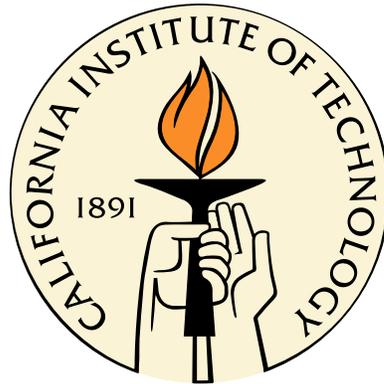


Lattice quantum codes and exotic topological phases of matter

Thesis by
Jeongwan Haah

In Partial Fulfillment of the Requirements
for the Degree of
Doctor of Philosophy



California Institute of Technology
Pasadena, California

2013
(Defended May 15, 2013)

© 2013

Jeongwan Haah

All Rights Reserved

Acknowledgments

I would like to thank my advisor John Preskill for his inspiring comments and advice, and forgiveness and encouragement during my graduate study. The thesis would not have been possible without reverence to his standard of clear understanding. I should add that my enjoyable last four years are deeply rooted in him.

A special thanks to Sergey Bravyi for the fruitful collaboration and numerous insights. It is not too much to say that the algebraic formulation of this thesis grew out from his note on the degeneracy computation. The interaction with him gave me an opportunity to do a research internship at IBM Watson Research Center, which was a valuable experience. I thank Charles Bennett, John Smolin, and Graeme Smith.

L. Yong-uck Chung, who had been my roommate for years, helped me to study algebra. He was always willing to explain concepts and related theorems however easy or hard they were. Informal discussions with him were absolutely important for me. I also thank Eric Rains and Tom Graber for giving insights and answers for mathematical questions.

I appreciate the inspiring discussion with Guifre Vidal and Daniel Gottesman while I was visiting Perimeter Institute, which led my attention to the entanglement renormalization group flow.

I also thank Alexei Kitaev for his encouragement and numerous useful comments. I was honored to have discussions with him.

I thank my friend I. Han-young Kim, who shared moments of inspiration.

Thanks to the members of IQI and more broadly IQIM for creating an exciting environment, including Ann Harvey, Michael Beverland, Ersen Bilgin, Peter Brooks, Bill Fefferman, Alex Kubica, Shaun Maguire, Prabha Mandayam, Sujeet Shukla, Gorjan Alagic, Salman Beigi, Sergio Boixo, Darrick Chang, Glen Evenbly, Steve Flammia, Lukasz Fidkowski, Alexey Gorshkov, Zhengcheng Gu, Liang Jiang, Stephen Jordan, Robert König, Yi-Kai Liu, Nate Lindner, Spiros Michalakis, Fernando Pastawski, Norbert Schuch, Stephanie Wehner, and Beni Yoshida.

I am grateful for comments from Soonwon Choi and Alex Kubica on drafts of these thesis chapters.

Abstract

This thesis addresses whether it is possible to build a robust memory device for quantum information. Many schemes for fault-tolerant quantum information processing have been developed so far, one of which, called topological quantum computation, makes use of degrees of freedom that are inherently insensitive to local errors. However, this scheme is not so reliable against thermal errors. Other fault-tolerant schemes achieve better reliability through active error correction, but incur a substantial overhead cost. Thus, it is of practical importance and theoretical interest to design and assess fault-tolerant schemes that work well at finite temperature without active error correction.

In this thesis, a three-dimensional gapped lattice spin model is found which demonstrates for the first time that a reliable quantum memory at finite temperature is possible, at least to some extent. When quantum information is encoded into a highly entangled ground state of this model and subjected to thermal errors, the errors remain easily correctable for a long time without any active intervention, because a macroscopic energy barrier keeps the errors well localized. As a result, stored quantum information can be retrieved faithfully for a memory time which grows exponentially with the square of the inverse temperature. In contrast, for previously known types of topological quantum storage in three or fewer spatial dimensions the memory time scales exponentially with the inverse temperature, rather than its square.

This spin model exhibits a previously unexpected topological quantum order, in which ground states are locally indistinguishable, pointlike excitations are immobile, and the immobility is not affected by small perturbations of the Hamiltonian. The degeneracy of the ground state, though also insensitive to perturbations, is a complicated number-theoretic function of the system size, and the system bifurcates into multiple noninteracting copies of itself under real-space renormalization group transformations. The degeneracy, the excitations, and the renormalization group flow can be analyzed using a framework that exploits the spin model's symmetry and some associated free resolutions of modules over polynomial algebras.

Contents

Acknowledgments	iii
Abstract	iv
1 Introduction	1
1.1 Topological order	3
1.2 String operators	6
1.3 Quantum codes and a new model	8
1.4 Summary of chapters	11
2 Additive quantum codes	14
2.1 Pauli group as a symplectic vector space	15
2.2 Additive/stabilizer codes	19
2.3 Cleaning lemma	21
2.4 Operator trade-off for local subsystem codes	25
3 Algebraic formulation for translationally invariant codes	30
3.1 Algebraic structure of code Hamiltonians	31
3.1.1 Pauli space on a group	31
3.1.2 Local Hamiltonians on groups	34
3.1.3 Excitations	35
3.2 Equivalent Hamiltonians	36
3.2.1 Symplectic transformations	37
3.2.2 Coarse-graining	41
3.2.3 Tensoring ancillas	41
3.3 Topological order	42
3.4 Ground-state degeneracy	47
3.4.1 Condition for degenerate Hamiltonians	49
3.4.2 Counting points in algebraic varieties	51

3.5	Fractal operators and topological charges	54
4	Structure of exact Hamiltonians on lattices	64
4.1	One dimension	65
4.2	Two dimensions	68
4.3	Three dimensions	74
4.4	Discussion	82
5	Cubic code	84
5.1	String segments and no-strings rule	85
5.2	Search for models	86
5.3	Cubic code	88
5.4	Real-space renormalization of the cubic code	93
5.5	Thermal partition function of the cubic code	107
6	Consequences of no-strings rule	110
6.1	Logarithmic energy barrier	111
6.2	Superlinear code distance	120
7	Renormalization group decoder and error threshold theorem	123
7.1	Assumptions and conventions	125
7.2	Renormalization group decoder	126
7.3	Cluster decomposition	128
7.4	Gröbner basis and broom algorithm	130
7.5	Threshold theorem for topological stabilizer codes	133
7.6	Benchmark of the decoder	137
8	Self-correcting quantum memory	138
8.1	Previous work	139
8.2	Storage scheme	140
8.3	Properties of the Lindbladian	142
8.4	Analysis of thermal errors	144
8.5	Correctability of errors with an energy barrier	147
8.6	A lower bound on memory time	150
8.7	Numerical simulation	151
A	Commutative algebra	156
A.1	Rings and homomorphisms	157
A.2	Ideals and modules	158

A.3 Gröbner basis	163
A.4 Localization	170
A.5 Determinantal ideal	175
A.6 Finite fields	181
Bibliography	184

Chapter 1

Introduction

The idea of quantum computer dates back at least to Feynman [1], who speculated a possibility for exploiting the computational power that Nature allows. The idea raises a deep question. The computation is a manipulation of symbols and numbers according to our logical system. If we can simulate the time evolution of Nature in a controllable and mechanical way, then it is unavoidable to conclude that the present Nature is really computing the future, and that the way she does is essentially the same as our arithmetic. If we cannot simulate what she does, then it means there is a fundamental difference between the time evolution and its artificial simulation by our logic and numbers. Either conclusion must have profound consequences.

An important problem in proving the possibility of a quantum computer is how to suppress decoherence. Shor discovered a scheme in which as long as elementary operations have a low enough error rate one can perform an arbitrarily long computation [2]. He showed there is a positive constant δ such that any ideal computation can be simulated by faulty elementary operations if they are close to ideal ones up to precision δ ; the scheme effectively reduces the error rate. Thus, the problem of decoherence is solved at least theoretically.

Kitaev proposed yet different scheme, called topological quantum computation, in which elementary operations are physically protected and hence are ideal for all practical purposes [3]. He pointed out that there is a naturally protected subspace in topologically ordered systems in two spatial dimensions. The subspace is accessible by braiding excitations, so-called anyons. As long as the anyons are geometrically well separated at any time step of the computation, the subspace remains decoherence-free. A classical analog is easy to understand. In a magnetic storage medium a bit is encoded into one of two polarizations of little ferromagnets. Each little ferromagnet consists of billions or more electrons whose spins are aligned together. An electron spin may be flipped by some error, but it is energetically unfavorable. Many errors require high energy, and it is very unlikely that the average magnetization would change the sign. The main idea of the encoding quantum information in the topologically ordered system is similar. The information is carried not by local degrees of freedom, but by collective degrees of freedom, where local errors are suppressed by natural

means.

A requirement for a system to be useful for the topological quantum computation is that the system must have eigenstates of the same energy that are locally indistinguishable. The states only look different when one has a full description of them; the local reduced density matrices are identical. This property has no classical analog. Systems whose ground states are locally indistinguishable are already found. The fractional quantum Hall systems with a filling fraction $\nu = p/q$ have q degenerate ground states that are locally indistinguishable [4, 5]. The local indistinguishability accompanied by a finite energy gap above the degenerate ground states, has a significant consequence that the degeneracy does not split in the thermodynamic limit, even under general local perturbations [5, 3, 6]. This intrinsic stability underlies the idea to build a quantum computer on topologically ordered systems [7, 8, 9].

However, a closer analysis reveals that the topologically ordered system is vulnerable to thermal fluctuations [10]. The collective degrees of freedom are well protected as long as the anyons are far separated, but the thermal fluctuations cause the anyons to propagate randomly throughout the system. The random motions are not a priori suppressed by, for example, energetics. Anyonic systems do not function as protected media as the magnetic media do for classical information storage. That any topologically ordered system has a naturally protected subspace is not entirely true.

We need to separate the problem for further concrete discussions. A computer is loosely divided into two parts: reliable storage and fault-tolerant processing of information. The division is not too fundamental since the storage may require some sort of ancillary information processing, and vice versa. It is a convenient division for the sake of analysis. The storage problem for quantum information concerns a possibility of a quantum analog of classical hard disk drive, which we call a *self-correcting quantum memory*. One asks if there is a system where a subspace is maintained coherently as collective phenomena [7, 11]. The processing problem concerns a wise choice of an elementary operation set and its implementation, and is thus contingent upon the storage scheme. In this thesis we focus on the storage problem.

The result of the present thesis can be summarized as follows. We find a spin model on a three-dimensional cubic lattice, whose excitations are immobile and point-like. Under any perturbation the excitations do not acquire a kinetic term — any hopping amplitude vanishes exactly. Moreover, the ground-state subspace is degenerate, exactly in the thermodynamic limit, and no local order parameter can be defined. These properties do not fit into intuitive pictures people had about the topological order. The reason why it is unconventional will be explained below. Given the model, we devise a scheme to use it as quantum memory and compute the storage time. We prove a rigorous lower bound on the storage time that grows with system size up to an optimal value $T_{mem} = e^{\Omega(\beta^2)}$ where β is an inverse temperature of a heat reservoir. It should contrast with a conjectured storage

time $e^{O(\beta)}$ of any two-dimensional topologically ordered system.

We briefly review how the concept of topological order has emerged, and discuss our results.

1.1 Topological order

The quantum Hall effects are phenomena in which the transversal conductance becomes a locally constant function (plateau) for ranges of perpendicular magnetic field strength. In the integer quantum Hall effect, as the magnetic field is increased, the Hall conductance develops plateaus at quantized values of ne^2/h in the vicinity of field $B = \rho_0 hc/ne$ where n is a small positive integer and ρ_0 is the electron number density [12]. The quantization is very accurate and universal. The measured conductances from various experiments all agree with one another within a relative error less than a part in a million [13]. The agreement is so remarkable because different experiments do not fine-tune every aspect of experimental setups up to precision 10^{-6} . Due to its simple reproducibility and high accuracy, the integer quantum Hall effect is now used to define an international standard of resistance [14].

The exact quantization can be explained by Laughlin's argument [15], refined by Halperin [16]. They consider an adiabatic insertion of magnetic flux near the boundary of the Hall sample. They conclude that the Hall conductance is quantized because extended (delocalized) electronic states near the sample edge whose energies are far from Fermi level are only responsible for the conductance. Thouless *et al.* [17] showed that those extended states actually define a topological vector bundle whose invariant, now called TKNN invariant or Chern number, is directly related to the quantized Hall conductance.

The awe of the quantum Hall effects does not end there. Soon after the discovery of the integer quantum Hall effects, another kind of quantization was measured — the fractional quantum Hall effects [18, 19]. The transversal conductance displays many plateaus at fractional multiples of e^2/h , not only at integral multiples of e^2/h . An interesting feature is the structure of the ground-state subspace. There are q -fold degenerate ground states for a fractional quantum Hall system of filling fraction $\nu = p/q$ defined on a torus, where p and q are co-prime integers [20, 4]. By taking a detour through an effective theory, the degeneracy is argued to be a function of topology [5]. More specifically, if a fractional quantum Hall Hamiltonian at $\nu = p/q$ is defined on a Riemann surface of genus g , the degeneracy is q^g .

It is much more interesting that quasi-particles of the fractional quantum Hall system are thought to be *anyons* [21]. They obey neither bosonic nor fermionic statistics under exchange. Rather, the wave function of two-anyon state may be transformed by a unitary operator if one anyon is transported around the other. It has been conjectured that the nonabelian case, where the unitary is not just a phase factor, could be realized in a fractional quantum Hall system at certain filling fractions

$\nu = p/q$ [22, 23]. Unfortunately, the nonabelian statistics has not been verified experimentally.

Meanwhile, the concept of topological order had emerged. It was introduced as an abstract notion to describe the fractional quantum Hall systems and spin liquid states [24]. A gapped system is generally said to be topologically ordered if the ground-state subspace is degenerate but no symmetry is spontaneously broken, and the degeneracy is robust under any perturbation in the thermodynamic limit [25, 26]. Also, the degeneracy as a function of physical space topology and the anyonic quasi-particle statistics are taken as defining characteristics of topological order [5, 3, 23].

Another important yet different characteristic is topological entanglement entropy [27, 28]. A ground-state wave function of a gapped Hamiltonian is believed to obey an area law. Namely, the von Neumann entropy $S(\rho)$ of the reduced density matrix ρ for a disk region is bounded from above by a constant times the area of the boundary. In our two-dimensional situation, the area is the perimeter of the boundary, so $S(\rho) \leq \alpha L$. The topological entanglement entropy is a negative constant correction to the area law; $S(\rho) = \alpha L - \gamma$. Remarkably, the γ is insensitive to microscopic details and constant under deformation of the Hamiltonian as long as the deformation does not close the energy gap. This quantity is quite different in nature compared with other characteristics of topological order, since it is computed from a single wave function whereas the others are defined for Hamiltonians.

The topological order can be better understood by studying lattice gauge theories [29] and the toric code model [3]. One of the purposes to introduce lattice gauge theories is to contrast how our new model, called *cubic code*, is different from models in a conventional picture. The simplest possible lattice gauge theory is the Ising gauge theory due to Wegner [30]. Ising gauge theory can be defined in any dimensions, but let us focus on the two-dimensional square lattice first. Later we will see a direct relation to the toric code model.

Consider the two-dimensional square lattice with a Ising variable (spin) $Z = \pm 1$ at each edge. For each vertex v , let $A(v)$ be an operator that flips four spins around v ; $A(v) : \pm 1 \mapsto \mp 1$. $A(v)$ is called a *gauge transformation*. We can express it as an operator.

$$A(v) = X(N, v)X(W, v)X(S, v)X(E, v)$$

where $X(N, v)$ means the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{matrix} | +1 \rangle \\ | -1 \rangle \end{matrix}$ acting on the north edge of the vertex v , and similarly for others. We identify all states that related by the gauge transformations. We look for a “local” Hamiltonian that is invariant under the action of $A(v)$. Here, the locality may be ambiguous since we have identified states that differ by the gauge transformations and formed a Hilbert space that is not a tensor product of local constituents. However, the locality is still a proper notion with respect to the square lattice.

The gauge invariance allows restricted possibilities of terms in the Hamiltonian. It is not hard

to see that a term in the Hamiltonian must be a product of Z 's along a closed loop. The simplest closed loop is a single plaquette. Thus, the simplest Hamiltonian would be given by the sum over all plaquettes p

$$H = -J \sum_p B(p) = -J \sum_p Z(b,p)Z(r,p)Z(t,p)Z(l,p) \quad (1.1)$$

where $J > 0$ and $B(p)$ is the product of four Ising variables on the bottom, right, top, and left of the plaquette p . It is important that the ground-state subspace does not spontaneously break any gauge symmetry. It is a general statement (Elitzur's theorem [31]) whose proof is not difficult [29, 32].

If H is defined on a torus with periodic boundary conditions, there are four ground states that are not equivalent under the gauge transformations. This can be understood by visualizing configurations by loops. The configuration C_0 with all spins taking $+1$ values is a ground state of H . Any equivalent state under the gauge transformations is obtained by applying $A(v)$ at vertices. A single $A(v)$ flips four spins. Imagine connecting those flipped spins by straight lines — they will form a loop. Applying more gauge transformations A at various vertices, one adds more loops or deforms the loops. What is always true is that the loops are homologically trivial. Indeed, A can be interpreted as a boundary operator in the cellular homology with $\mathbb{Z}/2$ coefficient acting on the dual 2-cells. What if we start with a configuration C_1 with all spins $+1$ except those -1 along a homologically nontrivial loop of the torus? Since A does not alter the homology class of the configuration, we conclude that C_0 and C_1 cannot be equivalent under the action of A . Since there are 4 distinct homology classes of the torus including the trivial one C_0 , the degeneracy is therefore 4. We emphasize that the homology classes are not locally distinguishable.

One can generalize the model so that it is defined on an arbitrary surface with a triangulation. The gauge transformations will be defined for each vertex, and the Hamiltonian will be a sum of all terms B , the product of Ising variables along the perimeter of elementary triangles. The homology description will be valid as well. The degeneracy is a function of homology of the surface.

Returning to the square lattice, we ask how an excited state looks like. It is described by unhappy terms $B(p) = -1$ in H . If we flip a spin from a ground state, then the two adjacent plaquette terms will become unhappy. If we flip two spins, say, one on the left and another on the right of a plaquette p_0 , $B(p_0)$ will remain happy but those on the left plaquette and on the right will not. Generally, if we flip spins from a ground state such that flipped spins form a string on the dual lattice, then only two plaquette terms positioned at the end of the string will be unhappy. Those unsatisfied terms can be isolated at constant energy cost, and appear as the end points of the strings. If the string is extended to the infinity in one direction, there will be a single excitation. This is a topological excitation, in the sense that it cannot be created by a local operator, unlike a pair of nearby excitations. Note that the string that creates excitation has no gauge-invariant meaning. Applying $A(v)$ in the middle of an extended string will deform the string. The homological argument above shows that if two

strings with the same end points differ by a homologically trivial cycle, the two strings describe exactly the same excited states.

The properties of the Ising gauge theory we have reviewed here satisfy several criteria for topological order. Its degeneracy is a function of topology, and no symmetry is spontaneously broken. The four-dimensional ground space is stable under gauge-invariant perturbations. Can we obtain a similar model without the gauge symmetry? A prescription is to promote gauge transformations to be dynamical [3], and take the Hilbert space as the tensor product of individual spins. In other words, one adds gauge fixing terms to the Hamiltonian.

$$H' = -J \sum_p B(p) - g \sum_v A(v) \quad (1.2)$$

Since the Hamiltonian H is constructed to be invariant under the gauge transformations, the new quantum Hamiltonian H' is exactly solvable. The ground state is an equal-weight superposition of all equivalent spin configurations under the old gauge transformations. Our analysis on the absence of local order parameters and the degeneracy using the cellular homology is still valid. As the homology classes of spin configuration in the Ising gauge theory were not locally distinguished, the quantum ground states of H' are not locally distinguished. It follows that the degeneracy is not lifted under any local perturbations [6]. Indeed, it is easily checked that the first order degenerate perturbation theory is vacuous because any local operator sandwiched between two ground states $|a\rangle$ and $|b\rangle$ is proportional to $\langle a|b\rangle$.

The gauge symmetry is not strictly imposed any more, but a particular gauge choice is energetically preferred. Accordingly, there is one more type of excitations given by unsatisfied $A(v)$ terms, known as e -particles. A violated $B(p)$ -term is known as m -particle. Note that there is a duality between A and B terms. A consists of Pauli $X = \sigma^x$ acting on a plaquette on the dual lattice, and B consists of Pauli $Z = \sigma^z$ acting on a plaquette on the primary lattice. A pair of m -particles can be created from a ground state by applying “spin flip” operators X along a string on the dual lattice. A pair of e -particles can be created from a ground state by applying “phase flip” operators Z along a string on the primary lattice. The e - and m -particles display mutual anyonic statistics. When one makes a complete circle around the other, the wave function acquires a phase factor -1 . The topological entanglement entropy is nonzero [27, 28]. We obtained an exactly solvable simple model with topological order, the *toric code*.

1.2 String operators

The string operators in the toric code deserve much attention. They are topological objects in that only the homological classes they represent matter. The fact that the strings are extended objects

makes it clear how two particles at a distance may interact by braiding. The nontrivial braiding, in turn, implies a nontrivial ground-state subspace. The argument is basically the same as the proof of the degeneracy of the fractional quantum Hall system using magnetic translations [4].

The string picture seems to be correct for all two-dimensional topologically ordered systems. The robust degeneracy implies that there is no local observable that can distinguish different ground states; otherwise, perturbing the system with that local observable will lift the degeneracy. A minimal “global” operator whose support is not local would be a string operator stretched across the system. Another conceivable argument is as follows. Consider a region R as large as possible on which no observable can resolve the ground-state subspace. If we assume translation invariance so we can unambiguously speak of thermodynamic limit, then a local operator is any operator with a bounded support. Hence, on a torus geometry, R can be taken as the whole system minus two narrow strips, ensuring R to be a contractible region. Since any operator in R cannot resolve the ground-state subspace, some operator in the strips must be able to resolve it, which suggests the existence of string operators. As we will see in Chapter 2, the argument here can be made rigorous for a class of models. Also, there is an attempt to understand every possible model in two dimensions with the string picture [33, 34].

What will happen if we go to three spatial dimensions? Consider a three-dimensional Ising gauge theory. The gauge transformation $A(v)$ is defined for each vertex v , and the Hamiltonian will be the sum of all plaquette terms $B(p)$. For the 3D simple cubic lattice, a single spin-flip at an edge will violate four plaquette terms attached to that edge. Many spin flips that form a surface on the dual lattice will violate plaquette terms along its boundary. In general, excited states are caused by *surface* operators and described by loops of unhappy plaquette terms, analogous to domain walls of the 2D Ising model.¹ Now we add gauge fixing terms $A(v)$ into the Hamiltonian to obtain a quantum model, called three-dimensional toric code. As before, there is a new type of excitation, an unsatisfied $A(v)$ term. Let us call $A(v)$ a *star* term. Unlike the plaquette excitations that form loops, the star excitation is attached to a *string* operator along a path in the primary lattice. The star excitations can therefore be isolated.

There are two types of operators acting on the degenerate ground-state subspace. A different ground state is obtained by flipping all spins on a plane that wraps around the system. When a finite system with periodic boundary conditions are considered, the locations of the flipped spins form a nontrivial homological 2-cycle of 3-torus. The other type of operator on the ground-state subspace is the string operator. If we apply the string operator along a nontrivial homological 1-cycle of the 3-torus, then the star excitation does not appear since there is no end points, and a ground state is mapped to a different one. There are three closed surface operators and three closed string operators, as the homology group of 1-cycles and 2-cycles are generated by three elements,

¹An exact mapping actually relates 3D Ising gauge theory with 3D Ising model [30].

respectively.

The closed surface operator \bar{X} and the closed string operator \bar{Z} generate a nontrivial algebra, because, when a pair of \bar{X} and \bar{Z} share a common support, the intersection is just a single spin on which the pair anti-commute. Of course, \bar{X} and \bar{Z} are topological objects and there are many equivalent representatives. One can easily check that in for any equivalent representatives the algebraic structure does not change.

The (closed) string and surface operators seem to be universal for any topologically ordered models. If the ground-state subspace is robust under any perturbations, the algebra generated by the operators acting on the ground-state subspace must also be robust. Note that operators of extended overlapping support may not define a robust algebra. For example, $\bigotimes_{i=1}^n \sigma^x$ and $\bigotimes_{i=1}^n \sigma^z$ commute if n is even, but anti-commute if n is odd. In order to make a well-defined algebra, it is the most straightforward for the operators of extended support to intersect at a point-like (zero-dimensional) support. In other words, an n -dimensional operator would have a nontrivial commutation relation with a $(D - n)$ -dimensional operator, where D is the total spatial dimension. If there were a three-dimensional model with all surface-like operators acting on the ground-state subspace, they must intersect along a one-dimensional line. The length of the one-dimensional line is not topological, and it would be hard for them to form a robust algebra. Therefore, in three dimensions, it seems necessary for the string operators to exist. In four spatial dimensions it is possible to construct a model that has a robust ground-state subspace such that all operators on it have two-dimensional support [7].

We remark that the existence of string operators implies that point-like excitations at the ends of the string are *mobile* generically. Although the e - and m -particles of the two-dimensional toric code, being eigenstates of H' , are stationary, the excitations will acquire a kinetic or hopping term under generic perturbations. This is the reason why the topological order at finite temperature is said to be not stable. At nonzero temperature there must be a nonzero density of the mobile excitations. Their spatial fluctuation induced by the thermal interaction is strong enough to disorder the ground state completely. Topological entanglement entropy calculation at nonzero temperatures supports this intuition [35]. In terms of a measure how difficult it is to generate a state, the Gibbs state of some topologically ordered model with string operators is not too different from a trivial product state [36]. Moreover, the relaxation time towards the Gibbs state of the two-dimensional toric code is only a constant independent of the system size [10].

1.3 Quantum codes and a new model

In our discussion so far, the topological order is characterized by a collection of very compelling properties of Hamiltonians or ground-state subspaces. However, it is not too clear which one is

more fundamental. Even, it is not clear whether all those characteristics should appear all together. The quantum Hall effects [13] and topological insulators [37] should serve as reference systems. It appears that the local indistinguishability of ground-state subspace is the most mathematically tractable definition of the topological order. We adhere to this definition. To obtain enough intuition, we would like to study toy models arising from quantum error correcting codes.

Shor’s fault-tolerant scheme [2] is based on the discovery of quantum error correcting codes. He demonstrated that there exists a subspace in a many-qubit Hilbert space such that local errors can be detected and corrected with a high probability without disturbing encoded (logical) quantum state. Measurements inevitably disturb the system, but a trick is that the logical state is encoded in the entanglement of the many qubits. It is essential that different encoded states look exactly the same to the local errors; they are locally indistinguishable.

It did not take too long for people to realize that the Shor’s error correcting code can be generalized and studied in an analogous way that one studies classical error correcting codes [38, 39, 40, 41]. The connection is due to the observation that the encoded state can be described as the eigenstate of pairwise commuting tensor products of Pauli spin- $\frac{1}{2}$ matrices; the state is stabilized by commuting operators. The commutativity is important because, otherwise, we cannot speak of common eigenstate. The encoded state is required to be highly entangled, and hence avoids in general an efficient classical description. However, the stabilizer operator language tells us that some class of highly entangled states has a simple description, which is enough to ensure the local indistinguishability. We explain this in detail in Chapter 2.

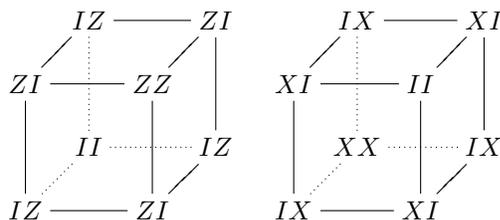
The toric code Hamiltonian H' in Eq. (1.2) can be viewed as a quantum code. The terms $A(v)$ and $B(p)$ consist of Pauli matrices and commute with each other. If the coupling constants J and g are both positive, then a ground state is a common eigenstate of eigenvalue $+1$. (Having $+1$ eigenvalue ensures H' is not frustrated.) In general, if a code is defined by a local commuting Pauli operators, we can write a corresponding Hamiltonian given by the negative sum of all the commuting Pauli operators. If the code has a good error correcting capability, the corresponding Hamiltonian must have a locally indistinguishable ground-state subspace.

As we have seen earlier, the toric code Hamiltonian captures essential characteristics of the topological order. It is one of good motivations to study Hamiltonians with commuting Pauli operators in order to understand the topological order. One might be uneasy with the fact that the Hamiltonian H' is a four-body interaction. This “unrealistic” interaction may be effective at low energies, if, for example, a realistic Hamiltonian is highly frustrated from which the effective H' is derived [26, 42]. We will be not concerned about the order of the interaction as long as it is local.

One of our guiding problems is the possibility of self-correcting quantum memory. We wish to have a system whose ground-state subspace is locally indistinguishable so that local errors do not corrupt an encoded state. In addition, we demand that there be a physical mechanism such that

local errors do not accumulate. The string operators of the previous section are against our goal. Since they make excitations mobile, the physical mechanism to prohibit the error accumulation cannot be achieved. Hence, in two dimensions it seems impossible to have a self-correcting quantum memory. Indeed, one can rigorously prove the existence of the strings operators for a class of models in two dimensions, starting from the local indistinguishability assumption [43, 44, 45]. We noted in the previous section that there is a four-dimensional topologically ordered model lacking the string operators [7]. This model indeed functions as a self-correcting quantum memory below a critical nonzero temperature [46].

A more realistic three-dimensional case is hence interesting. Based on the dimensional duality of the operators acting on the degenerate ground-state subspace, a no-go theorem seemed plausible [47]. In this thesis we present a concrete counterexample, cubic code, to this intuition.



The cubic code is a quantum error correcting code on the simple cubic lattice defined by local Pauli operators acting on elementary cubes. There are two qubits (spin- $\frac{1}{2}$) at each site. The two-letter symbol such as XI means a tensor product $\sigma^x \otimes I$, and ZZ means $\sigma^z \otimes \sigma^z$, etc. Each diagram represents a tensor product of eight Pauli matrices. The Hamiltonian is the negative sum of two diagrams over all elementary cubes. As required, the model has a degenerate ground-state subspace that is locally indistinguishable. Most importantly we can prove that there does not exist any string operator. However, it admits isolated point-like topological excitations. They do not appear as the end points of the string, but as the vertices of *fractal* operators. The fractal operators is supported on a self-similar structure. The absence of string operators implies that the point-like topological excitations are immobile; any hopping amplitude vanishes exactly. It is also interesting that the degeneracy depends sensitively on the number-theoretic property of the lattice size, illustrated in Figure 5.2 on page 92. The cubic code is a conceptually new phase of matter.

It is necessary to explain more how the vanishing hopping amplitude and the isolated point-like topological excitation are simultaneously possible. By a topological excitation, or a *charge* for short, we mean a localized excitation that cannot be created from a ground state by any finitely supported operator. A kink in the 1D Ising model is the simplest example. The isolation of a charge in the cubic code is possible under a self-similar construction as follows. In Figure 1.1, the first figure shows how excitations look like when an X error occurs on a ground state. The second figure show the excitations given four X errors. Note that when two charges are at the same position, they

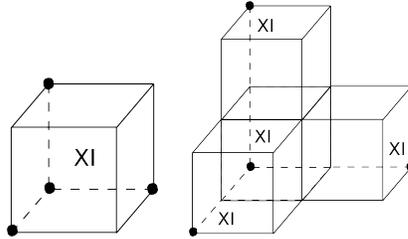


Figure 1.1: Isolating a topological excitation. The cubes are in the dual lattice; each vertex represents an elementary cube in the primary lattice.

cancel with each other. The configurations are similar by ratio 2, so one can construct even larger configuration where there are only four excitations that are far separated. In the limit of this process there is an isolated charge. The reason why the hopping amplitude vanishes can be heuristically understood by the construction. It is impossible to have a configuration where only one charge is moved away while the other three are held fixed. Such a configuration is forbidden in the spectrum of the Hamiltonian. The transition amplitude to a non-existing state from any state must be vacuous. We later prove it rigorously. A classical model where this happens was discovered by Newman and Moore [48]. Our model is inherently quantum with a locally indistinguishable ground-state subspace and has a gapped energy spectrum that is robust under generic perturbations [6].

We show that the cubic code model can be used as a quantum memory at nonzero temperatures in the following sense. We develop a well-defined read-out procedure (decoder) with which a ground state maintains coherence for time proportional to $L^{c\beta}$ where L is a linear system size and β is an inverse temperature. This statement is valid only if $L \leq e^{c'\beta}$. Roughly speaking, this is because of a large entropic contribution from the point-like excitations. For small system size, the entropic contribution is small. At an optimal system size, the memory time is $e^{cc'\beta^2}$. A natural question is then whether we could remove all such point-like excitations. We answer this question negatively: There must be an isolated point-like excitation in any topologically ordered three-dimensional quantum code model if it is translationally invariant. The proof is based on a formalism using translation group algebras and free resolutions of finitely generated modules.

1.4 Summary of chapters

In Chapter 2, we explain a general structure of a class of quantum error correcting codes, called additive or stabilizer codes. It is emphasized that the additive code is described by a binary vector space. A simple counting of vector space dimensions yields *cleaning lemma*. It states that the number of independent logical operators on complementary regions add up to the total number of independent logical operators of the code. Combining the geometric locality of two-dimensional Hamiltonian with the cleaning lemma, we prove a trade-off theorem about the support of the logical

operators. In particular, this implies that only string operators act on the ground-state subspace in two-dimensional quantum codes. The content is published in [44].

In Chapter 3, we develop a formulation of translationally invariant quantum codes. We observe that they have a succinct description by a matrix σ over the translation group algebra which is commutative. The local indistinguishability is interpreted as a vanishing homology of a complex defined by σ . Local unitary transformations and coarse-graining are described by simple matrix operations. The ground-state degeneracy is approximated as the number of points on an algebraic variety defined by σ over finite fields. Fractal operators and point-like excitations are defined, and the set of all point-like excitations modulo locally created ones is identified with a specific module. The content is published in [49].

In Chapter 4, we use the formalism of Chapter 3 to derive consequences of physical dimensionality. The translation invariance is imposed. One-dimensional codes are classified completely. Up to local unitary transformations, any code decomposes into finitely many 1D Ising models. In two dimensions, we prove that there are finitely many types of topological excitations and they all appear as end points of string operators. In three dimensions, we prove that there must exist a point-like topological excitation. If the ground-state degeneracy is constant independent of system size, we show that the point-like topological excitations are attached to string operators. Examples are presented for which our formalism is useful. The content is published in [49].

In Chapter 5, we explain how the cubic code is found. It is a result of an exhaustive but systematic search. We prove important properties of the cubic code such as the topological order, ground-state degeneracy, and the absence of string operators. The cubic code's thermal partition function is computed to show that the free energy density is smooth in the thermodynamic limit as a function of temperature. An entanglement renormalization group flow is presented. We find that the cubic code (A) bifurcates into itself (A) and another model B. The new model B shares all important properties of A, but is different from A. Under a further real-space renormalization, B bifurcates into two copies of itself. A part of the content in this chapter is published in [50]. Our presentation in this thesis is more succinct than that in the published paper, due to algebraic methods of Chapter 3 developed more recently.

In Chapter 6, we prove theorems implied by the absence of string operators. The theorems quantifies the energy landscape of the Hamiltonian on the “land” of energy eigenstates. Two states are considered to be “close” in the land if one state can be transformed to the other by a single spin operator; if it is necessary to apply many spin operators, the two states are considered to be far apart in the land. On this land of states, imagine hills whose height is given by the energy of the state. The landscape of this land is analogous to a potential energy barrier in a quantum mechanical tunneling problem. We define the *energy barrier* to be the height of the lowest hill on any path in the land connecting two states. We prove that between two ground states there exists an energy

barrier larger than the logarithm of the system size L , and the distance in the land is at least L^γ with $\gamma > 1$. A closely related statement reads that between a ground state and a state where a topological excitation is isolated from others by distance R , there exists an energy barrier $\geq \log R$, and the distance in the land is $\geq R^\gamma$ with $\gamma > 1$. The content is published in [51].

In Chapter 7, we design a decoding algorithm. Any physical memory cannot be pristine after contact with an error source. In order to retrieve correct information for the next step of processing, one needs to map the affected state to the ground state. For a ferromagnet this decoding process amounts to measuring average magnetization. For quantum codes, the first step is to detect errors. This is done by measuring the terms in the commuting Hamiltonian. The next step is to guess probable types and locations of errors, which we specifically call “decoding algorithm.” Once error locations and types are identified, the final step is to undo the errors. A good decoder should map corrupt states to its original pristine state with high probability. Our algorithm uses a hierarchy of subroutines which borrows ideas from renormalization group. It is widely applicable and is efficient with running time $O(V \log V)$ where V is the volume of the system. Moreover, we prove that there is a positive critical error probability, called a threshold, below which the decoding algorithm succeeds asymptotically perfectly in the limit of large system size. Our decoder is the first decoder that admits an efficient implementation and a rigorous threshold theorem. The content is published in [52].

In Chapter 8, we directly assess the performance of the cubic code as a robust quantum memory at nonzero temperature. One ingredient is to show that the decoding algorithm of Chapter 7 corrects errors of low energy barriers. Here, the energy barrier of an error is defined in the same way as above — the height of lowest hill in the energy landscape on any path connecting a ground state and the state affected by the error. Another ingredient is an analysis of Markovian master equation exploiting the fact that there exists a good decoder Φ_{ec} , a trace preserving completely positive quantum operation. An analytic bound on the trace distance between the initial state $\rho(0)$ and the error-corrected time-evolved state $\Phi_{ec}(\rho(t))$ is given as

$$\|\rho(0) - \Phi_{ec}(\rho(t))\| \leq t \frac{(1 + e^{-\beta})^V}{V^\beta}$$

where V is the system volume and β is the inverse temperature, neglecting all unimportant constant coefficients. If $V \leq e^\beta$, the bound says the fidelity of error-corrected $\Phi_{ec}(\rho(t))$ remains close to $\rho(0)$ until $t \sim V^\beta$. We complement the bound with a numerical simulation, which suggests that our bound is optimal up to constant coefficients. The content is published in [52].

Chapter 2

Additive quantum codes

The theory of quantum error correcting code is an important cornerstone for fault-tolerant quantum computers [2, 53]. One encodes states one wish to compute about into logical many-qubit states in such a way that errors that are likely to happen will be correctable. Thus, at the logical level an effective error rate is much smaller than the physical error rate. Computation can be carried on this logical level, and the overhead of error correction can be controlled, not to overwhelm the promised computation. After the discovery of the very first quantum error correcting code by Shor [54], people have quickly realized analogy between classical error correcting codes and a class of quantum error correcting codes [41, 40], which are now known as additive or stabilizer codes. Arguably, it is the most studied class of codes, and is the main object of the present thesis. The connection between the classical codes and quantum additive codes is provided by the parameterization of basis operators (Pauli matrices) by binary numbers. In this chapter we review and exploit this correspondence.

The chapter is organized as follows. Section 2.1 provides a convenient and important viewpoint under which the multiplicative group of all Pauli matrices are described by a vector space over the binary field. Section 2.2 builds on this viewpoint and explains how to choose a subspace of a many qubit Hilbert space, which we hope to have a capability to correct errors. Section 2.3 is devoted to derive an equation, called a cleaning lemma, that relates the numbers of logical operators that can be supported on complementary regions and the total number of logical qubits. It is remarked that the cleaning lemma implies that any error occurring within a region, where no nontrivial logical operator can be supported, can actually be corrected by a physical operation.

The last section 2.4 presents an application of the cleaning lemma which gives a constraint on the geometric shape of logical operators of local codes on lattices. Most importantly, it is proved that in two-dimensional lattice codes with geometrically local generators with large code distance, all logical operators have representatives supported on narrow strips. It had been known by Bravyi and Terhal [43] that there exists a nontrivial logical operator supported on a strip. Our conclusion extends this result by finding the geometric shape of *all* logical operators. If the minimal weight logical operator has weight proportional to the linear dimension of a two-dimensional system, then

all logical operator can be found on narrow strips [44].

