = \mathbb{F}^a[z_1, \ldots, z_D]$ be a polynomial ring in D variables. Let $\phi : S \to R/(I + \mathfrak{b}_L)$ be the ring homomorphism such that $z_i \mapsto y_i$ for $1 \le i \le d$ and $z_j \mapsto \tilde{x}_j$ for $d < j \le D$. By the choice of y_i, ϕ is clearly surjective. Consider the ideal J of S generated by the initial terms of $\ker \phi$ with respect to the lexicographical monomial order in which $x_1 < \cdots < x_D$. Since $\tilde{x}_j$ is integral over $\mathbb{F}[y_1, \ldots, y_d]$, the monomial ideal J contains $z_j^{n_j}$ for some positive n_j for all $d < j \le D$. Here, n_j is independent of L. Since $z_i^L \in J$ for $1 \le i \le d$, we conclude that

$$\dim_{\mathbb{F}^a} R/(I + \mathfrak{b}_L) = \dim_{\mathbb{F}^a} S/J \le L^d \cdot n_{d+1} n_{d+2} \cdots n_D$$

by Macaulay theorem (Theorem 15.3 of Eisenbud [19]). □

Corollary 4.8. *If $2 \nmid L$, and $d = \dim R/I_q(\sigma)$ is the characteristic dimension of a code Hamiltonian, then*

$$\dim_{\mathbb{F}_2} K(L) \le cL^d$$

for some constant c independent of L.

Proof. If $J = \mathfrak{b}_L + I(\sigma)$, N in Lemma 4.6 is equal to $\dim_{\mathbb{F}^a} R/\operatorname{rad} J$. This is at most $\dim_{\mathbb{F}^a} R/J$. □

Lemma 4.9. *Let d be the characteristic dimension. There exists an infinite set of integers $\{L_i\}$ such that*

$$\dim_{\mathbb{F}_2} K(L_i) \ge {L_i}^d$$

Proof. We replace the ground field with its algebraic closure $\mathbb{F}^a$. Let $\mathfrak{p}' \supseteq I(\sigma)$ be a prime of R of codimension $D - d$. Let $\mathfrak{p}$ be the contraction (pull-back) of $\mathfrak{p}'$ in the polynomial ring $S = \mathbb{F}^a[x_1, \ldots, x_D]$. Since the set of all primes of R is in one-to-one correspondence with the set of primes in S that does not include monomials, it follows that $\mathfrak{p}$ has codimension $D-d$ and does not contain any monomials. Let V denote the affine variety defined by $\mathfrak{p} = (g_1, \ldots, g_n)$. Since $\mathfrak{p}$ contains no monomials, V is not contained in any hyperplanes $x_i = 0$ $(i = 1, \ldots, D)$.

Let A_1 be a finite subfield of $\mathbb{F}^a$ that contains the coefficients of g_i so V can be defined over A_1. Let $A_n \subseteq \mathbb{F}^a$ be the finite extension fields of A_1 of extension degree n. Put $L_n = |A_n| - 1$. For any subfield A of $\mathbb{F}^a$, let us say a point of V is rational over A if its coordinates are in A. The number $N'(L_n)$ of points $(a_i) \in V$ satisfying $a_i^{L_n} = 1$ is precisely the number of the rational points of V over A_n that are not contained in the hyperplanes $x_i = 0$. Since $I(\sigma) \subseteq \mathfrak{p}'$, the number N in Lemma 4.6 is at least $N'(L_n)$. It remains to show $2N'(L_n) \geq L_n^d$ for all sufficiently large n.

This follows from the result by Lang and Weil [22], which states that the number of points of a projective variety of dimension d that are rational over a finite field of m elements is $m^d + O\left(m^{d-\frac{1}{2}}\right)$ asymptotically in m. Since Lang-Weil theorem is for projective variety and we are with an affine variety V, we need to subtract the number of points in the hyperplanes $x_i = 0$ $(i = 0, 1, \ldots, D)$ from the Zariski closure of V. The subvarieties in the hyperplanes, being closed, have strictly smaller dimensions, and we are done. □

5. One dimension

The group algebra $R = F_2[x, \bar{x}]$ for the one dimensional lattice $\mathbb{Z}$ is a Euclidean domain where the degree of a polynomial is defined to be the maximum exponent minus the minimum exponent. (In particular, any monomial has degree 0.) Given two polynomials f, g in R, one can find their gcd by the Euclid's algorithm. It can be viewed as a column operation on the 1×2 matrix $\begin{pmatrix} f & g \end{pmatrix}$. Similarly, one can find gcd of n polynomials by column operations on $1 \times n$ matrix

$$\begin{pmatrix} f_1 & f_2 & \cdots & f_n \end{pmatrix}.$$

The resulting matrix after the Euclid's algorithm will be

$$\begin{pmatrix} \gcd(f_1, \ldots, f_n) & 0 & \cdots & 0 \end{pmatrix}.$$

Given a matrix $\mathbf{M}$ of univariate polynomials, we can apply Euclid's algorithm to the first row and first column by elementary row and column operations in such a way that the degree of $(1,1)$-entry $\mathbf{M}_{11}$ decreases unless all other entries in the first row and column are divisible by $\mathbf{M}_{11}$. Since the degree cannot decrease forever, this process must end with all entries in the first row and column being zero except $\mathbf{M}_{11}$. By induction on the number of rows or columns, we conclude that $\mathbf{M}$ can be transformed to a diagonal matrix by the elementary row and column operations. This is known as the Smith's algorithm.

The following is a consequence of the finiteness of the ground field.

Lemma 5.1. *Let $\mathbb{F}$ be a finite field and $S = \mathbb{F}[x]$ be a polynomial ring. Let $\phi : S \xrightarrow{f(x)\times} S$ be a 1×1 matrix such that $f(0) \neq 0$. ϕ can be viewed as an $n \times n$ matrix acting on the free S'-module S where $S' = \mathbb{F}[x']$ and $x' = x^n$. Then, for some $n \geq 1$, the matrix ϕ is transformed by elementary row and column operations into a diagonal matrix with entries 1 or $x' - 1$. The number of $x' - 1$ entries in the transformed ϕ is equal to the degree of f.*

Proof. The splitting field $\tilde{\mathbb{F}}$ of $f(x)$ is a finite extension of $\mathbb{F}$. Since $\tilde{\mathbb{F}}$ is finite, every root of $f(x)$ is a root of $x^{n'}-1$ for some $n' \geq 1$. Choose an integer $p \geq 1$ such that 2^p is greater than any multiplicity of the roots of $f(x)$. Then, clearly $f(x)$ divides $(x^{n'}-1)^{2^p} = x^{2^p n'}-1$. Let n be the smallest positive integer such that $f(x)$ divides $x^n - 1$.

Consider the coarse-graining by $S' = \mathbb{F}[x']$ where $x' = x^n$. S is a free S'-module of rank n, and (f) is now an endomorphism of the module S represented as an $n \times n$ matrix. Since $f(x)g(x) = x^n - 1$ for some $g(x) \in \mathbb{F}[x]$, we have

$$AB = (x'-1)\mathrm{id}_n$$

where $x' = x^n$, and A, B are the matrix representation of $f(x)$ and $g(x)$ respectively as endomorphisms. A and B have polynomial entries in variable x'. The determinants of A, B are nonzero for their product is $(x'-1)^n \neq 0$. Let E_1 and E_2 be the products of elementary matrices such that $A' = E_1 A E_2$ is diagonal. Such matrices exist by the Smith's algorithm. Put $B' = E_2^{-1} B E_1^{-1}$. Then,

$$A'B' = E_1 A E_2 E_2^{-1} B E_1^{-1} = E_1 A B E_1^{-1} = (x'-1)\mathrm{id}_n.$$

Since A' and I_n are diagonal of non-vanishing entries, B' must be diagonal, too. It follows that the diagonal entries of A' divides $(x'-1)$; that is, they are 1 or $x'-1$.

The number of $x'-1$ entries can be counted by considering $S/(f(x))$ as an $\mathbb{F}$-vector space. It is clear that $\dim_F S/(f(x)) = \deg f(x)$. $S/(f(x)) = \operatorname{coker} \phi$ viewed as a S'-module is isomorphic to $S'^n / \operatorname{im} A'$, the vector space dimension of which is precisely the number of $x'-1$ entries in A'. □

Theorem 1. *If $\Lambda = \mathbb{Z}$, any system governed by a code Hamiltonian is equivalent to finitely many copies of Ising models, plus some non-interacting qubits. In particular, the topological order condition is never satisfied.*

We will make use of the elementary symplectic transformations and coarse-graining to deform σ to a familiar form. Recall that for any elementary row-addition E on the upper block of σ there is a unique symplectic transformation that restricts to E. We will freely apply elementary row-additions on the upper block of σ so σ becomes diagonal.

Proof. Applying Smith's algorithm to the first row and the first column of $2m \times t$ matrix σ, one gets

$$\begin{pmatrix} f_1 & 0 \\ 0 & A \\ \hline g_1 & g_2 \\ \vdots & B \end{pmatrix}$$

by elementary symplectic transformations. Let $1 \leq i < j \leq q$ be integers. If some $(1, q+j)$-entry is not divisible by f_1, apply Hadamard on j-th qubit to bring $(q+j)$-th row to the upper block, and then run Euclid's algorithm again to reduce the degree of $(1,1)$-entry. The degree is a positive integer, so this process must end after a finite number of iteration. Now every $(q+j, 1)$-entry is divisible by f_1 and hence can be made to be 0 by the controlled-NOT-Hadamard:

$$\left(\begin{array}{cc} f_1 & 0 \\ 0 & A \\ \hline g_1 & g_2 \\ 0 & B \end{array}\right).$$

Further we may assume $\deg f_1 \le \deg g_1$. Since $\sigma^\dagger \lambda_q \sigma = 0$, we have a commutativity condition

$$\bar{f}_1 g_1 - \bar{g}_1 f_1 = 0.$$

Let $g_1 = h f_1 + r$ be the result of the division where $\deg r < \deg f_1$. The commutativity condition reads, $(h - \bar{h}) \bar{f}_1 f_1 = \bar{r} f_1 - r \bar{f}_1$. If it is nonzero, the left-hand side has degree $\ge 2 \deg f_1$, while the right-hand side $< 2 \deg f_1$. Therefore, $h = \bar{h}$. The controlled-Phase $E_{q,1}(h)$ reduces the degree of g_1, which can then be swapped with f_1. Again, this iteration must end, and g_1 becomes 0. The commutativity condition between i-th($i > 1$) column and the first is $f_1 \bar{g}_i = 0$. Since $f_1 \neq 0$, we get $g_i = 0$:

$$\left(\begin{array}{cc} f_1 & 0 \\ 0 & A \\ \hline 0 & 0 \\ 0 & B \end{array}\right).$$

Continuing, we transform σ into a diagonal matrix. (We have shown that σ can be transformed via elementary symplectic transformations to the Smith normal form.)

Now the Hamiltonian is a sum of non-interacting purely classical spin chains plus some non-interacting qubits ($f_i = 0$). It remains to classify classical spin chains whose stabilizer module is generated by

$$(f)$$

where we omitted the lower half block. We can always choose $f = f(x)$ such that $f(x)$ has only non-negative exponents and $f(0) \neq 0$ since x is a unit in R. Lemma 5.1 says that (f) becomes a diagonal matrix of entries 1 or $x' - 1$ after a suitable coarse-graining followed by a symplectic transformation and column operations. 1 describes the ancilla qubits, and $x' - 1 = x' + 1$ does the Ising model. □

According to the proof, for the interaction range w of classical Hamiltonian, the amount of coarse-graining n needed to map it to the Ising models can be exponential in w. One cannot naively reduce n; if $n = 2^w - 1$, the minimal polynomial of a primitive n-th root of unity has degree w.

6. Two dimensions

We will be mainly interested in exact code Hamiltonians. If $D = 2$, the lattice is $\Lambda = \mathbb{Z}^2$, and our base ring is $R = F_2[x, \bar{x}, y, \bar{y}]$.

Example 2 (Toric Code)**.** Although the original two-dimensional toric code has qubits on edges [1], we put two qubits per site of the square lattice to fit it into our setting. Concretely, the first qubit to each site represents the one on its east edge, and the second qubit the one on its north edge. With this convention, the

Hamiltonian is the negative sum of the following two types of interactions:

$$\begin{tikzcd}
XI \arrow[r, dash] \arrow[d, dash] & XX \arrow[d, dash] & ZI \arrow[r, dash] \arrow[d, dash] & II \arrow[d, dash] & y \arrow[r, dash] \arrow[d, dash] & xy \arrow[d, dash] \\
II \arrow[r, dash] & IX & ZZ \arrow[r, dash] & IZ & 1 \arrow[r, dash] & x
\end{tikzcd}$$

where we used X, Z to abbreviate σ_x, σ_z, and omitted the tensor product symbol. Here, the third square specifies the coordinate system of the square lattice. Since there are $q = 2$ qubits per site, the Pauli module is of rank 4. The corresponding generating map $\sigma : R^2 \to R^4$ is the matrix

$$\sigma_{\text{2D-toric}} = \left(\begin{array}{cc} y + xy & 0 \\ x + xy & 0 \\ \hline 0 & 1 + y \\ 0 & 1 + x \end{array}\right) \cong \left(\begin{array}{cc} 1 + \bar{x} & 0 \\ 1 + \bar{y} & 0 \\ \hline 0 & 1 + y \\ 0 & 1 + x \end{array}\right).$$

Here the each column expresses one type of interaction. The upper $q = 2$ rows expresses σ_x and the lower σ_z. It is clear that

$$\epsilon_{\text{2D-toric}} = \sigma^\dagger \lambda_2 = \begin{pmatrix} 0 & 0 & 1 + x & 1 + y \\ 1 + \bar{y} & 1 + \bar{x} & 0 & 0 \end{pmatrix}$$

and $\ker \epsilon = \operatorname{im} \sigma$; the two dimensional toric code satisfies our exactness condition. The associated ideal is $I(\sigma) = ((1 + x)^2, (1 + x)(1 + y), (1 + y)^2)$. The characteristic dimension is $\dim R/I(\sigma) = 0$. Note also that $\operatorname{ann} \operatorname{coker} \epsilon = (x - 1, y - 1)$.

The connection with cellular homology can be mentioned. σ can be viewed as the boundary map from the free module of all 2-cells with $\mathbb{Z}_2$ coefficients of the cell structure of 2-torus induced from the tessellation by the square lattice. The ϵ then is interpreted as the boundary map from the free module of all 1-cells to that of all 0-cells. σ or ϵ is actually the direct sum of two boundary maps. Indeed, the space of symmetry operators (logical operators) $K(L) = \ker \epsilon_L / \operatorname{im} \sigma_L$ has four generators

$$l_y(X) = \begin{pmatrix} 1 + y + \cdots + y^{L-1} \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad l_x(X) = \begin{pmatrix} 0 \\ 1 + x + \cdots + x^{L-1} \\ 0 \\ 0 \end{pmatrix},$$

$$l_x(Z) = \begin{pmatrix} 0 \\ 0 \\ 1 + x + \cdots + x^{L-1} \\ 0 \end{pmatrix}, \qquad l_y(Z) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 + y + \cdots + y^{L-1} \end{pmatrix},$$

which correspond to the usual nontrivial homology classes of 2-torus.

The description by the cellular homology is more or less advantageous for the toric code over our description with pure Laurent polynomials; in this way, it is clear that the toric code can be defined on an arbitrary tessellation of compact orientable surfaces. However, it is unclear whether this cellular homology description is possible after all for other topologically ordered code Hamiltonians.

Example 3 (2D Ising model on square lattice)**.** The Ising model has nearest neighbor interactions: horizontal and vertical. In our formalism, they are represented as $1 + x$ and $1 + y$. Thus,

$$\sigma_{\text{2D Ising}} = \begin{pmatrix} 0 & 0 \\ 1 + x & 1 + y \end{pmatrix}.$$

Although $\sigma^\dagger \lambda_1 \sigma = 0$ so we have a complex $G \to P \to E$, it is not exact. Moreover, σ is not injective.

$$\sigma_{\text{2D Ising;1}} = \begin{pmatrix} 1+y \\ 1+x \end{pmatrix}$$

generates the kernel of σ. That is, the complex

$$0 \to G_1 \xrightarrow{\sigma_{\text{2D Ising;1}}} G \xrightarrow{\sigma_{\text{2D Ising}}} P$$

is exact.

We turn to general properties. The following asserts that the local relations — a few terms in the Hamiltonian that multiply to identity in a nontrivial way as in 2D Ising model, or the kernel of σ — among the terms in a code Hamiltonian, can be completely removed for exact Hamiltonians in two dimensions.

Lemma 6.1. *If $G \xrightarrow{\sigma} P \xrightarrow{\epsilon} E$ is exact over $R = F_2[x_1, \bar{x}_1, \dots, x_D, \bar{x}_D]$, There exists $\sigma' : G' \to P$ such that $\operatorname{im} \sigma' = \operatorname{im} \sigma$ and*

$$0 \to G_{D-2} \to \cdots \to G_1 \to G' \xrightarrow{\sigma'} P \xrightarrow{\epsilon} E$$

is an exact sequence of free R-modules. If $D = 2$, one can choose σ' to be injective.