Note that there are many interesting quantum codes that are not necessarily additive [55, 3, 34], but they are out of the scope of this thesis.

2.1 Pauli group as a symplectic 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**. When finitely many qubits are considered, a Pauli operator is of course an *arbitrary* tensor product of Pauli matrices.

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 $\bigoplus_{i \in \Lambda} V_i$, which we call **Pauli space**, 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 sym-

plectic form [41]. Let

$$\lambda_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

be a symplectic form on the vector space $(\mathbb{F}_2)^2$ of 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 and O_2 . Two multi-qubit Pauli operator (anti-)commutes, if and only if there are (odd) even number of pairs of the anticommuting single-qubit Pauli operators in their tensor product expression. Therefore, 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**.

Remark 2.1. For systems of qudits, a group corresponding to the Pauli group in the qubit case is the so-called generalized Pauli group [56, 57, 58, 59]. It is the set of all tensor products of powers of $d \times d$ matrices

$$X_d = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ & & \ddots & & \vdots \\ & & \cdots & 1 & 0 \end{pmatrix} \quad \text{and} \quad Z_d = \begin{pmatrix} 1 & & & & \\ & \omega & & & \\ & & \omega^2 & & \\ & & & \ddots & \\ & & & & \omega^{d-1} \end{pmatrix} \quad (\omega = e^{2\pi i/d}),$$

which satisfy

$$X_d Z_d = \omega^{-1} Z_d X_d.$$

Hence, any generalized Pauli operator on a single qudit is a product $X_d^n Z_d^m$. The abelianized generalized Pauli group is identified with $P = (\mathbb{Z}/d\mathbb{Z})^2$, a module over $\mathbb{Z}/d\mathbb{Z}$. If d is a prime number, $\mathbb{Z}/d\mathbb{Z} \cong \mathbb{F}_d$ is a field and the P is a vector space over \mathbb{F}_d . The commutation relation can be recovered by the symplectic form λ_1 . The generalization to a system of qudits is straightforward.

Most statements in this thesis are true or easily extended for qudits with prime dimensions. An exception is Levin-Wen fermion model of Example 4.4.

Since the Pauli group can be effectively described by a vector space equipped with a symplectic form, it is worth studying symplectic vector spaces in general. Any vector space in this section is with respect to some fixed field \mathbb{F} .

Let V be a (finite dimensional) vector space. A bilinear form $\lambda : V \times V \rightarrow \mathbb{F}$ is **symplectic** or

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

4. Replace b_{2m+j} ($j \geq 1$) with

$$b'_{2m+j} := b_{2m+j} + \sum_{i=1}^m (\lambda(b_{2m+1}, v_i)w_i - \lambda(b_{2m+1}, w_i)v_i).$$

One sees that the b'_{2m+j} are orthogonal to W_m and still linearly independent.

5. Iterate 1-4 with $\text{span}_{\mathbb{F}}\{b'_{2m+j} | j \geq 1\}$.

From the algorithm, we have a structure theorem for finite dimensional symplectic vector spaces.

Proposition 2.1.1. *Let V be a finite dimensional vector space equipped with a symplectic form over any field. Then, V is a direct sum of a hyperbolic subspace and a null subspace. In particular, if the symplectic form is non-degenerate, then V must be even dimensional.*

It is important that *the abelianized Pauli group is non-degenerate symplectic* over \mathbb{F}_2 , since any Pauli operator anticommutes with some Pauli operator.

As noted earlier, there are many canonical bases. The linear transformations that connect different bases are called **symplectic transformations**, i.e., T is a symplectic transformation if

$$T^T \lambda_q T = \lambda_q = \begin{pmatrix} 0 & \text{id}_q \\ -\text{id}_q & 0 \end{pmatrix}.$$

The symplectic transformation decomposes into a composition of three elementary transformations [41, 61], as any general linear transformation decomposes into a composition of row operations and scalar multiplications by Gauss elimination. For notational clarity, define $E_{i,j}(a)$ ($i \neq j$) to 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 $a \in \mathbb{F}_2$ is a scalar. The following are **elementary symplectic transformations**:

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

The fourth one is a combination of the first and the third.

Proposition 2.1.2. [41] *The elementary symplectic transformations generate the group of all symplectic transformations.*

Proof. It suffices to prove that an arbitrary symplectic transformation T is a finite composition of elementary ones. T is a $2q \times 2q$ matrix over \mathbb{F}_2 . Let us write $T \cong T'$ if two matrices are transformed by elementary symplectic transformations. Since any row operation in the upper half block of T can be compensated by an appropriate row operation in the lower half block by controlled-NOT (CNOT). One can then transform the upper half block into the reduced row echelon form. Since T has rank $2q$, the upper half block must have rank q . Therefore,

$$T \cong \begin{pmatrix} \text{id} & * \\ M & * \end{pmatrix}$$

where M and $*$ are all $q \times q$. Using CNOT-Hadamard, one can eliminate the first column of M . Then, since $T^T \lambda_q T = \lambda_q$, the first row of M must be zero. Inductively, one can completely eliminate all entries of M .

$$T \cong \begin{pmatrix} \text{id} & L \\ 0 & N \end{pmatrix}$$

The equation $T^T \lambda_q T = \lambda_q$ now implies that $N = \text{id}_q$. L can be made zero by a similar transformations as M was made zero. Thus, we have

$$T \cong \begin{pmatrix} \text{id} & 0 \\ 0 & \text{id} \end{pmatrix}.$$

An arbitrary symplectic transformation T is equivalent to the trivial transformation by elementary symplectic transformations. \square

As one can easily see, the elementary symplectic transformations are induced by the following unitary operators.

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{matrix}, \quad \text{Hadamard} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{matrix} |0\rangle \\ |1\rangle \end{matrix}, \quad \text{Phase} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-1} \end{pmatrix} \begin{matrix} |0\rangle \\ |1\rangle \end{matrix}$$

2.2 Additive/stabilizer codes

An **additive** [62] or **stabilizer** [40] **code** is a quantum code defined by the common eigenspace, called **code space**, of *commuting Pauli operators*, called **stabilizers**, of eigenvalue $+1$ acting on many physical qubits. It is required that the group of stabilizers should not contain $-I$ in order for the code space not to be zero. The number of physical qubits q is called **code length**. From the relation of the group of Pauli matrices and the binary linear space, each additive or stabilizer code

corresponds to a unique null-symplectic subspace of the abelianized Pauli group of q qubits. (The requirement that the stabilizer group should not contain $-I$ is however an independent condition.) If the null-symplectic subspace is spanned by columns of a matrix σ over \mathbb{F}_2 , then the nullity is expressed by a matrix equation

$$\sigma^T \lambda_q \sigma = 0 \quad (2.1)$$

where

$$\lambda_q = \bigoplus_{i=1}^q \lambda_1 = \begin{pmatrix} 0 & \text{id} \\ -\text{id} & 0 \end{pmatrix}$$

By fixing the form of λ_q , we also fix a convention for the abelianized Pauli group. The first q components represents Pauli matrices σ^x and the second q components σ^z .

In view of Eq. (2.1), an additive code is a classical linear code with an additional nullity condition. Calderbank and Shor [38], and Steane [39] (CSS) proposed a solution to this matrix equation of form

$$\sigma = \begin{pmatrix} C_1 & 0 \\ 0 & C_2 \end{pmatrix}$$

where $C_1^T C_2 = 0$, which we now call CSS code. The history actually goes backwards. CSS first constructed quantum codes. Later, Calderbank, Rains, Shor, and Sloane [41], and Gottesman [40] formulated a version with the full matrix equation Eq. (2.1). The matrix σ is called **generating matrix** of the code.

We may extend the basis for the null space V spanned by the columns of σ to a canonical basis B of whole Pauli space P by the Gram-Schmidt process. Another canonical basis C of P is induced by

$$\{\sigma^x \otimes I \otimes \cdots, I \otimes \sigma^x \otimes \cdots, \dots, \sigma^z \otimes I \otimes \cdots, I \otimes \sigma^z \otimes \cdots\}$$

Two bases are interchanged by a symplectic transformation, and due to Proposition 2.1, such a symplectic transformation is induced by *unitary* operators CNOT, Hadamard, and Phase. Under the basis C , the code space (trivial code) is the common eigenspace of

$$\{\sigma^z \otimes I \otimes \cdots, I \otimes \sigma^z \otimes \cdots\}$$

of eigenvalue $+1$. If $s = \dim_{\mathbb{F}_2} V \leq q$, then the code space consists of all states of $q - s$ qubits. That is, the **trivial code** is

$$|0\rangle^{\otimes s} \otimes \text{span}_{\mathbb{C}}\{|i_1 \cdots i_{q-s}\rangle | i_a \in \mathbb{F}_2\}.$$

It is clear that the orthogonal complement V^\perp with respect to the symplectic form is a direct sum of V itself and a hyperbolic subspace of P . In conclusion, if there are s independent stabilizers, the

code space dimension is 2^{q-s} and there are $q-s$ pairs of Pauli operators commuting with every stabilizer that give rise to a hyperbolic subspace in the symplectic Pauli space. These $q-s$ pairs of Pauli operators are logical operators. The **logical operators** are by definition operators that preserve the code space. If they are Pauli operators, they must belong to V^\perp . Focusing on the action on the code space by the logical operators, one realizes that different logical operators might have the same action. Indeed, if U is a logical operator, then US is also a logical operator for any stabilizer S of the same action on the code space:

$$US|\psi\rangle = U|\psi\rangle$$

where $|\psi\rangle$ is any code vector. Conversely, if two logical Pauli operators U_1 and U_2 have the same action, then $U_1^\dagger U_2$ have the trivial action so it must be proportional to a stabilizer. Therefore, an equivalence class of logical *Pauli* operators precisely corresponds to a coset of V^\perp/V . Sometimes, stabilizers are called **trivial logical operators**.

The **weight of a Pauli operator** is the number of its non-identity tensor factors. Likewise, the **weight of a vector** is the number of its nonzero components. A particularly interesting logical operator is one that corresponds to the *minimal weight* representative of nonzero elements of V^\perp/V . This minimal weight is called **code distance**, **minimal distance** or just distance for short. The importance of the code distance in relation to error correcting capability will become clear once we establish cleaning lemma in the next section.

2.3 Cleaning lemma

Although this thesis mainly discusses additive codes, the content of this section is stated in terms of *subsystem* codes. We continue to use the symplectic viewpoint for the Pauli group/space, and the terms group and space will be used interchangeably.

Let G be an arbitrary subspace of the Pauli space P . We denote by $[G]$ the dimension of G as a vector space over \mathbb{F}_2 . By Proposition 2.1.1, we have a decomposition $G = S \oplus W$ where S is null and W is hyperbolic. The orthogonal complement G^\perp consists of S and a hyperbolic subspace W' disjoint from W . Mapping to trivial code, we see that W' describes all Pauli operators acting on some qubits. A **subsystem code** is a selection of code space given by the states of qubits acted upon by W' [11, 63]. The common eigenspace of S has a nontrivial tensor decomposition $\mathcal{H}_{\text{gauge}} \otimes \mathcal{H}_{\text{logical}}$. The Pauli operators acting on $\mathcal{H}_{\text{gauge}}$ are represented by W , and those on the *subsystem* $\mathcal{H}_{\text{logical}}$ we wish to make use of are represented by W' . The code space of the subsystem code is identified with $\mathcal{H}_{\text{logical}}$. One may think of a subsystem code as a stabilizer code for which some logical operators are discarded. The group/space S is still called *stabilizer group/space*. G is

called **gauge group**. In this section *logical operators* only refer to Pauli operators. For subsystem codes, a **bare** logical operator is one that belongs to G^\perp , and a **dressed** logical operator is one that belongs to S^\perp . Since logical operators' action on $\mathcal{H}_{\text{gauge}}$ is ignored, the set of all equivalence classes of bare logical operators is G^\perp/S , and the set of all equivalence classes of dressed logical operators is S^\perp/G . It is clear that $G^\perp/S = W' = S^\perp/G$.

The cleaning lemma for subsystem codes relates the number of independent bare logical operators supported on a set of qubits M to the number of independent dressed logical operators supported on the complementary set M^c . The concept of the cleaning lemma was introduced in [43], then generalized in [64] and [65]. Here we use ideas from [64] to prove a version stated in [65]. (See also [66].)

We use P_A to denote the subgroup of the Pauli group P supported on a set A of qubits; likewise for any subgroup G of the Pauli group $G_A = G \cap P_A$, is the subgroup of G supported on A . We denote by $\Pi_A : P \rightarrow P_A$ the restriction map that maps a Pauli operator to its restriction supported on the set A , and we use $|A|$ to denote the number of qubits contained in A ; thus $[P_A] = 2|A|$.

If we divide n qubits into two complementary sets A and B , then a subgroup G of P can be decomposed into G_A , G_B , and a ‘‘remainder,’’ as follows:

Lemma 2.3.1. *Suppose that A and B are complementary sets of qubits. Then for any subgroup G of the Pauli group,*

$$G = G_A \oplus G_B \oplus G'$$

for some G' , where

$$[(G^\perp)_A] = 2|A| - [G_A] - [G'],$$

$$[(G^\perp)_B] = 2|B| - [G_B] - [G']$$

Proof. If V is a vector space and W is a subspace of V , then there is a vector space V' such that $V = W \oplus V'$; we may choose V' to be the span of the basis vectors that extend a basis for W to a basis for V . Since G_A and G_B are disjoint, i.e., $G_A \cap G_B = \{0\}$, $G_A \oplus G_B$ is a subspace of G , and thus there exists an auxiliary vector space $G' \leq G$ such that

$$G = G_A \oplus G_B \oplus G'.$$

The choice of G' is not canonical, but we need only its existence. Since the restriction map Π_A obviously annihilates G_B , we may regard it as a map from $G_A \oplus G'$ onto $\Pi_A G$. In fact this map is injective. Note that if $\Pi_A x = 0$ for some $x \in G_A \oplus G'$, then since $P = P_A \oplus P_B$ it must be that $x \in G_B$. But because the sum is direct, i.e., $G_B \cap (G_A \oplus G') = \{0\}$, it follows that $x = 0$, which proves injectivity. Hence $\Pi_A : G_A \oplus G' \rightarrow \Pi_A G$ is an isomorphism. Now, we may calculate $(G^\perp)_A$

by solving a system of linear equations. Noting that $x \in P_A$ is contained in G^\perp if and only if x commutes with the restriction to A of each element of G , we see that the number of independent linear constraints is $[\Pi_A G] = [G_A] + [G']$; hence $[(G^\perp)_A] = [P_A] - [G_A] - [G'] = 2|A| - [G_A] - [G']$. Likewise, $\Pi_B : G_B \oplus G' \rightarrow \Pi_B G$ is also an isomorphism, and hence $[(G^\perp)_B] = [P_B] - [G_B] - [G'] = 2|B| - [G_B] - [G']$. \square

Now we are ready to state and prove the cleaning lemma. For a subsystem code, let $g_{\text{bare}}(M)$ be the number of independent nontrivial bare logical operators supported on M , and let $g(M)$ be the number of independent nontrivial dressed logical operators supported on M , i.e.,

$$\begin{aligned} g_{\text{bare}}(M) &= [G^\perp \cap P_M / S_M] = [(G^\perp)_M / S_M], \\ g(M) &= [S^\perp \cap P_M / G_M] = [(S^\perp)_M / G_M]. \end{aligned}$$

Likewise, for a CSS subsystem code, let $g_{\text{bare}}^X(M)$ be the number of independent nontrivial bare X -type logical operators supported on M , and let $g^X(M)$ be the number of independent nontrivial dressed X -type logical operators supported on M , i.e.,

$$\begin{aligned} g_{\text{bare}}^X(M) &= [(G^Z)^\perp \cap P_M^X / S_M^X], \\ g^X(M) &= [(S^Z)^\perp \cap P_M^X / G_M^X], \end{aligned}$$

and similarly for the Z -type logical operators.

Lemma 2.3.2. (Cleaning lemma for subsystem codes) *Let k be the number of encoded qubits. For any subsystem code, we have*

$$g_{\text{bare}}(M) + g(M^c) = 2k,$$

where M is any set of qubits and M^c is its complement. Moreover, for a CSS subsystem code

$$g_{\text{bare}}^X(M) + g^Z(M^c) = k = g_{\text{bare}}^Z(M) + g^X(M^c).$$

Proof. We use Lemma 1 to prove the cleaning lemma by a direct calculation:

$$g_{\text{bare}}(M) = [(G^\perp)_M / S_M] = 2|M| - [G_M] - [G'] - [S_M],$$

and

$$g(M^c) = [(S^\perp)_{M^c} / G_{M^c}] = 2|M^c| - [S_{M^c}] - [S'] - [G_{M^c}].$$

Summing, we find

$$g_{\text{bare}}(M) + g(M_c) = 2|M| + 2|M_c| - ([G_M] + [G_{M_c}] + [G']) - ([S_M] + [S_{M_c}] + [S'])$$

and invoking Lemma 1 once again,

$$g_{\text{bare}}(M) + g(M_c) = 2n - [G] - [S] = 2k,$$

which proves the claim for general subsystem codes. For the CSS case, we apply the analogue of Lemma 1 to the X -type and Z -type Pauli operators, finding

$$g_{\text{bare}}^Z(M) = [(G^X)^\perp \cap P_M^Z/S_M^Z] = |M| - [G_M^X] - [(G^X)'] - [S_M^Z]$$

and also

$$g^X(M^c) = [(S^Z)^\perp \cap P_{M^c}^X/G_{M^c}^X] = |M^c| - [S_{M^c}^Z] - [(S^Z)'] - [G_{M^c}^X].$$

Summing and using Lemma 1 we have

$$g_{\text{bare}}^Z(M) + g^X(M^c) = n - [G^X] - [S^Z] = k;$$

a similar calculation yields

$$g_{\text{bare}}^X(M) + g^Z(M^c) = n - [G^Z] - [S^X] = k,$$

proving the claim for CSS subsystem codes. □

Of course, for a stabilizer code there is no distinction between bare and dressed logical operators; the statement of the cleaning lemma becomes

$$g(M) + g(M^c) = 2k$$

for general stabilizer codes, and

$$g^X(M) + g^Z(M^c) = k$$

for CSS stabilizer codes.

To understand how the cleaning lemma gets its name, note that it implies that if no bare logical operator can be supported on the set M then all dressed logical operators can be supported on its complement M^c . That is, any of the code's dressed logical Pauli operators can be “cleaned up” by applying elements of the gauge group G . The cleaned operator acts the same way on the

protected qubits as the original operator (though it might act differently on the gauge qubits), and acts trivially on M .

We say that a region M is *correctable* if there are no nontrivial dressed logical operators supported on M . If M is correctable then $g(M) = 0$ and thus $g_{\text{bare}}(M) = 0$. The cleaning lemma is then rephrased as follows.

Lemma 2.3.3. *For any subsystem code, if M is a correctable region and x is a dressed logical operator, then there is a dressed logical operator y supported on M^c that is equivalent to x .*

Remark 2.2. Given a correctable region M , we have a complete set of logical Pauli operators $\{y_a\}$ supported on M^c . Let U be the unitary transformation that maps the code space to that of the trivial code of the previous section; U is a composition of elementary symplectic transformations. Since any error e on M was (trivially) commuting with any y_a , it follows that UeU^\dagger acts by identity on the logical qubits of the trivial code. Replacing the non-logical qubits with fresh qubits and applying U^\dagger , we can map the damaged code vector to its original state. In conclusion, any error on the correctable region can be corrected. The code distance is the upper bound on the number of qubits in any correctable regions.

A more general error correcting criterion can be found in [61, Chapter 15].

2.4 Operator trade-off for local subsystem codes

In this section we consider local subsystem codes with qubits residing at the sites of a D -dimensional hypercubic lattice Λ . The code has **interaction range** w , meaning that the generators of the gauge group G can be chosen so that each generator has support on a hypercube containing w^D sites.

Definition 2.1. Given a set of gauge generators for a subsystem code, and a set of qubits M , let M' denote the support of all the gauge generators that act nontrivially on M . The **external boundary** of M is $\partial_+M = M' \cap M^c$, where M^c is the complement of M , and the **internal boundary** of M is $\partial_-M = (M^c)' \cap M$. The **boundary** of M is $\partial M = \partial_+M \cup \partial_-M$, and the **interior** of M is $M^\circ = M \setminus \partial_-M$.

Recall that a region (i.e., a set of qubits) M is said to be *correctable* if no nontrivial dressed logical operation is supported on M , in which case erasure of M can be corrected. Since the code distance d is defined as the minimum weight of a dressed logical operator, M is certainly correctable if $|M| < d$. But in fact much larger regions are also correctable, as follows from this lemma:

Lemma 2.4.1. *For a local subsystem code, if M and A are both correctable, where A contains ∂M , then $M \cup A$ is correctable.*

Proof. Given a subsystem code \mathcal{C} with gauge group G , we may define a subsystem code \mathcal{C}_{M^c} on M^c with gauge group $\Pi_{M^c}G$, where Π_{M^c} maps a Pauli operator to its restriction supported on M^c . We note that a Pauli operator x supported on M^c is a bare logical operator for \mathcal{C} if and only if x is a bare logical operator for \mathcal{C}_{M^c} ; that is, x commutes with all elements of G if and only if it commutes with all elements of the restriction of G to M^c .

Furthermore, if x is a dressed logical operator for \mathcal{C}_{M^c} supported on ∂_+M , then x can be extended to a dressed logical operator \bar{x} for \mathcal{C} supported on ∂M . Indeed, suppose $x = yz$, where y is a bare logical operator for \mathcal{C}_{M^c} (and hence also a bare logical operator for \mathcal{C} supported on M^c), while z is an element of the gauge group $\Pi_{M^c}G$ of \mathcal{C}_{M^c} . Then z can be written as a product $z = \prod_i g_i$ of generators of $\Pi_{M^c}G$, each of which can be expressed as $g_i = \Pi_{M^c}\bar{g}_i$, where \bar{g}_i is a generator of G supported on $M^c \cup \partial_-M$. Thus $\bar{x} = y \prod_i \bar{g}_i$ is a dressed logical operator for \mathcal{C} supported on ∂M . It follows that if ∂M is correctable for the code \mathcal{C} (i.e., code \mathcal{C} has no nontrivial dressed logical operators supported on ∂M), then ∂_+M is correctable for the code \mathcal{C}_{M^c} (\mathcal{C}_{M^c} has no nontrivial dressed logical operators supported on ∂_+M). By similar logic, if A is correctable for \mathcal{C} and contains ∂M , then $A \cap M^c$ is correctable for \mathcal{C}_{M^c} .

Suppose now that the code \mathcal{C} has k encoded qubits and that M is correctable, i.e., $g^{(\mathcal{C})}(M) = 0$. Therefore, applying Lemma 2.3.2 to the code \mathcal{C} , $g_{\text{bare}}^{(\mathcal{C})}(M^c) = 2k$. Suppose further that the set A containing ∂M is correctable for \mathcal{C} , implying that $A \cap M^c$ is correctable for \mathcal{C}_{M^c} , i.e., $g^{(\mathcal{C}_{M^c})}(A \cap M^c) = 0$. Then applying Lemma 2.3.2 to the code \mathcal{C}_{M^c} , we conclude that $g_{\text{bare}}^{(\mathcal{C}_{M^c})}(M^c \setminus A) = 2k$. Since each bare logical operator for \mathcal{C}_{M^c} , supported on $M^c \setminus A$, is also a bare logical operator for \mathcal{C} , supported on $M^c \setminus A$, we can now apply Lemma 2.3.2 once again to the code \mathcal{C} , using the partition into $M^c \setminus A$ and $M \cup A$, finding $g^{(\mathcal{C})}(M \cup A) = 0$. Thus $M \cup A$ is correctable. \square

If the interaction range is w , and M is a correctable hypercube with linear size $l - 2(w - 1)$, then we may choose $A \supseteq \partial M$ so that $M \cup A$ is a hypercube with linear size l and $M \setminus A$ is a hypercube with linear size $l - 4(w - 1)$. Then A contains

$$|A| = l^D - [l - 4(w - 1)]^D \leq 4(w - 1)Dl^{D-1}$$

qubits, and A is surely correctable provided $|A| < d$, where d is the code distance. Suppose that $d > 1$, so a single site is correctable. Applying Lemma 2.4.1 repeatedly, we can build up larger and larger correctable hypercubes, with linear size $1 + 2(w - 1), 1 + 4(w - 1), 1 + 6(w - 1), \dots$. This process continues as long as $|A| < d$. We conclude:

Lemma 2.4.2. *For a D -dimensional local subsystem code with interaction range $w > 1$ and distance $d > 1$, a hypercube with linear size l is correctable if*

$$4(w - 1)Dl^{D-1} < d. \tag{2.2}$$

Thus (roughly speaking) for the hypercube to be correctable it suffices for its $[2(w-1)]$ -thickened *boundary*, rather than its volume, to be smaller than the code distance. Bravyi [65] calls this property “the holographic principle for error correction,” because the *absence* of information encoded at the boundary of a region ensures that no information is encoded in the “bulk.”

For local stabilizer codes, the criterion for correctability is slightly weaker than for local subsystem codes. We say that a local stabilizer code has interaction range w if each stabilizer generator has support on a hypercube containing w^D sites. For this case, we can improve the criterion for correctability of a hypercube, found for local subsystem codes in Lemma 2.4.2.

Lemma 2.4.3. *For a local stabilizer code, suppose that ∂_+M , A , and $M \setminus A$ are all correctable, where $\partial_-M \subseteq A \subseteq M$. Then M is also correctable.*

Proof. Suppose, contrary to the claim, that there is a nontrivial logical operator x supported on M . Then, because A is correctable, Lemma 2.3.3 implies that there is a stabilizer generator y such that xy acts trivially on A . Furthermore, y can be expressed as a product of local stabilizer generators, each supported on $M' = M \cup \partial_+M$. Thus xy is a product of two factors, one supported on $M \setminus A$ and the other supported on ∂_+M . Because $\partial_-M \subseteq A$, no local stabilizer generator acts nontrivially on both $M \setminus A$ and ∂_+M ; therefore, each factor commutes with all stabilizer generators and hence is a logical operator. Because $M \setminus A$ and ∂_+M are both correctable, each factor is a trivial logical operator and therefore xy is also trivial. It follows that x is trivial, a contradiction. \square

Now, if the interaction range is w and M is a hypercube with linear size l , we choose A so that $M \setminus A$ is a hypercube with linear size $l - 2(w-1)$, and we notice that ∂_+M is contained in a hypercube with linear size $l + 2(w-1)$. Thus both $M \setminus A$ and ∂_+M are correctable provided that

$$\begin{aligned} |\partial_+M| &\leq [l + 2(w-1)]^D - l^D \\ &\leq 2(w-1)D [l + 2(w-1)]^{D-1} < d. \end{aligned}$$

Reasoning as in the proof of Lemma 2.4.2, we conclude that:

Lemma 2.4.4. *For a D -dimensional local stabilizer code with interaction range $w > 1$ and distance $d > 1$, a hypercube with linear size l is correctable if*

$$2(w-1)D [l + 2(w-1)]^{D-1} < d. \tag{2.3}$$

To ensure that the hypercube M is correctable, it suffices for its $(w-1)$ -thickened boundary, rather than its $[2(w-1)]$ -thickened boundary, to be smaller than the code distance.

Now we are ready to prove our first trade-off theorem.

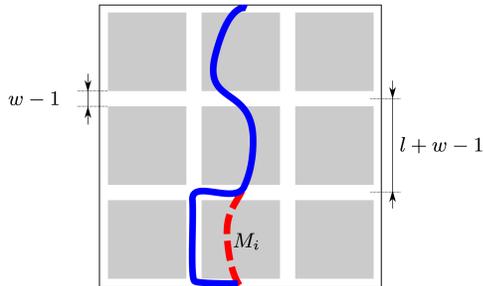


Figure 2.1: Lattice covering used in the proof of Theorem 1, shown in two dimensions. Each gray square is $l \times l$ and the white gap between squares has width $w - 1$. The solid blue curve represents the support of a nontrivial logical operator; because the square M_i is correctable, this square can be “cleaned.” We can find an equivalent logical operator supported on M_i^c , the complement of M_i . When all squares are cleaned, the logical operator is supported on the narrow strips between the squares.

Theorem 2.1. (Trade-off theorem for subsystem codes) *For a local subsystem code in $D \geq 2$ dimensions with interaction range $w > 1$ and distance $d \gg w$, defined on a hypercubic lattice with linear size L , every dressed logical operator is equivalent to an operator with weight \tilde{d} satisfying*

$$\tilde{d}d^{1/(D-1)} < cL^D, \quad (2.4)$$

where c is a constant depending on w and D .

Proof. As shown in Fig. 2.1, we fill the lattice with hypercubes, separated by distance $w - 1$, such that each hypercube has linear size l satisfying Eq. (2.2). (By “distance” we mean the number of sites in between — e.g., we say that adjacent sites are “distance zero” apart.) Thus no gauge generator acts nontrivially on more than one hypercube, and each hypercube is correctable by Lemma 2.4.2. Consider any nontrivial dressed logical operator x , and label the hypercubes $\{M_1, M_2, M_3, \dots\}$. By Lemma 3 there exists a gauge operator y_i that “cleans” the logical operator in the hypercube M_i , i.e., such that xy_i acts trivially in M_i . Furthermore, since no gauge generator acts nontrivially on more than one hypercube, we can choose y_i so that it acts trivially in all other hypercubes. Taking the product of all the y_i ’s we construct a gauge operator that cleans all hypercubes simultaneously; thus $\tilde{x} = x \prod_i y_i$ is equivalent to x and supported on the complement of the union of hypercubes $M = \cup_i M_i$. Therefore, the weight \tilde{d} of \tilde{x} is upper bounded by $|M^c|$.

The lattice is covered by hypercubes of linear size $l + (w - 1)$, each centered about one of the M_i ’s. There are $L^D / [l + (w - 1)]^D$ such hypercubes in this union, each containing no more than $[l + (w - 1)]^D - l^D \leq (w - 1)D [l + (w - 1)]^{D-1}$ elements of M^c . Thus

$$\tilde{d} \leq |M^c| \leq (w - 1)D [l + (w - 1)]^{D-1} \frac{L^D}{[l + (w - 1)]^D} = \frac{(w - 1)D}{l + (w - 1)} L^D.$$

We optimize this upper bound on \tilde{d} by choosing l to be the largest integer such that a hypercube with linear size l is known to be correctable, i.e., satisfying

$$l < \left(\frac{d}{4(w-1)D} \right)^{1/(D-1)},$$

thus obtaining Eq. (2.4). Note that Eq. (2.4) is trivial if d is a constant independent of L , since the weight \tilde{d} cannot be larger than L^D . □

Chapter 3

Algebraic formulation for translationally invariant codes

If an additive code is defined on a lattice with periodic boundary conditions by a translationally invariant set $\{g_i\}$ of local generators, then we can define a *code Hamiltonian*

$$H = - \sum_i g_i$$

whose ground space is identified with the code space. Prototypical is the toric code model [3]. If the stabilizer generators are given as translations of a finite collection of Pauli operators, we have a family of code Hamiltonians parameterized by the system size or boundary conditions. In this chapter we present a framework to study such translationally invariant code Hamiltonians. We will be particularly interested in the *phases of matter* represented by the code Hamiltonians. Hence, we should allow local unitary transformations and deformation of Hamiltonians as long as the deformation does not close the energy gap between the ground and first excited state, and we study properties of Hamiltonians that are invariant under these transformations.

If one does not make use of the translation structure, but insists on the use of usual symplectic vector space description, then one should deal with infinitely many qubits and the generating matrix of infinite size. However, the translation symmetry tells us that there is only a finite amount of data describing the family of code Hamiltonians. It is certainly uneconomical to study a general infinite matrix. We must look for a succinct description. The starting observation is that translation symmetry is mostly well expressed with the group algebra of the underlying translation group. Fortunately, the lattice is an abelian group isomorphic to \mathbb{Z}^D for some $D \geq 1$; the group algebra is a commutative ring, or actually, a Laurent polynomial ring. We will see that, inasmuch as the additive codes are described by null spaces in symplectic vector spaces, the translation-invariant code Hamiltonians have corresponding algebraic descriptions by certain submodules of finitely generated free modules.

We build an effective dictionary between lattice codes and commutative algebra in Section 3.1.1. The equivalence of phases of matter is re-expressed in an algebraic form in Section 3.2. Perhaps the most important entry in this dictionary is that the topological order condition can be expressed by the vanishing homology of a certain chain complex, presented in Section 3.3. As we will see in the next chapter, the physical dimension is essentially the length of the chain complex, which is a reminiscence of Hilbert syzygy theorem. The ground-state subspace can be analyzed by studying an algebraic set defined by the chain complex. In particular, the degeneracy, or the number of encoded qubits, can be approximated by counting points in the algebraic set, for which some bounds are given in Section 3.4. The last section 3.5 introduces fractal operators and establishes a precise algebraic description of topological charges in connection to the fractal operators. Our discussion assumes some familiarity with commutative algebra. In Appendix A, we include basic materials relevant to analysis of codes.

Note that in the classical coding theory the use of multivariate polynomial in multidimensional cyclic codes at least dates back to Imai [67]. Imai realized the importance of zero-locus of defining polynomials of the code, which had been emphasized in the one-dimensional cyclic code [68]. See also [69, 70] and references therein. In the classical coding theory, each lattice sites carries one bit $\{0, 1\}$, whereas in our quantum codes each lattice sites may have several qubits. For this generalization we use modules instead of ideals. Moreover, quantum additive codes require the nullity equation $\sigma^T \lambda \sigma = 0$. (See Section 2.2.) We decompose this equation into two parts $\epsilon = \sigma^T \lambda$ and σ , and view them as connecting maps of a chain complex $G \xrightarrow{\sigma} P \xrightarrow{\epsilon} E$. The chain complex is relevant only to quantum codes.

We will treat code Hamiltonians on sets of qubits, two-dimensional (two-level) local Hilbert spaces. However, our language naturally allows an extension to prime-dimensional *qudits*. This is because we only use the fact that the set of coefficients \mathbb{F}_2 is a field. The generalization is achieved simply by replacing the ground field \mathbb{F}_2 with \mathbb{F}_p for any prime number p .

3.1 Algebraic structure of code Hamiltonians

3.1.1 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 the 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

\mathbb{F}_2	binary field $\{0, 1\}$
D	spatial dimension
R	$\mathbb{F}_2[x_1, x_1^{-1}, \dots, x_D, x_D^{-1}]$
\mathfrak{b}_L	ideal $(x_1^L - 1, \dots, x_D^L - 1)$
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	$G \rightarrow P$, generating matrix or map for the stabilizer module
ϵ	$P \rightarrow E$, 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 $\begin{pmatrix} 0 & \text{id} \\ -\text{id} & 0 \end{pmatrix}$

Table 3.1: Reserved symbols in Chapter 3. Any ring in this thesis is commutative with 1.

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

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

for any $a \in R$.

Proposition 3.1.1 ([41]). *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

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

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

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

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

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 thesis. 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 3.1.1 we have

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

Since r was arbitrary, we must have $a\bar{b} - b\bar{a} = 0$.¹ 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, \dots, s_t such that any commutation value always vanishes, if and only if

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

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

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, \dots, s_t , the commutation value always vanishes on S , if and only if for all $i, j = 1, \dots, t$

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

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

¹A symmetric bilinear form $\langle r, s \rangle = \text{tr}(r\bar{s})$ on R is nondegenerate.

Let us summarize our discussion so far.

Proposition 3.1.2. *On a set of qubits $\Lambda \times \{1, \dots, q\}$ 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*

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

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

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

Proposition 3.1.1 [41] is a special case of Proposition 3.1.2 when Λ is a trivial group. When $\Lambda \cong \mathbb{Z}$, a similar equation appears in quantum convolutional codes [71].

3.1.2 Local Hamiltonians on groups

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

Definition 3.1. Let

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

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, \dots, 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 3.1. 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 3.1.2. H is commuting; $\sigma^\dagger \lambda_1 \sigma = 0$. \diamond

3.1.3 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 all configurations of 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, represent U_1 and U_2 . Therefore, the association $U_i \mapsto e_i$ induces a linear map from the Pauli space to the space of virtual 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

$$\epsilon : P \rightarrow E$$

from the Pauli module P to the **module of virtual 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 3.1.1 can be viewed as

$$\sigma : G \rightarrow P$$

from the module of generator labels to the Pauli module.

Proposition 3.1.3. *If σ is the generating map for the stabilizer module of a code Hamiltonian, then*

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

The matrix ϵ can be viewed as a generalization of the parity check matrix of the standard theory of classical or quantum error correcting codes [68, 38, 39, 40], when a translation structure is given.

Proof. This is a simple corollary of Proposition 3.1.2. Let $h_{i,g}$ be the terms in the Hamiltonian where $i = 1, \dots, t$, 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,

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

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

Remark 3.1. The commutativity condition in Proposition 3.1.2 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.

3.2 Equivalent Hamiltonians

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

Proposition 3.2.1. *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 $\prod_{\Lambda \times \{1, \dots, q\}} \mathbb{F}_2^2$, which is vector space isomorphic to the Pauli group of arbitrary support up to phase factors.²

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

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

is a desired path. □

The criterion of Proposition 3.2.1 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 3.2. 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.

3.2.1 Symplectic transformations

Definition 3.3. 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 \dagger is the transposition followed by the entry-wise antipode map.

When the translation group is trivial these transformations are given by so-called **Clifford operators**. Compare Section 2.2 and see [61, Chapter 15].

²If 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.

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

If the translation group is trivial, the proposition reduces to Theorem 15.6 of [61]

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 3.2.1, 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 $O = U$. \square

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

$$\sigma \rightarrow U\sigma$$

For example, the following is induced by uniform Hadamard, controlled-Phase, and controlled-NOT gates. For notational clarity, define $E_{i,j}(a)$ ($i \neq j$) as 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 $a \in R = \mathbb{F}_2[\Lambda]$. 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 3.4. The following are **elementary symplectic transformations**:

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

For the case of a trivial translation group, these transformations explicitly appear in [41] and [61, Chapter 15]. The one-dimensional case appears in the context of quantum convolutional codes [72].

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,

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

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 $E_{i+g, i}(g + \bar{g})$. The composition

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

of finitely many controlled-Phase gates $U_g^{(i)}$ with different g is represented as $E_{i+q, i}(f)$ 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

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

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 $1 \leq i \neq j \leq q$.

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.

3.2.2 Coarse-graining

Not all unitary operators conform with the lattice translation. In Example 3.1 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 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** $R' = \mathbb{F}_2[\Lambda']$ if we restrict the scalar ring R to R' for all modules pertaining to the system.

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.

Abstractly, the original translation group algebra R is a finitely generated free module over the coarse translation group algebra R' . Thus, the coarse-graining can be regarded as an exact functor from the category of R -modules to the category of R' -modules.

The one-dimensional case appears in the context of quantum convolutional codes [73].

3.2.3 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 3.1.2. By **tensoring ancilla**, we embed S as

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

This amounts to taking the direct sum of the original complex

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

and the trivial complex

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

to form

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

3.3 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 3.5. Let $\sigma : G \rightarrow P$ be the generating map for the stabilizer module of a code Hamiltonian H . We say H is **exact** if $(\text{im } \sigma)^\perp = \text{im } \sigma$, or equivalently

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

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

It follows that the exactness condition is a property of the equivalence class of code Hamiltonians in the sense of Definition 3.2.

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 lose 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 3.6. Let $H(L)$ be Hamiltonians on a finite system of linear size L in D -dimensional physical space, and Π_L 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

$$\Pi_L O \Pi_L \propto \Pi_L. \tag{3.1}$$

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 [74, 6, 75]. We say a **diamond region** $A(r)$ **of radius** r **at** $o \in \mathbb{Z}^D$ for the set

$$A(r)_o = \left\{ (i_1, \dots, i_D) + o \in \mathbb{Z}^D \mid \sum_{\mu} |i_{\mu}| \leq r \right\}.$$

Definition 3.7. Let $H(L)$ be code Hamiltonians on a finite system of linear size L in D -dimensional physical space. For any diamond region $A = A(r)$ of radius r , let Π_A be the projector onto the common eigenspace of the most negative eigenvalues of terms in the Hamiltonian $H(L)$ that are supported in 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 diamond region A of radius $r < L/2$ one has

$$\Pi_{A^b} O \Pi_{A^b} \propto \Pi_{A^b}. \quad (3.2)$$

Since any operator is a \mathbb{C} -linear combination of Pauli operators, if Eq. (3.1),(3.2) are satisfied for Pauli operators, then the (local) topological order condition follows. If a Pauli operator O is anticommuting with a term in a code Hamiltonian $H(L)$, The left-hand side of Eq. (3.1),(3.2) 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. (3.1) 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. (3.2) further demands that O must be a product of terms in $H(L)$ supported inside A^b up to $\pm i, \pm 1$.