We make use of a constructive version of Hilbert's syzygy theorem via Gröbner basis.

Proposition 6.2 (Theorem 15.10, Corollary 15.11 of Eisenbud [19]). *Let $\{g_1, \dots, g_n\}$ be a Gröbner basis of a submodule of a free module M_0 over a polynomial ring. Then, the S-polynomials τ_{ij} of $\{g_i\}$ in the free module $M_1 = \bigoplus_{i=1}^n Se_i$ generate the syzygies for $\{g_i\}$. If the variable $x_1, \dots, x_s$ are absent from the initial terms of g_i, one can define a monomial order on M_1 such that $x_1, \dots, x_{s+1}$ is absent from the initial terms of τ_{ij}. If all variables are absent from the initial terms of g_i, then $M_0/(g_1, \dots, g_n)$ is free.*

Proof of Lemma 6.1. Without loss of generality assume that the $t \times 2q$ matrix ϵ have entries with nonnegative exponents so they are in fact polynomials, not Laurent polynomials. Below, every module is over the polynomial ring $S = F_2[x_1, \dots, x_D]$ unless otherwise noted. Let E_+ be the free S-module of rank equal to $\operatorname{rank}_R E$.

If $g_1, \cdots, c_{2q}$ are the columns of ϵ, apply Buchberger's algorithm to obtain a Gröbner basis $g_1, \cdots, g_{2q}, \dots, g_n$ of $\operatorname{im} \epsilon$. Let ϵ' be the matrix whose columns are $g_1, \dots, g_n$. We regard ϵ' as a map $M_0 \to E_+$. By Proposition 6.2, the initial terms of the syzygy generators (S-polynomials) τ_{ij} for $\{g_i\}$ lacks the variable x_1. Writing each τ_{ij} in a column of a matrix τ_1, we have a map $\tau_1 : M_1 \to M_0$.

By induction on D, we have an exact sequence

$$M_D \xrightarrow{\tau_D} M_{D-1} \xrightarrow{\tau_{D-1}} \cdots \xrightarrow{\tau_1} M_0 \xrightarrow{\epsilon'} E_+$$

of free S-modules, where the initial terms of columns of τ_D lack all the variables. By Proposition 6.2 again, $M'_{D-1} = M_{D-1} / \operatorname{im} \tau_{\tau_D}$ is free. Since $\ker \tau_{D-1} = \operatorname{im} \tau_D$, we have

$$0 \to M'_{D-1} \xrightarrow{\tilde{\tau}_{D-1}} \cdots \xrightarrow{\tau_1} M_0 \xrightarrow{\epsilon'} E_+$$

Since $g_{2q+1}, \dots, g_n$ are S-linear combinations of $g_1, \dots, g_{2q}$, there is a basis change of M_0 so that the matrix representation of ϵ' becomes

$$\epsilon' \cong \begin{pmatrix} \epsilon & 0 \end{pmatrix}.$$

With respect to this basis of M_0, the matrix of τ_1 is

$$\tau_1 \cong \begin{pmatrix} \tau_{1u} \\ \tau_{1d} \end{pmatrix}$$

where τ_{1u} is the upper $2q \times t'$ submatrix. Since $\ker \epsilon' = \operatorname{im} \tau_1$, The first row r of τ_{1d} should generate $1 \in S$. (This property is called unimodularity.) Quillen-Suslin theorem (Theorem 3.5 in Chapter XXI of Lang [23]) states that there exists a basis change of M_1 such that r becomes $\begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$. Then, by some basis change of M_0, one can make

$$\epsilon' \cong \begin{pmatrix} \epsilon & 0 \end{pmatrix}, \quad \tau_{1d} \cong \begin{pmatrix} 1 & 0 \\ 0 & \tau'_{1d} \end{pmatrix}.$$

where τ'_{1d} is a submatrix. By induction on the number of rows in τ_{1d}, we deduce that the matrix of τ_1 can be brought to

$$\epsilon' \cong \begin{pmatrix} \epsilon & 0 \end{pmatrix}, \quad \tau_1 \cong \begin{pmatrix} \sigma'' & \sigma' \\ I & 0 \end{pmatrix}$$

Note that $\epsilon\sigma'' = 0$ and $\epsilon\sigma' = 0$. The basis change of M_0 by $\begin{pmatrix} I & -\sigma'' \\ 0 & I \end{pmatrix}$ gives

$$\epsilon' \cong \begin{pmatrix} \epsilon & 0 \end{pmatrix}, \quad \tau_1 \cong \begin{pmatrix} 0 & \sigma' \\ I & 0 \end{pmatrix}.$$

The kernel of $\begin{pmatrix} \sigma' \\ 0 \end{pmatrix}$ determines $\ker \tau_1 = \operatorname{im} \tau_2$. Let M'_1 denote the projection of M_1 such that the sequence

$$0 \to M'_{D-1} \xrightarrow{\tilde{\tau}_{D-1}} \cdots \to M_2 \to M'_1 \xrightarrow{\sigma'} M'_0 \xrightarrow{\epsilon} E_+$$

of free S-modules is exact.

Taking the ring of fractions with respect to the multiplicatively closed set

$$U = \{x_1^{i_1} \cdots x_D^{i_D} | i_1, \ldots, i_D \geq 0\},$$

we finally obtain the desired exact sequence over $U^{-1}S = R$ with $P = U^{-1}M'_0$ and $E = U^{-1}E_+$. Since $\operatorname{im} \sigma = \ker \epsilon$, we have $\operatorname{im} \sigma' = \operatorname{im} \sigma$. □

Lemma 6.3. *Let R be a Laurent polynomial ring in D variables over a finite field $\mathbb{F}$, and N be a module over R. Suppose $J = \operatorname{ann}_R N$ is a proper ideal such that $\dim R/J = 0$. Then, there exists an integer $L \geq 1$ such that*

$$\operatorname*{ann}_{R'} N = (x_1^L - 1, \ldots, x_D^L - 1) \subseteq R'$$

where $R' = \mathbb{F}[x_1^L, \bar{x}_1^L, \ldots, x_D^L, \bar{x}_D^L]$ is a subring of R.

This is a variant of Lemma 5.1.

Proof. Since R is a finitely generated algebra over a field, for any maximal ideal $\mathfrak{m}$ of R, the field $R/\mathfrak{m}$ is a finite extension of $\mathbb{F}$ (Nullstellensatz in the form of Theorem 4.19 of Eisenbud [19]). Hence, $R/\mathfrak{m}$ is a finite field. Since x_i is a unit in R, the image $a_i \in R/\mathfrak{m}$ of x_i is nonzero. a_i being an element of finite field, a power of a_i is 1. Therefore, there is a positive integer n such that $\mathfrak{b}_n = (x_1^n - 1, \ldots, x_D^n - 1) \subseteq \mathfrak{m}$. Since $x^n - 1$ divides $x^{nn'} - 1$, we see that there exists $n \geq 1$ such that $\mathfrak{b}_n \subseteq \mathfrak{m}_1 \cap \mathfrak{m}_2$ for any two maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2$. One extends this by induction to any finite number of maximal ideals.

Since $\dim R/J = 0$, any prime ideal of R/J is maximal and the Artinian ring R/J has only finitely many maximal ideals. rad J is then the intersection of the contractions (pull-backs) of these finitely many maximal ideals. Therefore, there is $n \geq 1$ such that

$$\mathfrak{b}_n \subseteq \text{rad } J.$$

Since R is Noetherian, $(\text{rad } J)^{p^r} \subseteq J$ for some $r \geq 0$ where p is the characteristic of $\mathbb{F}$. Hence, we have

$$\mathfrak{b}_{np^r} \subseteq \mathfrak{b}_n^{p^r} \subseteq (\text{rad } J)^{p^r} \subseteq J.$$

Let $L = np^r$. If $R' = \mathbb{F}[x_1^L, \bar{x}_1^L, \ldots, x_D^L, \bar{x}_D^L]$, $\operatorname{ann}_{R'} N$ is nothing but $J \cap R'$. We have just shown $\mathfrak{b}_L \cap R' \subseteq J \cap R'$. Since J is a proper ideal, we have $1 \notin J \cap R'$. Thus, $\mathfrak{b}_L \cap R' = J \cap R'$ since $\mathfrak{b}_L \cap R'$ is maximal in R'. □

Theorem 2. *For any two dimensional degenerate exact code Hamiltonian, there exists an equivalent Hamiltonian such that*

$$\operatorname{ann} \operatorname{coker} \epsilon = (x - 1, y - 1).$$

Proof. By Lemma 6.1, we can find an equivalent Hamiltonian such that the generating map σ for its stabilizer module is injective:

$$0 \to G \xrightarrow{\sigma} P.$$

Let t be the rank of G. The exactness condition says

$$0 \to G \xrightarrow{\sigma} P \xrightarrow{\epsilon} E$$

is exact where $\epsilon = \sigma^\dagger \lambda_q$ and E has rank t. Applying Proposition 3.2, since $\overline{I(\sigma)} = I(\epsilon)$ and hence in particular $\operatorname{codim} I(\sigma) = \operatorname{codim} I(\epsilon)$, we have that $q = t$ and $\operatorname{codim} I(\epsilon) \geq 2$ if $I(\epsilon) \neq R$. But, $I(\epsilon) \neq R$ by Corollary 4.2.

Since $q = t$, $I(\epsilon)$ is equal to the initial Fitting ideal, and therefore has the same radical as the annihilator of $\operatorname{coker} \epsilon = E/\operatorname{im} \epsilon$. (See Eisenbud Proposition 20.7 [19] or Lang Chapter XIX Proposition 2.5 [23].) In particular, $\dim R/(\operatorname{ann} \operatorname{coker} \epsilon) = 0$. Apply Lemma 6.3 to conclude the proof. □

An interpretation of the theorem is the following:

A (topological) *charge* is an isolated excitation that cannot be created alone from a ground state by an operator of finite support, but can be created if some other excitations are simultaneously created. If $v \in E$ represents a charge, then by definition $v \notin \operatorname{im} \epsilon$. Recall $\operatorname{coker} \epsilon = E/\operatorname{im} E$. If $\operatorname{coker} \epsilon = 0$, i.e, $E = \operatorname{im} \epsilon$, then any excitation can be realized by some operator of finite support, and in particular, there is no charge. If $\operatorname{coker} \epsilon \neq 0$ and $f \in \operatorname{ann} \operatorname{coker} \epsilon$ is nonzero, we have that $0 \neq fv \in \operatorname{im} \epsilon$. Since f must be non-unit, it consists of at least two terms, and fv is a union of v at different positions. For example, if $f = 1 + x^n$, then fv is a pair of v's, where one is a translation of another by distance n.

For systems of qubits, Theorem 2 says that $x + 1$ and $y + 1$ are in $\operatorname{ann} \operatorname{coker} \epsilon$. In other words, any element v of E is a charge, and a pair of v's of distance 1 apart can be created by a local operator. Equivalently, v can be translated by distance 1 by the local operator. Since translation by distance 1 generates all translations of the lattice, we see that any excitation can be moved though the system by some sequence of local operators. This is exactly what happens in the 2D toric code:

Any excited state is described by a configuration of magnetic and electric charge, which can be moved to a different position by a string operator.

Moreover, since $(x-1, y-1) = \operatorname{ann}\operatorname{coker}\epsilon$, the action of $x, y \in R$ on $\operatorname{coker}\epsilon$ is the same as the identity action. Therefore, the R-module $\operatorname{coker}\epsilon$ is completely determined up to isomorphism by its dimension k as an F_2-vector space. The module $K(L)$ of Pauli operators acting on the ground space (logical operators), can be viewed as $K(L) = \operatorname{Tor}_1(\operatorname{coker}\epsilon, R/\mathfrak{b}_L)$. Thus, $K(L)$ is determined by k up to isomorphisms. This implies that the translations of a logical operator are all equivalent. It is not too obvious whether the symplectic structure, or the commutation relations among the logical operators, of $K(L)$ is also completely determined.

A similar result is reported in [10, 11].

7. Three dimensions and fractal generators

Definition 9. For a complex $G \xrightarrow{\sigma} P \xrightarrow{\epsilon} E$, an element $f \in R \setminus \{0\}$ is a *fractal generator* if there exists $v \in E \setminus \operatorname{im}\epsilon$ such that $fv \in \operatorname{im}\epsilon$.

There is a natural reason the fractal generator deserves its name. Consider a code Hamiltonian with a single type of interaction: $t = 1$. So each configuration of excitations is described by one Laurent polynomial. For example, in two dimensions, $f = 1+x+y = \epsilon(p)$ represents three excitations, one at the origin of the lattice and another at $(2,1)$ created by a Pauli operator represented by p. In order to avoid repeating phrase, let us call each element of the Pauli module a Pauli operator, and instead of using multiplicative notation we use module operation $+$ to mean the product of the corresponding Pauli operators.

Consider the Pauli operator $fp = p + xp + yp \in P$. It describes the Pauli operator p at the origin multiplied by the translations of p at $(1,0)$ and at $(0,1)$. So fp consists of three copies of p. This Pauli operator maps the ground state to the excited state $f^2 = 1 + x^2 + y^2$. The number of excitations is still three, but ones at $(1,0), (0,1)$ have been replaced by the ones at $(2,0), (0,2)$. Similarly, the Pauli operator $f^{2+1}p = f^2(fp)$ consists of three copies of fp, or 3^2 copies of p. The excited state created by f^3p is $f^4 = (f^2)^2 = 1 + x^{2^2} + y^{2^2}$. Still it has three excitations, but they are further apart. The Pauli operator $f^{2^n-1}p$ consists of 3^n copies of p in a self-similar way, and the excited state caused by $f^{2^n-1}p$ consists of a constant number of excitations.

More generally, if there are $t > 1$ types of terms in the Hamiltonian, the excitations are described by a $t \times 1$ matrix. If it happens to be a of form fv for some $1 \neq f \in R$, there is a family of Pauli operators $f^{2^n-1}p$ in a self-similar fashion such that it only creates a bounded number of excitations. An obvious but uninteresting way to have such a situation is to put $fv = \epsilon(fp')$ for a Pauli operator p' where $v = \epsilon(p')$. Our definition avoids this triviality by requiring $v \notin \operatorname{im}\epsilon$.

Thus, if there does exist a fractal generator, we have a *charge* v that cannot be created from a ground state alone, but can be observed as an isolated cluster of excitations that is separated from the other by an arbitrary long distance. Since v has finite *size* anyway (the maximum exponent minus the minimum exponent of the Laurent polynomials in the $t \times 1$ matrix v), we can say that the charge v is *point-like.* Moreover, we shall have a description how the point-like charge can be separated from the other by a local process. By the *local process* we mean a sequence of Pauli operators $[[o_1, \dots, o_n]]$ such that $o_{i+1} - o_i$ is a monomial. The number of excitations, i.e., *energy*, at an instant i will be the number of terms in $\epsilon(o_i)$.

Theorem 3. *If there is a fractal generator of a code Hamiltonian, then for all sufficiently large r, there is a local process starting from the identity by which a point-like charge is separated from the other excitations by distance at least 2^r. One can choose the local process in such a way that at any intermediate step there are at most cr excitations for some constant c independent of r.*

For notational simplicity, we denote the local process $[[o_1, \dots, o_n]]$ by

$$s = [o_1,\ o_2 - o_1,\ o_3 - o_2, \dots, o_n - o_{n-1}].$$

It is a *recipe* to construct o_n, consisted of single qubit operators. o_n can be expressed as "$o_n = \int s$", the sum of all elements in the recipe.

Proof. Let f be a fractal generator, and put $fv = \epsilon(p)$ where $v \notin \operatorname{im} \epsilon$. We already know v is a point-like charge. Write

$$p = \sum_{i=1}^{n} p_i, \quad f = \sum_{i=1}^{l} f_i$$

where each of p_i and f_i is a monomial. Let $s_0 = [0, p_1, p_2, \dots, p_n]$ be a recipe for constructing p; $\int s_0 = p$. Given s_i, define inductively

$$s_{i+1} = (f_1^{2^i} \cdot s_i) \circ (f_2^{2^i} \cdot s_i) \circ \cdots \circ (f_l^{2^i} \cdot s_i)$$

where $\circ$ denotes the concatenation and $f_i \cdot [u_1, \dots, u_{n'}] = [f_i u_1, \dots, f_i u_{n'}]$. It is clear that s_{i+1} constructs the Pauli operator

$$\begin{aligned} \int s_r &= f^{2^{r-1}} \int s_{r-1} = f^{2^{r-1}} f^{2^{r-2}} \int s_{r-2} \\ &= f^{2^{r-1}+2^{r-2}+\cdots+1} \int s_0 = f^{2^r-1} p \end{aligned}$$

whose image under ϵ is $f^{2^r} v$. Thus, if r is large enough so that 2^r is greater than the size of v, the configuration of excitations is precisely l copies of v. The distance between v's is at least 2^r minus twice the size of v.