Lemma 3.3.1. *A code Hamiltonian H is exact if and only if $H(L)$ is locally topologically ordered for all sufficiently large L .*

In order to see this, it will be important to use *Laurent polynomials* to express elements of the group algebra $R = \mathbb{F}_2[\mathbb{Z}^D] \cong \mathbb{F}_2[x_1, x_1^{-1}, \dots, x_D, x_D^{-1}]$. The reader might want to see [67, 70] for classical multidimensional cyclic codes. For example,

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

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.

The Laurent polynomial viewpoint enables us to apply Gröbner basis techniques. The long division algorithm for polynomials in one variable yields an effective and efficient test whether a given polynomial is divisible by another. When two or more but finitely many variables are involved,

a more general question is how to test whether a given polynomial is a member of an ideal. For instance, $f = xy - 1$ is a member of an ideal $J = (x - 1, y - 1)$ because $xy - 1 = y(x - 1) + (y - 1)$. But, $g = xy$ is not a member of J because $g = y(x - 1) + (y - 1) + 1$ and the ‘remainder’ 1 cannot be removed. Here, the first term is obtained by looking at the initial term xy of f and comparing with the initial terms x and y of the generators of J . While one tries to eliminate the initial term of f and to eventually reach zero, if one cannot reach zero as for g , then the membership question is answered negatively.

Systematically, an well-ordering on the monomials, i.e., a *term order*, is defined such that the order is preserved by multiplications. And a set of generators $\{g_i\}$ for the ideal is given with a special property that any element in the ideal has an initial term (leading term) divisible by an initial term of some g_i . A Gröbner basis is precisely such a generating set. This notion generalizes to free modules over polynomial ring by refining the term order with the basis of the modules. An example is as follows. Let

$$\sigma_1 = \begin{pmatrix} \mathbf{x}^2 - y \\ x^2 + 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 \\ \mathbf{y} \end{pmatrix}$$

generate a submodule M of S^2 where $S = \mathbb{F}[x, y]$ is a polynomial ring. They form a Gröbner basis, and the initial terms are marked as bold. A member of S^2

$$\begin{pmatrix} x^2 + x^2 y - y^2 \\ y + 2x^2 y \end{pmatrix}$$

is in M because the following ‘division’ results in zero.

$$\begin{pmatrix} x^2 + \mathbf{x}^2 \mathbf{y} - y^2 \\ y + 2x^2 y \end{pmatrix} \xrightarrow{-y\sigma_1} \begin{pmatrix} x^2 \\ \mathbf{x}^2 \mathbf{y} \end{pmatrix} \xrightarrow{-x^2\sigma_2} 0$$

A comprehensive material can be found in [76, Chapter 15].

The situation for Laurent polynomial ring is less discussed, but is not too different. A direct treatment is due to Pauer and Unterkircher [77]. One introduces a well-order on monomials, that is preserved by multiplications with respect to a so-called *cone decomposition*. An ideal J over a Laurent polynomial ring can be thought of as a collection of configurations of coefficient scalars written on the sites of the integral lattice \mathbb{Z}^D . If we take a cone, say,

$$C = \{(i_1, i_2, i_3) \in \mathbb{Z}^3 \mid i_1 \leq 0, i_2 \geq 0, i_3 \geq 0\},$$

then $J_C = J \cap \mathbb{F}[C]$ looks very similar to an ideal I over a polynomial ring $\mathbb{F}[x, y, z]$. Concretely, I can be obtained by applying $x^{-1} \mapsto x, y \mapsto y, z \mapsto z$ to J_C . The initial terms of J_C should be treated similarly as those in I . This is where the cone decomposition plays a role. The lattice \mathbb{Z}^D decomposes

into 2^D cones, and the initial terms of J is considered in each of the cones. Correspondingly, a Gröbner basis is defined to generate the initial terms of a given module in each of the cones. An intuitive picture for the division algorithm is to consider the support of a Laurent polynomial as a finite subset of \mathbb{Z}^D around the origin (the least element of \mathbb{Z}^D), and to eliminate outmost points so as to finally reach the origin. If m is a column matrix of Laurent polynomials, each step in the division algorithm by a Gröbner basis $\{g\}$ replaces m with $m' = m - cg$, where c is a monomial, such that the initial term of m' is strictly smaller than that of m . Note that the absolute degree of c does not exceed that of m .³

Proof of 3.3.1. We have to show that if $v \in \ker \epsilon = \text{im } \sigma$ is supported in the diamond of radius r centered at the origin, 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 $w + r$. for some fixed w . A Gröbner basis [77] is computed solely from the matrix σ , and the division algorithm yields desired c_i .

Conversely, suppose $v \in \ker \epsilon$. We have to show $v \in \text{im } \sigma$. 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 $v \in \text{im } \sigma$. \square

The Buchsbaum-Eisenbud theorem [78] below characterizes an exact sequence from the properties of connecting maps. (See also [76, Theorem 20.9, Proposition 18.2],[79, Chapter 6 Theorem 15].) A few notions should be recalled. Let \mathbf{M} be a matrix, not necessarily square, over a ring. A minor is the determinant of a 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 side. The **rank** of \mathbf{M} is the largest k such that k -th determinantal ideal is nonzero. Thus, the rank of a matrix over an arbitrary ring is defined, although the dimension of the image in general is not defined or is infinite. The 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 [76, Corollary-Definition 20.4] states that determinantal ideals only depend on coker ϕ .

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

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

³Strictly speaking, one can introduce a term order such that this is true.

is defined to be n . Most importantly, the dimension of $\mathbb{F}[x_1, \dots, x_n]$ is n where \mathbb{F} is a field, as

$$(0) \subset (x_1) \subset (x_1, x_2) \subset \dots \subset (x_1, \dots, x_n).$$

Dimensions are in general very subtle, but intuitively, it counts the number of independent ‘variables.’ Geometrically, a ring is a function space of a geometric space, and the independent variables define a coordinate system on it. So the Krull dimension correctly captures the intuitive dimension. For instance, $y - x^2 = 0$ defines a parabola in a plane, and the functions that vanish on the parabola form an ideal $(y - x^2) \subset \mathbb{F}[x, y]$. Thus, the function space is identified with $\mathbb{F}[x, y]/(y - x^2) \cong \mathbb{F}[x]$, whose Krull dimension is, as expected, 1.

Facts we need are quite simple:

- In a zero-dimensional ring, every prime ideal is maximal.
- $\dim R = \dim \mathbb{F}_2[x_1^{\pm 1}, \dots, x_D^{\pm 1}] = D$
- When I is an ideal of R , $\dim R/I + \text{codim } I = D$.⁴

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 3.3.2 ([78]⁵). *If a complex of free modules over a ring*

$$0 \rightarrow F_n \xrightarrow{\phi_n} F_{n-1} \rightarrow \dots \rightarrow F_1 \xrightarrow{\phi_1} F_0$$

is exact, then

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

⁴ 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 . 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 $\text{codim } I + \dim R/I = \dim S$ [76, Chapter 13].

⁵The original result is stronger than what is presented here. It is stated with the *depths* of the determinantal ideals.

Remark 3.2. For an exact code Hamiltonian, we have an exact sequence $G \xrightarrow{\sigma} P \xrightarrow{\epsilon=\sigma^\dagger\lambda} E$. As we will see in Lemma 4.2.1, $\text{coker } \sigma$ has a finite free resolution, and we may apply the Proposition 3.3.2. Since $\overline{I_k(\sigma)} = I_k(\epsilon)$ for any $k \geq 0$, we have

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

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

3.4 Ground-state degeneracy

Let $H(L)$ be the Hamiltonians on finite systems obtained by imposing periodic boundary conditions as in Section 3.3. A symmetry operator of $H(L)$ is a \mathbb{C} -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

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

where

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

and

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

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 $v' \in \text{im } \sigma_L$. Therefore, the set of Pauli operators of distinct actions on the ground space is in one-to-one correspondence with the factor module

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

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 $\ker \epsilon_L = (\text{im } \sigma_L)^\perp$ by definition of ϵ , and $\text{im } \sigma_L$ as an \mathbb{F}_2 -vector space is a null space of the symplectic vector space $P/\mathfrak{b}_L P$, it follows that $\ker \epsilon_L = \text{im } \sigma_L \oplus W$ 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 [40, 41]. 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 $\frac{1}{2} \dim_{\mathbb{F}_2} K$.

Definition 3.8. 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 $\dim R/I_q(\sigma)$.

The associated ideals appears in Buchsbaum-Eisenbud theorem (Proposition 3.3.2), which says that the homology $K(L)$ is intimately related to the associated ideal. Imposing boundary conditions such as $x^L = 1$ amounts to treating x not as variables any more, but as a ‘solution’ of the equation $x^L - 1 = 0$. In order for $K(L)$ to be nonzero, the ‘solution’ x should make the associated ideal to vanish. Hence, by investigating the solutions of $I_q(\sigma)$ one can learn about the relation between the degeneracy and the boundary conditions. Roughly, a large number of solutions of $I_q(\sigma)$ compatible with the boundary conditions means a large degeneracy. As $d = \dim R/I_q(\sigma)$ is the geometric dimension of the algebraic set defined by $I_q(\sigma)$, a larger d means a larger number of solutions. Hence, the characteristic dimension d controls the growth of the degeneracy as a function of the system size.

For example, consider a chain complex over $R = \mathbb{F}[x^{\pm 1}, y^{\pm 1}]$.

$$0 \rightarrow R^1 \xrightarrow{\partial_2 = \begin{pmatrix} x-1 \\ y-1 \end{pmatrix}} R^2 \xrightarrow{\partial_1 = \begin{pmatrix} y-1 & -x+1 \end{pmatrix}} R^1$$

It is exact at R^2 . The smallest nonzero determinantal ideal I for either ∂_1 or ∂_2 is $I = (x-1, y-1)$. If we impose ‘boundary conditions’ such that $x = 1$ and $y = 1$, then I becomes zero, and according to Buchsbaum-Eisenbud theorem, the homology K at R^2 should be nontrivial. Since the solution of I consists of a single point $(1, 1)$ on a 2-plane, it is conceivable that ‘boundary conditions’ of form \mathfrak{b}_L would always give $K(L)$ of a constant \mathbb{F} -dimension, which is true in this case. If we insist that the complex is over $R' = \mathbb{F}[x^{\pm 1}, y^{\pm 1}, z^{\pm 1}]$, then the zero set of I is a line $(1, 1, z)$ in 3-space; there are many ‘solutions.’ In this case, $K^{R'}(L)$ has \mathbb{F} -dimension $2L$.

An obvious example where the homology K is always zero regardless of the boundary conditions is this:

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

Here, the determinantal ideal is $(1) = R$, and thus has no solution.

The intuition from these examples are made rigorous below.

3.4.1 Condition for degenerate Hamiltonians

A routine yet very important tool is *localization*. The origin of all difficulties in dealing with general rings is that nonzero elements do not always have multiplicative inverse; one cannot easily solve linear equations. The localization is a powerful technique to get around this problem. As we build rational numbers from integers by *declaring* that nonzero numbers have multiplicative inverse, the localization enlarges a given ring and *formally allows* certain elements to be invertible. It is necessary and sometimes desirable not to invert all nonzero elements, in order for the localization to be useful. For a consistent definition, we need a multiplicatively closed subset S containing 1, but not containing 0, of a ring R and declare that the elements of S is invertible. The new ring is written as $S^{-1}R$, in which a usual formula $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1s_2 + r_2s_1}{s_1s_2}$ holds. The original ring naturally maps into $S^{-1}R$ as $\phi : r \mapsto \frac{r}{1}$. The localization means that one views all data as defined over $S^{-1}R$ via the natural map ϕ .⁶

A localized ring, by definition, has more invertible elements, and hence has less nontrivial ideals. In fact, our Laurent polynomial ring is a localized ring of the polynomial ring by inverting monomials, e.g., $\{x^i y^j | i, j \geq 0\}$. Nontrivial ideals such as (x) or (x, y) in the polynomial ring become the unit ideal (1) in the Laurent polynomial ring. Further localizations in this thesis are with respect to prime ideals. In this case, we say the ring is **localized at a prime ideal \mathfrak{p}** . A prime ideal \mathfrak{p} has a defining property that $ab \notin \mathfrak{p}$ whenever $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$. Thus, the set-theoretic complement of \mathfrak{p} is a multiplicatively closed set containing 1. In $(R \setminus \mathfrak{p})^{-1}R$, denoted by $R_{\mathfrak{p}}$, any element outside \mathfrak{p} is invertible, and therefore \mathfrak{p} becomes a unique maximal ideal of $R_{\mathfrak{p}}$. Moreover, the localization sometimes simplifies the generators of an ideal. For instance, if $R = \mathbb{F}[x, x^{-1}]$ and $\mathfrak{p} = (x - 1)$, the ideal $((x - 1)(x^5 - x + 1)) \subseteq R$ localizes to $(x - 1)_{\mathfrak{p}} \subseteq R_{\mathfrak{p}}$ since $x^5 - x + 1$ is an invertible element of $R_{\mathfrak{p}}$.

An important fact about the localization is that a module is zero if and only if its localization at every prime ideal is zero. Further, the localization preserves exact sequences. So we can analyze a complex by localizing at various prime ideals. For a thorough treatment about localizations, see Chapter 3 of [80]. The term ‘localization’ is from geometric considerations where a ring is viewed as a function space on a geometric space.

Lemma 3.4.1. *Let I be the associated ideal of an exact code Hamiltonian, and \mathfrak{m} be a prime ideal of R . Then, $I \not\subseteq \mathfrak{m}$ implies that the localized homology*

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

⁶It is a functor from the category of R -modules to that of $S^{-1}R$ -modules.

is zero for all $L \geq 1$.

It is a simple variant of a well-known fact that a module over a local ring is free if its first non-vanishing Fitting ideal is the unit ideal [79, Chapter 1 Theorem 12].

Proof. Recall that the localization and the factoring commute. By assumption,

$$(I_q(\epsilon))_{\mathfrak{m}} = \overline{(I_q(\sigma))_{\mathfrak{m}}} = (1) = R_{\mathfrak{m}} =: S.$$

6 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 a 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 [79, Chapter 1 Theorem 12]. After q steps, $t \times 2q$ matrix ϵ becomes precisely

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

where id_q is the $q \times q$ identity matrix. Since localization preserves the exact sequence $G \rightarrow P \rightarrow E$, 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)

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

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

Corollary 3.4.2. *The associated ideal of an exact code Hamiltonian is the unit ideal, i.e., $I_q(\sigma) = R$, if and only if*

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

for all $L \geq 1$.

Proof. If $I(\sigma) = R$, $I(\sigma)$ is not contained in any prime 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 prime 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, $\mathfrak{m} = (x_1 - a_1, \dots, x_D - a_D)$ 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 $R_{\mathfrak{m}}$ and each $x_i^L - 1$ contains exactly one $x_i - a_i$ factor, we see $(\mathfrak{b}_L)_{\mathfrak{m}} = \mathfrak{m}_{\mathfrak{m}}$. 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, $\text{rank}_{\mathbb{F}^a}(\sigma_L)_{\mathfrak{m}} < q$. It is clear that $\dim_{\mathbb{F}^a} K(L)_{\mathfrak{m}} = \dim_{\mathbb{F}^a} \ker(\epsilon_L)_{\mathfrak{m}} / \text{im}(\sigma_L)_{\mathfrak{m}} \geq 1$. \square

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.

3.4.2 Counting points in algebraic varieties

It is important that the factor ring

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

is finite dimensional as a vector space over \mathbb{F}_2 , and hence is Artinian. In fact, $\dim_{\mathbb{F}_2} R/\mathfrak{b}_L = L^D$. This ring appears also in [70]. Due to the following structure theorem of Artinian rings, $K(L)$ can be explicitly analyzed by the localizations.

Proposition 3.4.3 (Chapter 8 of [80], Section 2.4 of [76]). *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 $\langle v, w \rangle = \text{tr}(v\bar{w})$. This scalar product naturally extends to a direct

sum of group algebras.

Lemma 3.4.4. *Let \mathbb{F} be a field, and $S = \mathbb{F}[\Lambda]$ be the group algebra of a finite abelian group Λ . If N is a submodule of S^n , then the dual vector space N^* is vector-space isomorphic to S^n/N^\perp , where \perp is with respect to the scalar product $\langle \cdot, \cdot \rangle$.*

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 . \square

Corollary 3.4.5. *Put $2k = \dim_{\mathbb{F}_2} K(L)$. Then,*

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

Further, if $q = t$, then

$$k = \dim_{\mathbb{F}_2} \ker \sigma_L = \dim_{\mathbb{F}_2} \text{coker } \epsilon_L.$$

The first formula is a rephrasing of the fact that the number of encoded qubits is the total number of qubits minus the number of independent stabilizer generators [40, 41].

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

$$\ker \sigma_L^\dagger = \lambda_q \ker \epsilon_L = \bigcap_i v_i^\perp = \left(\sum_i S v_i \right)^\perp = (\text{im } \sigma_L)^\perp. \quad (3.3)$$

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

Since $\text{im } \sigma_L \cong S^t / \ker \sigma_L$, if $t = q$, we have $k = \dim_{\mathbb{F}_2} \ker \sigma_L$ by the first claim. From Eq. (3.3), we conclude that $k = \dim_{\mathbb{F}_2} S^t / \text{im } \sigma_L^\dagger = \dim_{\mathbb{F}_2} \text{coker } \epsilon_L$. \square

We will apply these formulas in Section 5.3 and Example 4.3.

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 3.4.6. *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 contain $\mathfrak{b}_L + I_q(\sigma)$, then*

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

Proof. We replace the ground field \mathbb{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 $\mathfrak{m} = (x_1 - a_1, \dots, x_D - a_D)$ where $a_i^L = 1$ by Nullstellensatz. Since $2 \nmid L$, we see that $(\mathfrak{b}_L)_{\mathfrak{m}} = \mathfrak{m}_{\mathfrak{m}}$ and that $(R/\mathfrak{b}_L)_{\mathfrak{m}} \cong \mathbb{F}^a$ is the ground field. (See the proof of Corollary 3.4.2.)

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 $1 \leq \dim_{\mathbb{F}^a} K(L)_{\mathfrak{m}} \leq 2q$. Since by Proposition 3.4.3, $K(L)$ is a finite direct sum of localized ones, we are done. \square

Lemma 3.4.7. *Let I be an ideal such that $\dim R/I = d$. We have*

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

for all $L \geq 1$ 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 [76, Theorem 13.3], there exist $y_1, \dots, y_d \in R/I$ such that R/I is a finitely generated module over $\mathbb{F}^a[y_1, \dots, y_d]$. 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 . Making M into the reduced row echelon form, we may assume $y_i = \tilde{x}_i + \sum_{j>d} a_{ij} \tilde{x}_j$ for each $1 \leq i \leq d$.

Let $S = \mathbb{F}^a[z_1, \dots, z_D]$ be a polynomial ring in D variables. Let $\phi : S \rightarrow R/(I + \mathfrak{b}_L)$ be the ring homomorphism such that $z_i \mapsto y_i$ for $1 \leq i \leq d$ and $z_j \mapsto \tilde{x}_j$ for $d < j \leq D$. 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 $z_1 \prec \dots \prec z_D$. Since \tilde{x}_j is integral over $\mathbb{F}[y_1, \dots, y_d]$, the monomial ideal J contains $z_j^{n_j}$ for some positive n_j for $d < j \leq D$. Here, n_j is independent of L . Since $z_i^L \in J$ for $1 \leq i \leq d$, we conclude that

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

by Macaulay theorem [76, Theorem 15.3]. \square

Corollary 3.4.8. *If $2 \nmid L$, and $d = \dim R/I_q(\sigma)$ is the characteristic dimension of a code Hamiltonian, then*

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

for some constant c independent of L .

Proof. If $J = \mathfrak{b}_L + I(\sigma)$, N in Lemma 3.4.6 is equal to $\dim_{\mathbb{F}^a} \mathbb{F}^a \otimes R/\text{rad } J$. This is at most $\dim_{\mathbb{F}^a} \mathbb{F}^a \otimes R/J = \dim_{\mathbb{F}_2} R/J$. \square

Lemma 3.4.9. *Let d be the characteristic dimension. There exists an infinite set of integers $\{L_i\}$*

such that

$$\dim_{\mathbb{F}_2} K(L_i) \geq L_i^d/2$$

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 $S = \mathbb{F}^a[x_1, \dots, x_D]$. 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 $\mathfrak{p} = (g_1, \dots, g_n)$. Since \mathfrak{p} contains no monomials, V is not contained in any hyperplanes $x_i = 0$ ($i = 1, \dots, D$).

Let A_1 be a finite subfield of \mathbb{F}^a that contains all 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 3.4.6 is at least $N'(L_n)$. It remains to show $N'(L_n) \geq L_n^d/2$ for all sufficiently large n .

This follows from the result by Lang and Weil [81], 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 $m^d + O(m^{d-\frac{1}{2}})$ 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 $x_i = 0$ ($i = 0, 1, \dots, D$) from the Zariski closure of V . The subvarieties in the hyperplanes, being closed, have strictly smaller dimensions, and we are done. \square

3.5 Fractal operators and topological charges

This section is to provide a characterization of topological charges, and their dynamical properties. Before we turn to a general characterization and define fractal operators, let us review familiar examples. Note that for two dimensions the base ring is $R = \mathbb{F}_2[x, \bar{x}, y, \bar{y}]$.

Example 3.2 (Toric Code). Although the original two-dimensional toric code [3] has qubits on edges, 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:

$$\begin{array}{ccc} XI - XX & ZI - II & y - xy \\ \begin{array}{|c|} \hline \\ \hline \end{array} & \begin{array}{|c|} \hline \\ \hline \end{array} & \begin{array}{|c|} \hline \\ \hline \end{array} \\ II - IX & ZZ - IZ & 1 - x \end{array}$$

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 $\sigma : R^2 \rightarrow R^4$ is given by the matrix

$$\sigma_{2\text{D-toric}} = \begin{pmatrix} y + xy & 0 \\ x + xy & 0 \\ 0 & 1 + y \\ 0 & 1 + x \end{pmatrix} \cong \begin{pmatrix} 1 + \bar{x} & 0 \\ 1 + \bar{y} & 0 \\ 0 & 1 + y \\ 0 & 1 + x \end{pmatrix}.$$

Here, the each column expresses each type of interaction. It is clear that

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

and $\ker \epsilon = \text{im } \sigma$; 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 $\text{ann coker } \epsilon = (x - 1, y - 1)$. The electric and magnetic charge are represented by $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in E \setminus \text{im } \epsilon$, respectively.

The connection with cellular homology should 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. Then, ϵ 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 $K(L) = \ker \epsilon_L / \text{im } \sigma_L$ of operators acting on the ground space (logical operators) has four generators

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

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

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

The description by the cellular homology might be 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 3.3 (2D Ising model on square lattice). The Ising model has nearest neighbor interactions that are horizontal and vertical. In our formalism, they are represented as $1 + x$ and $1 + y$. Thus,

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

As it is not topologically ordered, the complex $G \rightarrow P \rightarrow E$ is not exact. Moreover, σ is not injective.

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

generates the kernel of σ . That is, the complex $0 \rightarrow G_1 \xrightarrow{\sigma_{2\text{D Ising};1}} G \xrightarrow{\sigma_{2\text{D Ising}}} P$ is exact. ◇

In both examples, there exist isolated excitations. In the toric code, the isolated excitation can be (topologically) nontrivial since the electric charge is not in $\text{im } \epsilon$. On the contrary, in 2D Ising model, any isolated excitation is actually created by an operator of finite support because any excitation created by some Pauli operator appears as several connected loops. This difference motivates the following definition for charges.

Let \tilde{R} be the set of all \mathbb{F}_2 -valued functions on the translation group Λ , not necessarily finitely supported. For instance, if $\Lambda = \mathbb{Z}$,

$$\tilde{f} = \cdots + x^{-4} + x^{-2} + 1 + x^2 + x^4 + \cdots \in \tilde{R}$$

represents a function whose value is 1 at even lattice points, and 0 at odd points. Note that \tilde{R} is a R -module, since the multiplication is a convolution between an arbitrary function and a finitely supported function. For example,

$$\begin{aligned} (1 + x) \cdot \tilde{f} &= \cdots + x^{-2} + x^{-1} + 1 + x + x^2 + \cdots, \\ (1 + x)^2 \cdot \tilde{f} &= 0. \end{aligned}$$

Let $\tilde{P} = \tilde{R}^{2q}$ be the module of Pauli operators of possibly infinite support. Similarly, let \tilde{E} be the module of virtual excitations of possibly infinitely many terms. Formally, \tilde{P} is the module of all $2q$ -tuples of functions on the translation group, and \tilde{E} is that of all t -tuples. Clearly, $P \subseteq \tilde{P}$ and $E \subseteq \tilde{E}$. The containment is strict if and only if the translation group is infinite. Since the matrix ϵ consists of Laurent polynomials with finitely many terms, $\epsilon : P \rightarrow E$ extends to a map from \tilde{P} to \tilde{E} .

Definition 3.9. A **topological charge**, or **charge** for short, $e = \epsilon(\tilde{p}) \in E$ is an excitation of finite energy (an element of the virtual excitation module) created by a Pauli operator $\tilde{p} \in \tilde{P}$ of possibly infinite support. A charge e is called **trivial** if $e \in \epsilon(P)$.

By definition, the set of all charges modulo trivial ones is in one-to-one correspondence with the superselection sectors. According to the definition, any charge of 2D Ising model is trivial. A nontrivial charge may appear due to the following fractal generators.

Definition 3.10. We call zero-divisors on $\text{coker } \epsilon$ as **fractal generators**. In other words, an element $f \in R \setminus \{0\}$ is a *fractal generator* if there exists $v \in E \setminus \text{im } \epsilon$ such that $fv \in \text{im } \epsilon$.

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 the others at $(1, 0)$ and $(0, 1)$ created by a Pauli operator represented by p . (This example is adopted from [48].) 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 the excitations at $(1, 0), (0, 1)$ have been replaced by those 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 $f^4 = (f^2)^2 = 1 + x^2 + y^2$. 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 of form fv for some $f \in R$ consisted of two or more terms, there is a family of Pauli operators $f^{2^n-1}p$ with self-similar support 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 $v \notin \text{im } \epsilon$. The reader may wish to compare the fractals with finite cellular automata [82].

Proposition 3.5.1. [83, 16.33] Suppose $\text{coker } \epsilon \neq 0$. Then, the following are equivalent:

- There does not exist a fractal generator.
- $\text{coker } \epsilon$ is torsion-free.

- There exists a free R -module E' of finite rank such that

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

is exact.

Proof. The first two are equivalent by definition. The sequence above is exact if and only if $0 \rightarrow \text{coker } \epsilon \rightarrow E'$ is exact. Since $\text{coker } \epsilon$ has a finite free resolution, the second is equivalent to the third. \square

The following theorem states that the fractal operators produces all nontrivial charges.

Theorem 3.1. *Suppose $\Lambda = \mathbb{Z}^D$ is the translation group of the underlying lattice. The set of all charges modulo trivial ones is in one-to-one correspondence with the torsion submodule of $\text{coker } \epsilon$.*

To illustrate the idea of the proof, consider a (classical) excitation map⁷

$$\phi = \begin{pmatrix} 1+x+y & 0 \\ 0 & 1+x \\ 0 & 1+y \end{pmatrix} : R^2 \rightarrow R^3.$$

A nonzero element $f = 1+x+y \in R$ is a fractal generator since $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^T \notin \text{im } \phi$ and $(1+x+y) \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^T \in \text{im } \phi$; f is a zero-divisor on a torsion element $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^T \in \text{coker } \epsilon$. It is indeed a charge since $\phi(\tilde{f} \begin{pmatrix} 1 & 0 \end{pmatrix}^T) = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^T$ where

$$\tilde{f} = \lim_{n \rightarrow \infty} f^{2^n - 1} \in \mathbb{F}[[x, y]]$$

is a formal power series, which can be viewed as an element of \tilde{R} . The limit is well-defined since $f^{2^{n+1}-1} - f^{2^n-1}$ only contains terms of degree 2^n or higher. That is to say, only higher order ‘corrections’ are added and lower order terms are not affected. Of course, there is no natural notion of smallness in the ring $\mathbb{F}[x, y]$. But one can formally call the members of the ideal power $(x, y)^n \subseteq \mathbb{F}[x, y]$ *small*. It is legitimate to introduce a topology in R defined by the *ever shrinking* ideal powers $(x, y)^n$. They play a role analogous to the ball of radius $1/n$ in a metric topological space. The *completion* of $\mathbb{F}[x, y]$ where every Cauchy sequence with respect to this topology is promoted to a convergent sequence, is nothing but the formal power series ring $\mathbb{F}[[x, y]]$. For a detailed treatment, see Chapter 10 of [80].

⁷ It is classical because it is not derived from an interesting quantum commuting Pauli Hamiltonian. For a classical Hamiltonian where all terms are tensor products of σ_z , there is no need to keep a $t \times 2q$ matrix ϵ since the right half ϵ is zero. Just the left half suffices, which can be arbitrary since the commutativity equation $\epsilon \lambda \epsilon^\dagger = 0$ is automatic. Nevertheless, the excitations and fractal operators are relevant. Our proof of the theorem is not contingent on the commutativity equation.

The completion and the limit only make sense in the polynomial ring $\mathbb{F}[x, y]$. The reason \tilde{f} is well-defined is that $f \in \mathbb{F}[x^{\pm 1}, y^{\pm 1}]$ is accidentally expressed as a usual polynomial with lowest order term 1. In the proof below we show that every fractal generator can be expressed in this way. Hence, a torsion element of $\text{coker } \epsilon$ is really a charge.

Proof. For a module M , let $T(M)$ denote the torsion submodule of M :

$$T(M) = \{m \in M \mid \exists r \in R \setminus \{0\} \text{ such that } rm = 0\}$$

Suppose first that $T(\text{coker } \epsilon) = 0$. We claim that in this case there is no nontrivial charge. Let $e = \epsilon(\tilde{p}) \in E$ be a charge, where $\tilde{p} \in \tilde{P}$. By Proposition 3.5.1 we have an exact sequence of finitely generated free modules $P \xrightarrow{\epsilon} E \xrightarrow{\epsilon_1} E_1$. Since the matrix ϵ_1 is over R , the complex extends to a complex of modules of tuples of functions on the translation group.

$$\tilde{P} \xrightarrow{\epsilon} \tilde{E} \xrightarrow{\epsilon_1} \tilde{E}_1$$

(This extended sequence may not be exact.) Then, $\epsilon_1(e) = \epsilon_1(\epsilon(\tilde{p})) = 0$ since $\epsilon_1 \circ \epsilon = 0$ identically. But, $e \in E$, and therefore, $e \in \ker \epsilon_1 \cap E = \epsilon(P)$. It means that e is a trivial charge, i.e., e maps to zero in $\text{coker } \epsilon$, and proves the claim.⁸

Now, allow $\text{coker}(P \xrightarrow{\epsilon} E)$ to contain torsion elements. $Q = (\text{coker } \epsilon)/T(\text{coker } \epsilon)$ is torsion-free, and is finitely presented as $Q = \text{coker}(\epsilon' : P' \rightarrow E)$ where P' is a finitely generated free module. In fact, we may choose ϵ' by adding more columns representing the generators of the torsion submodule of $\text{coker } \epsilon$ to the matrix ϵ .

$$\epsilon = \begin{pmatrix} \# & \# \\ \# & \# \end{pmatrix} \quad \epsilon' = \begin{pmatrix} \# & \# & * & * \\ \# & \# & * & * \end{pmatrix}$$

Then, P can be regarded as a direct summand of P' .⁹

Let $e = \epsilon(\tilde{p}) \in E$ be any charge. Since the matrix ϵ' contains ϵ as submatrix, we may write $e = \epsilon'(\tilde{p}) \in E$. Since $T(\text{coker } \epsilon') = 0$, we see by the first part of the proof that $e = \epsilon'(p')$ for some $p' \in P'$. Then, e maps to zero in Q , and it follows that e maps into $T(\text{coker } \epsilon)$ in $\text{coker } \epsilon$. In other words, the equivalence class of e modulo trivial charges is a torsion element of $\text{coker } \epsilon$.

Conversely, we have to prove that for every element $e \in E$ such that $fe = \epsilon(p)$ for some $f \in R \setminus \{0\}$ and $p \in P$, there exists $\tilde{p} \in \tilde{P}$ such that $e = \epsilon(\tilde{p})$. Here, \tilde{P} is the module of all $2q$ -tuples of \mathbb{F}_2 -

⁸ One may wish to consider ϵ to consist of the second column of ϕ above. Then $\epsilon_1 = (1 + y \quad -1 - x)$.

⁹ If we take $\epsilon = \phi$ above, then

$$\epsilon' = \begin{pmatrix} 1 + x + y & 0 & 1 \\ 0 & 1 + x & 0 \\ 0 & 1 + y & 0 \end{pmatrix}.$$

Note that $P' = P \oplus R$.

valued functions on the translation group. Consider the lexicographic total order on \mathbb{Z}^D in which $x_1 \succ x_2 \succ \cdots \succ x_D$. It induces a total order on the monomials of R . Choose the least term f_0 of f . By multiplying f_0^{-1} , we may assume $f_0 = 1$.¹⁰

We claim that the sequence

$$f, f^2 f, f^4 f^2 f, \dots, f^{2^n} f^{2^{n-1}} \cdots f^2 f, \dots \quad (3.4)$$

converges to $\tilde{f} \in \tilde{R}$, where \tilde{R} is the set of all \mathbb{F}_2 -valued functions on Λ . Given the claim, since $f^{2^n} e = e + (f - 1)^{2^n} e = \epsilon(f^{2^{n-1}} \cdots f^2 f p)$ where $p \in P$, we conclude that $e = \epsilon(\tilde{f} p)$ is a charge.

If f is of nonnegative exponents, and hence $f \in S = \mathbb{F}_2[x_1, \dots, x_D]$, then the claim is clearly true. Indeed, the positive degree terms of $f^{2^n} = 1 + (f - 1)^{2^n}$ are in the ideal power $(x_1, \dots, x_D)^{2^n} \subset S$. Therefore, the sequence Eq. (3.4) converges in the formal power series ring $\mathbb{F}_2[[x_1, \dots, x_D]]$, which can be regarded as a subset of \tilde{R} . If f is not of nonnegative exponents, one can introduce the following change of basis of the lattice \mathbb{Z}^D such that f becomes of nonnegative exponents. In other words, the sequence Eq. (3.4) is in fact contained in a ring that is isomorphic to the formal power series ring, where the convergence is clear.

For any nonnegative integers m_1, \dots, m_{D-1} , define a linear transformation

$$\zeta_m = \zeta_{(m_1, m_2, \dots, m_{D-1})} : \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_D \end{pmatrix} \mapsto \begin{pmatrix} a'_1 \\ a'_2 \\ \vdots \\ a'_D \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ m_1 & 1 & 0 & & 0 \\ m_1 & m_2 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ m_1 & m_2 & \cdots & m_{D-1} & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_D \end{pmatrix} \text{ on } \mathbb{Z}^D.$$

ζ_m induces the map $x_1^{a_1} \cdots x_D^{a_D} \mapsto x_1^{a'_1} \cdots x_D^{a'_D}$ on R . Let $u = x_1^{a_1} \cdots x_D^{a_D}$ be an arbitrary term of f other than 1, so $u \succ 1$. For the smallest $i \in \{1, \dots, D\}$ such that $a_i \neq 0$, one has $a_i > 0$ due to the lexicographic order. Hence, if we choose m_i large enough and set $m_j = 0$ ($j \neq i$), then $\zeta_m(u)$ has nonnegative exponents. Since any ζ_m maps a nonnegative exponent term to a nonnegative exponent term, and there are only finitely many terms in f , it follows that there is a finite composition ζ of ζ_m 's which maps f to a polynomial of nonnegative exponents.¹¹ \square

Since a nontrivial charge 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 $[[o_1, \dots, o_n]]$

¹⁰ If $D = 1$, f would be a polynomial of nonnegative exponents with the lowest order term being 1. If $D = 2$ and $f = y + y^2 + x$, then the least term is y . After multiplying f_0^{-1} , it becomes $1 + y + xy^{-1}$.

¹¹ For our previous example $f = 1 + y + xy^{-1}$, one takes $\zeta : x^i y^j \mapsto x^i y^{i+j}$, so $\zeta(f) = 1 + y + x$.

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 3.2. [48] *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 $v \notin \text{im } \epsilon$. We already know v is a point-like nontrivial 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

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

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

$$\int s_r = f^{2^{r-1}} \int s_{r-1} = f^{2^{r-1}} f^{2^{r-2}} \int s_{r-2} = f^{2^{r-1} + 2^{r-2} + \dots + 1} \int s_0 = f^{2^r - 1} p$$

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. \square

Fractal operators appear in Newman-Moore model [48] where classical spin glass is discussed. Their model has generating matrix $\sigma = \begin{pmatrix} 0 & 1+x+y \end{pmatrix}^T$. The theorem is a simple generalization of Newman and Moore's construction. Another explicit example of fractal operators in a quantum model can be found in Section 8.7.

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 Chapter 5.

Below, we point out a couple of sufficient conditions for nontrivial charges, or equivalently, fractal generators to exist.

Proposition 3.5.2. *For code Hamiltonians, the existence of a fractal generator is a property of an equivalence class of Hamiltonians in the sense of Definition 3.2.*

Proof. Suppose $\text{im } \sigma = \text{im } \sigma'$. 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 $\text{im } \epsilon'$ and $\text{im } \epsilon$, respectively. In particular, B' and B are injective on $\text{im } \epsilon'$ and $\text{im } \epsilon$, 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 $Bv \in \text{im } \epsilon'$, then $v = B'Bv \in \text{im } \epsilon$, 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 $\text{coker } \epsilon$ 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 $\text{coker } \epsilon$. \square

Proposition 3.5.3. *For any ring S and $t \geq 1$, if $0 \rightarrow S^t \rightarrow S^{2t} \xrightarrow{\phi} S^t$ is exact and $I(\phi) \neq S$, then $\text{coker } \phi$ 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 3.3.2, $\text{rank } \phi = t$. Since $0 \subsetneq I_t(\phi) \subsetneq S$ is the initial Fitting ideal, we have $0 \neq \text{ann } \text{coker } \phi \neq S$. That is, $\text{coker } \phi$ is not torsion-free.

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

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

By Remark 3.2, $t = \text{rank } G = \text{rank } \sigma = \text{rank } \epsilon = q$. □

Proposition 3.5.4. *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 3.5.1,

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

is exact for some finitely generated free module E' . Together with Hilbert syzygy theorem [76, Corollary 15.11],¹² Proposition 3.3.2 implies $\text{codim } I(\sigma) \geq 3$ unless $I(\sigma) = R$. But, $\text{codim } I(\sigma) = 2$ and $I(\sigma) \neq R$ by Corollary 3.4.2. This is a contradiction. □

¹²We will prove a stronger version in Lemma 4.2.1.

Chapter 4

Structure of exact Hamiltonians on lattices

One of the goals of the formalism in the previous chapter is to classify all code Hamiltonians that are translationally invariant. A satisfactory classification should be comprised of a complete set of invariants, and a table of inequivalent code Hamiltonians or a machinery to obtain them. In this chapter we present preliminary results towards this goal.

In one dimension, the classification problem is completely solved. A particularly nice property of one dimension is that its translation group algebra $\mathbb{F}_2[x, x^{-1}]$ is a Euclidean domain, over which any matrix is diagonal up to multiplications on the left and right by invertible matrices. We show that this diagonalization is possible even if the left multiplications are restricted to symplectic transformations. Exploiting the finiteness of the ground field \mathbb{F}_2 , we conclude that there are only Ising models [84]. An almost identical treatment appears in quantum convolutional codes [71, 72]. (A more general statement is proved by Beigi [85].)

In two dimensions, we find that any excitation of an exact code Hamiltonian is described by a collection of point-like ones, each of which is attached to a string operator. Furthermore, it seems that one can prove a stronger statement that there are only toric codes [84, 86], although we do not complete the proof. In three dimensions, we show that there must be point-like excitations for exact code Hamiltonians. This implies that it is unavoidable in the translation-invariant case to have a topological charge penetrating through the system, for which the energy penalty is only logarithmic in the displacement. If we assume that the degeneracy under periodic boundary conditions should be constant independent of system size, then the energy penalty is upper bounded by a constant, reproducing the result of Yoshida [47].

Note that all the lemmas and theorems in this chapter are valid over qudits with prime dimensions. We conclude this chapter with several examples.

4.1 One dimension

The group algebra $R = \mathbb{F}_2[x, \bar{x}]$ 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

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

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 4.1.1. *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 $x^n - 1$.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

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

¹This part is well known, at least in the linear cyclic coding theory [68].

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,

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

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

For example, consider $f(x) = x^2 + x + 1 \in S = \mathbb{F}_2[x]$. It is the primitive polynomial of the field \mathbb{F}_4 of four elements over \mathbb{F}_2 . Any element in \mathbb{F}_4 is a solution of $x^4 - x = 0$. Since $f(0) = 1$, we see that $n = 3$ is the smallest integer such that $f(x)$ divides $x^n - 1$. As a module over $S' = \mathbb{F}_2[x^3]$, the original ring S is free with (ordered) basis $\{1, x, x^2\}$. The multiplication by x on S viewed as an endomorphism has a matrix representation

$$x = \begin{pmatrix} 0 & 0 & x^3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Thus, $f(x)$ as an endomorphism of S' -module S has a matrix representation as follows.

$$f(x) = \begin{pmatrix} 1 & x^3 & x^3 \\ 1 & 1 & x^3 \\ 1 & 1 & 1 \end{pmatrix} \cong \begin{pmatrix} 1 & 0 & 0 \\ 0 & x^3 + 1 & 0 \\ 0 & 0 & x^3 + 1 \end{pmatrix}$$

Here, the second matrix is obtained by row and column operations. There are 2 diagonal entries $x^3 + 1$ as $f(x)$ is of degree 2.

Theorem 4.1. *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.*

Yoshida [84] arrived at a similar conclusion assuming that the ground space degeneracy when the Hamiltonian is defined on a ring should be independent of the length of the ring. If translation group is trivial, the proof below reduces to a well-known fact that the Clifford group is generated by controlled-NOT, Hadamard, and Phase gates [61, Proposition 15.7]. The proof in fact implies that

the group of all symplectic transformations in one dimension is generated by elementary symplectic transformations of Section 3.2.1.

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 .

Proof. Applying Smith's algorithm to the first row and the first column of $2q \times t$ 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 $(q+j)^{\text{th}}$ 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:

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

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

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

Write $f_1 = \alpha x^a + \dots + \beta x^b$ and $g_1 = \gamma x^c + \dots + \delta x^d$ where $a \leq b$ and $c \leq d$ and $\alpha, \beta, \gamma, \delta \neq 0$. Then, $\bar{f}_1 g_1 = \beta \gamma x^{c-b} + \dots + \alpha \delta x^{d-a}$. Since $f_1 \bar{g}_1 = \bar{f}_1 g_1$, it must hold that $-(c-b) = d-a$ and $\alpha \delta = \beta \gamma$. Since $\deg f_1 \leq \deg g_1$, we have $d-b = -(c-a) \geq 0$. The controlled-Phase $E_{1+q,1}(-(x^{d-b} + x^{c-a})\delta/\beta)$ will decrease the degree of g_1 by two, which eventually becomes smaller than $\deg f_1$. One may then apply Hadamard to swap f_1 and g_1 . Since the degree of $(1,1)$ -entry cannot decrease forever, the process must end with $g_1 = 0$.

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 $g_i = 0$:

$$\begin{pmatrix} f_1 & 0 \\ 0 & A \\ \hline 0 & 0 \\ 0 & B \end{pmatrix}.$$

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

$$\begin{pmatrix} f \end{pmatrix}$$

where we omitted the lower half block. We can always choose $f = f(x)$ such that $f(x)$ has only nonnegative exponents and $f(0) \neq 0$ since x is a unit in R . Lemma 4.1.1 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. \square

Note that an almost identical treatment appears in [72].

4.2 Two dimensions

If $D = 2$, the lattice is $\Lambda = \mathbb{Z}^2$, and our base ring is $R = \mathbb{F}_2[x, \bar{x}, y, \bar{y}]$.

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 [87]. We prove a more general version.

Lemma 4.2.1. *If $G \xrightarrow{\sigma} P \xrightarrow{\epsilon} E$ is exact over $R = \mathbb{F}_2[x_1, \bar{x}_1, \dots, x_D, \bar{x}_D]$, There exists $\sigma' : G' \rightarrow P$ such that $\text{im } \sigma' = \text{im } \sigma$ and*

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

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

The lemma is almost the same as the Hilbert syzygy theorem [76, Corollary 15.11] applied to $\text{coker } \epsilon$, which states that any finitely generated module over a polynomial ring with n variables has a finite free resolution of length $\leq n$, by finitely generated free modules. A difference is that our two maps

on the far right in the resolution has to be related as $\epsilon = \sigma^\dagger \lambda$. To this end, we make use of a constructive version of Hilbert syzygy theorem via Gröbner basis.

Proposition 4.2.2. [76, Theorem 15.10, Corollary 15.11] *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 $M_1 = \bigoplus_{i=1}^n S e_i$ 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 4.2.1. Without loss of generality assume that the $t \times 2q$ matrix ϵ have entries with nonnegative exponents, so ϵ has entries in $S = \mathbb{F}_2[x_1, \dots, x_D]$. Below, every module is over the polynomial ring S unless otherwise noted. Let E_+ be the free S -module of rank equal to $\text{rank}_R E$.

If g_1, \dots, g_{2q} are the columns of ϵ , apply Buchberger's algorithm to obtain a Gröbner basis $g_1, \dots, g_{2q}, \dots, g_n$ of $\text{im } \epsilon$. Let ϵ' be the matrix whose columns are g_1, \dots, g_n . We regard ϵ' as a map $M_0 \rightarrow E_+$. By Proposition 4.2.2, 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 $\tau_1 : M_1 \rightarrow M_0$.

By induction on D , we have an exact sequence

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

of free S -modules, where the initial terms of columns of τ_D lack all the variables. By Proposition 4.2.2 again, $M'_{D-1} = M_{D-1}/\text{im } \tau_D$ is free. Since $\ker \tau_{D-1} = \text{im } \tau_D$, we have

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

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 $\ker \epsilon' = \text{im } \tau_1$, The first row r of τ_{1d} should generate $1 \in S$. (This property is called unimodularity.) Quillen-Suslin theorem [60, Chapter XXI Theorem 3.5] states that there exists a basis change of M_1 such that r becomes $\begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix}$.

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 $\ker \tau_1 = \text{im } \tau_2$. Let M'_1 denote the projection of M_1 such that the sequence

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

of free S -modules is exact.

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

$$U = \{x_1^{i_1} \cdots x_D^{i_D} \mid i_1, \dots, i_D \geq 0\},$$

we finally obtain the desired exact sequence over $U^{-1}S = R$ with $P = U^{-1}M'_0$ and $E = U^{-1}E_+$.

Since $\text{im } \sigma = \ker \epsilon$, we have $\text{im } \sigma' = \text{im } \sigma$. \square

Lemma 4.2.3. *Let R be a Laurent polynomial ring in D variables over a finite field \mathbb{F} , and N be a module over R . Suppose $J = \text{ann}_R N$ is a proper ideal such that $\dim R/J = 0$. Then, there exists an integer $L \geq 1$ such that*

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

where $R' = \mathbb{F}[x_1^{\pm L}, \dots, x_D^{\pm L}]$ is a subring of R .

This is a variant of Lemma 4.1.1. The annihilator $J = \text{ann}_R N$ is the set of all elements $r \in R$ such that $rn = 0$ for any $n \in N$. It is an ideal; if $r_1, r_2 \in \text{ann}_R N$, then $r_1 + r_2$ is an annihilator since $(r_1 + r_2)n = r_1n + r_2n = 0$, and $ar_1 \in \text{ann}_R N$ for any $a \in R$ since $(ar_1)n = a(r_1n) = 0$. If $R' \subseteq R$ is

a subring and N is an R -module, N is an R' -module naturally. Clearly, $J' = \text{ann}_{R'} N$ is by definition equal to $(\text{ann}_R N) \cap R'$. Note that J' is the kernel of the composite map $R' \hookrightarrow R \rightarrow R/J$. Hence, we have an algebra homomorphism $\varphi' : R'/J' \rightarrow R/J$. Although R' is a subring, it is isomorphic to R via the correspondence $x_i^L \leftrightarrow x_i$. Therefore, we may view φ' as a map $\varphi : R/I \rightarrow R/J$ for some ideal $I \subseteq R$. It is a homomorphism such that $\varphi(x_i) = x_i^L$. Considering the algebras as the set of all functions on the algebraic sets $V(I)$ and $V(J)$ defined by I and J , respectively, we obtain a map $\hat{\varphi} : V(J) \rightarrow V(I)$. Intuitively, $\hat{\varphi}$ maps each point $(a_1, \dots, a_D) \in \mathbb{F}^D$ to $(a_1^L, \dots, a_D^L) \in \mathbb{F}^D$. In a finite field, any nonzero element is a root of unity. Since $\dim R/J = 0$, which means that $V(J)$ is a finite set, we can find a certain L so $V(I)$ would consist of a single point. A formal proof is as follows.

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 [76, Theorem 4.19]). 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 $\mathfrak{b}_n = (x_1^n - 1, \dots, x_D^n - 1) \subseteq \mathfrak{m}$. Since $x^n - 1$ divides $x^{mn} - 1$, 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. $\text{rad } J$ 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 $R' = \mathbb{F}[x_1^L, \bar{x}_1^L, \dots, x_D^L, \bar{x}_D^L]$, $\text{ann}_{R'} N$ 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' . \square

Theorem 4.2. *For any two-dimensional degenerate exact code Hamiltonian, there exists an equivalent Hamiltonian such that*

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

Thus, coker ϵ is a torsion module.

The content of Theorem 4.2 is presented in [87]. We will comment on it after the proof.

Proof. By Lemma 4.2.1, we can find an equivalent Hamiltonian such that the generating map σ for its stabilizer module is injective:

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

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

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

is exact where $\epsilon = \sigma^\dagger \lambda_q$ and E has rank t . Applying Proposition 3.3.2, since $\overline{I(\sigma)} = I(\epsilon)$ and hence in particular $\text{codim } I(\sigma) = \text{codim } I(\epsilon)$, we have that $q = t$ and $\text{codim } I(\epsilon) \geq 2$ if $I(\epsilon) \neq R$. But, $I(\epsilon) \neq R$ by Corollary 3.4.2.

Since $q = t$, $I(\epsilon)$ is equal to the initial Fitting ideal, and therefore has the same radical as the annihilator of $\text{coker } \epsilon = E/\text{im } \epsilon$. (See [76, Proposition 20.7] or [60, Chapter XIX Proposition 2.5].) In particular, $\dim R/(\text{ann coker } \epsilon) = 0$. Apply Lemma 4.2.3 to conclude the proof. \square

An interpretation of the theorem is the following. For systems of qubits, Theorem 4.2 says that $x + 1$ and $y + 1$ are in $\text{ann coker } \epsilon$. 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 through 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 $(x - 1, y - 1) = \text{ann coker } \epsilon$, the action of $x, y \in R$ on $\text{coker } \epsilon$ is the same as the identity action. Therefore, the R -module $\text{coker } \epsilon$ is completely determined up to isomorphism by its dimension k as an \mathbb{F}_2 -vector space. In particular, $\text{coker } \epsilon$ is a finite set, which means there are finitely many charges. The module $K(L)$ of Pauli operators acting on the ground space (logical operators), can be viewed as $K(L) = \text{Tor}_1(\text{coker } \epsilon, R/\mathfrak{b}_L)$. Thus, $K(L)$ is determined by k up to R -module isomorphisms. This implies that the translations of a logical operator are all equivalent. It is not too obvious at this moment whether the symplectic structure, or the commutation relations among the logical operators, of $K(L)$ is also completely determined.

Yoshida [84] argued a similar result assuming that the ground-state degeneracy should be independent of system size. Bombin [87] later claimed without the constant degeneracy assumption that one can choose locally independent stabilizer generators in a ‘translationally invariant way’ in two dimensions, for which Lemma 4.2.1 is a generalization, and that there are finitely many topological charges, which is immediate from Theorem 4.2 since $\text{coker } \epsilon$ is a finite set. The claim is further strengthened assuming extra conditions by Bombin *et al.* [86], which can be summarized by saying that σ is a finite direct sum of $\sigma_{2\text{D-toric}}$ in Example 3.2.

Remark 4.1. Although the strings are capable of moving charges on the lattice, it could be very long compared to the interaction range. Consider

$$\epsilon_p = \begin{pmatrix} p(x) & p(y) & 0 & 0 \\ 0 & 0 & p(\bar{y}) & -p(\bar{x}) \end{pmatrix}$$

where p is any polynomial. It defines an exact code Hamiltonian. For instance, the choice $p(t) = t - 1$ reproduces the 2D toric code of Example 3.2. Now let $p(t)$ be a primitive polynomial of the extension field \mathbb{F}_{2^w} over \mathbb{F}_2 . $p(t)$ has coefficients in the base field \mathbb{F}_2 and factorizes in \mathbb{F}_{2^w} as $p(t) = (t - \theta)(t - \theta^2)(t - \theta^{2^2}) \cdots (t - \theta^{2^{w-1}})$. (See [60, Chapter V Section 5].) The multiplicative order of θ is $N = 2^w - 1$. The degree w of $p(t)$ may be called the interaction range. If the charge $e = \begin{pmatrix} 1 & 0 \end{pmatrix}^T$ at $(0, 0) \in \mathbb{Z}^2$ is transported to $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ by some finitely supported operator, we have $(x^a y^b - 1)e \in \text{im } \epsilon$. That is, $x^a y^b - 1 \in (p(x), p(y))$. Substituting $x \mapsto \theta$ and $y \mapsto \theta^{2^m}$, we see that $\theta^{a+2^m b} = 1$ or $a + 2^m b \equiv 0 \pmod{N}$ for any $m \in \mathbb{Z}$. In other words, $a \equiv -b \equiv -2b \pmod{N}$. It follows that $|a| + |b| \geq N$.² Therefore, the length of the string segment transporting a charge is exponential in the interaction range w .

Example 4.1 (Wen plaquette [88]). This model consists of a single type of interaction ($t = q = 1$)

$$\begin{array}{ccc} X & - & Y \\ | & & | \\ Y & - & X \end{array} \quad \sigma_{\text{Wen}} = \left(\frac{1 + x + y + xy}{1 + xy} \right)$$

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

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

(The coarse-graining considered in this example is intended to demonstrate a non-square blocking of the old lattice to obtain a ‘tilted’ new lattice, and is by no means special.) 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

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

²In case of qudits with prime dimensions p , the lower bound will be $N/(p-1)$.

our new σ on the coarse-grained lattice becomes

$$\sigma' = \begin{pmatrix} 1 + x'y' & y' + x'y' \\ 1 + x' & 1 + x'y' \\ 1 + x'y' & 0 \\ 0 & 1 + x'y' \end{pmatrix}.$$

By a sequence of elementary symplectic transformations, we have

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

which is exactly the 2D toric code. ◇

4.3 Three dimensions

In the previous section, we derived a consequence of the exactness of code Hamiltonians. The two-dimensional Hamiltonian was special so we were able to characterize the behavior of the charges more or less completely. Here, we prove a weaker property of three dimensions that there must exist a nontrivial charge for any exact code Hamiltonian. It follows from Theorems 3.1,3.2 that such a charge can spread through the system by surmounting the logarithmic energy barrier.

Lemma 4.3.1. *Suppose $D = 3$,*

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

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

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

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

If $G_1 = 0$, Proposition 3.5.3 implies the conclusion. So we assume $G_1 \neq 0$, and therefore we have

$I(\sigma_1) = R$ by Proposition 3.3.2.

Let us localize the sequence at \mathfrak{m} , so $I(\sigma_1)_{\mathfrak{m}} = R_{\mathfrak{m}}$. Since $\text{rank}(G_1)_{\mathfrak{m}} = \text{rank}(\sigma_1)_{\mathfrak{m}}$, 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 3.4.1. In other words, there is an invertible matrix $B \in \text{GL}_{t \times t}(R_{\mathfrak{m}})$ such that

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

where $\tilde{\sigma}$ is the $2q \times t'$ submatrix. Note that the antipode map is a well-defined automorphism of $R_{\mathfrak{m}}$ since $\bar{\mathfrak{m}} = \mathfrak{m}$.

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

$$B^\dagger \epsilon_{\mathfrak{m}} = \begin{pmatrix} \tilde{\sigma}^\dagger \\ 0 \end{pmatrix} \lambda_q = \begin{pmatrix} \tilde{\sigma}^\dagger \lambda_q \\ 0 \end{pmatrix}. \quad (4.1)$$

Therefore, we get a new exact sequence

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

where $G' = G_{\mathfrak{m}} / \text{im}(\sigma_1)_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$ -module and $t' = \text{rank } G'$. It is clear that $\text{rank } \tilde{\epsilon} = \text{rank } \tilde{\sigma}$. Setting $S = R_{\mathfrak{m}}$ in Proposition 3.5.3 implies that $\text{coker } \tilde{\epsilon}$ is not torsion-free. But, since we are assuming $\text{coker } \epsilon_m$ is torsion-free, $\text{coker } \tilde{\sigma}^\dagger$ is also torsion-free by Eq. (4.1). This is a contradiction. \square

Theorem 4.3. *For any three-dimensional, degenerate and exact code Hamiltonian, there exists a fractal generator.*

Proof. By Lemma 4.2.1, there exists an equivalent Hamiltonian such that

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

is exact. The existence of a fractal generator is a property of the equivalence class by Proposition 3.5.2. If we can find a coarse-graining such that $I(\sigma') \subseteq (x' - 1, y' - 1, z' - 1)$, then Lemma 4.3.1 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. 3.4. There exists L such that $K(L) = \ker \epsilon_L / \text{im } \sigma_L \neq 0$ by Corollary 3.4.2. Consider the coarse-grain by $x' = x^L$, $y' = y^L$, $z' = z^L$. Let $R' = F_2[x'^{\pm 1}, y'^{\pm 1}, z'^{\pm 1}]$ denote the coarse-grained base ring. If $K'(L')$ denotes $\ker \epsilon'_{L'} / \text{im } \sigma'_{L'}$ 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 3.4.1, we have $I(\sigma') \subseteq \mathfrak{m}$. □

Yoshida argued that when the ground-state degeneracy is constant independent of system size there exists a string operator [47]. To prove it, we need an algebraic fact.

Proposition 4.3.2. *Let M be a finitely presented R -module, and T be its torsion submodule. Let I be the first non-vanishing Fitting ideal of M . Then,*

$$\text{rad } I \subseteq \text{rad ann } T.$$

Proof. Let \mathfrak{p} be any prime ideal of R such that $I \not\subseteq \mathfrak{p}$. By the calculation of the proof of Lemma 3.4.1, $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$ -module, and hence is torsion-free. Since T is embedded in M , it follows that $T_{\mathfrak{p}} = 0$, or equivalently, $\text{ann } T \not\subseteq \mathfrak{p}$. Since the radical of an ideal is the intersection of all primes containing it [80, Proposition 1.8], the claim is proved. □

Corollary 4.3.3. *Let T be the set of all point-like charges modulo locally created ones of a degenerate and exact code Hamiltonian in three dimensions of characteristic dimension zero. Then, one can coarse-grain the lattice such that*

$$\text{ann } T = (x - 1, y - 1, z - 1).$$

The corollary says that any point-like charge is attached to strings and is able to move freely through the lattice. The condition is implied by Lemma 3.4.9 if the ground-state degeneracy is constant independent of the system size when defined on a periodic lattice.

Proof. By Theorem 3.1, T is the torsion submodule of $\text{coker } \epsilon$. By Theorem 4.3, T is nonzero. Setting $M = \text{coker } \epsilon$ in Proposition 4.3.2, the associated ideal $I_q(\epsilon)$ is the first non-vanishing Fitting ideal of M . Since $\dim R/I_q(\epsilon) = 0$ by assumption, we have $\dim R/\text{ann } T = 0$. Lemma 4.2.3 implies the claim. □

Example 4.2 (Toric codes in higher dimensions). Any higher-dimensional toric code can be treated similarly as for the two-dimensional case. In three dimensions one associates each site with $q = 3$

qubits. It is easily checked that

$$\sigma_{3\text{D-toric}} = \begin{pmatrix} 1 + \bar{x} & 0 & 0 & 0 \\ 1 + \bar{y} & 0 & 0 & 0 \\ 1 + \bar{z} & 0 & 0 & 0 \\ \hline 0 & 0 & 1 + z & 1 + y \\ 0 & 1 + z & 0 & 1 + x \\ 0 & 1 + y & 1 + x & 0 \end{pmatrix}.$$

Both two- and three-dimensional toric codes have the property that $\text{coker } \epsilon$ is not torsion-free. However, in two dimensions any element of E is a physical charge, whereas in three dimensions E contains physically irrelevant elements. Note that in both cases, $1+x$ and $1+y$ are fractal generators. Being consisted of two terms, they generate the ‘string operators.’

The 4D toric code [7] has σ_x -type interaction and σ_z -type interaction. Originally the qubits are placed on every plaquette of 4D hypercubic lattice; instead we place $q = 6$ qubits on each site. The generating map σ for the stabilizer module is written as a 12×8 -matrix ($t = 8$)

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

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 4.3 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 is enough to consider σ_Z since

$\overline{\text{coker } \sigma_X^\dagger} \cong \text{coker } \sigma_Z^\dagger$ as R_4 -modules, where $R_4 = \mathbb{F}_2[x^{\pm 1}, y^{\pm 1}, z^{\pm 1}, w^{\pm 1}]$. If

$$\epsilon_1 = \begin{pmatrix} 1+x & 1+y & 1+z & 1+w \end{pmatrix} : R_4^4 \rightarrow R_4,$$

then

$$R_4^6 \xrightarrow{\sigma_Z^\dagger} R_4^4 \xrightarrow{\epsilon_1} R_4$$

is exact. (A direct way to check it is to compute S-polynomials [76, Chapter 15] of the entries of ϵ_1 , and to verify that they all are in the rows of σ_Z .) Hence, $\text{coker } \sigma_Z^\dagger$ is torsion-free by Proposition 3.5.1.

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 $\mathfrak{m} = (x_1 - 1, \dots, x_D - 1)$. 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 3.4.1. Therefore, if $2 \nmid L$, $K(L)$ has constant vector space dimension independent of L .

There is a more direct way to compute the R -module $K(L)$. For the three-dimensional case, consider a free resolution of R_3/\mathfrak{m} , where $R_3 = \mathbb{F}_2[x^{\pm 1}, y^{\pm 1}, z^{\pm 1}]$, as

$$0 \rightarrow R_3^1 \xrightarrow{\partial_3 = \begin{pmatrix} a \\ b \\ c \end{pmatrix}} R_3^3 \xrightarrow{\partial_2 = \begin{pmatrix} 0 & -c & b \\ c & 0 & -a \\ -b & a & 0 \end{pmatrix}} R_3^3 \xrightarrow{\partial_1 = \begin{pmatrix} a & b & c \end{pmatrix}} R_3^1 \rightarrow R_3/\mathfrak{m} \rightarrow 0$$

where $a = x - 1$, $b = y - 1$, and $c = z - 1$. We see that

$$\sigma_{3\text{D-toric}} = \bar{\partial}_3 \oplus \partial_2, \quad \text{and} \quad \epsilon_{3\text{D-toric}} = \bar{\partial}_2 \oplus \partial_1. \quad (4.2)$$

Therefore,

$$K(L)_{3\text{D-toric}} \cong \text{Tor}_1(\text{coker } \epsilon_{3\text{D-toric}}, R_3/\mathfrak{b}_L) \cong \text{Tor}_2(\overline{R_3/\mathfrak{m}}, R_3/\mathfrak{b}_L) \oplus \text{Tor}_1(R_3/\mathfrak{m}, R_3/\mathfrak{b}_L).$$

Using $\text{Tor}(M, N) \cong \text{Tor}(N, M)$ and the fact that a resolution of R_3/\mathfrak{b}_L is Eq. (4.2) with a, b, c replaced by $x^L - 1, y^L - 1, z^L - 1$, respectively, we have

$$\text{Tor}_i(R_3/\mathfrak{m}, R_3/\mathfrak{b}_L) \cong \text{Tor}_i(R_3/\mathfrak{m}, R_3/\mathfrak{m}) \cong (\mathbb{F}_2)^{3C_i}$$

for each $0 \leq i \leq 3$. Therefore, $K(L)_{3\text{D-toric}} \cong (\mathbb{F}_2)^{3C_2} \oplus (\mathbb{F}_2)^{3C_1} \cong (\mathbb{F}_2)^6$. The four-dimensional case is similar:

$$K(L)_{4\text{D-toric}} \cong \text{Tor}_2(R_4/\mathfrak{m}, R_4/\mathfrak{b}_L) \oplus \text{Tor}_2(\overline{R_4/\mathfrak{m}}, R_4/\mathfrak{b}_L) \cong ((\mathbb{F}_2)^{4C_2})^2.$$

The calculation here is closely related to the cellular homology interpretation of toric codes. \diamond

Example 4.3 (Chamon model [89, 90]). 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 3.4.5. 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

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

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 $x \prec y \prec z$, 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,

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

\diamond

Example 4.4 (Levin-Wen fermion model [33]). The 3-dimensional model is originally defined in terms of Hermitian bosonic operators $\{\gamma^{ab}\}_{a,b=1,\dots,6}$, squaring to identity if nonzero, such that $\gamma^{ab} = -\gamma^{ba}$, $[\gamma^{ab}, \gamma^{cd}] = 0$ if a, b, c, d are distinct, and $\gamma^{ab}\gamma^{bc} = i\gamma^{ac}$ if $a \neq c$. An irreducible

representation is given by Pauli matrices acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$, and their commuting Hamiltonian fits nicely into our formalism. The model was proposed to demonstrate that the point-like excitations may actually be fermions.

$$\sigma_{\text{Levin-Wen}} = \begin{pmatrix} 1+z & 1+z & x+y \\ y+yz & x+xz & x+y \\ y+z & 1+x & 1+x \\ y+z & z+xz & y+xy \end{pmatrix}$$

$$\epsilon_{\text{Levin-Wen}} = \begin{pmatrix} y+z & y+z & y+yz & 1+z \\ z+xz & 1+x & x+xz & 1+z \\ y+xy & 1+x & x+y & x+y \end{pmatrix}$$

Here we multiplied the rows of $\epsilon_{\text{Levin-Wen}}$ by suitable monomials to avoid negative exponents. One readily verifies that $\ker \epsilon_{\text{Levin-Wen}} = \text{im } \sigma_{\text{Levin-Wen}}$. The model is symmetric under the spatial rotation by $\pi/3$ about $(1, 1, 1)$ axis. Indeed, if one changes the variables as $x \mapsto y \mapsto z \mapsto x$ and apply a symplectic transformation

$$\omega = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} : \begin{cases} XI \mapsto YI \\ IX \mapsto IY \\ ZI \mapsto XI \\ IZ \mapsto IX \end{cases}, \quad (4.3)$$

then $\sigma_{\text{Levin-Wen}}$ remains the same up to permutations of columns.

The torsion submodule T of $C = \text{coker } \epsilon_{\text{Levin-Wen}}$, which describes the point-like charges according to Theorem 3.1, is

$$T = R \cdot \begin{pmatrix} 1+y \\ 1+x \\ 0 \end{pmatrix}. \quad (4.4)$$

In order to see this, first shift the variables $a = x+1, b = y+1, c = z+1$. Then, $\epsilon_{\text{Levin-Wen}}$ becomes

$$\epsilon_{\text{Levin-Wen}} = \begin{pmatrix} b+c & b+c & c+bc & c \\ a+ac & a & c+ac & c \\ a+ab & a & a+b & a+b \end{pmatrix} =: \phi$$

We will verify that $N = C/T$ is torsion-free. A presentation of $N = \text{coker } \phi'$ is obtained by joining

the generator of T to the matrix ϕ .

$$\phi' = \begin{pmatrix} b+c & b+c & c+bc & c & b \\ a+ac & a & c+ac & c & a \\ a+ab & a & a+b & a+b & 0 \end{pmatrix}$$

Column operations of ϕ' give

$$\phi' \cong \begin{pmatrix} 0 & c & b & 0 & 0 \\ c & 0 & a & 0 & 0 \\ b & a & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} \partial_2 & 0 & 0 \end{pmatrix}$$

where ∂_2 is from Eq. (4.2). Therefore, ϕ' generates the kernel of ∂_1 , and by Proposition 3.5.1, $N = \text{coker } \phi' = \text{coker } \partial_2$ is torsion-free.

The torsion submodule T of $C = \text{coker } \phi$ is annihilated by a , b , or c (See Corollary 4.3.3):

$$a \begin{pmatrix} b \\ a \\ 0 \end{pmatrix} = \phi \begin{pmatrix} 1 \\ 1+a \\ 0 \\ a \end{pmatrix}, \quad b \begin{pmatrix} b \\ a \\ 0 \end{pmatrix} = \phi \begin{pmatrix} 1 \\ 1+b \\ 1 \\ 1 \end{pmatrix}, \quad c \begin{pmatrix} b \\ a \\ 0 \end{pmatrix} = \phi \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}.$$

Therefore, T is isomorphic to $\text{coker } \partial_1 \cong \mathbb{F}_2$ of Eq. (4.2). The arguments h_x, h_y, h_z of ϕ can be thought of as *hopping* operators for the charge. According to [33], one can check that the charge is actually a fermion from the commutation values among, for example, $h_x, h_y, \bar{y}h_y$.

Consider a short exact sequence

$$0 \rightarrow T \rightarrow C \rightarrow N \rightarrow 0.$$

The corresponding sequence for 3D toric code splits, i.e., $C \cong T \oplus N$, while this does not. It implies that this model is not the same as the 3D toric code.

Now we can compute the ground-state degeneracy, or $\dim_{\mathbb{F}_2} K(L)$. Tensoring the boundary condition

$$B = R/\mathfrak{b}_L = R/(x^L - 1, y^L - 1, z^L - 1)$$

to the short exact sequence, we have a long exact sequence

$$\dots \rightarrow \text{Tor}_1(T, B) \xrightarrow{\delta'} \text{Tor}_1(C, B) \xrightarrow{\delta} \text{Tor}_1(N, B) \rightarrow T \otimes B \rightarrow C \otimes B \rightarrow N \otimes B \rightarrow 0.$$

Hence, $K(L) \cong \text{Tor}_1(C, B)$ has vector space dimension $\dim_{\mathbb{F}_2} \text{im } \delta + \dim_{\mathbb{F}_2} \text{ker } \delta$. Since the sequence

is exact, $\dim_{\mathbb{F}_2} \ker \delta = \dim_{\mathbb{F}_2} \text{im } \delta'$. As we have seen in Example 4.2,

$$\begin{aligned} \text{Tor}_1(T, B) &\cong \text{Tor}_1(R/\mathfrak{m}, B) \cong (\mathbb{F}_2)^3, \quad \text{and} \\ \text{Tor}_1(N, B) &\cong \text{Tor}_2(R/\mathfrak{m}, B) \cong (\mathbb{F}_2)^3. \end{aligned}$$

It follows that $\dim_{\mathbb{F}_2} K(L) \leq \dim_{\mathbb{F}_2} \text{Tor}_1(N, B) + \dim_{\mathbb{F}_2} \text{Tor}_1(T, B) = 6$.

It is routine to verify that $\mathfrak{b}_4 \subseteq I_2(\phi) \subseteq \mathfrak{m} := (x+1, y+1, z+1)$. Recall the decomposition $K(L) = \bigoplus_{\mathfrak{p}} K(L)_{\mathfrak{p}}$ where \mathfrak{p} runs over all maximal ideals of R/\mathfrak{b}_L . Due to Lemma 3.4.1, this decomposition consists of only one summand $K(L)_{\mathfrak{m}}$. When L is odd, since $(\mathfrak{b}_L)_{\mathfrak{m}} = \mathfrak{m}_{\mathfrak{m}}$, we know $K(L)_{\mathfrak{m}} = K(1)_{\mathfrak{m}}$. Since $\phi \mapsto 0$ under $a = b = c = 0$, we see $\dim_{\mathbb{F}_2} K(1) = 4$. The logical operators in this case are

$$\begin{pmatrix} 0 \\ 0 \\ \widehat{z} \\ \widehat{z} \end{pmatrix} \smile \widehat{x} \cdot \widehat{y\widehat{z}} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad ; \quad \begin{pmatrix} \widehat{x} \\ \widehat{x} \\ 0 \\ 0 \end{pmatrix} \smile \widehat{z} \cdot \widehat{xy} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

where $\widehat{\mu} = \sum_{n=0}^{L-1} \mu^n$ so $\mu \cdot \widehat{\mu} = \widehat{\mu}$, and symplectic pairs are tied. The left elements are string-like, and the right surface-like.

When L is even, the following are \mathbb{F}_2 -independent elements of $K(L)$. As there are 6 in total, the largest possible number, we conclude that $K(L)$ is 6-dimensional, i.e., the number of encoded qubits is 3 when linear dimensions are even.

$$\begin{pmatrix} 0 \\ 0 \\ \widehat{z} \\ \widehat{z} \end{pmatrix} \smile \widehat{x'\widehat{y'}} \begin{pmatrix} 1+y \\ x+xy \\ 0 \\ 1+x+y+xy \end{pmatrix} \quad ; \quad \begin{pmatrix} \widehat{x} \\ \widehat{x} \\ 0 \\ 0 \end{pmatrix} \smile \widehat{y'\widehat{z'}} \begin{pmatrix} 1+z \\ 1+z \\ 1+z \\ y+yz \end{pmatrix} \quad ; \quad \begin{pmatrix} \widehat{y} \\ \widehat{y} \\ \widehat{y} \\ \widehat{y} \end{pmatrix} \smile \widehat{z'\widehat{x'}} \begin{pmatrix} 0 \\ 1+x+z+xz \\ 1+x \\ 1+x \end{pmatrix}$$

where $\widehat{\mu}' = \sum_{i=0}^{L/2-1} \mu^{2i}$ so $(1+\mu)\widehat{\mu}' = \widehat{\mu}$. The pairs are transformed cyclically by $x \mapsto y \mapsto z \mapsto x$ together with the symplectic transformation ω of Eq. (4.3). \diamond

4.4 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. However, the geometry of the algebraic set seems to be crucial to prove, for example, “no-strings rule.” See Chapter 5.

It is interesting on its own to prove or disprove that the elementary symplectic transformations generate the whole symplectic transformation group. In the zero-dimensional case where Λ is the trivial group, it is true as we have already seen in Proposition 2.1. The one-dimensional case is also true because it is implied by the computation in the proof of Theorem 4.1. A classical problem answered affirmatively by Suslin [91] is that any sufficiently large invertible matrix over a polynomial ring is a finite product of elementary matrices such as row operations and scalar multiplications. Later, an algorithmic proof is given by Park and Woodburn [92]. A similar problem under a confusingly similar name ‘symplectic group’ over polynomial rings is solved by Grunewald *et al.* [93], who defined the ‘symplectic group’ as $\{S \in \text{Mat}(n, \mathbb{F}[x_1, \dots, x_n]) \mid S^T \lambda S = \lambda\}$ where T is the transpose. Kopeyko [94] generalized it to include Laurent polynomials, but still the ‘symplectic group’ is different from ours since the antipode map is absent from the definition

$$\{S \in \text{Mat}(n, \mathbb{F}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]) \mid S^T \lambda S = \lambda\}.$$

The characteristic dimension is not proven to be invariant under coarse-graining. It suffices to have an upper bound on $\dim_{\mathbb{F}_2} K(L)$ in Corollary 3.4.8. without the condition that $2 \nmid L$. A closely related object is the Hilbert function. Given a graded module $M = \bigoplus_{s=0}^{\infty} M_s$ over a polynomial ring with coefficients in a field \mathbb{F} , the Hilbert function f_M is a numerical function defined by $f_M(s) = \dim_{\mathbb{F}} M_s$. Since $K(L) = \dim_{\mathbb{F}_2} \text{Tor}_1(\text{coker } \epsilon, R/\mathfrak{b}_L)$, the Hilbert function might be useful if we could make $\text{coker } \epsilon$ graded. A technical difficulty would be that the ideal $\mathfrak{b}_L = (x_1^L - 1, \dots, x_D^L - 1)$ is not a power of $\mathfrak{m} = (x_1 - 1, \dots, x_D - 1)$. See [76, Chapter 12] and [95].

Lastly, an important problem is to give a criterion to a module M that can be realized as $\text{coker } \sigma^\dagger$ for an exact code Hamiltonian described by σ . In the two-dimensional case, we know the answer — $\text{ann } M = (x - 1, y - 1)$ by Theorem 4.2.

Chapter 5

Cubic code

The toric code [3] is usually defined on a planar graph with qubits residing on edges. The star operator and plaquette operators are defined according to the data of the graph. The model is thus a priori lattice dependent. However, a certain set of important properties of the model turns out to be lattice independent. Particularly the ground-state subspace conveys a structure that depends only on the topology of the underlying space, insensitive to the microscopic detail. If the underlying space is a genus g (oriented) surface, the degeneracy is 4^g . Even if the Hamiltonian is perturbed, the energy splitting of lowest 4^g states is exponentially small in the system size as long as the perturbation is small enough [5, 3, 6]. It is a signature of *topological order*.

Authors have used the term ‘topological quantum order’ to mean all or a part of the following properties: Ground-state degeneracy as a function of topology, no spontaneous symmetry breaking, anyonic particle content [24, 96, 97, 5, 26, 25], robust edge modes against perturbations [98, 99, 37], locally indistinguishable ground states [6, 75, 74], and topological entanglement entropy [27, 28]. Here, we take the local indistinguishability of ground states as a definition of topological quantum order. The local indistinguishability is precisely the one used in Chapter 3, as well as in the proof of gap stability results [75, 74]. See Lemma 3.3.1. We ask what quantum phases are possible in the class of code Hamiltonians.

An important example of topological quantum order presented in this thesis is *cubic code*. In this chapter we explain how the model is found, and study its consequences. The cubic code is an exact local additive code with translation symmetry on the simple cubic lattice, where the exactness is as in Chapter 3. This model is a gapped unfrustrated spin Hamiltonian, and is topologically ordered in the very sense we just defined, but breaks many aspects of conventional models of topological order. Most prominently, the excitations or charges of the cubic code *cannot* be interpreted as particles since they are immobile; the hopping term appears only after L -th or higher order perturbation theory, where L is the linear system size. The immobility implies that the system spends quite a long time to reach its thermal equilibrium in response to environment’s change. (Later, we will give quantitative statements regarding this.) Moreover, due to the topological quantum order, the

phase is stable with respect to arbitrary but small perturbations; the immobility of excitations is also protected [6].

The immobility of the charges translates into the theory of quantum error correcting codes as the absence of string logical operators. We call this property by *no-strings rule*. The notion of string logical operators might be intuitive if one imagines the toric codes in two or three dimensions [7]. However, this intuition is too model specific; the strings in discrete lattices are not well-defined objects since a set of points in the lattice does not in general have a well-defined dimensionality. We overcome this issue by defining *string segments* that capture characteristics that are responsible for the mobility of charges.