Therefore, there is a constant $e > 0$ such that for any $r \geq 0$ the energy of $f^{2^r} v \in E$ is $\leq e$. Let $\Delta(r)$ be the maximum energy during the process s_r. We prove by induction on r that

$$\Delta(r) \leq el(r+1).$$

When $r = 0$, it is trivial. In s_{r+1}, the energy is $\leq \Delta(r)$ until $f_1^{2^r} s_r$ is finished. At the end of $f_1^{2^r} s_r$, the energy is $\leq e$. During the subsequent $f_2^{2^r} s_r$, the energy is $\leq \Delta(r) + e$, and at the end of $(f_1^{2^r} s_r) \circ (f_2^{2^r} s_r)$, the energy is $\leq 2e$. During the subsequent $f_j^{2^r} s_r$, the energy is $\leq \Delta(r) + je$. Therefore,

$$\Delta(r+1) \leq \Delta(r) + el \leq el(r+2)$$

by the induction hypothesis. This proves the theorem with $c = 2el$. □

Note that the notion of fractal generators includes that of 'string operators'. In fact, a fractal generator that contains exactly two terms gives a family of nontrivial *string segments* of unbounded length, as defined in [7]. The proof here mimics the explicit construction of fractal operators in [8].

Algebraically, a charge is a torsion element of $\operatorname{coker}\epsilon$, and a fractal generator is a zero divisor on $\operatorname{coker}\epsilon$.

Proposition 7.1. *For code Hamiltonians, the existence of a fractal generator is a property of an equivalence class of Hamiltonians defined in Definition 2.*

Proof. Suppose $\operatorname{im}\sigma = \operatorname{im}\sigma'$. Each column of σ' is a R-linear combination of those of σ, and vice versa. Thus, there is a matrix B and B' such that $\epsilon' = B\epsilon$ and $\epsilon = B'\epsilon'$. BB' and $B'B$ are identity on $\operatorname{im}\epsilon'$ and $\operatorname{im}\epsilon$ respectively. In particular, B' and B are injective on $\operatorname{im}\epsilon'$ and $\operatorname{im}\epsilon$ respectively. Suppose f is a fractal generator for ϵ, i.e., $fv = \epsilon p \neq 0$. Then, $0 \neq Bfv = fBv = B\epsilon(p) = \epsilon'(p)$. If $Bv \in \operatorname{im}\epsilon'$, then $v = B'Bv \in \operatorname{im}\epsilon$, a contradiction. Therefore, f is also a fractal generator for ϵ'. By symmetry, a fractal generator for ϵ' is a fractal generator for ϵ, too.

Suppose $R' \subseteq R$ is a coarse-grained base ring. If $\operatorname{coker}\epsilon$ is torsion-free as an R-module, then so it is as an R'-module. If $f \in R$ is a fractal generator, the determinant of f as a matrix over R' is a fractal generator.

A symplectic transformation or tensoring ancillas does not change $\operatorname{coker}\epsilon$. □

Proposition 7.2. *Suppose* $\operatorname{coker}\epsilon \neq 0$. *Then, the following are equivalent:*

- *There does not exist a fractal generator.*
- $\operatorname{coker}\epsilon$ *is torsion-free.*
- *There exists a free R-module E' of finite rank such that*

$$P \xrightarrow{\epsilon} E \to E'$$

is exact.

Proof. The first two are equivalent by definition. The sequence is exact if and only if $0 \to \operatorname{coker}\epsilon \to E'$ is exact. Since $\operatorname{coker}\epsilon$ has a finite free resolution, the second is equivalent to the third. See Bruns-Vetter 16.33 [24]. □

Corollary 7.3. *For any ring S and $t \geq 1$, if $0 \to S^t \to S^{2t} \xrightarrow{\phi} S^t$ is exact and $I(\phi) \neq S$,* $\operatorname{coker}\phi$ *is not torsion-free. In particular, for a degenerate exact code Hamiltonian, if σ is injective, then there exists a fractal generator.*

Proof. By Proposition 3.2, $\operatorname{rank}\phi = t$. Since $0 \subsetneq I_t(\phi) \subsetneq S$ is the initial Fitting ideal, we have $0 \neq \operatorname{ann}\operatorname{coker}\phi \neq S$. That is, $\operatorname{coker}\phi$ is not torsion-free.

For the second statement, set $S = R$. If σ is injective, we have an exact sequence

$$0 \to G \xrightarrow{\sigma} P \xrightarrow{\epsilon} E.$$

By Remark 2, $t = \operatorname{rank} G = \operatorname{rank}\sigma = \operatorname{rank}\epsilon = q$. □

Corollary 7.4. *Suppose the characteristic dimension is $D - 2$ for a degenerate exact code Hamiltonian. Then, there exists a fractal generator.*

Proof. Suppose on the contrary there are no fractal generators. Then, by Proposition 7.2,

$$G \xrightarrow{\sigma} P \xrightarrow{\epsilon} E \to E'$$

is exact for some finitely generated free module E'. Since $\operatorname{coker}\epsilon$ has finite free resolution by Lemma 6.1, Proposition 3.2 implies $\operatorname{codim} I(\sigma) \geq 3$ unless $I(\sigma) = R$. But, $\operatorname{codim} I(\sigma) = 2$ and $I(\sigma) \neq R$ by Corollary 4.2. This is a contradiction. □

Lemma 7.5. *Suppose $D = 3$,*

$$0 \to G_1 \xrightarrow{\sigma_1} G \xrightarrow{\sigma} P \xrightarrow{\epsilon=\sigma^\dagger \lambda_q} E$$

is exact, and $I(\sigma) \subseteq \mathfrak{m} = (x-1, y-1, z-1)$. Then, $\operatorname{coker} \epsilon$ *is not torsion-free.*

Proof. Suppose on the contrary $\operatorname{coker}\epsilon$ is torsion-free. We have an exact sequence

$$0 \to G_1 \xrightarrow{\sigma_1} G \xrightarrow{\sigma} P \xrightarrow{\epsilon} E \to E'.$$

If $G_1 = 0$, Corollary 7.3 implies the conclusion. So we assume $G_1 \neq 0$, and therefore we have $I(\sigma_1) = R$.

Let us localize the sequence at $\mathfrak{m}$ to have $I(\sigma_1)_\mathfrak{m} = R_\mathfrak{m}$. Since $\operatorname{rank}(G_1)_\mathfrak{m} = \operatorname{rank}(\sigma_1)_\mathfrak{m}$, the matrix of $(\sigma_1)_\mathfrak{m}$ becomes

$$(\sigma_1)_\mathfrak{m} = \begin{pmatrix} 0 \\ I \end{pmatrix}$$

for some basis of $(G_1)_\mathfrak{m}$ and $G_\mathfrak{m}$. See the proof of Lemma 4.1. In other words, there is an invertible matrix $B \in \mathrm{GL}_{t\times t}(R_\mathfrak{m})$ such that

$$\sigma_\mathfrak{m} B = \begin{pmatrix} \tilde\sigma & 0 \end{pmatrix}$$

where $\tilde\sigma$ is the $2q \times t'$ submatrix. Since the antipode map of R preserves $\mathfrak{m}$, it is a well-defined automorphism of $R_\mathfrak{m}$. Indeed, if $\alpha : R \to R$ denotes the antipode map,

$$\alpha(\mathfrak{m}) = (x^{-1}-1, y^{-1}-1, z^{-1}-1) = (1-x, 1-y, 1-z) = \mathfrak{m}.$$

Since $\epsilon = \sigma^\dagger \lambda_q$, we have

$$B^\dagger \epsilon_\mathfrak{m} = \begin{pmatrix} \tilde\sigma^\dagger \\ 0 \end{pmatrix} \lambda_q = \begin{pmatrix} \tilde\sigma^\dagger \lambda_q \\ 0 \end{pmatrix}. \tag{4}$$

Therefore, we get a new exact sequence

$$0 \to G' \xrightarrow{\tilde\sigma} P_\mathfrak{m} \xrightarrow{\tilde\epsilon = \tilde\sigma^\dagger \lambda_q} R_\mathfrak{m}^{t'}$$

where $G' = G_\mathfrak{m} / \operatorname{im}(\sigma_1)_\mathfrak{m}$ is a free $R_\mathfrak{m}$-module and $t' = \operatorname{rank} G'$. It is clear that $\operatorname{rank}\tilde\epsilon = \operatorname{rank}\tilde\sigma$. Setting $S = R_\mathfrak{m}$ in Corollary 7.3 implies that $\operatorname{coker}\tilde\epsilon$ is not torsion-free. But, since we are assuming $\operatorname{coker}\epsilon_m$ is torsion-free, $\operatorname{coker}\tilde\sigma^\dagger$ is also torsion-free by Eq. (4). This is a contradiction. □

Theorem 4. *For any three dimensional, degenerate and locally topologically ordered code Hamiltonian, there exists a fractal generator.*

Proof. By Lemma 6.1, there exists an equivalent Hamiltonian such that

$$0 \to G_1 \xrightarrow{\sigma_1} G \xrightarrow{\sigma} P \xrightarrow{\epsilon=\sigma^\dagger \lambda_q} E$$

is exact. The existence of a fractal generator is a property of the equivalence class by Proposition 7.1. If we show that $I(\sigma)$ is contained in $(x-1, y-1, z-1)$ after some coarse-graining, then Lemma 7.5 shall imply the conclusion.