We proceed by translating conditions for the absence of the logical string segments into our algebraic framework, in order to systematically search for codes without logical strings; the cubic code is not an ad hoc model. By Corollary 4.3.3 [47], the characteristic dimension of the cubic code must be 1 and the degeneracy must generally grow with the system size. An explicit formula for the degeneracy is given. Additionally, a real-space renormalization computation is presented. It seems that the cubic code is a fixed point of a certain unconventional kind. Namely, the model is a direct sum of two daughter models A and B at a coarse-grained lattice where one daughter model A is the same as the original model, but the other B is not. The model B produces two copies of itself at a further coarse-grained lattice. The renormalization group flow continues to branch. Next, we compute the thermal partition function, and show that there is no finite temperature phase transition.

5.1 String segments and no-strings rule

The most important property of one-dimensional objects is that a finite part of it has two disjoint boundary points. An intuitive role of string operator is to move an excitation at its one boundary point to another boundary point. Essentially, it is a concatenation or juxtaposition of hopping operators. The hopping operator is, as a whole, a finitely supported operator. Therefore, if the hopping operator acts on the vacuum (ground state), the overall effect is to create a trivial or neutral charge, which consists of two spatially separated charges. When either of the two charges is neutral by itself, the hopping is meaningless because trivial charges can be annihilated locally and created anywhere arbitrarily; only the hopping of nontrivial charges is important. Now we can define string segments and their absence.

Definition 5.1. [50, 51] A **string segment** is a finitely supported Pauli operator that creates excitations contained in the union of two finite boxes of **width** w . The string segment is **nontrivial** if the charge contained in one of the boxes is nontrivial. The distance between the boxes is the **length** of the string segment. We say a model obeys **no-strings rule** if the length of any nontrivial

string segment of width w is bounded by αw for some constant $\alpha \geq 1$.

The no-strings rule may seem too strong than necessary; why do we need an upper bound by a *linear* function? It is rather a technicality that is necessary to prove a logarithmic energy barrier theorem in Section 6.1. However, our definition seems sharp yet broad enough to derive further results.

An immediate consequence of the no-strings rule in the case of a translation-invariant code Hamiltonian is that there are infinitely many charges. If there were only finitely many, then in the sequence of all translations of a charge c there would be an equivalent charge c' . It means $c - c'$ is neutral and therefore $c - c'$ is created by a finitely supported operator, which is a nontrivial string segment. This string segment can be juxtaposed many times to give arbitrarily long string segments with fixed width. This is a contradiction to the no-strings rule. Also, in view of Corollary 4.3.3 and Lemma 3.4.9, a translationally invariant three-dimensional exact code Hamiltonian that obeys the no-strings rule, must have a growing ground-state degeneracy with respect to the system size when defined on lattices with periodic boundary conditions.

5.2 Search for models

We wish to find an interesting class of models that are relatively handy to deal with. The following lemma shows such a family. Recall that for an exact code Hamiltonian, we have $\ker \sigma^\dagger \lambda = \text{im } \sigma$.

Lemma 5.2.1. *The generating matrix of a code Hamiltonian*

$$\sigma = \begin{pmatrix} f & 0 \\ g & 0 \\ 0 & g' \\ 0 & f' \end{pmatrix},$$

where $f, g, f', g' \in R$, elements of group algebra of \mathbb{Z}^D , is exact if and only if

$$\gcd(f, g) = 1, \quad g' = \bar{g}, \quad f' = -\bar{f}$$

up to units of R .

It is a generalization of σ in Remark 4.1. The 2D toric code of Example 3.2 falls into this form.

Proof. Observe that there is no mixing between the σ^x part (the upper two rows of σ) and the σ^z part (the lower two rows of σ). So $\ker \sigma^\dagger \lambda = \text{im } \sigma$ can be checked separately. That is, we need to verify whether the kernel of

$$\epsilon_z = \begin{pmatrix} \bar{f} & \bar{g} \end{pmatrix}$$

is generated by $\begin{pmatrix} g' \\ f' \end{pmatrix}$, and whether the kernel of

$$\epsilon_x = \begin{pmatrix} \bar{g}' & \bar{f}' \end{pmatrix}$$

is generated by $\begin{pmatrix} f \\ g \end{pmatrix}$. If $f = f_1 h$ and $g = g_1 h$ where $\gcd(f, g) = h$, then $\begin{pmatrix} \bar{g}_1 \\ -\bar{f}_1 \end{pmatrix} \in \ker \epsilon_z$. We have $\begin{pmatrix} \bar{g}_1 & -\bar{f}_1 \end{pmatrix} = r \begin{pmatrix} g' & f' \end{pmatrix}$ for some $r \in R$. Since $\gcd(g_1, f_1) = 1$, r must be a unit. Hence, we may set $g' = \bar{g}_1$ and $f' = -\bar{f}_1$. Then, $\begin{pmatrix} f_1 \\ g_1 \end{pmatrix} \in \ker \epsilon_x$, so h is a unit. The converse is straightforward. \square

We stay with the form of σ as in Lemma 5.2.1 for its simplicity. Now we consider the no-strings rule. The equivalence classes of topologically nontrivial charges is $\text{coker } \epsilon$ by Theorem 3.1, which decomposes as $\text{coker } \epsilon_z \oplus \text{coker } \epsilon_x$. Since the two summands are related by the antipode map, it suffices to consider $\text{coker } \epsilon_x \cong R/(f, g)$ only. A necessary condition for the no-strings rule is that any fractal generator should *not* consist of two terms. For Theorem 4.2, the minimal dimension we should be interested in is 3; $R = \mathbb{F}_2[x^{\pm 1}, y^{\pm 1}, z^{\pm 1}]$. Let $I = (f, g)$, the ideal of R generated by f and g . If, for example, f factorizes as $f = (1+x)f_1$ and $f_1 \notin I$, then $(1+x)$ is a string generator. So it is necessary that the Gröbner basis of the ideal (f, g) does not have any two-term factor such as $x+1$, $y+1$, or $z+1$. In order to have a degenerate code Hamiltonian (Corollary 3.4.2), we have to have a non-unit associated ideal. For simplicity, we demand that $x=y=z=1$ is a root of f and g so that the associated ideal is contained in a maximal ideal $(x+1, y+1, z+1)$.

We further assume that f and g have exponents 0 or 1 in each variable. Thus, f and g are linear combinations of $1, x, y, z, xy, yz, zx, xyz$ over \mathbb{F}_2 . Naively there are 2^{16} possibilities, but they are not all different. For example, three choices $(f(x, y, z), g(x, y, z))$, $(xf(\frac{1}{x}), y, z)$, $xg(\frac{1}{x}, y, z)$, and $(f(y, z, x), g(y, z, x))$ define the same models because they are related by the reflection about yz -plane or the $\pi/3$ rotation about $(1, 1, 1)$ -axis. Up to these symmetries of the unit cube, there are 392 pairs of f, g . An exhaustive search gives 10 models in Table 5.1 that satisfy all our requirements. The most symmetric model defined by

$$f = 1 + x + y + z, \quad g = 1 + xy + yz + zx$$

will be called **cubic code**.

	f	g
1	$1 + x + y + z$	$1 + xy + xz + yz$
2	$x + y + z + yz$	$1 + y + xy + z + xz + xyz$
3	$1 + x + y + z$	$1 + xz + yz + xyz$
4	$1 + x + z + yz$	$1 + y + xy + xz$
5	$1 + x + z + yz$	$y + z + xz + yz$
6	$1 + x + y + z$	$1 + y + xz + yz$
7	$1 + x + y + z$	$1 + z + yz + xyz$
8	$1 + x + z + yz$	$1 + y + xy + z + xz + yz$
9	$1 + x + y + z$	$xy + z + xz + yz$
10	$1 + x + z + yz$	$1 + y + xy + xz + yz + xyz$

Table 5.1: Complete list of cubic codes. Each pair of polynomials defines an exact degenerate code Hamiltonian according to Lemma 5.2.1. They potentially obey the no-strings rule. Especially, code 1 indeed obeys the no-strings rule as proven in Section 5.3. The table is exhaustive, up to symmetries of simple cubic lattice and local symplectic transformations, under the following criteria: (i) f and g have exponents 0 or 1 for each variable, (ii) any member of the Gröbner basis of the ideal (f, g) is not divided by any two-term factor, and (iii) f and g become zero when $x = y = z = 1$. In the main text, the *cubic code* refers specifically to the code 1 in the table. The numbering is consistent with a table in [50].

5.3 Cubic code

Written out explicitly, cubic code is the translation-invariant negative sum of two types of interaction terms as in Figure 5.1. There are two qubits per site, and the two-letter notation stands for tensor product of Pauli matrices. For example, $XI = \sigma^x \otimes I$, $ZZ = \sigma^z \otimes \sigma^z$, etc. The third cube specifies the coordinate system of the simple cubic lattice. The generating map for the stabilizer module is

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

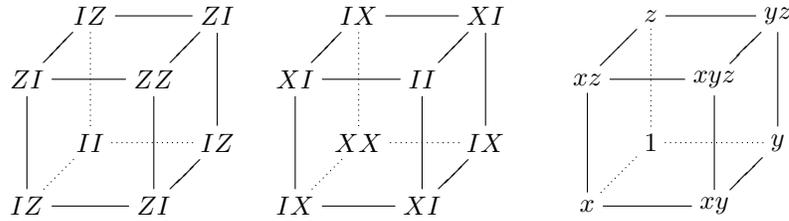


Figure 5.1: Stabilizer generators of the 3D cubic code. Here $X \equiv \sigma^x$ and $Z \equiv \sigma^z$ represent single-qubit Pauli operators, while I is the identity operator. Double-letter indices represent two-qubit Pauli operators, for example, $IZ \equiv I \otimes Z$, $ZZ \equiv Z \otimes Z$, $II \equiv I \otimes I$, etc.

where one has to interchange the first and second qubit. The associated ideal is contained in a prime ideal of codimension 2 in $\mathbb{F}_2[x^{\pm 1}, y^{\pm 1}, z^{\pm 1}]$:

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

Since $\text{codim } I(\sigma) \geq 2$, the characteristic dimension is 1. Since $\text{coker } \epsilon_{\text{cubic-code}} = R/\mathfrak{p}_{xyz} \oplus R/\overline{\mathfrak{p}_{xyz}}$, any nonzero element of \mathfrak{p}_{xyz} is a fractal generator. Since the conditions used in the search for the model were only necessary conditions for the no-strings rule. A rigorous treatments is as follows. We prove a purely algebraic statement, of which the no-strings rule is an interpretation. A more elementary method can be found in [50].

Lemma 5.3.1. *Let $S = \mathbb{F}_2[x, y, z]$ be a polynomial ring, and $\mathfrak{p} = (1+x+y+z, 1+xy+yz+zx) \subseteq S$ an ideal. If $m_1e_1 + m_2e_2 \in \mathfrak{p}$ for polynomials e_1, e_2 and monomials m_1, m_2 such that $\text{gcd}(m_1, m_2) = 1$, then only one of the following is true:*

- $e_1 \in \mathfrak{p}$ and $e_2 \in \mathfrak{p}$.
- $\max(\deg e_1, \deg e_2) \geq \max(\deg m_1, \deg m_2)$.

Proof. Put $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, i.e., ω is the primitive third root of unity over the binary field. Consider a ring homomorphism $\phi : S \rightarrow U := \mathbb{F}_4[t]$ defined by

$$\phi : x \mapsto 1 + t, \quad y \mapsto 1 + \omega t, \quad z \mapsto 1 + \omega^2 t.$$

It maps the two generators of \mathfrak{p} to zero in U .

$$\phi(1 + x + y + z) = 4 + (1 + \omega + \omega^2)t = 0,$$

$$\phi(1 + xy + yz + zx) = 4 + 2(1 + \omega + \omega^2)t + (1 + \omega + \omega^2)t^2 = 0.$$

Moreover, $\ker \phi$ is precisely \mathfrak{p} . (This can be verified by eliminating the variable x and computing the Gröbner basis of $((y+1)+\omega(z+1), \omega^2+\omega+1)$ in an elimination monomial order.) If $m_1e_1 + m_2e_2 \in \mathfrak{p}$, then $\phi(m_1)\phi(e_1) = \phi(m_2)\phi(e_2)$. Since m_1 and m_2 are co-prime monomials and $\phi(x), \phi(y), \phi(z)$ are pairwise co-prime, it follows that $\phi(m_1)$ and $\phi(m_2)$ are nonzero and co-prime. Therefore, $\phi(e_1) = 0$ if and only if $\phi(e_2) = 0$ if and only if $e_1, e_2 \in \mathfrak{p}$, which is the first case. If $\phi(e_1) \neq 0$, then $\phi(m_1)$ must divide $\phi(e_2)$ and $\phi(m_2)$ must divide $\phi(e_1)$. Since ϕ is degree-preserving, we have the second case. \square

Theorem 5.1. *The cubic code obeys the no-strings rule with the constant $\alpha = 1$ under ℓ_∞ -metric.*

Proof. Since the cubic code is translationally invariant, we may use the formalism of Chapter 3. Since the cubic code is of CSS type, where $\text{coker } \epsilon$ is a direct sum of isomorphic summands, we only

have to consider σ^x -type charges. The set of all virtual charges is $R^1 = R = \mathbb{F}_2[x^{\pm 1}, y^{\pm 1}, z^{\pm 1}]$ and the set of all trivial charges are given by a submodule (ideal) $\mathfrak{p}_{xyz} = (1 + x + y + z, 1 + xy + yz + zx) \subseteq R$. Note that R is the localization of $S = \mathbb{F}_2[x, y, z]$ by a single element xyz , and \mathfrak{p}_{xyz} is the localization of $\mathfrak{p} = (1 + x + y + z, 1 + xy + yz + zx)$ by the same single element xyz .

Let e_1 and e_2 be the charges contained in two boxes of a string segment. Since they are overall trivial, we have $e_1 + x^i y^j z^k e_2 \in \mathfrak{p}$ where $i, j, k \in \mathbb{Z}$. Equivalently, we may write $m_1 e_1 + m_2 e_2 \in \mathfrak{p}$ where e_1 and e_2 have nonnegative exponents, and m_1, m_2 are monomials such that each variable (x , y , or z) appears only in one of m_1 or m_2 . Since $\mathfrak{p}_{xyz} \cap S = \mathfrak{p}$, which can be verified using Gröbner basis techniques, we are in the situation of Lemma 5.3.1. The width of the string segment is the maximum of the degrees of e_1 and e_2 , and the ℓ_1 -distance between the boxes enclosing e_1 and e_2 is $\leq \max(\deg m_1, \deg m_2)$. If we use ℓ_∞ -distance, the constant α in the no-strings rule is 1. \square

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 3.4.5,

$$k = \dim_{\mathbb{F}_2} R/(\mathfrak{p}_{xyz} + \mathfrak{b}_L) \oplus R/(\overline{\mathfrak{p}_{xyz}} + \mathfrak{b}_L) = 2 \dim_{\mathbb{F}_2} R/(\mathfrak{p}_{xyz} + \mathfrak{b}_L),$$

where $\mathfrak{b}_L = (x^L - 1, y^L - 1, z^L - 1)$. 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 3.4.3, 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 $l_1 \leq l_2 \leq l_3$. 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 $x \rightarrow x + 1, y \rightarrow y + 1$, 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 $m \geq 0$. 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 $a \neq 0$, i.e., $x_0 \neq 1$, then $b \neq 0$ 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

$$V = \left\{ (x, y, z) \in \mathbb{F}^3 \left| \begin{array}{l} x + y + z + 1 = xy + xz + yz + 1 = 0 \\ x^{n'_1} - 1 = y^{n'_2} - 1 = z^{n'_3} - 1 = 0 \end{array} \right. \right\}$$

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 $l_1 \leq l_2 \leq l_3$ 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

$$d_1 = \deg_x \gcd \left((1 + x)^{n'_1} + 1, (1 + \omega x)^{n'_2} + 1, (1 + \omega^2 x)^{n'_3} + 1 \right).$$

Using $(\alpha + \beta)^{2^p} = \alpha^{2^p} + \beta^{2^p}$ and $\omega^2 + \omega + 1 = 0$, one can easily compute some special cases as summarized in the following corollary. Some values of k for small L are presented in Table 5.2 and Figure 5.2.

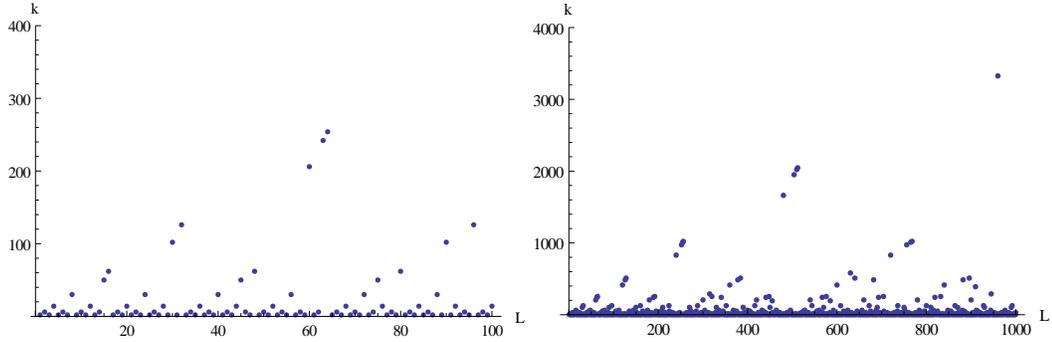


Figure 5.2: Number of encoded qubits k of the cubic code defined on $L \times L \times L$ periodic lattice

Corollary 5.3.2. *Let 2^k be the ground-state degeneracy of the cubic code on the cubic lattice of size L^3 with periodic boundary conditions. ($k = k(L)$ is the number of encoded qubits.) Then*

$$\begin{aligned} \frac{k+2}{4} &= \deg_x \gcd \left((1+x)^L + 1, (1+\omega x)^L + 1, (1+\omega^2 x)^L + 1 \right)_{\mathbb{F}_4} \\ &= \begin{cases} 1 & \text{if } L = 2^p + 1, \\ L & \text{if } L = 2^p, \\ L - 2 & \text{if } L = 4^p - 1, \\ 1 & \text{if } L = 2^{2p+1} - 1. \end{cases} \end{aligned}$$

where $\omega^2 + \omega + 1 = 0$ and $p \geq 1$ is any integer. If $L = 2^r L'$, then $k(L) + 2 = 2^r (k(L') + 2)$.

$(k+2)/4 = 1 + 12 \sum_n q_n(L)$ $q_n(L)$ is nonzero only if $n L$.			
$q_n(L)$	n		
1	15	$= 2^4 - 1$	$= 3 \cdot 5$
5	63	$= 2^6 - 1$	$= 3^2 \cdot 7$
20	255	$= 2^8 - 1$	$= 3 \cdot 5 \cdot 17$
80	1023	$= 2^{10} - 1$	$= 3 \cdot 11 \cdot 31$
322	4095	$= 2^{12} - 1$	$= 3^2 \cdot 5 \cdot 7 \cdot 13$
5	341	$= (2^{10} - 1)/(2^2 - 1)$	$= 11 \cdot 31$
6	1365	$= (2^{12} - 1)/(2^2 - 1)$	$= 3 \cdot 5 \cdot 7 \cdot 13$
49	5461	$= (2^{14} - 1)/(2^2 - 1)$	$= 43 \cdot 127$
4	455	$= (2^{12} - 1)/(2^3 + 1)$	$= 5 \cdot 7 \cdot 13$
3	585	$= (2^{12} - 1)/(2^3 - 1)$	$= 3^2 \cdot 5 \cdot 13$
9	9709	$= (2^{18} - 1)/(3(2^3 + 1))$	$= 7 \cdot 19 \cdot 73$
5	11275	$= 11(2^{10} + 1)$	$= 5^2 \cdot 11 \cdot 41$

Table 5.2: Numerical values of k for *odd* linear size L computed from Corollary 5.3.2. The list is complete if $2 \leq L \leq 20000$. For example, if $L = 945 = 15 \cdot 63$, then $\frac{k+2}{4} = 1 + 12 \cdot (1 + 5) = 73$.

5.4 Real-space renormalization of the cubic code

Renormalization group refers to a machinery to extract essential properties of the system at long distances. For lattice spin models, the so-called “block spin” method amounts to considering a sequence of coarse-grained lattices and finding effective Hamiltonians pertaining to the coarse-grained lattices [100, 101]. In the sequence of coarse-graining, short-ranged correlations will disappear, and long-ranged essential correlations will remain. Thus, if a generic Hamiltonian retains its form under the renormalization group flow, we expect that the Hamiltonian should represent a proper phase of matter, and can wonder about universal aspects of the phase.

For topologically ordered systems, it is interesting to look at entanglement structure instead of correlation functions, since, as they are gapped, the correlation functions of local operators would decay exponentially with the distance between the regions the operators act on [102], and hence, if they are renormalization group fixed points, they will have zero correlation length. As we wish to ignore local deformations of the system, it is legitimate to apply a finite depth quantum circuit (local unitary) to the system so as to remove some local entanglement [103, 104, 105, 106, 107]. More precisely, one applies a finite composition of unitary operators on a ground state, each of which can be written as a product of local unitary operators of disjoint supports, and then try to identify spins in a product state.

Code Hamiltonians admit an even simpler renormalization scheme. Under the local unitaries the Hamiltonian is conjugated, and spins in product states is readily identified by single-spin operators such as σ^z acting on unentangled spins. If we restrict ourselves to translationally invariant case, we may also assume that the local unitaries obey the translation invariance. For example, it is well-known that the 2D toric code model is a renormalization group fixed point under this scheme [105].

In Chapter 3, we have developed enough tools for the simplified renormalization group flow computation. In fact, we have done a computation in Example 4.1. To warm up, let us compute the renormalization of the 2D toric code. The generating matrix is

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

If we coarse-grain the lattice by blocking two sites in x -direction, then every module is now viewed as a module over $\mathbb{F}_2[x^{\pm 2}, y^{\pm 1}]$, and each entry of σ is replaced by a 2×2 matrix, since σ is a map between free modules G and P . Concretely,

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

where the double line distinguishes σ^x -part and σ^z -part. Here, the variable x really means the translation along x -direction by *two* units of the original lattice. Applying local unitaries, we see

$$\sigma' \rightarrow \left(\begin{array}{cccc|cccc} 1 & 1 & 0 & 0 & & & & \\ 0 & 1+x & 0 & 0 & & & & \\ 0 & 1+y & 0 & 0 & & & & \\ 0 & 1+y & 0 & 0 & & & & \\ \hline 0 & 0 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1+\frac{1}{y} & & & & \\ 0 & 0 & 1 & \frac{1}{x} & & & & \\ 0 & 0 & 1 & 1 & & & & \end{array} \right) \rightarrow \left(\begin{array}{cccc|cccc} 1 & 1 & 0 & 0 & & & & \\ 0 & 1+x & 0 & 0 & & & & \\ 0 & 1+y & 0 & 0 & & & & \\ 0 & 0 & 0 & 0 & & & & \\ \hline 0 & 0 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1+\frac{1}{y} & & & & \\ 0 & 0 & 0 & 1+\frac{1}{x} & & & & \\ 0 & 0 & 1 & 1 & & & & \end{array} \right) \rightarrow \left(\begin{array}{c|c|c|c} 1 & 0 & 0 & 0 \\ \hline 0 & 1+x & 0 & 0 \\ 0 & 1+y & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1+\frac{1}{y} \\ 0 & 0 & 0 & 1+\frac{1}{x} \\ \hline 0 & 0 & 1 & 0 \end{array} \right).$$

In the last matrix, it is evident that the first qubit (all the first qubits on every site) and the fourth qubit are disentangled. Ignoring those, we see that the generating matrix and also the Hamiltonian retain the original form. A drawback of this computation is that it is hard to understand why this should happen. Fortunately, there is a better understanding for two-dimensional quantum double

models [3], which includes the 2D toric code model, using so-called G -injective PEPS by Schuch, Cirac, and Pérez-García [108]. Their conclusion is that the quantum double model is constructed with the regular representation of a finite symmetry group G , and it is a renormalization group fixed point because of the plethysm $\mathbb{C}G \otimes \mathbb{C}G \cong \mathbb{C}G \otimes (\mathbb{C}1)^{\oplus|G|}$ of the regular representation.

Now we return to the cubic code. We perform a similar computation as above, and find that under blocking of $2 \times 2 \times 2$ sites (16 spins in total) the cubic code model A decomposes into two non-interacting Hamiltonians A and B living in the coarse-grained lattice, one of which is the same as the original A , but the other B looks different. Detailed calculation will be given below. The generating matrices are as follows.

$$\sigma_A = \begin{pmatrix} 1+x+y+z & 0 \\ 1+xy+yz+zx & 0 \\ 0 & 1+\frac{1}{xy}+\frac{1}{yz}+\frac{1}{zx} \\ 0 & 1+\frac{1}{x}+\frac{1}{y}+\frac{1}{z} \end{pmatrix}, \quad \sigma_B = \begin{pmatrix} x+z & 1+x \\ 1+x & 1+z \\ x+y & 1+y \\ 1+y & 1+x \\ \hline & 1+\frac{1}{y} & \frac{1}{x}+\frac{1}{y} \\ & 1+\frac{1}{x} & 1+\frac{1}{y} \\ & 1+\frac{1}{x} & \frac{1}{x}+\frac{1}{z} \\ & 1+\frac{1}{z} & 1+\frac{1}{x} \end{pmatrix}.$$

We can repeat the renormalization group flow computation for the model B only. We find that after blocking of $2 \times 2 \times 2$ sites, B is renormalized to the identical two copies of B itself. (Calculation will be given below.)

$$A \xrightarrow{2 \times 2 \times 2} A \oplus B, \quad \text{and} \quad B \xrightarrow{2 \times 2 \times 2} B \oplus B.$$

The renormalization group yields an explicit method to produce the ground states of the cubic code, Start with a state one wish to encode, put auxiliary qubits in the trivial state, apply the inverse local unitaries, and iterate the overall process on the *refined* lattice with more auxiliary qubits. It is slightly different from the MERA (Multiscale Entanglement Renormalization Ansatz) prescription of 2D toric code state developed in [105]. Rather a so-called branching MERA [109] is more appropriate.

We do not have a deeper understanding why this should happen. However, there are some consistency checks from the degeneracy formula and the annihilator of the module of topological charges. Corollary 5.3.2 says that the number of encoded qubits k is

$$\begin{aligned} k(L) = 4L - 2 &= \left(4\frac{L}{2} - 2\right) && + \left(4\frac{L}{2}\right) \\ &= \left(4\frac{L}{4} - 2\right) + \left(4\frac{L}{4}\right) && + \left(4\frac{L}{4}\right) + \left(4\frac{L}{4}\right) \end{aligned}$$

when the linear system size L is a power of 2. The expression is decomposed to display contributions from the model A and the model B explicitly. It suggests that the model A , the original cubic code, cannot give rise to an identical pair of models at coarse-grained lattice, whereas B can. It is not too clear whether the two models A and B are really non-isomorphic.

On the other hand, the annihilator of the topological charge module tells us there is something special about $2 \times 2 \times 2$ blocking. The topological charge module is the torsion part of the virtual excitation module factored by trivial charge module, i.e., the torsion submodule of $\text{coker } \epsilon$. As for the cubic code, $\text{coker } \epsilon$ is a torsion module, which is a direct sum of two isomorphic summands.

$$\begin{aligned}\text{coker } \epsilon &= R/\mathfrak{p}_{xyz} \oplus R/\overline{\mathfrak{p}_{xyz}}, \\ R &= \mathbb{F}_2[x^{\pm 1}, y^{\pm 1}, z^{\pm 1}], \\ \mathfrak{p}_{xyz} &= (1 + x + y + z, 1 + xy + yz + zx) \subset R.\end{aligned}$$

where the bar denotes antipode map. We focus on the first summand R/\mathfrak{p}_{xyz} . If we replace \mathbb{F}_2 with its algebraic closure \mathbb{F} for convenience, $R/\mathfrak{p}_{xyz} = (\mathbb{F}[x, y, z]/\mathfrak{p})_{xyz}$ is the coordinate ring of an affine variety defined by \mathfrak{p} localized on the complement of the union of three planes $xyz = 0$. The variety is a union of two isomorphic lines, as we have seen in the degeneracy calculation of Section 5.3. One line is parameterized as

$$x = 1 + t, \quad y = 1 + \omega t, \quad z = 1 + \omega^2 t$$

and the other is

$$x = 1 + t, \quad y = 1 + \omega^2 t, \quad z = 1 + \omega t$$

where ω is the primitive third root of unity. The ideal \mathfrak{p}_{xyz} is the annihilator of a module $M = R/\mathfrak{p}_{xyz}$. Under coarse-graining M is promoted to a module over the coarse-grained translation group algebra, which is $R' = \mathbb{F}_2[x^{\pm 2}, y^{\pm 2}, z^{\pm 2}]$ in our $2 \times 2 \times 2$ blocking. Then, the annihilator of M in the new ring R' is just $R' \cap I$. It is easy to verify that $R' \cap \mathfrak{p}_{xyz} = (1 + x^2 + y^2 + z^2, 1 + x^2 y^2 + y^2 z^2 + z^2 x^2) = \mathfrak{p}'$ using Gröbner basis. As rings, R'/\mathfrak{p}' and R/\mathfrak{p}_{xyz} are isomorphic. Thus, it is consistent that A renormalizes to something similar to itself. Further, we see that the charge annihilator of B must be the same as that of A .

This observation tells us that 2^3 blocking is special. If we had blocked 3^3 sites, we would not see the self-reproducing behavior, since the charge annihilator would be different:

$$\begin{aligned}\mathbb{F}_2[x^{\pm 3}, y^{\pm 3}, z^{\pm 3}] \cap \mathfrak{p}_{xyz} &= \left(1 + y' + y'^2 + y'^3 + z' + y'z' + y'^2 z' + z'^2 + y'z'^2 + z'^3, \right. \\ &\quad \left. 1 + x' + x'^2 + y' + x'y' + y'^2 + z' + x'z' + y'z' + z'^2 \right)\end{aligned}$$

where $x' = x^3, y' = y^3, z' = z^3$.

Calculation

The generating matrix σ_A for the stabilizer module of the cubic code transforms under the coarse-graining by blocking two sites along x -direction as

$$\sigma_A \xrightarrow{\text{coarse-grain } x^2 \rightarrow x} \sigma_1 = \begin{pmatrix} \sigma_{1X} & 0 \\ 0 & \sigma_{1Z} \end{pmatrix}$$

$$\sigma_{1X} = \begin{pmatrix} 1+y+z & 1 \\ x & 1+y+z \\ 1+yz & y+z \\ xy+xz & 1+yz \end{pmatrix}, \quad \sigma_{1Z} = \begin{pmatrix} 1 + \frac{1}{yz} & \frac{1}{xy} + \frac{1}{xz} \\ \frac{1}{y} + \frac{1}{z} & 1 + \frac{1}{yz} \\ 1 + \frac{1}{y} + \frac{1}{z} & \frac{1}{x} \\ 1 & 1 + \frac{1}{y} + \frac{1}{z} \end{pmatrix}.$$

We apply elementary symplectic transformations. Recall \dagger is the transpose followed by entry-wise antipode map $x \mapsto x^{-1}, y \mapsto y^{-1}, z \mapsto z^{-1}$.

$$\sigma_2 = \begin{pmatrix} \sigma_{2X} & 0 \\ 0 & \sigma_{2Z} \end{pmatrix} = \begin{pmatrix} r_1 & 0 \\ 0 & r_1^\dagger \end{pmatrix} \begin{pmatrix} \sigma_{1X} & 0 \\ 0 & \sigma_{1Z} \end{pmatrix} \begin{pmatrix} c_1 & 0 \\ 0 & c_1^\dagger \end{pmatrix}$$

where

$$\sigma_{2X} = \left(\begin{array}{ccc|c} 0 & & & 1 \\ \hline 1+x+y^2+z^2 & & & 0 \\ 1+y+y^2+z+yz+z^2 & & & 0 \\ \hline 0 & & & 0 \end{array} \right), \quad \sigma_{2Z} = \left(\begin{array}{c|ccc} 0 & & & 0 \\ \hline 0 & 1 + \frac{1}{y^2} + \frac{1}{y} + \frac{1}{z^2} + \frac{1}{z} + \frac{1}{yz} & & \\ 0 & 1 + \frac{1}{x} + \frac{1}{y^2} + \frac{1}{z^2} & & \\ \hline 1 & & & 0 \end{array} \right),$$

$$r_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1+y+z & 1 & 0 & 0 \\ y+z & 0 & 1 & 0 \\ 1+yz & y+z & 1+y+z & 1 \end{pmatrix}, \quad c_1 = \begin{pmatrix} 1 & 0 \\ 1+y+z & 1 \end{pmatrix}.$$

The first and fourth qubit may be factored out from σ_2 . A subsequent coarse-graining by blocking two sites in each y - and z -direction gives

$$\sigma_2 \xrightarrow{y^2 \rightarrow y, z^2 \rightarrow z} \sigma_3 = \begin{pmatrix} \sigma_{3X} & 0 \\ 0 & \sigma_{3Z} \end{pmatrix}$$

$$\sigma_{3X} = \begin{pmatrix} 1+x+y+z & 0 & 0 & 0 \\ 0 & 1+x+y+z & 0 & 0 \\ 0 & 0 & 1+x+y+z & 0 \\ 0 & 0 & 0 & 1+x+y+z \\ 1+y+z & 1 & 1 & 1 \\ z & 1+y+z & z & 1 \\ y & y & 1+y+z & 1 \\ yz & y & z & 1+y+z \end{pmatrix},$$

$$\sigma_{3Z} = \begin{pmatrix} 1 + \frac{1}{y} + \frac{1}{z} & \frac{1}{z} & \frac{1}{y} & \frac{1}{yz} \\ 1 & 1 + \frac{1}{y} + \frac{1}{z} & \frac{1}{y} & \frac{1}{y} \\ 1 & \frac{1}{z} & 1 + \frac{1}{y} + \frac{1}{z} & \frac{1}{z} \\ 1 & 1 & 1 & 1 + \frac{1}{y} + \frac{1}{z} \\ 1 + \frac{1}{x} + \frac{1}{y} + \frac{1}{z} & 0 & 0 & 0 \\ 0 & 1 + \frac{1}{x} + \frac{1}{y} + \frac{1}{z} & 0 & 0 \\ 0 & 0 & 1 + \frac{1}{x} + \frac{1}{y} + \frac{1}{z} & 0 \\ 0 & 0 & 0 & 1 + \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \end{pmatrix}$$

We keep applying elementary symplectic transformations.

$$\sigma_4 = \begin{pmatrix} \sigma_{4X} & 0 \\ 0 & \sigma_{4Z} \end{pmatrix} = \begin{pmatrix} r_{2X} & 0 \\ 0 & r_{2Z} \end{pmatrix} \begin{pmatrix} \sigma_{3X} & 0 \\ 0 & \sigma_{3Z} \end{pmatrix} \begin{pmatrix} c_{2X} & 0 \\ 0 & c_{2Z} \end{pmatrix}$$

where

$$\sigma_{4X} = \left(\begin{array}{c|c|cc} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1+x+y+z & 0 \\ 0 & 0 & 0 & 1+x+y+z \\ 1+x+y+z & 0 & 0 & 0 \\ x+xy+z+xz & 0 & 1+y & y+z \\ y+xy & 0 & 1+z & 1+y \\ xy+yz & 0 & y+z & 1+z \end{array} \right),$$

$$\sigma_{4Z} = \left(\begin{array}{c|ccc} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 1 + \frac{1}{y} & 1 + \frac{1}{z} & \frac{1}{y} + \frac{1}{z} \\ 0 & \frac{1}{y} + \frac{1}{z} & 1 + \frac{1}{y} & 1 + \frac{1}{z} \\ 0 & \frac{1}{x} + \frac{1}{xy} + \frac{1}{z} + \frac{1}{xz} & \frac{1}{y} + \frac{1}{xy} & \frac{1}{xy} + \frac{1}{yz} \\ 0 & 1 + \frac{1}{x} + \frac{1}{y} + \frac{1}{z} & 0 & 0 \\ 0 & 0 & 1 + \frac{1}{x} + \frac{1}{y} + \frac{1}{z} & 0 \\ 0 & 0 & 0 & 1 + \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \end{array} \right),$$

$$r_{2X} = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 + y + z & 1 & 1 & 1 & 1 + x + y + z & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 + y + z & 0 & 0 & 0 & 1 + y + z & 1 & 0 & 0 \\ y & 0 & 0 & 0 & y & 0 & 1 & 0 \\ y & 0 & 0 & 0 & y & 0 & 0 & 1 \end{array} \right),$$

$$r_{2Z} = \left(\begin{array}{cccc|cccc} 0 & 1 + \frac{1}{x} + \frac{1}{y} + \frac{1}{z} & 0 & 0 & 1 & 1 + \frac{1}{y} + \frac{1}{z} & \frac{1}{y} & \frac{1}{y} \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & \frac{1}{x} & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right).$$

$$c_{2X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ x & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad c_{2Z} = \begin{pmatrix} 1 & 1 + \frac{1}{y} + \frac{1}{z} & \frac{1}{y} & \frac{1}{y} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

Factoring out the first and second qubit from σ_4 and applying elementary symplectic transformations, we arrive at

$$\sigma_5 = \begin{pmatrix} \sigma_{5X} & 0 \\ 0 & \sigma_{5Z} \end{pmatrix} = \begin{pmatrix} r_{3X} & 0 \\ 0 & r_{3Z} \end{pmatrix} \left(\left(\begin{pmatrix} \sigma_{4X} & 0 \\ 0 & \sigma_{4Z} \end{pmatrix} \right) \Big|_{\{1,2\}^c} \right) \begin{pmatrix} c_{3X} & 0 \\ 0 & c_{3Z} \end{pmatrix}$$

where

$$\sigma_{5X} = \begin{pmatrix} 1+x+y+z & 0 & 0 \\ 1+xy+xz+yz & 0 & 0 \\ 0 & x+z & 1+x \\ 0 & 1+x & 1+z \\ 0 & x+y & 1+y \\ 0 & 1+y & 1+x \end{pmatrix}, \quad \sigma_{5Z} = \begin{pmatrix} 0 & 0 & 1 + \frac{1}{xy} + \frac{1}{xz} + \frac{1}{yz} \\ 0 & 0 & 1 + \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \\ 1 + \frac{1}{y} & \frac{1}{x} + \frac{1}{y} & 0 \\ 1 + \frac{1}{x} & 1 + \frac{1}{y} & 0 \\ 1 + \frac{1}{x} & \frac{1}{x} + \frac{1}{z} & 0 \\ 1 + \frac{1}{z} & 1 + \frac{1}{x} & 0 \end{pmatrix},$$

$$r_3 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & x & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1+x & 1 & 0 & 0 \end{pmatrix}, \quad r_{3Z} = \begin{pmatrix} 1 & \frac{1}{x} & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix},$$

$$c_3 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ x & 0 & 1 \end{pmatrix}, \quad c_{3Z} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

It is clear that σ_A , σ_1 , σ_2 , σ_3 , σ_4 , and σ_5 are all equivalent because we applied only elementary symplectic transformations. σ_5 shows a decomposition of σ into two non-interacting two models, one of which is σ_A at $2 \times 2 \times 2$ coarse-grained lattice and another is σ_B . We perform a similar

renormalization for σ_B . The coarse-graining by blocking two sites in x -direction gives

$$\sigma_B \xrightarrow{x^2 \rightarrow x} \sigma_{B1} = \begin{pmatrix} \sigma_{B1X} & 0 \\ 0 & \sigma_{B1Z} \end{pmatrix}$$

$$\sigma_{B1X} = \begin{pmatrix} z & 1 & 1 & 1 \\ x & z & x & 1 \\ 1 & 1 & 1+z & 0 \\ x & 1 & 0 & 1+z \\ y & 1 & 1+y & 0 \\ x & y & 0 & 1+y \\ 1+y & 0 & 1 & 1 \\ 0 & 1+y & x & 1 \end{pmatrix}, \quad \sigma_{B1Z} = \begin{pmatrix} 1 + \frac{1}{y} & 0 & \frac{1}{y} & \frac{1}{x} \\ 0 & 1 + \frac{1}{y} & 1 & \frac{1}{y} \\ 1 & \frac{1}{x} & 1 + \frac{1}{y} & 0 \\ 1 & 1 & 0 & 1 + \frac{1}{y} \\ 1 & \frac{1}{x} & \frac{1}{z} & \frac{1}{x} \\ 1 & 1 & 1 & \frac{1}{z} \\ 1 + \frac{1}{z} & 0 & 1 & \frac{1}{x} \\ 0 & 1 + \frac{1}{z} & 1 & 1 \end{pmatrix}.$$

Apply elementary symplectic transformations to factor out trivial qubits.

$$\sigma_{B2} = \begin{pmatrix} \sigma_{B2X} & 0 \\ 0 & \sigma_{B2Z} \end{pmatrix} = \begin{pmatrix} r_{4X} & 0 \\ 0 & r_{4Z} \end{pmatrix} \begin{pmatrix} \sigma_{B1X} & 0 \\ 0 & \sigma_{B1Z} \end{pmatrix} \begin{pmatrix} c_{4X} & 0 \\ 0 & c_{4Z} \end{pmatrix}$$

where

$$\sigma_{B2X} = \left(\begin{array}{c|ccc|c} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 1+y & y+z & 0 \\ 0 & 1+x+z+yz & y+z & 0 \\ 0 & 0 & x+y+z+yz & 0 \\ 0 & y+z & 1+x+y+yz & 0 \end{array} \right), \quad \sigma_{B2Z} = \left(\begin{array}{c|cc|cc} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 1 + \frac{1}{x} + \frac{1}{z} + \frac{1}{yz} & 0 & \frac{1}{y} + \frac{1}{z} \\ 0 & 1 + \frac{1}{y} & 0 & \frac{1}{y} + \frac{1}{z} \\ 0 & \frac{1}{y} + \frac{1}{z} & 0 & 1 + \frac{1}{x} + \frac{1}{y} + \frac{1}{yz} \\ 0 & 0 & 0 & \frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{yz} \end{array} \right),$$

$$\begin{aligned}
r_{4X} &= \begin{pmatrix} 1 & 0 & z & 0 & 0 & 0 & 0 & 0 \\ y & 1 & 1+y & 0 & z & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1+y & 0 & 1 & 1 & 1 & 1 & 1+z & 0 \\ 0 & 0 & y & 0 & 1 & 0 & 0 & 0 \\ 1+y & 0 & x+z+yz & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1+y & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & z & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, & r_{4Z} &= \begin{pmatrix} 1 & 1 & 0 & 1+\frac{1}{z} & 0 & 1+\frac{1}{y} & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{z} & \frac{1}{x} & 1 & \frac{1}{x} & \frac{1}{y} & \frac{1}{x} & 1+\frac{1}{y} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{z} & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1+\frac{1}{z} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1+\frac{1}{z} & 0 & 0 & 1 & 1 \end{pmatrix}, \\
c_{4X} &= \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1+z & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1+z & z & 1 \end{pmatrix}, & c_{4Z} &= \begin{pmatrix} 1 & 1 & 0 & \frac{1}{y} \\ 0 & 1 & 0 & 1 \\ 0 & 1+\frac{1}{y} & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix},
\end{aligned}$$

Factoring out trivial qubits from σ_{B2} and coarse-graining by blocking two sites along z -direction, we have

$$\sigma_{B2}|_{\{1,2,3,4\}^c} \xrightarrow{z^2 \rightarrow z} \sigma_{B3} = \begin{pmatrix} \sigma_{B3X} & 0 \\ 0 & \sigma_{B3Z} \end{pmatrix}, \text{ where}$$

$$\begin{aligned}
\sigma_{B3X} &= \begin{pmatrix} 1+y & 0 & y & 1 \\ 0 & 1+y & z & y \\ 1+x & 1+y & y & 1 \\ z+yz & 1+x & z & y \\ 0 & 0 & x+y & 1+y \\ 0 & 0 & z+yz & x+y \\ y & 1 & 1+x+y & y \\ z & y & yz & 1+x+y \end{pmatrix}, & \sigma_{B3Z} &= \begin{pmatrix} 1+\frac{1}{x} & \frac{1}{z}+\frac{1}{yz} & \frac{1}{y} & \frac{1}{z} \\ 1+\frac{1}{y} & 1+\frac{1}{x} & 1 & \frac{1}{y} \\ 1+\frac{1}{y} & 0 & \frac{1}{y} & \frac{1}{z} \\ 0 & 1+\frac{1}{y} & 1 & \frac{1}{y} \\ \frac{1}{y} & \frac{1}{z} & 1+\frac{1}{x}+\frac{1}{y} & \frac{1}{yz} \\ 1 & \frac{1}{y} & \frac{1}{y} & 1+\frac{1}{x}+\frac{1}{y} \\ 0 & 0 & \frac{1}{x}+\frac{1}{y} & \frac{1}{z}+\frac{1}{yz} \\ 0 & 0 & 1+\frac{1}{y} & \frac{1}{x}+\frac{1}{y} \end{pmatrix}.
\end{aligned}$$

Again apply elementary symplectic transformations.

$$\sigma_{B4} = \begin{pmatrix} \sigma_{B4X} & 0 \\ 0 & \sigma_{B4Z} \end{pmatrix} = \begin{pmatrix} r_{5X} & 0 \\ 0 & r_{5Z} \end{pmatrix} \begin{pmatrix} \sigma_{B3X} & 0 \\ 0 & \sigma_{B3Z} \end{pmatrix} \begin{pmatrix} c_{5X} & 0 \\ 0 & c_{5Z} \end{pmatrix}$$

where

$$\sigma_{B4X} = \left(\begin{array}{ccc|cc|ccc} 0 & & & 0 & 1 & & & 0 \\ \hline 1+x+y+xy^2+z+yz & & & 0 & 0 & & & xy+y^2+xy^2+yz \\ \hline 0 & & & 0 & 0 & & & 0 \\ \hline 1+x^2+xy+x^2y+z+y^2z & & & 0 & 0 & & & x^2y+z+yz+y^2z \\ x+y+xy+y^2 & & & 0 & 0 & & & 1+y+xy+y^2 \\ z+y^2z & & & 0 & 0 & & & x+y+yz+y^2z \\ \hline 0 & & & 1 & 0 & & & 0 \\ \hline y+xy+xy^2+y^2z & & & 0 & 0 & & & 1+x+y+y^2+xy^2+z+yz+y^2z \end{array} \right),$$

$$\sigma_{B4Z} = \left(\begin{array}{ccc|cc|ccc} 0 & 0 & & 0 & & & & 0 \\ \hline 1+\frac{1}{y^2} & 1+\frac{1}{x} & & 0 & & & & 1+\frac{1}{x}+\frac{1}{y}+\frac{1}{yz} \\ \hline 0 & 0 & & 1 & & & & 0 \\ \hline 1+\frac{1}{y} & 1+\frac{1}{y} & & 0 & & & & 1+\frac{1}{z} \\ 1+\frac{1}{x}+\frac{1}{xy} & \frac{1}{z} & & 0 & & & & \frac{1}{xz}+\frac{1}{yz} \\ \hline \frac{1}{y^2} & \frac{1}{y} & & 0 & & & & 1+\frac{1}{x}+\frac{1}{z}+\frac{1}{yz} \\ \hline 0 & 0 & & 0 & & & & 0 \\ \hline 1+\frac{1}{y^2} & 0 & & 0 & & & & \frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{yz} \end{array} \right),$$

$$r_{5X} = \left(\begin{array}{ccccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1+x+y+xy+z & 1 & 0 & 0 & 0 & 0 & 1+y & 0 & 0 \\ 1+x+y & y & 1 & 1 & 1+x & 1+y & x+y & 1+y & 0 \\ 1+x^2+yz & 0 & 0 & 1 & 0 & 0 & 1+x & 0 & 0 \\ x+y & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ z+yz & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ y+xy+z+yz & 0 & 0 & 0 & 0 & 0 & y & 1 & 0 \end{array} \right),$$

$$r_{5Z} = \left(\begin{array}{cccccccc} 1 & 1+\frac{1}{x}+\frac{1}{y}+\frac{1}{xy}+\frac{1}{z} & \frac{1}{xy} & 1+\frac{1}{x^2}+\frac{1}{yz} & \frac{1}{x}+\frac{1}{y} & \frac{1}{z}+\frac{1}{yz} & 0 & \frac{1}{y}+\frac{1}{xy}+\frac{1}{z}+\frac{1}{yz} \\ 0 & 1 & \frac{1}{y} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1+\frac{1}{x} & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1+\frac{1}{y} & 0 & 0 & 1 & 0 & 0 \\ 0 & 1+\frac{1}{y} & 1+\frac{1}{y} & 1+\frac{1}{x} & 0 & 0 & 1 & \frac{1}{y} \\ 0 & 0 & 1+\frac{1}{y} & 0 & 0 & 0 & 0 & 1 \end{array} \right),$$

$$c_{5X} = \begin{pmatrix} y & 0 & 1 & 1+y \\ 1+x+xy & 1 & 1+x & y+xy \\ 1+y & 0 & 1 & y \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad c_{5Z} = \begin{pmatrix} \frac{1}{y} & 0 & 1 & \frac{1}{z} \\ 0 & 1 & 0 & 1 \\ 1+\frac{1}{y} & 0 & 1 & \frac{1}{z} \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Factor out the first, third, and seventh qubits from σ_{B4} , and coarse-grain by blocking two sites along y -direction.

$$\sigma_{B4} \xrightarrow{y^2 \rightarrow y} \sigma_{B5} = \begin{pmatrix} \sigma_{B5X} & 0 \\ 0 & \sigma_{B5Z} \end{pmatrix}, \text{ where}$$

$$\sigma_{B5X} = \begin{pmatrix} 1+x+xy+z & 1+z & y+xy & x+z \\ y+yz & 1+x+xy+z & xy+yz & y+xy \\ 1+x^2+z+yz & x+x^2 & z+yz & x^2+z \\ xy+x^2y & 1+x^2+z+yz & x^2y+yz & z+yz \\ x+y & 1+x & 1+y & 1+x \\ y+xy & x+y & y+xy & 1+y \\ z+yz & 0 & x+yz & 1+z \\ 0 & z+yz & y+yz & x+yz \\ xy+yz & 1+x & (1+x+z)(1+y) & 1+z \\ y+xy & xy+yz & y+yz & (1+x+z)(1+y) \end{pmatrix},$$

$$\sigma_{B5Z} = \begin{pmatrix} 1+\frac{1}{y} & 0 & 1+\frac{1}{x} & 0 & 1+\frac{1}{x} & \frac{1}{y}+\frac{1}{yz} \\ 0 & 1+\frac{1}{y} & 0 & 1+\frac{1}{x} & 1+\frac{1}{z} & 1+\frac{1}{x} \\ 1 & \frac{1}{y} & 1 & \frac{1}{y} & 1+\frac{1}{z} & 0 \\ 1 & 1 & 1 & 1 & 0 & 1+\frac{1}{z} \\ 1+\frac{1}{x} & \frac{1}{xy} & \frac{1}{z} & 0 & \frac{1}{xz} & \frac{1}{yz} \\ \frac{1}{x} & 1+\frac{1}{x} & 0 & \frac{1}{z} & \frac{1}{z} & \frac{1}{xz} \\ \frac{1}{y} & 0 & 0 & \frac{1}{y} & 1+\frac{1}{x}+\frac{1}{z} & \frac{1}{yz} \\ 0 & \frac{1}{y} & 1 & 0 & \frac{1}{z} & 1+\frac{1}{x}+\frac{1}{z} \\ 1+\frac{1}{y} & 0 & 0 & 0 & \frac{1}{x}+\frac{1}{z} & \frac{1}{y}+\frac{1}{yz} \\ 0 & 1+\frac{1}{y} & 0 & 0 & 1+\frac{1}{z} & \frac{1}{x}+\frac{1}{z} \end{pmatrix}.$$

Apply elementary symplectic transformations to factor out two more qubits.

$$\sigma_{B6} = \begin{pmatrix} \sigma_{B6X} & 0 \\ 0 & \sigma_{B6Z} \end{pmatrix} = \begin{pmatrix} r_{6X} & 0 \\ 0 & r_{6Z} \end{pmatrix} \begin{pmatrix} \sigma_{B5X} & 0 \\ 0 & \sigma_{B5Z} \end{pmatrix} \begin{pmatrix} \text{id}_{4 \times 4} & 0 \\ 0 & c_{6Z} \end{pmatrix}$$

$$r_{6Z} = \begin{pmatrix} 1 & 0 & 1 + \frac{1}{y} & 0 & 0 & 0 & 0 & \frac{1}{x} + \frac{1}{y} & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 + \frac{1}{x} & 0 & 1 & 0 & 0 & 1 + \frac{1}{x} + \frac{1}{z} & 0 & 0 \\ 0 & 0 & \frac{1}{x} & 0 & 0 & 1 & 0 & \frac{1}{x} & 0 & 0 \\ 0 & 0 & \frac{1}{y} & 0 & 0 & 0 & 1 & \frac{1}{y} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 + \frac{1}{y} & 0 & 0 & 0 & 0 & 1 + \frac{1}{y} & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$c_{6Z} = \begin{pmatrix} 1 & 0 & 1 & \frac{1}{y} & 1 & 1 + \frac{1}{x} + \frac{1}{z} \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{y} & 1 & 0 & \frac{1}{z} & 1 + \frac{1}{x} + \frac{1}{z} \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The third and eighth qubits in σ_{B6} are trivial. We finally finish our lengthy transformation.

$$\sigma_{B7} = \begin{pmatrix} \sigma_{B7X} & 0 \\ 0 & \sigma_{B7Z} \end{pmatrix} = \begin{pmatrix} r_{7X} & 0 \\ 0 & r_{7Z} \end{pmatrix} \left(\left(\begin{pmatrix} \sigma_{B6X} & 0 \\ 0 & \sigma_{B6Z} \end{pmatrix} \Big|_{\{3,8\}^c} \right) \begin{pmatrix} c_{7X} & 0 \\ 0 & c_{7Z} \end{pmatrix} \right)$$

where

$$\sigma_{B7X} = \begin{pmatrix} x+z & 1+x & 0 & 0 \\ 1+x & 1+z & 0 & 0 \\ x+y & 1+y & 0 & 0 \\ 1+y & 1+x & 0 & 0 \\ 0 & 0 & x+z & 1+x \\ 0 & 0 & 1+x & 1+z \\ 0 & 0 & x+y & 1+y \\ 0 & 0 & 1+y & 1+x \end{pmatrix}, \quad \sigma_{B7Z} = \begin{pmatrix} 1 + \frac{1}{y} & \frac{1}{x} + \frac{1}{y} & 0 & 0 \\ 1 + \frac{1}{x} & 1 + \frac{1}{y} & 0 & 0 \\ 1 + \frac{1}{x} & \frac{1}{x} + \frac{1}{z} & 0 & 0 \\ 1 + \frac{1}{z} & 1 + \frac{1}{x} & 0 & 0 \\ 0 & 0 & 1 + \frac{1}{y} & \frac{1}{x} + \frac{1}{y} \\ 0 & 0 & 1 + \frac{1}{x} & 1 + \frac{1}{y} \\ 0 & 0 & 1 + \frac{1}{x} & \frac{1}{x} + \frac{1}{z} \\ 0 & 0 & 1 + \frac{1}{z} & 1 + \frac{1}{x} \end{pmatrix},$$

$$\begin{aligned}
r_{7X} &= \begin{pmatrix} 1+z & 1 & 0 & 0 & z & 0 & 0 & 1 \\ 1+x & 1 & 1 & x & 0 & 1 & 0 & 1 \\ 1+x+y & 0 & 1 & x & 1 & 1+y & y & 1 \\ 1+y & 1 & 1 & 0 & 1+x & y & y & 1 \\ 1+x & 1 & 1 & x+z & 0 & 0 & 0 & 1 \\ x & 1 & 1 & x+z & 0 & 1 & 1 & 1 \\ 1+x & 1 & 1 & 1+x+z & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \\
r_{7Z} &= \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & \frac{1}{x} & 0 & 1 & 0 & 1 & 0 \\ 1+\frac{1}{y} & 1 & 1+\frac{1}{x}+\frac{1}{xy} & 0 & 1+\frac{1}{y} & 1 & 1+\frac{1}{y} & \frac{1}{y} \\ 1+\frac{1}{x}+\frac{1}{y} & \frac{1}{x} & \frac{1}{x^2}+\frac{1}{x}+\frac{1}{xy}+\frac{1}{z} & 0 & \frac{1}{x}+\frac{1}{y} & 0 & \frac{1}{x}+\frac{1}{y} & 1+\frac{1}{y}+\frac{1}{z} \\ 1+\frac{1}{x} & \frac{1}{x} & \frac{1}{x^2}+\frac{1}{x}+\frac{1}{z} & 0 & \frac{1}{x} & 0 & 1+\frac{1}{x} & 1+\frac{1}{z} \\ 1+\frac{1}{z} & \frac{1}{z} & \frac{1}{xz} & 1 & \frac{1}{z} & \frac{1}{z} & 1 & 1+\frac{1}{z} \end{pmatrix}, \\
c_{7X} &= \begin{pmatrix} 1 & 0 & 0 & 1+z \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1+z \\ 1 & 1 & 0 & 1+z \end{pmatrix}, \quad c_{7Z} = \begin{pmatrix} \frac{1}{z} & 1+\frac{1}{z} & 1 & 0 \\ 1 & 1 & 0 & 0 \\ \frac{1}{y} & 1+\frac{1}{y} & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}.
\end{aligned}$$

We see that σ_{B7} is a direct sum of two copies of σ_B . This verifies the bifurcation:

$$A \xrightarrow{2 \times 2 \times 2} A \oplus B, \text{ and } B \xrightarrow{2 \times 2 \times 2} B \oplus B.$$

5.5 Thermal partition function of the cubic code

The only relevant property of the cubic code in relation to a thermal partition function is that the generating map σ for the stabilizer module is injective.

$$0 \rightarrow G \xrightarrow{\sigma} P$$

This property is shared with 1D Ising model (Example 3.1), 2D toric code (Example 3.2), and 3D Chamon model (Example 4.3). Slightly more generally, Lemma 4.2.1 says that for two-dimensional exact code Hamiltonians one can choose an injective generating map that gives rise to an equivalent Hamiltonian in the sense of Definition 3.2.

Let $H = -\sum_i P_i$ be the Hamiltonian of the cubic code on $L \times L \times L$ periodic lattice. We set the coupling constant to be 1 so that each term literally squares to the identity $P_i^2 = 1$. The thermal partition function is

$$\mathcal{Z} = \mathcal{Z}(\beta) = \text{Tr} \exp(-\beta H)$$

where β is an inverse temperature. Since H consists of commuting terms, the exponential function can be written as products.

$$\mathcal{Z} = \text{Tr} \prod_i (\cosh \beta + P_i \sinh \beta) = \cosh^M \beta \text{Tr} \prod_i (1 + x P_i)$$

where $M = tL^3$ is the number of terms in H and $x = \tanh \beta$. Since the trace of a Pauli operator that is not identity is zero, only the term in the expansion of the product that is proportional to the identity contributes to \mathcal{Z} . If there are $N = qL^3$ qubits in the system, the trace of the identity operator is 2^N .

$$\frac{\mathcal{Z}}{2^N \cosh^M \beta} = \sum_{\gamma \in \Gamma} x^{|\gamma|}$$

where γ runs over all possible collections of terms P_i of H that multiply to the identity. Γ contains the empty collection. Thus, Γ is in one-to-one correspondence with $\ker \sigma_L$. (It may be nonzero due to the periodic boundary conditions although σ was injective. See Section 3.4.) Therefore, the cardinality of Γ is precisely

$$|\Gamma| = 2^{\dim_{\mathbb{F}_2} \ker \sigma_L} = 2^k,$$

the ground-state degeneracy. The second equality is implied by Corollary 3.4.5.

We know from Corollary 5.3.2 that k is bounded by a linear function of L for the cubic code; $k = O(L)$. Therefore, the partition function is sandwiched as

$$|\log \mathcal{Z}(\beta) - L^3 \log(2^q \cosh^t \beta)| \leq k \log 2 = O(L).$$

Thus, the free energy per unit volume in the thermodynamic limit is just a smooth function $\log(2^q \cosh^t \beta)$ for all nonzero temperatures. This should contrast with three- or higher-dimensional toric code model where the free energy density has a singularity at a nonzero temperature [110].

The analyticity of the free energy does not directly invalidate a possibility of self-correction of encoded quantum information. The latter is rather a dynamical process, which may have little to do with the thermal equilibrium. In fact, it is quite subtle to analyze self-correcting power or to give a criterion on it, based on the thermal partition function. The existence or possibility of a good decoding process to extract the encoded quantum information would be a more appropriate way to address the question of self-correction. For instance, in the four-dimensional toric code model the thermal expectation value for any bare logical operator is zero. However, a special dressed logical

operator defined with respect to a decoding algorithm can have a non-vanishing expectation value in the thermodynamic limit [32]. For the cubic code, the analyticity of the partition function suggests that it does not allow such a nonzero thermal expectation value for logical operators. Nevertheless, we can show that the characteristic time scale of the expectation values of logical operators dressed by a decoding algorithm, is very large at low temperatures. This is the topic of the next chapters.

Chapter 6

Consequences of no-strings rule

The no-strings rule prohibits a nontrivial charge to travel a distance longer than a constant times its size. We repeat the rule.

Definition 5.1: A string segment is a finitely supported Pauli operator that creates excitations contained in the union of two finite boxes (anchor regions) of width w . The string segment is nontrivial if the charge contained in one of the boxes is nontrivial. The distance between the boxes is the length of the string segment. We say that a model obeys no-strings rule if the length of any nontrivial string segment of width w is bounded by αw for some constant $\alpha \geq 1$.

The cubic code is an extreme case where a point charge cannot move distance 1 (Theorem 5.1). It does not mean that isolation or diffusion of charges is impossible; Theorem 3.2 actually gives a local process for the isolation to happen in the translationally invariant case. The isolation process for a charge has to pay an energy penalty upper bounded by the logarithm of the distance from others.

In this chapter, we illustrate the energy landscape of the cubic code Hamiltonian in a view towards self-correcting quantum memory. We show that the separation or isolation of charges requires an energy barrier logarithmically high in the separation distance. This can be visualized as follows. Imagine all the energy eigenstates as points on an imaginary “land,” and introduce a metric on the land by the minimum number of local operations one has to apply in order to map one state to another. Consider a function on the land given by the energy of the energy eigenstate. Our logarithmic energy barrier means that the energy function, or “energy landscape,” has a macroscopic number of local minimums separated by macroscopic energy barriers. These minimums correspond to low-energy excited states in which the separation between defects is approximately the system size.

The energy landscape with the large number of the local minimums suggests a possibility of a spin glass phase at a sufficiently low temperature. Note that there is no quenched disorder in the Hamiltonian [111, 112], and the glassy feature, if present, would be protected “topologically” [6]. A spin glass phase can indeed be realized for some classical spin Hamiltonians with logarithmic energy

barriers such as the model discovered by Newman and Moore [48]. Interplay between the topological order and the spin glassiness has been studied recently by several authors [89, 113].

The logarithmic energy barrier is an optimal bound up to constants because of Theorem 3.2 and 4.3. An obvious difficulty in proving the lower bound on the energy barrier is that there are a huge number of paths to isolate a charge. Relying on scale-invariant nature of the no-strings rule, we introduce a technique which may be regarded as a renormalization group in the space of error paths.

Also, we attempt to estimate the length of the separation process: How many local operations do we need in order to isolate a charge? Put differently, how large is a quantum mechanical tunneling probability between two ground states in presence of local perturbations? Since the tunneling amplitude would be non-vanishing only for virtual process that is mediated by an operator acting on the ground space, the question translates into the theory of error correcting codes as to find the weight distribution of logical operators. We do not answer this question at a satisfactory level, but we find a superlinear lower bound on the code distance assuming the no-strings rule.

6.1 Logarithmic energy barrier

We consider a regular D -dimensional cubic lattice Λ with periodic boundary conditions and linear size L , that is, $\Lambda = \mathbb{Z}_L^D$. Each site $u \in \Lambda$ is populated by a finite number of qubits. The class of models we are going to discuss is that of code Hamiltonians

$$H = - \sum_{a=1}^M G_a, \quad (6.1)$$

where each term G_a is a multi-qubit Pauli operator (a tensor product of I, X, Y, Z with an overall ± 1 sign) and different terms commute with each other; $G_a G_b = G_b G_a$ and $G_a^2 = I$. We assume that each generator G_a acts nontrivially (by X, Y or Z) only on a set of qubits located at vertices of an elementary cube. It is allowed to have more than one generator per cube. Any short-range stabilizer Hamiltonian can be written in this form by performing a coarse-graining of the lattice. We continue to assume that H is frustration-free¹, The Hamiltonian may or may not be translation-invariant.

Consider any multi-qubit Pauli operator E . A state $\psi = E \psi_0$ is an excited eigenstate of H . Obviously, $G_a \psi = \pm \psi$ where the sign depends on whether G_a commutes (plus) or anticommutes (minus) with E . Any flipped generator ($G_a \psi = -\psi$) will be referred to as a **defect**. Different defects may occupy the same elementary cube. It should be emphasized that a *configuration of defects*, called a **syndrome**, in ψ is the same for all ground states ψ_0 . An eigenstate with m defects has energy $2m$ above the ground state. For brevity, we shall use the term **vacuum** for a ground state of H whenever its choice is not important. A Pauli operator E whose action on the vacuum

¹This is always the case for independent generators G_a . Since our goal is to obtain a lower bound on the energy barrier, we can assume that the generators are independent, although it does not play any role in our analysis.

creates no defects is either a stabilizer ($E \in \mathcal{G}$), or a **logical operator** ($E \notin \mathcal{G}$, but E commutes with \mathcal{G}). In the former case any ground state of H is invariant under E . In the latter case E maps some ground state of H to an orthogonal ground state.

A Hamiltonian is said to have topological order if it has a degenerate ground state and different ground states are locally indistinguishable. We shall need a slightly stronger version of this condition that involves properties of both ground and excited states. These properties depend on a length scale L_{tqo} that must be bounded as $L_{tqo} \geq L^\gamma$ for some constant $\gamma > 0$. (For code Hamiltonians, L_{tqo} corresponds to the code distance.) Most of stabilizer code Hamiltonians with topological order satisfy our conditions with $L_{tqo} \sim L$. Our first topological quantum order condition concerns ground states, which is a rephrasing of Definition 3.6:

Definition 6.1. TQO1 refers to the following condition: If a Pauli operator E creates no defects when applied to the vacuum and its support can be enclosed by a cube of linear size L_{tqo} then E is a stabilizer, $E \in \mathcal{G}$.

Our second TQO condition concerns excited states. A cluster of defects S will be called **neutral** if it can be created from the vacuum by a Pauli operator E whose support can be enclosed by a cube of linear size L_{tqo} without creating any other defects. Otherwise we say that S is a **charged** cluster. Given a region $A \subseteq \Lambda$ we shall use a notation $\mathcal{B}_r(A)$ for the r -neighborhood of A , that is, a set of all points that have distance at most r from A . Here and below we use ℓ_∞ -distance on \mathbb{Z}_L^D . We shall need the following condition saying that neutral clusters of defects can be created from the vacuum locally.²

Definition 6.2. TQO2 refers to the following condition: Let S be a neutral cluster of defects and $C_{min}(S)$ be the smallest cube that encloses S . Then S can be created from the vacuum by a Pauli operator supported on $\mathcal{B}_1(C_{min}(S))$.

Remark 6.1. A translationally invariant exact code Hamiltonian satisfies both of our topological order conditions. In particular, the cubic code satisfies the present TQO conditions. [∵ TQO1 is immediate from Lemma 3.3.1, and TQO2 follows from an argument similar to the proof of Lemma 3.3.1. Indeed, given a neutral cluster e of defects, we have an equation $e = \epsilon p$ for some p of the Pauli module. p is computed by the standard division algorithm applied to the columns of the excitation map ϵ . If e is centered at origin, then the degree of p does not exceed that of e , which implies the second TQO condition.]

Let us consider a process of building a cluster of defects S (syndrome) from the vacuum. It can be described by an **error path** — a finite sequence of local Pauli errors E_1, \dots, E_T such that $E = E_T \cdots E_2 E_1$ creates S from the vacuum. For simplicity, we assume that each local error E_t is

²If a lattice has a boundary, charged defects might be created locally on the boundary, as it is the case for the planar version of the toric code. This is the reason why we restrict ourselves to periodic boundary conditions.

a single-qubit Pauli operator σ^x , σ^y , or σ^z . Applying this sequence of errors to a ground state ψ_0 generates a sequence of states $\{\psi(t)\}_{t=0,\dots,T}$, where and $\psi(T) = E\psi_0$ is the excited state of defect configuration S . We will say that S has **energy barrier** ω if for any Pauli operator E that creates S from the vacuum and for any error path implementing E , at least one of the intermediate states has more than ω defects. Note that we do not impose any restriction on the length of the path T as long as it is finite. In particular, one and the same error may be repeated in the error path several times at different time steps. Similarly, we consider the energy barrier for a logical operator \bar{P} ; we say that a logical operator \bar{P} has **energy barrier** ω if for any error path implementing $\psi_0 \mapsto \bar{P}\psi_0$ at least one of the intermediate states $\psi(t)$ has more than ω defects.

For any integer $p \geq 0$, define a **level- p unit of length** $\xi(p)$ as³

$$\xi(p) = (10\alpha)^p, \quad p = 0, 1, \dots \quad (6.2)$$

Let S be any non-empty syndrome. Recall that each defect in S can be associated with some elementary cube of the lattice.

Definition 6.3. A syndrome S is said to be **sparse at level p** if the set of elementary cubes occupied by the defects in S can be partitioned into a disjoint union of clusters such that each cluster has diameter at most $\xi(p)$ and any pair of distinct clusters combined together has diameter larger than $\xi(p+1)$. Otherwise, S is **non-sparse at level p** .

For example, suppose all defects in S occupy the same elementary cube. Since an elementary cube has diameter 1, such a syndrome $S(t)$ is sparse at any level $p \geq 0$. If S occupies a pair of adjacent cubes, $S(t)$ is sparse at any level $p \geq 1$, but is non-sparse at level $p = 0$. Note that the partition of S into clusters required for level- p sparsity is unique whenever it exists. The non-sparsity provides a lower bound on the number of defects in a cluster as follows.

Lemma 6.1.1. *A non-empty syndrome S that is non-sparse at all levels $q = 0, \dots, p$ contains at least $p+2$ defects.*

Proof. Let $C_1^{(0)}, \dots, C_g^{(0)}$ be elementary cubes occupied by S . Obviously, S contains at least g defects. Since S is non-empty and non-sparse at level 0, we have $g \geq 2$ and there exists a pair of cubes $C_a^{(0)}, C_b^{(0)}$ such that the union $C_a^{(0)} \cup C_b^{(0)}$ has diameter at most $\xi(1)$. Combining the pair $C_a^{(0)}, C_b^{(0)}$ into a single cluster, we obtain a partition $S = C_1^{(1)} \cup \dots \cup C_{g-1}^{(1)}$ where each cluster $C_a^{(1)}$ has diameter at most $\xi(1)$. Since S is non-sparse at level 1, we have $g-1 \geq 2$, and there exists a pair of clusters $C_a^{(1)}, C_b^{(1)}$ such that the union $C_a^{(1)} \cup C_b^{(1)}$ has diameter at most $\xi(2)$. Combining the pair $C_a^{(1)}, C_b^{(1)}$ into a single cluster and proceeding in the same way we arrive at $g \geq p+2$. \square

³The choice of the constant 10 is somewhat arbitrary. We do not try to optimize constants in our proof.

A configuration of defects created by applying a Pauli operator E to the vacuum will be called a *syndrome caused by E* . The process of building up a logical operator \bar{P} by a sequence of local errors E_1, \dots, E_T can be described by a **syndrome history** $\{S(t)\}_{t=0, \dots, T}$. Here $S(t)$ is the syndrome caused by the product $E_t \cdots E_2 E_1$, a partial implementation of \bar{P} up to a step t . The following concerns the size of local errors

Lemma 6.1.2. *Let Q_j be Pauli operators causing a chain of transitions*

$$\text{vac} \xrightarrow{Q_1} S_1 \xrightarrow{Q_2} S_2 \xrightarrow{Q_3} \dots \xrightarrow{Q_r} S_r \xrightarrow{Q_{r+1}} \text{vac}.$$

Let P_j be some Pauli operator creating the syndrome S_j from the vacuum. Suppose the support of any operator P_j and any operator Q_j can be enclosed by n or less cubes of linear size R such that $4nR < L_{tq_0}$. Then, the product $\bar{Q} = Q_1 \cdots Q_r Q_{r+1}$ is a stabilizer.

Proof. Let ψ_0 be any ground state. Define a sequence of states

$$\begin{aligned} \psi(1) &= P_1 Q_1 \cdot \psi_0, \\ \psi(j+1) &= (P_j P_{j+1}) Q_{j+1} \cdot \psi(j) \quad \text{for } j = 1, \dots, r-1, \\ \psi(r+1) &= Q_{r+1} P_r \cdot \psi(r). \end{aligned}$$

Obviously,

$$\begin{aligned} \psi(j) &= \pm P_j \cdot (Q_1 \cdots Q_j) \cdot \psi_0 \quad \text{for } j = 1, \dots, r \\ \psi(r+1) &= \pm \bar{Q} \cdot \psi_0. \end{aligned}$$

It follows that all states $\psi(j)$ are ground states, and the transition from $\psi(j)$ to $\psi(j+1)$ can be caused by a Pauli operator

$$O_j = P_j P_{j+1} Q_{j+1}.$$

Let M_j be the support of O_j . By assumption, M_j can be enclosed by at most $3n$ cubes of linear size R . If M_j is a connected set, i.e., one can connect any pair of qubits from M_j by a path (u_1, \dots, u_l) such that the distance between u_a and u_{a+1} is 1, then M_j can be enclosed by a single cube of linear size at most $3nR$. That $3nR < L_{tq_0}$ implies O_j is a stabilizer by the topological order condition. Generally, M_j consists of several disconnected components M_j^α , such that the distance between any pair of distinct components is at least 2. The restriction of O_j on a connected component commutes with any stabilizer generator, and is supported in a box of linear size $3nR$, which is smaller than L_{tq_0} by assumption. Therefore, the restrictions are stabilizers, and their product O_j is also a stabilizer. In other words, $\psi(j+1) = \pm \psi(j)$ for all j . It means that $\bar{Q} \psi_0 = \pm \psi_0$ for any ground state ψ_0 . We

conclude that \overline{Q} is a stabilizer. \square

The no-strings rule says that an isolated charged defect belonging to some sparse syndrome cannot be moved further than distance α away by a sequence of local errors. Since the no-strings rule is scale invariant, it may be applied to a coarse-grained lattice to show that isolated charged clusters cannot be moved further than distance $\alpha\xi(p)$ away. In order to exploit the scale invariance, we define a **level- p syndrome history** as a subsequence of the original syndrome history $\{S(t)\}_{t=0,\dots,T}$ that includes only those syndromes $S(t)$ that are non-sparse at all levels $q = 0, \dots, p-1$. The level-0 syndrome history includes all syndromes $S(t)$, the level-1 syndrome history omits $S(t)$ that is sparse at level 0, and so on. When $S(t')$ and $S(t'')$ are a consecutive pair of level- p syndromes, we define a **level- p error** E connecting $S(t')$ and $S(t'')$ as the product of all single-qubit errors E_j that occurred between $S(t')$ and $S(t'')$. Level- p errors are represented by horizontal arrows on Fig. 6.1. Note that we do not have any bound on the number of single-qubit errors E_j in the interval between $S(t')$ and $S(t'')$. In the worst case, E could act nontrivially on every qubit in the system. A main technical lemma of this chapter below asserts, loosely speaking, that if a syndrome history does not have a deep enough non-sparse hierarchy, any error path is equivalent to one that is localized around the defects.

Lemma 6.1.3. *Let $S' = S(t')$ and $S'' = S(t'')$ be a consecutive pair of syndromes in the level- p syndrome history of a Hamiltonian obeying the no-strings rule. Let E be the product of all errors E_j that occurred between S' and S'' . Suppose that any $S(t)$ contains at most m defects. If*

$$16m\xi(p) < L_{tq_0},$$

then there exists an error \tilde{E} supported on $\mathcal{B}_{\xi(p)}(S' \cup S'')$ such that $E\tilde{E}$ is a stabilizer.

Proof. The proof is by induction in p . When $p = 0$, $E = E_j$ is a single-qubit error. If the qubit acted on by E does not belong to $\mathcal{B}_1(S' \cup S'')$, one must have $S' = S''$. It means that E is a single-qubit error with a trivial syndrome. The topological order condition implies that E is a stabilizer. Choosing $\tilde{E} = I$ proves the lemma for $p = 0$.

Suppose the assertion is true for some level $p \geq 0$. Let $S' = S(t')$ and $S'' = S(t'')$ be consecutive syndromes in the level- $(p+1)$ history. Consider first the trivial case when $S' = S(t')$ and $S'' = S(t'')$ are also consecutive syndromes in the level- p history. Then S' and S'' are connected by a single⁴ level- p error E which, by induction hypothesis, has support on $\mathcal{B}_{\xi(p)}(S' \cup S'')$ modulo stabilizers. The latter is contained in $\mathcal{B}_{\xi(p+1)}(S' \cup S'')$ which proves the induction step.

⁴The word ‘single’ does not necessarily mean a single blob of errors supported in a small ball; it just means a single arrow in the level- p history. For instance, suppose that a model permits neutral point defects. Two neutral defects separated by distance 1 is a non-sparse at level 0 and 1. If we annihilate one of them, put sparsely many neutral defects, and finally put a neutral defect adjacent to one of the defects, then the whole process is described by a consecutive pair in the level 1 history. The ‘single’ level-1 error in this case consists of many components.

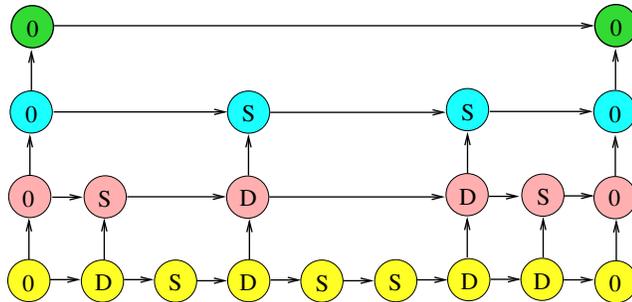


Figure 6.1: Renormalization group technique used to prove a logarithmic lower bound on the energy barrier for logical operators. Horizontal axis represents time. Vertical axis represents RG level $p = 0, 1, \dots, p_{max}$. A sequence of level-0 errors (single-qubit Pauli operators) implementing a logical operator \bar{P} defines a level-0 syndrome history (yellow circles) that consists of sparse (S) and non-sparse (D) syndromes. The history begins and ends with the vacuum (0). For any level $p \geq 1$ we define a level- p syndrome history by retaining only non-sparse syndromes at the lower level. A syndrome is called non-sparse at level p if it cannot be partitioned into clusters of size $\leq (10\alpha)^p$ separated by distance $\geq (10\alpha)^{p+1}$, where α is a constant coefficient from the no-strings rule. Each level- p error (horizontal arrows) connecting syndromes S', S'' is equivalent to the product of all level- $(p-1)$ errors between S', S'' modulo a stabilizer. We prove that these stabilizers can be chosen such that level- p errors act on $2^{O(p)}$ qubits. Since at the highest level $p = p_{max}$ a single level- p error is a logical operator, one must have $p_{max} = \Omega(\log L)$. We prove that level- p non-sparse syndromes contain $\Omega(p)$ defects which implies that at least one syndrome at level $p = p_{max} - 2$ consists of $\Omega(\log L)$ defects.