Recall that ϵ_L and σ_L denote the induced maps by factoring out $\mathfrak{b}_L = (x^L - 1, y^L - 1, z^L - 1)$. See Sec. 4. There exists L such that $K(L) = \ker\epsilon_L / \operatorname{im}\sigma_L \neq 0$ by Corollary 4.2. Consider the coarse-grain by $x' = x^L$, $y' = y^L$, $z' = z^L$. Let $R' = F_2[x'^{\pm1}, y'^{\pm1}, z'^{\pm1}]$ denote the coarse-grained base ring. If $K'(L')$ denotes $\ker\epsilon'_{L'} / \operatorname{im}\sigma'_{L'}$ as R'-module, we see that $K'(1) = K(L)$ as $\mathbb{F}_2$-vector space. In particular, $K'(1) \neq 0$. Put $\mathfrak{m} = (x'-1, y'-1, z'-1) = \mathfrak{b}'_1 \subseteq R'$. Then, $K'(1)_\mathfrak{m} = K'(1) \neq 0$. By Lemma 4.1, we have $I(\sigma') \subseteq \mathfrak{m}$. □

8. Examples

Example 4 (Toric codes in higher dimensions)**.** Any higher dimensional toric code can be treated similarly as for two dimensional case. In three dimensions one associates each site with $q = 3$ qubits. It is easily checked that

$$\sigma_{\text{3D-toric}} = \left(\begin{array}{cccc} 1+\bar{x} & 0 & 0 & 0 \\ 1+\bar{y} & 0 & 0 & 0 \\ 1+\bar{z} & 0 & 0 & 0 \\ \hline 0 & 0 & 1+z & 1+y \\ 0 & 1+z & 0 & 1+x \\ 0 & 1+y & 1+x & 0 \end{array}\right).$$

Both two- and three-dimensional toric codes have the property that $\operatorname{coker}\epsilon$ is not torsion-free. Indeed, $1+x$ and $1+y$ are fractal generators. Being consisted of two terms, they generate the 'string operators'.

The 4D toric code [4] has σ_x-type interaction and σ_z-type interaction. Originally the qubits are placed on every plaquette of 4D hypercubic lattice; we place $q = 6$ qubits on each site. The generating map σ for the stabilizer module is written as a 12×8-matrix ($t = 8$)

$$\sigma_{\text{4D-toric}} = \begin{pmatrix} \sigma_X & 0 \\ 0 & \sigma_Z \end{pmatrix}$$

where

$$\sigma_X = \begin{pmatrix} 1+y & 1+x & 0 & 0 \\ 1+w & 0 & 0 & 1+x \\ 1+z & 0 & 1+x & 0 \\ 0 & 1+z & 1+y & 0 \\ 0 & 1+w & 0 & 1+y \\ 0 & 0 & 1+w & 1+z \end{pmatrix},$$

$$\bar{\sigma}_Z = \begin{pmatrix} 0 & 0 & 1+w & 1+z \\ 0 & 1+z & 1+y & 0 \\ 0 & 1+w & 0 & 1+y \\ 1+w & 0 & 0 & 1+x \\ 1+z & 0 & 1+x & 0 \\ 1+y & 1+x & 0 & 0 \end{pmatrix}.$$

Note the bar on σ_Z.

Theorem 4 does not prevent the absence of a fractal generator in four or higher dimensions. Indeed, this 4D toric code lacks any fractal generator. To see this, it enough to consider σ_Z since $\overline{\operatorname{coker}\sigma_X^\dagger} \cong \operatorname{coker}\sigma_Z^\dagger$ as R-modules. If

$$\epsilon_1 = \begin{pmatrix} 1+x & 1+y & 1+z & 1+w \end{pmatrix} : R^4 \to R,$$

then

$$R^6 \xrightarrow{\sigma_Z^\dagger} R^4 \xrightarrow{\epsilon_1} R$$

is exact. (A direct way to check it is to compute S-polynomials of the entries of ϵ_1, and to verify that they all are in the rows of σ_Z. See Chapter 15 of Eisenbud [19].) Hence, $\operatorname{coker}\sigma_Z^\dagger$ is torsion-free by Proposition 7.2.

For the toric codes in any dimensions, σ has nonzero entries of form $x_i - 1$. The radical of the associated ideal $I(\sigma)$ is equal to $\mathfrak{m} = (x_1 - 1, \ldots, x_D - 1)$. So $\mathfrak{m}$ is the only maximal ideal of R that contains $I(\sigma)$. The characteristic dimension is zero.

If $2 \nmid L$, since $(\mathfrak{b}_L)_\mathfrak{m} = \mathfrak{m}_\mathfrak{m}$, $(\sigma_L)_\mathfrak{m}$ is a zero matrix. Any other localization of σ_L does not contribute to $\dim_{\mathbb{F}_2} K(L)$ by Lemma 4.1. Therefore, if $2 \nmid L$, $K(L)$ has constant vector space dimension independent of L; the ground state degeneracy is independent of system size.

Example 5 (Wen plaquette [25])**.** This model consists of a single type of interaction $(t = q = 1)$

$$\begin{array}{ccc} X & — & Y \\ | & & | \\ Y & — & X \end{array} \qquad \sigma_{\text{Wen}} = \begin{pmatrix} 1+x+y+xy \\ 1+xy \end{pmatrix}$$

where X, Y are abbreviations of σ_x, σ_y. It is known to be equivalent to the 2D toric code. Take the coarse-graining given by $R' = \mathbb{F}_2[x', y', \bar{x}', \bar{y}']$ where

$$x' = x\bar{y}, \qquad y' = y^2.$$

As an R'-module, R is free with basis $\{1, y\}$. With the identification $R = (R' \cdot 1) \oplus (R' \cdot y)$, we have $x \cdot 1 = x' \cdot y$, $x \cdot y = x'y' \cdot 1$, and $y \cdot 1 = 1 \cdot y$, $y \cdot y = y' \cdot 1$. Hence, x and y act on R'-modules as the matrix-multiplications on the left:

$$x \mapsto \begin{pmatrix} 0 & x'y' \\ x' & 0 \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & y' \\ 1 & 0 \end{pmatrix}.$$

Identifying

$$R^n = [(R' \cdot 1) \oplus (R' \cdot y)] \oplus \cdots \oplus [(R' \cdot 1) \oplus (R' \cdot y)],$$

our new σ on the coarse-grained lattice becomes

$$\sigma' = \left(\begin{array}{cc} 1+x'y' & y'+x'y' \\ 1+x' & 1+x'y' \\ \hline 1+x'y' & 0 \\ 0 & 1+x'y' \end{array}\right).$$

By a sequence of elementary symplectic transformations, we have

$$\sigma' \xrightarrow[E_{1,3}(1)]{E_{2,4}(1)} \begin{pmatrix} 0 & y'+x'y' \\ 1+x' & 0 \\ 1+x'y' & 0 \\ 0 & 1+x'y' \end{pmatrix} \xrightarrow[E_{3,2}(y')]{E_{4,1}(\bar{y}')} \begin{pmatrix} 0 & y'+x'y' \\ 1+x' & 0 \\ 1+y' & 0 \\ :0 & x'y'+x' \end{pmatrix}$$

$$\xrightarrow[\times \bar{x}'\bar{y}']{\text{col.2}} \begin{pmatrix} 0 & 1+\bar{x}' \\ 1+x' & 0 \\ 1+y' & 0 \\ 0 & 1+\bar{y}' \end{pmatrix} \xrightarrow{1 \leftrightarrow 3} \begin{pmatrix} 1+y' & 0 \\ 1+x' & 0 \\ 0 & 1+\bar{x}' \\ 0 & 1+\bar{y}' \end{pmatrix},$$

which is exactly the 2D toric code.