The nontrivial case is when there is at least one level- p syndrome between S' and S'' . The interval of the level- p syndrome history between S' and S'' can be represented (after properly redefining the time variable t) as

$$S' \xrightarrow{E_{lead}} S(1) \xrightarrow{E_1} S(2) \xrightarrow{E_2} \dots \xrightarrow{E_{\tau-1}} S(\tau) \xrightarrow{E_{tail}} S''.$$

Here all syndromes $S(1), \dots, S(\tau)$ are sparse at the level p and all transitions are caused by level- p errors. The sparsity implies that the set of elementary cubes occupied by $S(t)$ has a unique partition into a disjoint union of clusters $C_a(t)$ such that each cluster has diameter at most $\xi(p)$ and the distance between any pair, if any, of clusters is at least

$$\text{dist}(C_a(t), C_b(t)) \geq \xi(p+1) - 2\xi(p) \geq (10\alpha - 2)\xi(p) \geq 8\alpha\xi(p).$$

Represent any intermediate syndrome as a disjoint union

$$S(t) = S^c(t) \cup S^n(t), \quad t = 1, \dots, \tau, \quad (6.3)$$

where $S^c(t)$ and $S^n(t)$ include all charged and all neutral clusters $C_a(t)$, respectively. Let g be the number of clusters in $S^c(t)$. We claim that g does not depend on t . Indeed, since a level- p error E_t acts on $\xi(p)$ -neighborhood of $S(t) \cup S(t+1)$ by the induction hypothesis, the sparsity condition implies that E_t cannot create or annihilate a charged cluster $C_a(t)$ from the vacuum, or map a

charged cluster to a neutral cluster and vice versa. The same argument shows that each cluster $C_a(t) \subseteq S^c(t)$ can ‘move’ at most by $\xi(p)$ per time step, that is, we can parameterize

$$S^c(t) = C_1(t) \cup \dots \cup C_g(t)$$

such that a ‘world-line’ of the a -th charged cluster obeys the continuity condition

$$\text{dist}(C_a(t+1), C_a(t)) \leq \xi(p). \quad (6.4)$$

We can now use the no-strings rule to show that all charged clusters are ‘locked’ near their initial positions, so that their world-lines are essentially parallel to the time axis. More precisely, we claim that

$$\text{dist}(C_a(t), C_a(1)) \leq \alpha\xi(p) \quad \text{for all } 1 \leq t \leq \tau. \quad (6.5)$$

Indeed, suppose Eq. (6.5) is false for some a . Using the continuity Eq. (6.4), one can find a time step t_1 such that $\text{dist}(C_a(t_1), C_a(1)) > \alpha\xi(p)$ and $\text{dist}(C_a(t), C_a(1)) \leq \alpha\xi(p)$ for all $1 \leq t < t_1$. Let E_{close} be the product of all level- p errors E_j that occurred between $S(1)$ and $S(t_1)$ within distance $(2 + \alpha)\xi(p)$ from $C_a(1)$. Since all intermediate syndromes are sparse at level p , the net effect of E_{close} is to annihilate the charged cluster $C_a(1)$ and create the charged cluster $C_a(t_1)$. Equivalently, applying E_{close} to the vacuum creates a pair of charged clusters $C_a(1)$ and $C_a(t_1)$. However, this contradicts to the no-strings rule since $C_a(1)$ and $C_a(t_1)$ have linear size at most $\xi(p)$ while the distance between them is greater than $\alpha\xi(p)$. Thus we have proved Eq. (6.5).

We say that $\vec{x} \in \Lambda$ is *close to* S' if $\vec{x} \in \mathcal{B}_{\xi(p+1)}(S')$, and $\vec{x} \in \Lambda$ is *close to* S'' if $\vec{x} \in \mathcal{B}_{\xi(p+1)}(S'')$. Let E_t be the level- p error causing the transition from $S(t)$ to $S(t+1)$, where $t = 1, \dots, \tau - 1$. By induction hypothesis, we may assume that the support of E_t is in $\mathcal{B}_{\xi(p)}(S(t) \cup S(t+1))$. Let E_t^c be the restriction of E_t onto $\mathcal{B}_{\xi(p)}(S^c(t) \cup S^c(t+1))$, and E_t^n be the restriction of E_t onto $\mathcal{B}_{\xi(p)}(S^n(t) \cup S^n(t+1))$. The sparsity of $S(t)$ implies that

$$E_t = E_t^c \cdot E_t^n. \quad (6.6)$$

We claim that *any error* E_t^c *is close to* S' . Indeed, each cluster in $S^c(1)$ is within distance $2\xi(p)$ from S' since, otherwise, a single level- p error E_{lead} , supported in $\mathcal{B}_{\xi(p)}(S' \cup S(1))$ by induction hypothesis (modulo stabilizers), would be able to create a charged cluster from the vacuum. Using Eq. (6.5), we infer that $C_a(t) \subseteq \mathcal{B}_{(2+\alpha)\xi(p)}(S')$ for all $a = 1, \dots, g$. Therefore, E_t^c is close to S' .

We wish to find a ‘localized’ leading error \tilde{E}_{lead} that maps the syndrome S' to $S^c(1)$ such that the support of \tilde{E}_{lead} is close to S' . For each neutral cluster $C \in S^n(1)$ of diameter at most $\xi(p)$, let $O'(C)$ be a Pauli operator creating C from the vacuum. Because of our TQO2, we can choose

$O'(C)$ to be supported in $\mathcal{B}_1(C)$. Set

$$\tilde{E}_{\text{lead}} = E_{\text{lead}} \prod_{C \in S^n(1)} O'(C),$$

We have seen that $S^c(1)$ is within $(2 + \alpha)\xi(p)$ -neighborhood of S' . If E_{lead} has a disconnected component $E(C)$, isolated by distance $\xi(p)$ and centered at a neutral cluster C of $S^n(1)$, then $E(C)O'(C)$ is a stabilizer. Hence, \tilde{E}_{lead} is close to S' modulo stabilizers. If E_{lead} does not have such a component, \tilde{E}_{lead} is already close to S' . Certainly, \tilde{E}_{lead} maps S' to $S^c(1)$. We can apply the same rules to the error E_{tail} and the syndrome $S^n(\tau)$. We find a localized error

$$\tilde{E}_{\text{tail}} = E_{\text{tail}} \cdot \prod_{C \in S^n(\tau)} O''(C)$$

modulo stabilizers such that \tilde{E}_{tail} maps $S^c(\tau)$ to S'' and the support of \tilde{E}_{tail} is close to S'' . The operator $O''(C)$ above creates a neutral cluster $C \in S^n(\tau)$ from the vacuum.

We can now define a localized level- $(p + 1)$ error \tilde{E} whose support is close to $S' \cup S''$ as

$$\tilde{E} = \tilde{E}_{\text{tail}} \cdot E_{\tau-1}^c \cdots E_1^c \cdot \tilde{E}_{\text{lead}}. \quad (6.7)$$

By construction, it describes an error path

$$S' \xrightarrow{\tilde{E}_{\text{lead}}} S^c(1) \xrightarrow{E_1^c} S^c(2) \xrightarrow{E_2^c} \cdots \xrightarrow{E_{\tau-1}^c} S^c(\tau) \xrightarrow{\tilde{E}_{\text{tail}}} S''.$$

It remains to check that $E \cdot \tilde{E}$ is a stabilizer. Combining Eq. (6.6) and Eq. (6.7) we conclude that

$$E \cdot \tilde{E} = \pm(\tilde{E}_{\text{lead}}E_{\text{lead}}) \cdot E_1^n \cdots E_{\tau-1}^n \cdot (\tilde{E}_{\text{tail}}E_{\text{tail}}).$$

Applying $E \cdot \tilde{E}$ to the vacuum generates the following chain of transitions:

$$\text{vac} \xrightarrow{\tilde{E}_{\text{lead}}E_{\text{lead}}} S^n(1) \xrightarrow{E_1^n} S^n(2) \xrightarrow{E_2^n} \cdots \xrightarrow{E_{\tau-1}^n} S^n(\tau) \xrightarrow{\tilde{E}_{\text{tail}}E_{\text{tail}}} \text{vac} \quad (6.8)$$

Each syndrome $S^n(t)$ consists of at most m neutral clusters of diameter $\xi(p)$, i.e., it can be created from the vacuum by an error whose support can be enclosed by at most m cubes of linear size $2 + \xi(p)$, due to our TQO2. The first transition $\tilde{E}_{\text{lead}}E_{\text{lead}}$ or the last transition $\tilde{E}_{\text{tail}}E_{\text{tail}}$ is caused by errors whose support can be enclosed by at most m cubes of linear size $2 + \xi(p)$. All intermediate ones are supported on $\mathcal{B}_{\xi(p)}(S^n(t) \cup S^n(t + 1))$. Hence their support can be enclosed by at most $2m$ cubes of linear size $2 + \xi(p)$. Now the statement that $E \cdot \tilde{E}$ is a stabilizer follows from Lemma 6.1.2. \square

Now we state two theorems that apply to any stabilizer Hamiltonian Eq. (6.1) on a D -dimensional

lattice that obeys the topological order condition (TQO1,2) and the no-strings rule. The numerical constants for the Hamiltonian are $\alpha \geq 1$ in the no-strings rule and $1 \geq \gamma > 0$ in the bound $L_{tqo} \geq L^\gamma$ where L is the linear system size.

Theorem 6.1. *The energy barrier for any logical operator is at least $c \log L$ for some constant $c = c(\alpha, \gamma)$.*

Proof. Consider a syndrome history of an implementation of a logical operator E . We keep the initial and the final syndromes (the empty syndromes) at all levels; the syndrome history starts and ends with the vacuum at any level p . It suffices to treat the case where all intermediate syndromes $S(t)$ are non-empty. Let p_{max} be the highest RG level, that is, the smallest integer $p \geq 0$ such that a single level- p error E maps the vacuum to itself, see Fig. 6.1. Let m be the maximum number of defects in the syndrome history at any given moment.

Suppose that $16m\xi(p_{max}) < L_{tqo}$. Then Lemma 6.1.3 applied to the level- p_{max} syndrome history with $S' = S'' = \emptyset$ (vacuum), would imply $\tilde{E} = I$. Since E is not a stabilizer by assumption, we must have $16m\xi(p_{max}) \geq L_{tqo}$. Since the syndrome history must contain a syndrome $S(t)$ non-sparse at all levels $0, \dots, p_{max} - 2$, Lemma 6.1.1 implies $m \geq p_{max}$. And, TQO1 requires $L_{tqo} \geq L^\gamma$. Therefore, $16(10\alpha)^{2m} \geq 16m(10\alpha)^m \geq 16m(10\alpha)^{p_{max}} \geq L^\gamma$, and $m = \Omega(L)$. \square

Theorem 6.2. *Let S be a neutral cluster of defects containing a charged cluster $S' \subseteq S$ of diameter r such that there are no other defects within distance R from S' . If $r + R < L_{tqo}$, then the energy barrier for creating S from the vacuum is at least $c \log R$ for some constant $c = c(\alpha)$.*

Proof. Let S be a neutral cluster of defects and E be a Pauli operator creating S from the vacuum, with $S' \subset S$ of diameter r being charged. Consider a hierarchy of syndrome histories similar to the one shown on Fig. 6.1, where we now maintain the initial syndrome \emptyset and the final syndrome S for all levels. Let p_{max} be the highest RG level. Then a single level- p_{max} error E creates S from the vacuum. Since there must be a syndrome that is non-sparse for all levels $0, 1, \dots, p_{max} - 2$, Lemma 6.1.1 implies $m \geq p_{max}$ where m is the maximum number of defects in the syndrome history.

Suppose $16m\xi(p_{max}) < L_{tqo}$. Lemma 6.1.3 implies that E is the equivalent modulo stabilizers to \tilde{E} supported on $\mathcal{B}_{\xi(p_{max})}(S)$. If $\xi(p_{max}) < R/4$, then \tilde{E} must act on two separated regions, one near S' and another far from S' . This means that S' alone can be created by a Pauli operator whose support is enclosed by a cube of linear size $r + R/2$. Since $r + R < L_{tqo}$, it is contradictory to the assumption that S' is charged. Therefore, $\xi(p_{max}) \geq R/4$, and $m = \Omega(R)$. If $16m\xi(p_{max}) \geq L_{tqo}$, then, since $L_{tqo} > R$, we also have $m = \Omega(R)$. \square

6.2 Superlinear code distance

We have shown that in a process of isolating a charged cluster, there is a logarithmic energy barrier. The following theorem quantifies how long the process must be. The proof again makes use of renormalization group, and shows that there is a subset of ‘fractal dimension’ $\gamma > 1$ in the support of E , the operator that makes two separated clusters from the vacuum of which one is charged. We assume that E has weight minimum possible.

Let w be an odd positive number. We say a set of sites $C \subset \Lambda$ is a **level- p chunk** if $\text{diam}(C) < w^p$. A *path* in the lattice is a finite sequence of sites (u_1, u_2, \dots, u_n) such that $d(u_i, u_{i+1}) = 1$. (Recall that we use the l_∞ metric d .) Using paths, we can say whether a set is connected.

Definition 6.4. A connected level- p chunk $C \subseteq S$ is *maximal* with respect to a set of sites S if there exist a connected subset $C^\circ \subseteq C$ and a path $\zeta = (u_1, \dots, m, \dots, u_n) \subseteq C^\circ$ satisfying

$$(i) \quad d(u_1, u_n) = w^p - w^{p-1},$$

$$(ii) \quad d(u_1, m), d(u_n, m) \geq \frac{w^p - w^{p-1}}{2},$$

(iii) C° contains the connected component of m in $\mathcal{B}_{\frac{w^p - w^{p-1}}{2}}(m) \cap S$, and

(iv) C contains the connected component of C° in $\mathcal{B}_{\frac{w^{p-1}}{2}}(C^\circ) \cap S$.

The last two conditions restricts the position of ζ in C such that ζ lies sufficiently far from the boundary of C . The site m will be referred to as a **midpoint** of C . Let S be the support of the Pauli operator E , any restriction of which obeys the no-strings rule.

Lemma 6.2.1. *Given a path ζ in S joining u_1 and u_n such that $d(u_1, u_n) = lw^p - 1$, there are l disjoint maximal chunks of level p whose midpoints are on ζ .*

Proof. For convenience, we assume that the z -coordinates of u_1 and u_n are 0 and $lw^p - 1$, respectively. Consider $l+1$ planes P_i perpendicular to the z -axis, whose z -coordinates are iw^p for $i = 0, 1, \dots, l$. In each region between the two consecutive planes P_{i-1} and P_i , there is a subpath $\zeta_i = (u_{j_{i-1}}, \dots, u_{j_i})$ such that $d(u_{j_{i-1}}, u_{j_i}) = w^p - 1$. Choose $m_i \in \zeta_i$ such that $d(u_{j_{i-1}}, m_i), d(m_i, u_{j_i}) \geq \frac{w^p - 1}{2}$. Let C_i be the connected component of m_i within $S \cap \mathcal{B}_{\frac{w^p}{2}}(m_i)$. Add, if necessary, some points of ζ_i to C_i to get a maximally connected C'_i . This C'_i is a maximal chunk of sites with midpoint being m_i . Any two C'_i 's are disjoint since each of them lies in a unique region enclosed by P_{i-1} and P_i . \square

Lemma 6.2.2. *For sufficiently large w , a maximal level $(p+1)$ chunk C with respect to S admits a decomposition into $w+1$ or more maximal chunks of level p with respect to S .*

Proof. Recall that S is the support of the Pauli operator E , any restriction of which obeys no-strings rule. Define the *boundary* of a subset U of S to be $\partial U = \mathcal{B}_1(U) \cap U^c \cap S$. Then, any subset U of sites with boundary enclosed in a two disjoint regions can be regarded as a string segment.

By the definition of the maximal chunk, there exists a path $(u_1, \dots, m, \dots, u_n)$ in $C^\circ \subseteq C$ such that $d(u_1, u_n) = w^{p+1} - w^p$. We assume that the z -coordinates of u_1, u_n differ by $w^{p+1} - w^p$. We will show that there are sufficiently long and separated paths in C° , to which we apply Lemma 6.2.1 to find $w + 1$ maximal chunks of level p . They will lie in $\mathcal{B}_{\frac{w^p}{2}}(C^\circ)$, and hence in C .

Let M (N) be the subset of S consisted of sites whose z -coordinates differ from that of u_1 (u_n) by at most ηw^p . First, suppose ∂C° is not contained in $M \cup N$. Since $u_1 \in M$ and $u_n \in N$, there is a site $s \in C^\circ$ adjacent (of distance 1) to ∂C° such that $d(s, u_1), d(s, u_n) > \eta w^p$. Furthermore, $d(s, m) \geq \frac{w^{p+1} - w^p}{2} - 1$; otherwise, C° contains a site in the boundary, which is a contradiction.

Consider the shortest network \mathcal{N} of paths in C° connecting four sites u_1, m, u_n, s . (The length of a network of paths is the number of sites in the union of the paths.) Let ζ be the shortest path in \mathcal{N} from u_1 to u_n . If s is not contained in $\mathcal{B}_{3w^p}(\zeta)$, then $\zeta' \subseteq \mathcal{N}$ joining s to a site on ζ has a subpath $\zeta'' \subseteq \zeta'$ of diameter at least $2w^p$ such that ζ'' is separated from ζ by w^p . Applying Lemma 6.2.1 to ζ and ζ'' , we find at least $w + 1$ maximal chunk of level p . If m is not contained in $\mathcal{B}_{3w^p}(\zeta)$, a similar argument reveals at least $w + 1$ maximal chunk of level p .

Suppose both s and m are contained in $\mathcal{B}_{3w^p}(\zeta)$. Observe that $\zeta \setminus (\mathcal{B}_{4w^p}(s) \cup \mathcal{B}_{4w^p}(m))$ consists of three connected components $\zeta_1, \zeta_2, \zeta_3$, two of which have diameter $\geq \frac{w^{p+1} - w^p}{2} - 8w^p$ and the other has diameter $\geq (\eta - 4)w^p$. Two distinct $\mathcal{B}_{\frac{w^p}{2}}(\zeta_i)$ and $\mathcal{B}_{\frac{w^p}{2}}(\zeta_j)$ ($i, j = 1, 2, 3$) do not overlap because of the minimality of ζ . Applying Lemma 6.2.1, we find $w + \eta - 21$ maximal chunks of level p . Choosing $\eta > 21$, we get the desired result.

Next, suppose ∂C° is contained in $M \cup N$. Let $s_M, s_N \in C^\circ \setminus (M \cup N)$ be sites adjacent to M and N , respectively. The separation between M and N is $(w - 1 - 2\eta)w^p$. If it is greater than $\eta' \alpha w^p$, there must be a z -plane P that contains s_M or s_N such that $P \cap C^\circ$ has diameter $> \eta' w^p$; Otherwise, the no-strings rule is violated. Let $v_1, v_2 \in P \cap C^\circ$ be sites separated by $\eta' w^p$. The four sites, u_1, u_n, v_1, v_2 are sufficiently separated and connected by some paths in C° . Arguing as before, we find $(w - 1) + \eta' - 16$ maximal chunks of level p . The choice of $\eta' > 17$ and $w > 1 + 2\eta + \eta' \alpha$ proves the lemma. \square

Theorem 6.3. *Let E be a Pauli operator creating S , a neutral cluster of defects containing a charged cluster $S' \subseteq S$ of diameter r such that there are no other defects within distance R from S' . If $r + 2R < L_{tqo}$, then the weight of E must be $\geq cR^\gamma$ for some constant $\gamma > 1$ and c .*

Proof. The support of the minimal Pauli operator E in Theorem 6.3 must admit a path connecting S' and $S \setminus S'$. Otherwise, S' can be regarded as being created locally, and our topological order condition demands the cluster be neutral. Since the path has length $\geq R$, Lemma 6.2.1 says we have a maximal chunk of level p where p is such that $w^p \leq R < w^{p+1}$. Lemma 6.2.2 implies any maximal chunk of level p must contain at least $(w + 1)^p$ sites. This concludes the proof with $\gamma = \frac{\log(w+1)}{\log w} > 1$. \square

A similar argument proves the lower bound $d = \Omega(L^\gamma)$ on the code distance d of the cubic code since the minimal logical operator must contain a path of length L .

Chapter 7

Renormalization group decoder and error threshold theorem

Any error correcting scheme would be comprised of a chosen code space, an encoding procedure, and a decoding procedure. We have studied a way to choose a code space via additive/stabilizer code formalism. Our focus has been the situation where the code space is realized as a ground space of a local Hamiltonian. The encoding is a process in which one prepares a state that is to be transferred or stored, and then one embeds the state into the designed code space. For a concatenated code the encoding would be hierarchical resembling the very way the code is constructed. Interestingly, a ground state of toric code model can also be prepared in a similarly hierarchical way [105]. In case of the cubic code, for example, the encoding can be done by inverting the real-space renormalization group procedure presented in Section 5.4.

The decoder of a quantum code restores a damaged state into the code space. In contrast to its name, the decoder should not reveal any information that is encoded. Rather, it prepares the state appropriate for next information processing step which assumes that the state is in the code space; it detects errors and suggests an operator that would undo the errors. The performance of the decoder is measured by how closely the damaged state is restored to the original encoded state. In this chapter, we explain a decoding algorithm, called *renormalization group decoder*, that is applicable for a family of topological codes including the cubic code. A very similar idea appears in Harrington's thesis [114]. A decoder for 2D toric code with a similar name was proposed by Duclos-Cianci and Poulin [115]. The two decoders are conceptually similar, and the running times are the same up to a multiplicative constant. Our decoder is however advantageous for its simplicity and applicability. In particular, our decoder is the only decoder so far that has a positive error threshold under stochastic error when used with the cubic code. In fact, our decoder provides a universal positive error threshold for all topological codes in a given number of spatial dimensions, as we prove in Section 7.5.

Formally, if we restrict ourselves to local additive codes, the decoder is an association of a Pauli

operator P to any possible syndrome S such that the Pauli operator P transforms S to the empty syndrome. Recall that the syndrome measurement reveals locations of defects (flipped stabilizer generators) created by an unknown error. The renormalization group (RG) decoder attempts to annihilate the defects comprising the syndrome S by dividing them into disjoint connected clusters $S = C_1 \cup \dots \cup C_m$ and then trying to annihilate each cluster C_a individually. More specifically, the decoder checks whether C_a can be annihilated by a Pauli operator P_a supported on a sufficiently small spatial region $b(C_a)$ enclosing C_a . If such a local annihilation operator P_a exists, the decoder updates the syndrome by erasing all the defects comprising C_a , records the operator P_a , and moves on to the next cluster. If C_a cannot be annihilated, the decoder skips it. The annihilation operator P_a is not unique. However, if the enclosing region $b(C_a)$ is small enough to ensure that no logical operator can be supported on $b(C_a)$, all annihilation operators P_a must be equivalent modulo stabilizers and the choice of P_a does not matter.

After all clusters C_a have been examined, the decoder is left with a new configuration of defects S' , which is typically smaller than the original one. If no defects are left, i.e., $S' = \emptyset$, the decoder stops and returns the product of all recorded Pauli operators P_a . If $S' \neq \emptyset$, the decoder applies a scale transformation increasing the unit of length by some constant factor and repeats all the above steps starting from the syndrome S' . The scale transformation potentially merges several unerased clusters C_a into a single connected cluster whereby giving the decoder one more attempt to annihilate them.

The full decoding algorithm is the iteration of partitioning the defects into the connected clusters and calculating the annihilation operators. It declares failure and aborts if the recorded operator cannot annihilate all the defects before the rescaled unit length is comparable to the lattice size.

A detailed implementation of the RG decoder must be tailored to a specific lattice geometry and a stabilizer code under consideration. It must include a precise definition of the connected clusters of defects C_a and the enclosing regions $b(C_a)$. It must also include an algorithm for choosing the annihilation operators P_a , a schedule for increasing the unit of length, and clearly stated conditions under which the decoder aborts. In the rest of this chapter we describe an efficient implementation of the RG decoder for arbitrary stabilizer codes satisfying topological order conditions defined in the previous chapter. The only part of this implementation specialized for the 3D cubic code is the “broom algorithm” of Section 7.4. As we have noted in Remark 6.1, the our topological order conditions are satisfied by every translationally invariant exact code. It turns out that the broom algorithm is also applicable for every translationally invariant code.

7.1 Assumptions and conventions

Let Λ be the regular 3D cubic lattice of linear size L with periodic boundary conditions along all coordinates x, y, z . We shall label sites of Λ by triples of integers (i, j, k) defined modulo L and measure the distance between sites using the ℓ_∞ -metric. In other words, the distance $d(u, v)$ between a pair of sites u and v is the smallest integer r such that u and v can be enclosed by a cubic box with dimensions $r \times r \times r$. For example, $d(u, v) = 1$ whenever u and v belong to the same edge, plaquette, or elementary cube of the lattice. Each site of Λ represents one or several physical qubits (two qubits for the 3D Cubic Code). Each elementary cube c represents a spatial location of one or several stabilizer generators. For example, there are two generators for the 3D Cubic Code. A generator located at cube c may act only on qubits located at vertices of c . We shall label each elementary cube by coordinates of its center, the triple of half-integers (i, j, k) defined modulo L . The distance $d(c, c')$ between a pair of cubes c and c' is the distance between their centers. For example, $d(c, c') = 1$ whenever c and c' share a vertex, an edge, or a plaquette.

A **defect** is a stabilizer generator whose eigenvalue has been flipped as a result of the error. We shall use a term **cluster of defects**, or simply **cluster** for any set of defects. Define the *diameter* of a cluster $d(C)$ as the maximum distance $d(c, c')$ where $c, c' \in C$. Here and below the distance between defects is defined as the distance between the cubes occupied by these defects. Given two non-empty clusters C and C' , define a distance $d(C, C')$ as the minimum distance $d(c, c')$ where $c \in C$ and $c' \in C'$. Given an integer r , we shall say that a cluster C is **connected at scale r** , or simply **r -connected**, if C cannot be partitioned into two proper subsets $C = C' \cup C''$ such that $d(C', C'') > r$. A maximal r -connected subset of a cluster C is called a **r -connected component** of C . The **minimal enclosing box** $b(C)$ of a cluster C is the smallest rectangular box B enclosing all defects of C such that all vertices of B are dual sites of Λ . Note that the minimal enclosing box $b(C)$ is unique as long as $d(C) < L/2$; if a cluster C has diameter $L/2$, one may have two boxes with the same dimensions enclosing C that ‘wrap’ around the lattice in two different ways.

Let \mathcal{G} be the abelian group generated by the stabilizer generators. Elements of \mathcal{G} are called stabilizers. Let $S(P)$ be the **syndrome** of a Pauli operator P , that is, the set of all stabilizer generators anticommuting with P . The syndrome can be viewed as a cluster of defects.

We assume that our topological code obeys TQO1 and TQO2 of Definitions 6.1, 6.2 throughout the chapter, but not the no-strings rule of Definition 5.1.

The 3D cubic code satisfies both of TQO1 and TQO2 with $L_{tqo} = \frac{1}{2}L$, since it is exact. In order to avoid unnecessary complications due to boundaries, we always assume that $L_{tqo} \leq \frac{1}{2}L$. Below we consider only topological stabilizer codes. Continued from the previous chapter, a cluster of defects C is called **neutral** if it can be created from the vacuum by a Pauli operator P supported on a cube of linear size L_{tqo} . Otherwise, the cluster is said to be **charged**. For example, the 2D toric code [3]

has two types of defects: magnetic charges (flipped plaquette operators) and electric charges (flipped star operators). In this case, a cluster of defects C is neutral if and only if C contains even number of magnetic charges and even number of electric charges. It follows from TQO2 that any neutral cluster of defects C can be annihilated by a Pauli operator supported on the 1-neighborhood of the minimum enclosing box $b(C)$.

7.2 Renormalization group decoder

We are now ready to define our RG decoder precisely. Recall that $d(C)$ is the diameter of a cluster C , and $L_{tqo} \leq \frac{1}{2}L$ by convention.

TestNeutral

Input S : a set of defects, **Output** P : a Pauli operator.

1. Compute the minimal enclosing box B of S .
2. **if** $d(B) > L_{tqo}$, **then return** I .
3. Try to compute a Pauli P supported on the 1-neighborhood of B such that $S(P) = S$.
4. **if** a consistent P is found **then return** P **else return** I .

TQO2 implies that TestNeutral successfully computes the correcting Pauli operator for any neutral cluster. Step 1 is easy as we discuss in the end of Section 7.3. The specification of Step 3 depends on the code, but it always has an efficient implementation using the standard stabilizer formalism [116]. In general, the condition $S(P) = S$ can be described by a system of $O(V)$ linear equations over $O(V)$ binary variables parameterizing P , where V is the volume of B . The running time is then $O(V^3)$ by the Gauss elimination. In the special case of the 3D cubic code or more generally all translationally invariant codes, there is a much more efficient algorithm running in time $O(V)$ which we describe in Section 7.4.

Let p_M be the largest integer such that $2^{p_M} < L_{tqo}$. For any integer $0 \leq p \leq p_M$, we define the **level- p error correction**:

EC(p)

Input S : a syndrome, **Output** P : a Pauli operator.

1. Partition S into 2^p -connected components: $S = C_1 \cup \dots \cup C_m$.
2. For each component, compute $P_a = \text{TestNeutral}(C_a)$.
3. **return** the product $P_1 P_2 \dots P_m$.

The overall running time of EC(p) is polynomial in the number of qubits N . Step 1 can be done, for example, by examining the distance between all pairs of defects, forming a graph whose edges connect pairs of defects separated by distance $\leq 2^p$, and finding connected components of this graph. A more efficient algorithm with the running time $O(N)$ is described in Section 7.3. Since $V = O(N)$ and $m = O(N)$, we see that the worst-case running time of EC(p) is $O(N^2)$. For instance, one can

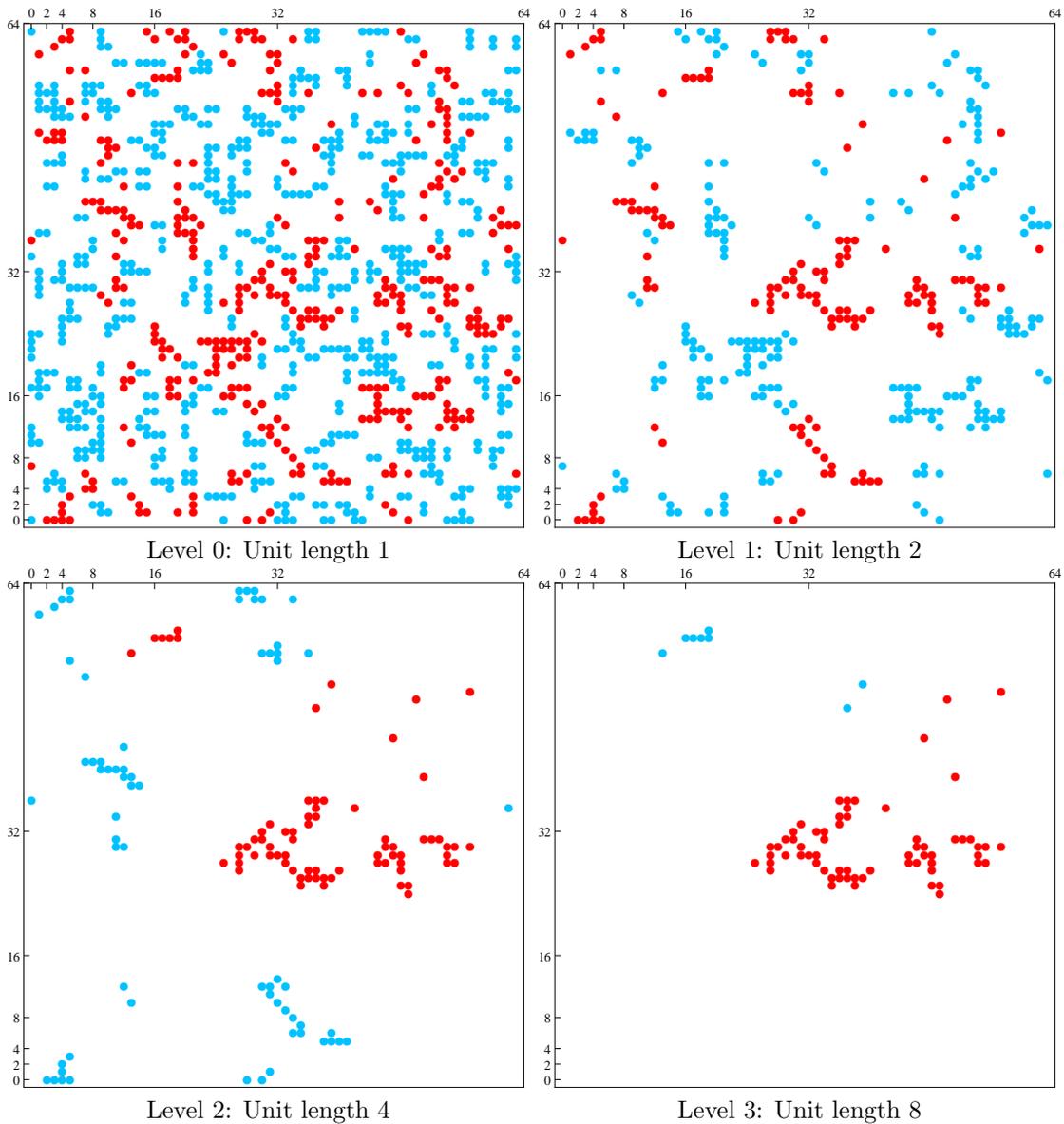


Figure 7.1: Configuration of defects at consecutive levels of renormalization group decoder. Bit-flip errors are generated stochastically for an illustrative purpose, over 64×64 lattice with a uniform error rate 8% per qubit. The dots are flipped stabilizer generators (defects) of the 2D toric code. At each level p , RG decoder decomposes the set of defects into connected clusters — connected components in a graph with vertices representing defects and edges connecting pairs of defects separated by distance 2^p or less (not shown). Each neutral cluster containing even number of defects (blue) is annihilated by applying a local Pauli operator supported in the smallest rectangular box enclosing the cluster. Charged clusters containing odd number of defects (red) cannot be annihilated locally. All defects in the red clusters are passed to the next RG level $p + 1$. In this example the red clusters from level 3 are annihilated at level 4 (not shown) and RG decoder successfully annihilated all defects returning the corrupted state to the originally encoded state.

consider nested boxes, near the faces of which many defects lie. However, clusters are created from the vacuum with some probability which we expect to be smaller than, say, $\frac{1}{2}$. So the number of clusters that have overlapping minimal enclosing box appears with exponentially small probability. On average, the running time of $\text{EC}(p)$ will be $O(N)$. The full RG decoding algorithm is as follows.

RG Decoder

Input S : the syndrome, **Output** P_{ec} : a Pauli operator.

1. Set $P_{ec} = I$.
2. **for** $p = 0$ **to** p_M **do**
 - Let $Q = \text{EC}(p)(S)$.
 - Update $P_{ec} \leftarrow P_{ec} \cdot Q$ and $S \leftarrow S \oplus S(Q)$.
- end for**
3. **if** $S = 0$ **then** return P_{ec} **else** declare failure.

Here the notation $S \oplus S(Q)$ stands for the symmetric difference of the sets S and $S(Q)$ or addition modulo two, if the syndromes are represented by binary strings. The discussion above implies that the RG decoder has running time $O(N^2 \log N)$ in the worst case, and $O(N \log N)$ in the case of sparse syndromes. An example of RG decoder in action is illustrated in Figure 7.1.

Being a physically realizable operation, any decoder should be written as a trace preserving completely positive map on the set of density matrices. By measuring a syndrome S , the decoder projects the state onto a subspace Π_S of the syndrome S , and then applies a correcting operator $P_{ec}(S)$:

$$\Phi_{ec}(\rho) = \sum_S P_{ec}(S) \Pi_S \rho \Pi_S P_{ec}(S)^\dagger$$

where the sum is over all possible syndromes. Thus, to conform with this equation our decoder should return some operator that is consistent with the measured syndrome, rather than declaring a “failure.” It is however no better than initializing the memory with an arbitrary state.

7.3 Cluster decomposition

Given a length scale r , the cluster decomposition of defects is to partition the defects into maximally connected subsets (connected components) of the syndrome at scale r . Naively, the task to compute the decomposition of all the defects into clusters will take time $O(m^2)$ where m is the total number of defects. The density of defects will typically be constant irrespective of the system size, and the computation time for decomposition will be $O(N^2)$, where N is the volume of the system. However, by exploiting the geometry of simple cubic lattice, we can do it in time $O(N)$. This is the optimal scaling since we have to sweep through the whole system anyway to identify the position of defects.

If $r = 1$, the problem is to label the connected components of binary array [117, 118]. Given a

defect u_0 , we can compute the connected component containing u_0 in time $O(m)$ where m is the number of defects in the component. One prepares an empty queue (first-in-first-out data structure), and puts u_0 into it. The subsequent computing is as follows: (i) Pop out the first element u from the queue, and of the neighborhood put the *unlabeled* defects into the queue and label them. (ii) Repeat until the queue becomes empty. Every defect in a connected component j is stored in the queue only once. Hence, this process computes the component j of a given defect in time proportional to the number m_j of defects in j . One examines the whole system in some order and finds the connected component whenever there is an unlabeled defect. The total computation time is proportional to $N + O(1) \sum_j m_j = O(N)$, since the connected components are disjoint.

For $r > 1$, the algorithm begins by dividing the whole lattice into boxes of linear size r or smaller. The defects in a box certainly belong to a single connected component (recall that we use the ℓ_∞ metric). The defects in the boxes B, B' belong to the same component if and only if there is a pair $u \in B, v \in B'$ of defects such that $d(u, v) \leq r$. In other words, we evaluate the binary function

$$\delta(B, B') = \begin{cases} 1 & \text{if there are } u \in B, v \in B' \text{ such that } d(u, v) \leq r, \\ 0 & \text{otherwise} \end{cases}$$

for each neighbor B' of B ; if B does not meet B' , we know that $\delta(B, B') = 0$.

Given the table of δ , we can finish computing the decomposition in time $O((L/r)^D)$ as in the $r = 1$ case. We show that the computation of $\delta(B, B')$ can be done in time $O(r^D)$ where D is the dimension of the lattice. Then, the total time to compute the table of δ for all adjacent boxes will be $O(r^D(L/r)^D) = O(N)$. Let B and B' be adjacent. For clarity of presentation, we restrict to $D = 2$. Suppose B and B' meet along an edge parallel to x -axis. Since any difference $|x - x'|$ of x -coordinates of the defects in $B \cup B'$ is at most r , we only need to compare y -coordinates. That is, the problem is reduced to one dimension. It suffices to pick two defects from B and B' , respectively, that are the closest to the x -axis. If the y -coordinates differ at most by r , then $\delta(B, B') = 1$; otherwise, $\delta(B, B') = 0$.

Suppose B and B' meet at a vertex. Without loss of generality, we assume B is in the third quadrant, and B' is in the first quadrant. Define a binary function δ' on B' as

$$\delta'(i, j) = \begin{cases} 1 & \text{if there is a defect } (x, y) \in B' \text{ where } x \leq i \text{ and } y \leq j, \\ 0 & \text{otherwise.} \end{cases}$$

The function table of δ' is computed in time $O(r^2)$. It is important to note that $\delta'(i, j) = 1$ implies $\delta'(i + 1, j) = \delta'(i, j + 1) = 1$. One starts from the origin and sets $\delta'(\frac{1}{2}, \frac{1}{2}) = 1$ if there is a defect at $(\frac{1}{2}, \frac{1}{2})$; otherwise $\delta'(\frac{1}{2}, \frac{1}{2}) = 0$. Here, $(\frac{1}{2}, \frac{1}{2})$ means the elementary square in the first quadrant

that is the closest to the origin. Proceeding by a lexicographic order of the coordinates, one sets $\delta'(i, j) = 1$ if $\delta'(i - 1, j) = 1$, or $\delta'(i, j - 1) = 1$, or there is a defect at (i, j) ; otherwise $\delta'(i, j) = 0$. It is readily checked that this procedure correctly computes δ' . Equipped with this δ' table, we can immediately test for each defect in B whether there is a defect in B' within distance r . Thus, we have computed $\delta(B, B')$ in time $O(r^2) + O(m)$ where m is the number of defects in B , which is at most $O(r^2)$. The computation of δ in higher dimensions is similar.

The computation of the minimal enclosing box for each cluster is also efficient. Given the coordinates of the m points in the cluster, we read out, say, x -coordinates x_1, \dots, x_m . The minimal enclosing interval B_x of x_1, \dots, x_m under periodic boundary conditions, is the complement of the longest interval between consecutive points x_i and x_{i+1} which can be computed in time $O(m)$. B_x is unambiguous if the diameter of the cluster is smaller than $L/2$. The minimal enclosing box is the product set $B_x \times B_y \times B_z$, whose vertices are computed in time $O(m)$.