Example 6 (Chamon model [26, 27])**.** This three dimensional model consists of single type of term in the Hamiltonian. The generating map is

$$\sigma_{\text{Chamon}} = \begin{pmatrix} x+\bar{x}+y+\bar{y} \\ z+\bar{z}+y+\bar{y} \end{pmatrix}.$$

Since

$$\sigma^\dagger \lambda_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = (1+x\bar{y}) \begin{pmatrix} 0 \\ \bar{x}+y \end{pmatrix},$$

$1+x\bar{y}$ is a fractal generator. Consisted of two terms, it generates a string operator. The degeneracy can be calculated using Corollary 4.5. Assume all the three linear dimensions of the system are even. Put

$$S = R/(x+\bar{x}+y+\bar{y}, z+\bar{z}+y+\bar{y}, x^{2l}-1, y^{2m}-1, z^{2n}-1).$$

Then, the $\log_2$ of the degeneracy is $k = \dim_{\mathbb{F}_2} S$. In S, we have $x+\bar{x} = y+\bar{y} = z+\bar{z}$. Since S has characteristic 2, it holds that

$$w^{p+1} + w^{-p-1} = (w+w^{-1})(w^p + w^{p-2} + \cdots + w^{-p})$$

for $p \geq 1$ and $w = x, y, z$. By induction on p, we see that $w^p + w^{-p}$ is a polynomial in $w + w^{-1}$. Therefore,

$$x^p + \bar{x}^p = y^p + \bar{y}^p = z^p + \bar{z}^p$$

for all $p \geq 1$ in S. Put $g = \gcd(l,m,n)$. Since $x^l + x^{-l} = y^m + y^{-m} = z^n + z^{-n} = 0$ in S, we have $x^g + x^{-g} = y^g + y^{-g} = z^g + z^{-g} = 0$.

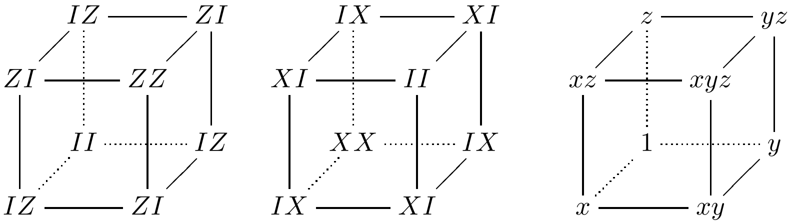
Applying Buchberger's criterion with respect to the lexicographic order in which $x < y < z$, we see that

$$S = \mathbb{F}_2[x,y,z]/(z^2 + zx^{2l-1} + zx + 1, y^2 + yx^{2l-1} + yx + 1, x^{2g} + 1)$$

is expressed with a Gröbner basis. Therefore,

$$k = \dim_{\mathbb{F}_2} S = 8\gcd(l,m,n).$$

Example 7 (Cubic Code)**.** The Hamiltonian of code 1 in [7] is the translation-invariant negative sum of the following two types of interaction terms:



Here, the third cube specifies the coordinate system of the simple cubic lattice. The corresponding generating map for the stabilizer module is

$$\sigma_{cubic-code} = \begin{pmatrix} 1+xy+yz+zx & 0 \\ 1+x+y+z & 0 \\ 0 & 1+\bar{x}+\bar{y}+\bar{z} \\ 0 & 1+\bar{x}\bar{y}+\bar{y}\bar{z}+\bar{z}\bar{x} \end{pmatrix}$$

The associated ideal is contained in a prime ideal of codimension 2:

$$I(\sigma) \subseteq (1+x+y+z, 1+xy+yz+zx) = \mathfrak{p}.$$

Since $\operatorname{codim} I(\sigma) \geq 2$, the characteristic dimension is 1. Since $\operatorname{coker} \epsilon_{\text{cubic-code}} = R/\mathfrak{p} \oplus R/\bar{\mathfrak{p}}$, any nonzero element of $\mathfrak{p}$ is a fractal generator.

Let us explicitly calculate the ground state degeneracy when the Hamiltonian is defined on $L \times L \times L$ cubic lattice with periodic boundary conditions. By Corollary 4.5,

$$k = \dim_{\mathbb{F}_2} R/(\mathfrak{p} + \mathfrak{b}_L) \oplus R/(\bar{\mathfrak{p}} + \mathfrak{b}_L) = 2\dim_{\mathbb{F}_2} R/(\mathfrak{p} + \mathfrak{b}_L).$$

So the calculation of ground state degeneracy comes down to the calculation of

$$d = \dim_{\mathbb{F}_2} T'/\mathfrak{p}$$

where $T' = \mathbb{F}_2[x,y,z]/(x^{n_1}-1, y^{n_2}-1, z^{n_3}-1)$.

We may extend the scalar field to any extension field without changing d. Let $\mathbb{F}$ be the algebraic closure of $\mathbb{F}_2$ and let

$$T = \mathbb{F}[x,y,z]/(x^{n_1}-1, y^{n_2}-1, z^{n_3}-1)$$

be an Artinian ring. By Proposition 4.3, it suffices to calculate for each maximal ideal $\mathfrak{m}$ of T the vector space dimension

$$d_{\mathfrak{m}} = \dim_{\mathbb{F}} (T/\mathfrak{p})_{\mathfrak{m}}$$

of the localized rings, and sum them up.

Suppose $n_1, n_2, n_3 > 1$. By Nullstellensatz, any maximal ideal of T is of form $\mathfrak{m} = (x - x_0, y - y_0, z - z_0)$ where $x_0^{n_1} = y_0^{n_2} = z_0^{n_3} = 1$. (If $n_1 = n_2 = n_3 = 1$, then T becomes a field, and there is no maximal ideal other than zero.) Put $n_i = 2^{l_i} n_i'$ where n_i' is not divisible by 2. Since the polynomial $x^{n_1} - 1$ contains the factor $x - x_0$ with multiplicity 2^{l_1}, it follows that

$$T_{\mathfrak{m}} = \mathbb{F}[x,y,z]_{\mathfrak{m}}/(x^{2^{l_1}} + a',\ y^{2^{l_2}} + b',\ z^{2^{l_3}} + c')$$

where $a' = x_0^{2^{l_1}}, b' = y_0^{2^{l_2}}, c' = z_0^{2^{l_3}}$. Hence, $(T/\mathfrak{p})_{\mathfrak{m}} \cong \mathbb{F}[x,y,z]/I'$ where

$$I' = (x + y + z + 1, xy + xz + yz + 1,\ x^{2^{l_1}} + a',\ y^{2^{l_2}} + b',\ z^{2^{l_3}} + c').$$

If $I' = \mathbb{F}[x,y,z]$, then $d_{\mathfrak{m}} = 0$.

Without loss of generality, we assume that $l_1 \le l_2 \le l_3$. By powering the first two generators of I', we see that (x_0, y_0, z_0) must be a solution of them in order for I' not to be a unit ideal. Eliminating z and shifting $x \to x+1$, $y \to y+1$, our objective is to calculate the Gröbner basis for the proper ideal

$$I = (x^2 + xy + y^2, x^{2^{l_1}} + a,\ y^{2^{l_2}} + b)$$

where $a = a' + 1$ and $b = b' + 1$. So

$$d_{\mathfrak{m}} = \dim_{\mathbb{F}} \mathbb{F}[x,y]/I.$$

One can easily deduce by induction that $y^{2^m} + x^{2^m - 1}(mx + y) \in I$ for any integer $m \ge 0$. And $b = \omega a^{2^{l_2 - l_1}}$ for a primitive third root of unity ω. So we arrive at

$$I = (y^2 + yx + x^2,\ yx^{2^{l_2}-1} + b(1 + l_2\omega^2),\ x^{2^{l_1}} + a)$$

We apply the Buchberger criterion. If $a \ne 0$, i.e., $x_0 \ne 1$, then $b \ne 0$ and $I = (x + (\omega^2 + l_2)y, x^{2^{l_1}} + a)$, so $d_{\mathfrak{m}} = 2^{l_1}$

If $a = b = 0$, then $I = (y^2 + yx + x^2, yx^{2^{l_2}-1}, x^{2^{l_1}})$. The three generators form Gröbner basis if $l_2 = l_1$. Thus, in this case, $d_{\mathfrak{m}} = 2^{l_1+1} - 1$. If $l_2 > l_1$, then $d_{\mathfrak{m}} = 2^{l_1+1}$.

To summarize, except for the special point $(1,1,1) \in \mathbb{F}^3$ of the affine space, each point in the algebraic set

$$V = \left\{ (x,y,z) \in \mathbb{F}^3 \;\middle|\; \begin{array}{c} x + y + z + 1 = xy + xz + yz + 1 = 0 \\ x^{n_1'} - 1 = y^{n_2'} - 1 = z^{n_3'} - 1 = 0 \end{array} \right\}$$

contribute 2^{l_1} to d. The contribution of $(1,1,1)$ is either 2^{l_1+1} or $2^{l_1+1} - 1$. The latter occurs if and only if l_1 and l_2, the two smallest numbers of factors of 2 in

n_1, n_2, n_3, are equal. Let $d_0 = \# V$ be the number of points in V. The desired answer is

$$d = 2^{l_1}(d_0 - 1) + \begin{cases} 2^{l_1+1} - 1 & \text{if } l_1 = l_2 \\ 2^{l_1+1} & \text{otherwise} \end{cases}$$

where $l_1 \le l_2 \le l_3$ are the number of factors of 2 in n_i.

The algebraic set defined by $(x+y+z+1,\ xy+xz+yz+1)$ is the union of two isomorphic lines intersecting only at $x = y = z = 1$, one of which is parametrized by $x \in \mathbb{F}$ as

$$(1+x, 1+\omega x, 1+\omega^2 x) \in \mathbb{F}^3,$$

and another is parametrized as

$$(1+x, 1+\omega^2 x, 1+\omega x) \in \mathbb{F}^3.$$

where ω is a primitive third root of unity. Therefore, the purely geometric number $d_0 = 2d_1 - 1$ can be calculated by

$$d_1 = \deg_x \gcd\left((1+x)^{n_1'} + 1, (1+\omega x)^{n_2'} + 1, (1+\omega^2 x)^{n_3'} + 1\right).$$

In particular, if $L = n_1 = n_2 = n_3 > 1$ (including all the factors of 2),

$$\frac{d+1}{2} = \deg_x \gcd\left((1+x)^L + 1,\ (1+\omega x)^L + 1,\ (1+\omega^2 x)^L + 1\right) \tag{5}$$

for any $L \ge 2$. The true ground state degeneracy is $2^k = 4^d$. Some special cases are explicitly computed:

Corollary 8.1. *Let k be $\log_2$ of the ground state degeneracy of the cubic code on the cubic lattice of size L^3 with periodic boundary conditions. Let $p \ge 1$ be any integer. Then,*

$$\frac{k}{2} = \begin{cases} 1 & \text{if } L = 2^p + 1, \\ 2L - 1 & \text{if } L = 2^p, \\ 2L - 5 & \text{if } L = 4^p - 1, \\ 1 & \text{if } L = 2^{2p+1} - 1. \end{cases}$$

Proof. Recall $k = 2d$ in Eq. (5). Use $(\alpha+\beta)^{2^p} = \alpha^{2^p} + \beta^{2^p}$ and $\omega^2 + \omega + 1 = 0$. □

9. Discussion

There are many natural questions left unanswered. Perhaps, it would be the most interesting to answer how much the associated ideal $I(\sigma)$ determines about the Hamiltonian. Note that the very algebraic set defined by the associated ideal is not invariant under coarse-graining. For instance, in the characteristic dimension zero case, the algebraic set can be a several points in the affine space, but becomes a single point under a suitable coarse-graining.

It is reasonable to conceive that the algebraic set is mapped by the affine map $(a_i) \mapsto (a_i^n)$ under the coarse-graining by $x_i' = x_i^n$. This is true if $t = q$ so the q-th determinantal ideal of ϵ, being the initial Fitting ideal, has the same radical as $\operatorname{ann}\operatorname{coker}\epsilon$. In fact, we have implicitly used this idea in the proofs of Lemma 5.1, 6.3, and Theorem 4. The case $t > q$ is not explicitly handled here.

Also, it is an interesting on its own to prove or disprove that the elementary symplectic transformations generate the whole symplectic transformation group.

The author would like to thank Sergey Bravyi, Lawrence Chung, Alexei Kitaev, John Preskill, Eric Rains, and Ari Turner for useful discussions.

References

[1] A. Yu. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303:2–30, 2003. `arXiv:quant-ph/9707021`, `doi:10.1016/S0003-4916(02)00018-0`.

[2] Xiao-Gang Wen. Mean-field theory of spin-liquid states with finite energy gap and topological orders. *Phys. Rev. B*, 44:2664–2672, Aug 1991. `doi:10.1103/PhysRevB.44.2664`.

[3] M. Z. Hasan and C. L. Kane. Topological insulators. *Rev. Mod. Phys.*, 82:3045, February 2010. `arXiv:1002.3895`.

[4] Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill. Topological quantum memory. *J. Math. Phys.*, 43:4452–4505, 2002. `arXiv:quant-ph/0110143`, `doi:10.1063/1.1499754`.

[5] R. Alicki, M. Horodecki, P. Horodecki, and R. Horodecki. On thermal stability of topological qubit in kitaev's 4d model. *Open Syst. Inf. Dyn.*, 17:1, 2010. `arXiv:0811.0033`, `doi:10.1142/S1230161210000023`.

[6] Stefano Chesi, Daniel Loss, Sergey Bravyi, and Barbara M. Terhal. Thermodynamic stability criteria for a quantum memory based on stabilizer and subsystem codes. *New J. Phys.*, 12,:025013, 2009. `arXiv:0907.2807`, `doi:10.1088/1367-2630/12/2/025013`.

[7] Jeongwan Haah. Local stabilizer codes in three dimensions without string logical operators. *Phys. Rev. A*, 83(4):042330, Apr 2011. `arXiv:1101.1962`, `doi:10.1103/PhysRevA.83.042330`.

[8] Sergey Bravyi and Jeongwan Haah. On the energy landscape of 3d spin hamiltonians with topological order. *Phys. Rev. Lett.*, 107:150504, May 2011. `arXiv:1105.4159`, `doi:10.1103/PhysRevLett.107.150504`.

[9] Sergey Bravyi and Jeongwan Haah. Analytic and numerical demonstration of quantum self-correction in the 3d cubic code. December 2011. `arXiv:1112.3252`.

[10] H. Bombin. Structure of 2D topological stabilizer codes. July 2011. `arXiv:1107.2707`.

[11] H. Bombin, Guillaume Duclos-Cianci, and David Poulin. Universal topological phase of 2d stabilizer codes. March 2011. `arXiv:1103.4606`.

[12] Cem Güneri and Ferruh Özbudak. Multidimensional cyclic codes and artinschreier type hypersurfaces over finite fields. *Finite Fields and Their Applications*, 14(1):44 – 58, 2008. `doi:10.1016/j.ffa.2006.12.003`.

[13] V. D. Goppa. Algebraico-geometric codes. *Mathematics of the USSR-Izvestiya*, 21(1):75, 1983. `doi:10.1070/IM1983v021n01ABEH001641`.

[14] Isaac H. Kim. 3d local qupit quantum code without string logical operator. February 2012. `arXiv:1202.0052`.

[15] A. R. Calderbank, E. M Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys.Rev.Lett.*, 78:405–408, 1997. `arXiv:quant-ph/9605005`, `doi:10.1103/PhysRevLett.78.405`.

[16] Spyridon Michalakis and Justyna Pytel. Stability of frustration-free hamiltonians. 2011. `arXiv:1109.1588`.

[17] Sergey Bravyi, Matthew Hastings, and Spyridon Michalakis. Topological quantum order: stability under local perturbations. *J. Math. Phys.*, 51:093512, January 2010. `arXiv:1001.0344`, `doi:10.1063/1.3490195`.

[18] S. Bravyi and M. B. Hastings. A short proof of stability of topological order under local perturbations. *Communications in Mathematical Physics*, 307:609–627, 2011. `arXiv:1001.4363`, `doi:10.1007/s00220-011-1346-2`.

[19] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer, 2004.

[20] Douglas G. Northcott. *Finite Free Resolutions*. Cambridge University Press, 1976.

[21] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Westview, 1969.

[22] Serge Lang and Andre Weil. Number of points of varieties in finite fields. *American Journal of Mathematics*, 76(4):819–827, 1954. Available from: `http://www.jstor.org/stable/2372655`.

[23] Serge Lang. *Algebra*. Springer, revised 3rd ed. edition, 2002.

[24] Winfried Bruns and Udo Vetter. *Determinantal Rings*. Lecture Notes in Mathematics 1327. Springer-Verlag, 1988. Available from: `http://www.home.uni-osnabrueck.de/wbruns/brunsw/detrings.pdf`.

[25] Xiao-Gang Wen. Quantum orders in an exact soluble model. *Phys. Rev. Lett.*, 90:016803, Jan 2003. `arXiv:quant-ph/0205004`, `doi:10.1103/PhysRevLett.90.016803`.

[26] Claudio Chamon. Quantum glassiness. *Phys. Rev. Lett.*, 94:040402, 2005. `arXiv:cond-mat/0404182`, `doi:10.1103/PhysRevLett.94.040402`.

[27] Sergey Bravyi, Bernhard Leemhuis, and Barbara M. Terhal. Topological order in an exactly solvable 3D spin model. *Annals of Physics*, 326(4):839 – 866, 2011. `arXiv:1006.4871`, `doi:doi:10.1016/j.aop.2010.11.002`.

Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, California

E-mail address: `jwhaah@caltech.edu`