7.4 Gröbner basis and broom algorithm

Now we describe an efficient algorithm for the 3D cubic code that tests whether a cluster is neutral. If the test is positive, the algorithm also returns a Pauli operator E that annihilates the cluster.

A crucial property of the 3D cubic code is that it is translationally invariant; it is described by a few Laurent polynomials over the variables that represent translations. See Chapter 3. The polynomials form a matrix σ satisfying $\sigma^\dagger \lambda \sigma = 0$, where \dagger is transposition followed by entry-wise antipode map, $x \mapsto x^{-1}$, etc., and λ is an alternating full rank matrix. Since we are working with qubits, the alternating matrix is actually symmetric. More important than σ is the excitation map $\epsilon = \sigma^\dagger \lambda$. A Pauli operator described by a column matrix p produces a syndrome described by ϵp . Thus, the neutrality of a cluster c is equivalent to the existence of p of finitely many terms such that $c = \epsilon p$. That is, c is neutral if and only if $c \in \text{im } \epsilon$; the neutrality test is really a submodule membership problem. Gröbner basis provides an efficient algorithmic answer to the membership problem: Compute a Gröbner basis B for the module $\text{im } \epsilon$. It can be done by, for example, Buchberger algorithm applied to columns of ϵ [77]. The Gröbner basis is computed only once for a given code. Then, the neutrality test is straightforward:

- (1) Express a cluster as a column matrix e of Laurent polynomials. This step takes running time $O(V)$ where V is the volume of the cluster.
- (2) Run a standard division algorithm with respect to B . It generates an explicit expression

$$e = \sum_i c_i b_i + r$$

where $b_i \in B$, and r is a unique remainder that cannot be further reduced by B . During the

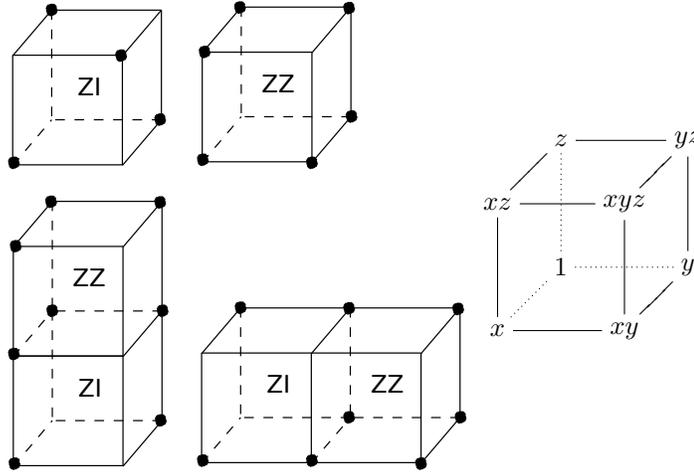


Figure 7.2: Elementary syndromes created by Z errors. The vertices which are on the dual lattice, represent the defects created by the error at the center. The elementary syndrome by ZI is used to push the defects to the bottom and to the left. The syndromes by errors of weight three is used to push the defects to the bottom-left corner. The cube on the right specifies the coordinate system.

division the degree does not increase. Therefore, the running time of the division is $O(V)$.

- (3) If $r = 0$, then the cluster is neutral, and c_i give the annihilating operator for the cluster. If $r \neq 0$, then the cluster is charged.

The 3D cubic code is simple because it is Calderbank-Shor-Steane type code; X - and Z -type errors can be treated separately. Since there is one X -type stabilizer generator, the syndrome caused by Z errors is expressed by one Laurent polynomial, which we call a *syndrome polynomial*. And neutral syndromes are described by an ideal (submodule) $I = (xyz + xy + yz + zx, xyz + x + y + z)$.¹ For simplicity, suppose that the syndrome polynomial is of nonnegative exponents. A Gröbner basis² of I is

$$\begin{aligned}
 & x + y + z + \mathbf{xyz}, \\
 & x + y + \mathbf{xy} + z + xz + yz, \\
 & x + y + z + xz + yz + z^2 + \mathbf{xz}^2 + yz^2, \\
 & x + y + xy + y^2 + \mathbf{xy}^2 + z + yz + y^2z, \\
 & y^2 + yz + y^2z + z^2 + yz^2 + \mathbf{y}^2\mathbf{z}^2
 \end{aligned} \tag{7.1}$$

where leading terms are marked as bold. The following is a graphical explanation for the division algorithm. Figure 7.2 shows a subset of a Gröbner basis for the cubic code. One can directly see

¹ The generators of I are different from those presented in Chapter 5, but they are related by redefinition of lattice coordinate system. The antipode map applied to I yields $(1 + x + y + z, 1 + xy + yz + zx)$.

²The basis presented here is not the *reduced* Gröbner basis, by which we mean a basis where no term is divisible by a leading term of other elements in the basis. The presented basis is actually what is used in the numerical simulation of the cubic code in Chapter 8. It also matches with Figure 7.2.

that the first four polynomials in Eq. (7.1) matches the diagrams. A step-by-step explanation is as follows. We fix a box B that encloses all the defects in the neutral cluster. We will sweep the defects to bottom-left-back corner. Since each defect is a Z_2 charge, they will disappear in the end. The algorithm begins with the top-right foremost vertex of B on the dual lattice. If there is a defect at $(x + \frac{1}{2}, y + \frac{1}{2}, z + \frac{1}{2})$, we apply ZI at (x, y, z) to eliminate it. This might create another defects as there are four defects in the elementary syndrome. Important is that the potentially new defects are all contained in the box B we started with. Continuing with ZI we push all the defects in the foremost plane of B to the left vertical line and the bottom horizontal line. During this process, we record where ZI has been applied.

For the defects on the vertical line at the left or on the horizontal line at the bottom, we use the operator of weight 3 to further move the defects to the bottom-left corner. See Fig. 7.2. This will in general create more defects behind, all of which are still contained in B . Thus, we have moved all the defects on the foremost plane to the bottom-left corner except for the three sites t, u, v :

$$\begin{array}{cc} t & o \\ | & \\ u & - v \end{array} \tag{7.2}$$

That is, if E' is the recorded operator during the sweeping process, the syndrome $S(EE') \subseteq B$ has potential defects only at t, u, v on the foremost plane.

Let o be at $(x_o + \frac{1}{2}, y_o + \frac{1}{2}, z_o + \frac{1}{2})$. By considering the multiplication by suitable stabilizer generators Q^Z , we can assume that EE' is the identity on the plane $x = x_o$, except (x_o, y_o, z_o) . Since there is no defect at o , the operator at (x_o, y_o, z_o) has to commute with XX ; it is either II or ZZ . Applying ZZ if necessary, the operator at (x_o, y_o, z_o) will become II , and the defects at t, u, v will disappear. In this way, we have successfully pushed all the defects to the next-to-foremost plane. We emphasize that the box B still envelops all the defects, and further B can be shrunk in one direction.

Due to the threefold symmetry of the cubic code, one can carry out this broom algorithm along any of three directions. We will have, at last, a box B of volume 1 that encloses all defects. The defects in the cluster must be from one of the three elementary syndrome cubes created either by ZI , IZ , or ZZ , which are easily eliminated. It is clear that in time $O(V)$ the error operator has been computed up to stabilizer, where V is the initial volume of the minimal enclosing box of the cluster.

7.5 Threshold theorem for topological stabilizer codes

In this section we prove that any topological stabilizer code can tolerate stochastic local errors with a small constant rate assuming that the error correction is performed using the RG decoder. We assume without loss of generality that each stabilizer generator is supported on a unit cube. Each site of the lattice may contain finitely many qubits. A generator at a cube c may act only on qubits of c . We shall assume that errors at different sites are independent and identically distributed. More precisely, let $E(P)$ be the set of sites at which a Pauli error P acts nontrivially. We shall assume that

$$\Pr[E(P) = E] = (1 - \epsilon)^{V - |E|} \epsilon^{|E|} \quad (7.3)$$

where $0 \leq \epsilon \leq 1$ is the error rate and $V = L^D$ is the total number of sites (the volume of the lattice). For example, the depolarizing noise in which every qubit experiences X, Y, Z errors with the probability $p/3$ each, satisfies Eq. (7.3) with the error rate $\epsilon = 1 - (1 - p)^q$, where q is the number of qubits per site.

Theorem 7.1. *Suppose a family of stabilizer codes has topological order satisfying TQO1,2. (In particular, every translationally invariant exact codes do.) Then, there exists a constant threshold $\epsilon_0 > 0$ such that for any $\epsilon < \epsilon_0$ the RG decoder corrects random independent errors with rate ϵ with the failure probability at most $e^{-\Omega(L^\eta)}$ for some constant $\eta > 0$.*

In the rest of this section we prove the theorem. Our proof borrows some techniques from [119, 120, 114], specifically Section 5.1 of Gray’s review [119] on Gács’ 1D cellular automata [120].

Recall that we use ℓ_∞ -metric, so a cube of linear size r thus has diameter r . We keep the terminologies and conventions from Section 7.1, and our decoder is what we have explained in the previous sections: The *level- p error correction* $EC(p)$ on a syndrome S is the following subroutine. (i) find all neutral 2^p -connected components M of S , (ii) for each M found at step 1, calculate and apply a Pauli operator P supported on the 1-neighborhood of $b(M)$ that annihilates M , and update the syndrome accordingly. Calling the full RG decoder on a syndrome S involves the following steps: (i) run $EC(0), EC(1), \dots, EC(\lceil \log_2 L_{tqo} \rceil)$, (ii) if the resulting syndrome S is empty, return the accumulated Pauli operator applied by the subroutines $EC(p)$. Otherwise, declare a failure.

Below we shall use the term ‘error’ both for the error operator P and for the subset of sites E acted on by P , whenever the meaning is clear from the context. Let us choose an integer $Q \gg 1$ and find a class of errors which are properly corrected by the RG decoder, see Lemma 7.5.2 below. We will see later that this class of errors actually includes all errors which are likely to appear for small enough error rate.

Definition 7.1. Let E be a fixed error. A site $u \in E$ is called a **level-0 chunk**. A non-empty subset of E is called a **level- n chunk** ($n \geq 1$) if it is a disjoint union of two level- $(n - 1)$ chunks

and its diameter is at most $Q^n/2$.

The term ‘chunk,’ not to be confused with the usage in Section 6.2, is chosen in order to avoid confusion with ‘cluster’, which is used for a set of defects. Note that a level- n chunk contains exactly 2^n sites. Given an error E , let E_n be the union of all level- n chunks of E . If $u \in E_{n+1}$, then by definition u is an element of a level- $(n+1)$ chunk. Since a level- $(n+1)$ chunk is a union of two level- n chunks, u is contained in a level- n chunk. Hence, $u \in E_n$, and the sequence E_n form a descending chain

$$E = E_0 \supseteq E_1 \supseteq \cdots \supseteq E_m,$$

where m is the smallest integer such that $E_{m+1} = \emptyset$. Let $F_i = E_i \setminus E_{i+1}$, so $E = F_0 \cup F_1 \cup \cdots \cup F_m$ is expressed as a disjoint union, which we call the *chunk decomposition* of E .

Proposition 7.5.1. *Let $Q \geq 6$ and M be any Q^n -connected component of F_n . Then M has diameter $\leq Q^n$ and is separated from $E_n \setminus M$ by distance $> \frac{1}{3}Q^{n+1}$.*

Proof. We claim that for any pair of sites $u \in F_n = E_n \setminus E_{n+1}$ and $v \in E_n$ we have $d(u, v) \leq Q^n$ or $d(u, v) > \frac{1}{3}Q^{n+1}$. Suppose on the contrary to the claim, that there is a pair $u \in F_n$ and $v \in E_n$ such that $Q^n < d(u, v) \leq Q^{n+1}/3$. Let $C_u \ni u$ and $C_v \ni v$ be level- n chunks that contains u and v , respectively. Since the diameters of $C_{u,v}$ are $\leq Q^n/2$ and $d(u, v) > Q^n$, we deduce that C_u and C_v are disjoint. On the other hand,

$$d(C_u \cup C_v) \leq d(u, v) + d(C_u) + d(C_v) \leq Q^{n+1}/2$$

since $Q \geq 6$. Thus, $C_u \cup C_v$ is a level- $(n+1)$ chunk that contains u which shows that $u \in E_{n+1}$. It contradicts to our assumption that $u \in F_n = E_n \setminus E_{n+1}$. \square

Note that in the chunk decomposition a Q^n -connected component P of E_n may not be separated from the rest $E \setminus P$ by distance $> Q^n$.

Lemma 7.5.2. *Let $Q \geq 10$. If the length m of the chunk decomposition of an error E satisfies $Q^{m+1} < L_{tq_0}$, then E is corrected by the RG decoder.*

Proof. Consider any fixed error P supported on a set of sites E . Let $E = F_0 \cup F_1 \cup \cdots \cup F_m$ be the chunk decomposition of E , and let $F_{j,\alpha}$ be the Q^j -connected components of F_j . Also, let $B_{j,\alpha}$ be the 1-neighborhood of the smallest box enclosing the syndrome created by the restriction of P onto $F_{j,\alpha}$. Proposition 7.5.1 implies that

$$d(B_{j,\alpha}) \leq Q^j + 2 \quad \text{and} \quad d(B_{j,\alpha}, B_{k,\beta}) > \frac{1}{3}Q^{1+\min(j,k)} - 2. \quad (7.4)$$

Let $P_{ec}^{(p)}$ be the accumulated correcting operator returned by the levels $0, \dots, p$ of the RG decoder. Let us use induction in p to prove the following statement.

1. The operator $P_{ec}^{(p)}$ has support on the union of the boxes $B_{j,\alpha}$.
2. The operators $P_{ec}^{(p)}$ and P have the same restriction on $B_{j,\alpha}$ modulo stabilizers for any j such that $2^p \geq Q^j + 2$.

The base of induction is $p = 0$. Using Eq. (7.4) we conclude that any 1-connected component of the syndrome $S(P)$ is fully contained inside some box $B_{j,\alpha}$. It proves that $P_{ec}^{(0)}$ has support on the union of the boxes $B_{j,\alpha}$. The second statement is trivial for $p = 0$.

Suppose we have proved the above statement for some p . Then the operator $P \cdot P_{ec}^{(p)}$ has support only inside boxes $B_{j,\alpha}$ such that $2^p < Q^j + 1$ (modulo stabilizers). It follows that any 2^{p+1} -connected component of the syndrome caused by $P \cdot P_{ec}^{(p)}$ is contained in some box $B_{j,\alpha}$ with $2^p < Q^j + 1$. Note that the RG decoder never adds new defects; we just need to check that 2^{p+1} -connected components do not cross the boundaries between the boxes $B_{j,\alpha}$ with $2^p < Q^j + 1$. This follows from Eq. (7.4). Hence $P_{ec}^{(p+1)}$ has support in the union of $B_{j,\alpha}$. Furthermore, if $2^p < Q^j + 1 \leq 2^{p+1}$, the cluster of defects created by $P \cdot P_{ec}^{(p)}$ inside $B_{j,\alpha}$ forms a single 2^{p+1} -connected component of the syndrome examined by $EC(p+1)$. This cluster is neutral since we assumed $Q^{m+1} < L_{tqo}$. Hence $P_{ec}^{(p+1)}$ will annihilate this cluster. The annihilation operator is equivalent to the restriction of $P \cdot P_{ec}^{(p)}$ onto $B_{j,\alpha}$ modulo stabilizers, since the linear size of $B_{j,\alpha}$ is smaller than L_{tqo} . It proves the induction hypothesis for the level $p+1$. \square

The preceding lemma says that errors by which the RG decoder could be confused are those from very high level chunks. What is the probability of the occurrence of such a high level chunk if the error is random according to Eq.(7.3)? Since our probability distribution of errors depend only on the number of sites in E , this question is completely percolation-theoretic.

Let us review some terminology from the percolation theory[121]. An event is a collection of configurations. In our setting, a configuration is a subset of the lattice. Hence, we have a partial order in the configuration space by the set-theoretic inclusion. An event \mathcal{E} is said to be *increasing* if $E \in \mathcal{E}, E \subseteq E'$ implies $E' \in \mathcal{E}$. For example, the event defined by the criterion that there exists an error at $(0, 0)$, is increasing. The *disjoint occurrence* $\mathcal{A} \circ \mathcal{B}$ of the events \mathcal{A} and \mathcal{B} is defined as the collection of configurations E such that $E = E_a \cup E_b$ is a disjoint union of $E_a \in \mathcal{A}$ and $E_b \in \mathcal{B}$. To illustrate the distinction between $\mathcal{A} \circ \mathcal{B}$ and $\mathcal{A} \cap \mathcal{B}$, consider two events defined as $\mathcal{A} =$ “there are errors at $(0, 0)$ and at $(1, 0)$ ”, and $\mathcal{B} =$ “there are errors at $(0, 0)$ and at $(0, 1)$ ”. The intersection $\mathcal{A} \cap \mathcal{B}$ contains a configuration $\{(0, 0), (1, 0), (0, 1)\}$, but the disjoint occurrence $\mathcal{A} \circ \mathcal{B}$ does not. A useful inequality by van den Berg and Kesten (BK) reads [122, 121]

$$\Pr[\mathcal{A} \circ \mathcal{B}] \leq \Pr[\mathcal{A}] \cdot \Pr[\mathcal{B}] \tag{7.5}$$

provided the events \mathcal{A} and \mathcal{B} are increasing.

Proof of Theorem 7.1. Consider a D -dimensional lattice and a random error E defined by Eq. (7.3). Let B_n be a fixed cubic box of linear size Q^n and B_n^+ be the box of linear size $3Q^n$ centered at B_n . Define the following probabilities:

$$p_n = \Pr [B_n \text{ has a nonzero overlap with a level-}n \text{ chunk of } E]$$

$$\tilde{p}_n = \Pr [B_n^+ \text{ contains a level-}n \text{ chunk of } E]$$

$$q_n = \Pr [B_n^+ \text{ contains 2 disjoint level-}(n-1) \text{ chunks of } E]$$

$$r_n = \Pr [B_n^+ \text{ contains a level-}(n-1) \text{ chunk of } E]$$

Note that all these probabilities do not depend on the choice of the box B_n due to translation invariance. Since a level-0 chunk is just a single site of E , we have $p_0 = \epsilon$. We begin by noting that

$$p_n \leq \tilde{p}_n \leq q_n.$$

Here we used the fact that any level- n chunk has diameter at most $Q^n/2$ and that any level- n chunk consists of a disjoint pair of level- $(n-1)$ chunks. Let us fix the box B_n^+ and let \mathcal{Q}_n be the event that B_n^+ contains a disjoint pair of level- $(n-1)$ chunks of E . Let \mathcal{R}_n be the event that B_n^+ contains a level- $(n-1)$ chunk of E . Then $\mathcal{Q}_n = \mathcal{R}_n \circ \mathcal{R}_n$. It is clear that \mathcal{Q}_n and \mathcal{R}_n are increasing events. Applying the van den Berg and Kesten inequality we arrive at

$$q_n \leq r_n^2.$$

Finally, since B_n^+ is a disjoint union of $(3Q)^D$ boxes of linear size Q^{n-1} , the union bound yields

$$r_n \leq (3Q)^D p_{n-1}.$$

Combining the above inequalities we get $p_n \leq (3Q)^{2D} p_{n-1}^2$, and hence

$$p_n \leq (3Q)^{-2D} ((3Q)^{2D} \epsilon)^{2^n}.$$

The probability p_n is doubly exponentially small in n whenever $\epsilon < (3Q)^{-2D}$. If there exists at least one level- n chunk, there is always a box of linear size Q^n that overlaps with it. Hence, on the finite system of linear size L , the probability of the occurrence of a level- m chunk is bounded above by $L^D p_m$. Employing Lemma 7.5.2, we conclude that the RG decoder fails with probability at most $p_{fail} = L^D p_m$ for any m such that $Q^{m+1} < L_{tq_0}$. Since we assumed that $L_{tq_0} \geq L^\delta$, one can choose $m \approx \delta \log L / \log Q$. In this case $p_{fail} = \exp(-\Omega(L^\eta))$ for $\eta \approx \delta / \log Q$. We have proved our theorem with $\epsilon_0 = (3Q)^{-2D}$ where $Q = 10$. \square

7.6 Benchmark of the decoder

Given a decoder, a family of quantum codes indexed by code length (system size) is said to have an *error threshold* p_c if the probability for decoder to fail approaches zero in the limit of large code length provided the random error rate p is less than p_c . We tested our decoder with respect to random uncorrelated bit-flip errors on the well-studied 2D toric code. The error threshold is measured to be 8.4(1)% using ℓ_1 -metric. See Fig. 7.3. It is reasonably close to the best known value 10.3% based on the perfect matching algorithm [7, 114], or 9% based on a renormalization group decoder of similar nature to ours [115]. This is remarkable for our decoder's simplicity and applicability. The 3D cubic code has threshold $\gtrsim 1.1\%$ under independent bit-flip errors using ℓ_∞ -metric. Note that in these simulations we do not use TestNeutral' of Remark 8.1.

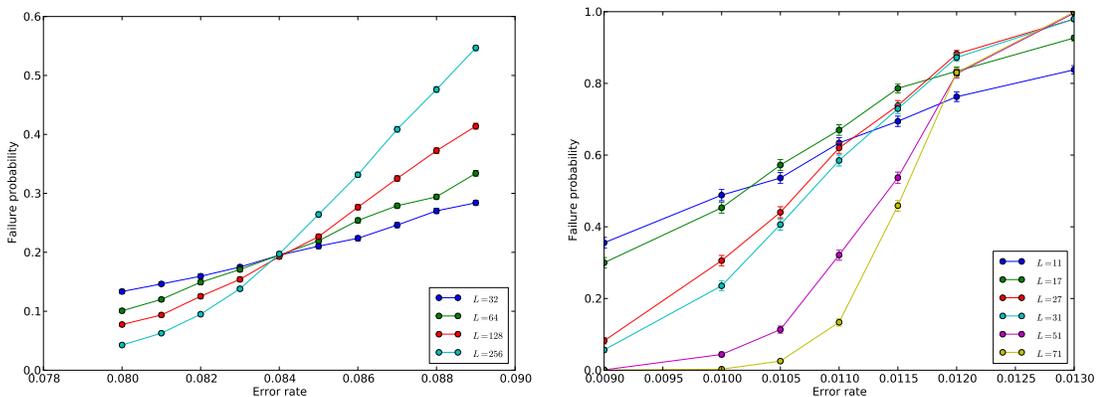


Figure 7.3: The thresholds of 2D toric code (left) and 3D cubic code (right) under independent random bit-flip errors using our RG decoder. The left shows simulation data for 2D toric code under ℓ_1 -metric, The right shows the data for 3D cubic code under ℓ_∞ -metric. The thresholds are measured to be $p_c(2D \text{ toric}) = 8.4(1)\%$ and $p_c(3D \text{ cubic}) \gtrsim 1.1\%$.

Chapter 8

Self-correcting quantum memory

We now directly assess the cubic code as a self-correcting quantum memory. The results in this chapter depend on previous chapters. In Chapter 6 we have found an energy barrier to isolate a nontrivial charge. It implies that nontrivial charges are localized in their original position where they are created. It suggests further that geometrically localized defects would form a neutral cluster, and the annihilation of them would not likely cause any undetected logical error. The renormalization group decoder and the threshold theorem in Chapter 7 have been motivated by this intuition. In this chapter, we show that the performance of the RG decoder against thermal errors matches our expectation, too. We prove that if the no-strings rule is satisfied, then the memory time grows as a power law $L^{c\beta}$ where β is the inverse temperature of the heat bath. The bound is valid when the system size is small enough $L \leq e^{c'\beta}$. Note that our analysis does not tell anything conclusive for the system in thermodynamic limit.

A few remarks can be made to the validity regime $L \leq e^{c'\beta}$. It is reasonable to expect that the no-strings rule and a good decoder would be sufficient to guarantee that the memory time increases with the system size. However, when the entropy is considered, the situation is more complicated. From the degeneracy formula of the cubic code in Chapter 5, we know that there are system sizes where the number k of encoded qubits is 2. Since the cubic code has exactly one X -type stabilizer generator G_X in each elementary cube, $k/2$ is equal to the number of ways that G_X 's multiply to the identity. Therefore, when $k = 2$, any configuration of defects is allowed as long as they are in an even number, and the number of excited states at a particular energy is given by a combinatorial factor. In contrast, the two-dimensional Ising model has only exponentially many configurations at a particular energy (the number of self-avoiding walks). The energy barrier of the cubic code is lower than that of the 2D Ising model, while the entropic contribution is stronger in the cubic code than in the 2D Ising model. The inequality $L \leq e^{c'\beta}$ can be understood as a requirement that entropic contribution should not be too large.

Perhaps, this is already hinted from the smooth thermal partition function of the cubic code presented in Section 5.5. It appears that the strong entropic contribution is unavoidable at the

presence of point-like defects. We have seen from Chapter 4 that the point-like defects always exists in three-dimensional translationally invariant topological codes. Thus, it would be impossible to have a truly self-correcting quantum memory based on local translationally invariant quantum codes in three dimensions whose memory time increases unbounded with the system size, similar to the 4D toric code [46, 32].

We model the thermal interaction by taking Davies weak coupling limit [123]. In order to make use of the results from previous chapters, we continue to assume topological quantum order (TQO) condition 1 and 2 defined in Chapter 6, and the no-strings rule of Chapter 5. The two TQO conditions demand that ground states must be locally indistinguishable, and that any locally created cluster of defects must be created from a ground state by an operator supported on the immediate neighborhood of the cluster. Note that any translationally invariant exact code Hamiltonian, such as the cubic code, automatically satisfies both of the TQO conditions. Of course, the cubic code satisfies the no-strings rule.

One more technical requirement to show the long memory time is that the number k of encoded qubits, or the ground-state degeneracy must be small. It is an ironic requirement at least for the cubic code because the small k implies a large number of excited states and large entropic contribution. In the three-dimensional case, we know from Corollary 4.3.3 that the characteristic dimension must be 1 in order for the no-strings rule to be obeyed. The nonzero characteristic dimension generally implies a growing $k(L)$ as a function of L . It is not so clear whether it is always possible to find a family of lattice sizes $\{L_i\}$ such that $k(L_i)$ is small. Although we do not know how to resolve this, the cubic code causes no problem since we know there is an infinite family $\{L_i\}$ such that $k(L_i) = 2$ by Corollary 5.3.2.

8.1 Previous work

Alternative routes towards quantum self-correction in topological memories proposed in the literature, focus on finding new mechanisms for suppressing diffusion of topological defects (here and below we only consider zero-dimensional defects). Arguably, the simplest of such mechanisms would be to have no topological defects in the first place. Unfortunately, this seems to require four spatial dimensions. The 4D toric code [7] provides the only known example of a truly self-correcting quantum memory. As was shown by Alicki and Horodecki's [46], the memory time of the 4D toric code grows exponentially with the lattice size for small enough bath temperature. The first 3D topological memory in which diffusion of defects is constrained by superselection rules was proposed by Chamon [89], see also [90]. Topological defects in this model have a limited mobility restricted to certain subspaces of \mathbb{R}^3 or have no mobility at all. However, the model has no macroscopic energy barrier that could suppress the diffusion. 2D topological memories in which diffusion of anyons is

suppressed by effective long-range interactions were studied by Chesi et al. [124] and Hamma et al [125]. A quenched disorder and Anderson localization were proposed as a means of suppressing propagation of defects at the zero temperature by Wootton and Pachos [126] and, independently, by Stark et al. [127], see also [128]. A no-go theorem for quantum self-correction based on 3D stabilizer Hamiltonians in which ground-state degeneracy does not depend on lattice dimensions was proved by Yoshida [47]. A different line of research initiated by Pastawski et al. [129] focuses on quantum memories in which active error correction is imitated by engineered dissipation driving the memory system towards the ground state (as opposed to the Gibbs state). Finally, let us emphasize that quantum self-correction is technically different from the thermal stability of topological phases, see, for instance, [35, 130, 110, 36]. While the latter attempts to establish the presence (or absence) of topological order in the equilibrium thermal state, quantum self-correction is mostly concerned with the relaxation time towards the equilibrium state.

8.2 Storage scheme

In order to use any memory, either classical or quantum, a user must be able to write, store, and read information. In this section we describe these steps formally for a topological quantum memory based on the 3D cubic code. The Hamiltonian of the memory is

$$H = -J \sum_c G_c^X + G_c^Z,$$

where the sum runs over all L^3 elementary cubes c and the operators G_c^X , G_c^Z act on the qubits of c as shown on Fig. 5.1. The positive coupling constant J is set to $J = \frac{1}{2}$ for simplicity.

Suppose at time $t = 0$ the memory system is initialized in some ground state $\rho(0)$ encoding a quantum state to be stored; the ground space is the code space. We model interaction between the memory system and the thermal bath using the Davies weak coupling limit [123]. It provides a Markovian master equation of the following form:

$$\dot{\rho}(t) = -i[H, \rho(t)] + \mathcal{L}(\rho(t)), \quad t \geq 0. \quad (8.1)$$

Here $\rho(t)$ is the state of the memory system at time t and \mathcal{L} is the Lindblad generator describing dissipation of energy. To define \mathcal{L} , let us choose some set of self-adjoint operators $\{A_\alpha\}$ through which the memory can couple to the bath. We assume that each A_α acts nontrivially on a constant number of qubits. For example, $\{A_\alpha\}$ could be the set of all single-qubit Pauli operators. Let

$$A_\alpha(t) = e^{iHt} A_\alpha e^{-iHt} = \sum_\omega e^{-i\omega t} A_{\alpha,\omega}. \quad (8.2)$$

We will see later in Eq. (8.7) that $A_{\alpha,\omega}$ maps eigenvectors of H with energy E to eigenvectors with energy $E - \omega$. Then

$$\mathcal{L}(\rho) = \sum_{\alpha} \sum_{\omega} h(\alpha, \omega) \left(A_{\alpha,\omega} \rho A_{\alpha,\omega}^{\dagger} - \frac{1}{2} \{ \rho, A_{\alpha,\omega}^{\dagger} A_{\alpha,\omega} \} \right). \quad (8.3)$$

The coefficient $h(\alpha, \omega)$ is the rate of quantum jumps caused by A_{α} transferring energy ω from the memory to the bath. It must obey the detailed balance condition [123]

$$h(\alpha, -\omega) = e^{-\beta\omega} h(\alpha, \omega), \quad (8.4)$$

where β is the inverse bath temperature. The detailed balance condition Eq. (8.4) is the only part of our model that depends on the bath temperature. It guarantees that the Gibbs state $\rho_{\beta} \sim e^{-\beta H}$ is the fixed point of the dynamics as $\mathcal{L}(\rho_{\beta}) = 0$. Identities in the proof of Proposition 8.3.4 are useful to see $\mathcal{L}(\rho_{\beta}) = 0$. This is a unique fixed point under certain natural ergodicity conditions [131]. Furthermore, we shall assume that $\|A_{\alpha}\| \leq 1$ and

$$\max_{\alpha,\omega} h(\alpha, \omega) = O(1). \quad (8.5)$$

Let us remark that the Davies weak coupling limit was adopted as a model of the thermal dynamics in most of the previous works with a rigorous analysis of quantum self-correction; see, for instance, [46, 10, 32, 124].

The final state $\rho(t)$ generated by the Davies dynamics can be regarded as a corrupted version of the initial encoded state $\rho(0)$. A decoder retrieves the encoded information from $\rho(t)$ by performing a syndrome measurement and an error correction. A syndrome measurement involves a non-destructive eigenvalue measurement of all stabilizer generators G_c^X, G_c^Z . The measured syndrome S can be regarded as a classical bit string that assigns an eigenvalue ± 1 to each generator. The error correction step is specified by an algorithm that takes as input the measured syndrome S and returns a correcting Pauli operator $P_{ec}(S)$. Let Π_S be the projector onto the subspace with syndrome S . The net action of the decoder on states can be described by a trace preserving completely positive (TPCP) linear map

$$\Phi_{ec}(\rho) = \sum_S P_{ec}(S) \Pi_S \rho \Pi_S P_{ec}(S)^{\dagger}, \quad (8.6)$$

where the sum runs over all possible syndromes. We choose the renormalization group decoder presented in Chapter 7.

8.3 Properties of the Lindbladian

Proposition 8.3.1 ([32]). *Each operator $A_{\alpha,\omega}$ acts non-trivially only on $O(1)$ qubits. Furthermore,*

$$\|\mathcal{L}_+\|_1 \equiv \sup_X \frac{\|\mathcal{L}_+(X)\|_1}{\|X\|_1} = O(N).$$

Proof. Recall that each operator A_α acts on $O(1)$ qubits. Since H is a sum of pairwise commuting terms, we can represent $A_\alpha(t)$ as $A_\alpha(t) = e^{iH_\alpha t} A_\alpha e^{-iH_\alpha t}$ where H_α is obtained from H by retaining only those stabilizer generators that do not commute with A_α . (Compare it with Eq. (8.2).) All such generators must share at least one qubit with A_α . Therefore $A_\alpha(t)$ and $A_{\alpha,\omega}$ act non-trivially only $O(1)$ qubits. Furthermore, since H_α has $O(1)$ distinct integer eigenvalues, $A_\alpha(t)$ has only $O(1)$ distinct Bohr frequencies; the summation over ω in Eq. (8.2) is finite. The bound $\|A_{\alpha,\omega}\| \leq 1$ follows trivially from our assumption $\|A_\alpha\| \leq 1$. The norm of \mathcal{L}_+ is then bounded from Eq. (8.3) using triangle inequality, $\|XY\|_1 \leq \|X\| \cdot \|Y\|_1$, and Eq. (8.5). \square

Proposition 8.3.2.

$$HA_{\alpha,\omega} - A_{\alpha,\omega}H = -\omega A_{\alpha,\omega} \quad \text{and} \quad HA_{\alpha,\omega}^\dagger - A_{\alpha,\omega}^\dagger H = +\omega A_{\alpha,\omega}^\dagger \quad (8.7)$$

Proof. Let us drop the subscript α momentarily for notational convenience. The spectral component A_ω is given by a Fourier transformation

$$A_\omega = \int \frac{dt}{T} e^{i\omega t} (e^{iHt} A e^{-iHt})$$

where the integral is over a period T such that $\frac{fT}{2\pi}$ is an integer for every Bohr frequency f of $A(t)$. Since there are only finitely many Bohr frequencies, such T exists. Let $|\psi\rangle$ be any energy eigenstate of energy E . Then,

$$\begin{aligned} HA_\omega |\psi\rangle &= \int \frac{dt}{T} e^{i\omega t} H e^{iHt} A e^{-iHt} |\psi\rangle \\ &= \int \frac{dt}{T} e^{i(\omega-E)t} H e^{iHt} A |\psi\rangle \\ &= \int \frac{dt}{T} e^{i(\omega-E)t} (-i) \frac{\partial}{\partial t} e^{iHt} A |\psi\rangle \\ &= \int \frac{dt}{T} (-i) \frac{\partial}{\partial t} e^{i(\omega-E)t} e^{iHt} A |\psi\rangle - (\omega - E) \int \frac{dt}{T} e^{i(\omega-E)t} e^{iHt} A |\psi\rangle \\ &= \frac{-i}{T} [e^{i\omega t} A(t)]_0^T + (E - \omega) \int \frac{dt}{T} e^{i\omega t} e^{iHt} A e^{-iHt} |\psi\rangle \\ &= (E - \omega) A_\omega |\psi\rangle \\ &= -\omega A_\omega |\psi\rangle + A_\omega H |\psi\rangle. \end{aligned}$$

Since $|\psi\rangle$ was an arbitrary energy eigenstate, we have Eq. (8.7). \square

Proposition 8.3.3. *Let \hat{H} be the linear map defined by $\hat{H}(X) = HX - XH$. The map \hat{H} commutes with the Lindblad generator \mathcal{L} . Therefore, $\hat{H}(\rho(t)) = 0$, and $\rho(t) = e^{\mathcal{L}t}(\rho(0))$.*

Proof. It is elementary that $\hat{H}(XY) = \hat{H}(X)Y + X\hat{H}(Y)$. Eq. (8.7) reads $\hat{H}(A_{\alpha,\omega}) = -\omega A_{\alpha,\omega}$ and $\hat{H}(A_{\alpha,\omega}^\dagger) = +\omega A_{\alpha,\omega}^\dagger$. Hence, $\hat{H}(A_{\alpha,\omega}A_{\alpha,\omega}^\dagger) = 0$. Clearly,

$$\begin{aligned}\hat{H}\mathcal{L}(\rho) &= \hat{H}h\left(a\rho a^\dagger - \frac{1}{2}\rho a^\dagger a - \frac{1}{2}a^\dagger a\rho\right) \\ &= -h\omega a\rho a^\dagger + ha\hat{H}(\rho)a^\dagger + h\omega a\rho a^\dagger - \frac{1}{2}h\hat{H}(\rho)a^\dagger a - \frac{1}{2}ha^\dagger a\hat{H}(\rho) \\ &= \mathcal{L}\hat{H}(\rho)\end{aligned}$$

where $a = A_{\alpha,\omega}$, $h = h(\alpha,\omega)$ with the sum over α and ω understood, and ρ is arbitrary. It follows that

$$\rho(t) = e^{-i\hat{H}t + \mathcal{L}t}(\rho(0)) = e^{\mathcal{L}t} \circ e^{-i\hat{H}t}(\rho(0)) = e^{\mathcal{L}t}(\rho(0)),$$

since $\hat{H}(\rho(0)) = [H, \rho(0)] = 0$. It implies that $\hat{H}(\rho(t)) = 0$. \square

Proposition 8.3.4 ([46]). *Let \mathcal{L}^* be the adjoint linear map of \mathcal{L} (the one describing time evolution in the Heisenberg picture) with respect to Hilbert-Schmidt inner product. Define Liouville inner product by $\langle X, Y \rangle_\beta \equiv \text{Tr} \rho_\beta X^\dagger Y$. Then, \mathcal{L}^* is self-adjoint with respect to Liouville inner product; $\langle X, \mathcal{L}^*(Y) \rangle_\beta = \langle \mathcal{L}^*(X), Y \rangle_\beta$.*

Proof. We suppress the index α for notational convenience. Using $e^H X e^{-H} = e^{\hat{H}}(X)$ and $\hat{H}(A_\omega) = -\omega A_\omega$, we have $e^{\beta H} A_\omega e^{-\beta H} = e^{\beta \hat{H}}(A_\omega) = e^{-\beta \omega} A_\omega$, or $A_\omega \rho_\beta = e^{-\beta \omega} \rho_\beta A_\omega$. Hence, $\rho_\beta (A_\omega^\dagger A_\omega) = (A_\omega^\dagger A_\omega) \rho_\beta$. Now,

$$\begin{aligned}\langle \mathcal{L}^* X, Y \rangle - \langle X, \mathcal{L}^* Y \rangle &= \sum_\omega h(\omega) \text{Tr} \left(A_\omega^\dagger X^\dagger A_\omega Y \rho_\beta - \frac{1}{2} X^\dagger A_\omega^\dagger A_\omega Y \rho_\beta - \frac{1}{2} A_\omega^\dagger A_\omega X^\dagger Y \rho_\beta \right. \\ &\quad \left. - X^\dagger A_\omega^\dagger Y A_\omega \rho_\beta + \frac{1}{2} X^\dagger Y A_\omega^\dagger A_\omega \rho_\beta + \frac{1}{2} X^\dagger A_\omega^\dagger A_\omega Y \rho_\beta \right) \\ &= \sum_\omega h(\omega) \text{Tr} (A_\omega^\dagger X^\dagger A_\omega Y \rho_\beta - X^\dagger A_\omega^\dagger Y A_\omega \rho_\beta) \\ &= \sum_\omega h(\omega) \text{Tr} (A_\omega^\dagger X^\dagger A_\omega Y \rho_\beta - X^\dagger A_\omega^\dagger Y \rho_\beta A_\omega e^{-\beta \omega})\end{aligned}$$

Applying the detailed balance condition $e^{-\beta \omega} h(\omega) = h(-\omega)$ of Eq. (8.4), we see that

$$= \sum_\omega h(\omega) \text{Tr} (A_\omega^\dagger X^\dagger A_\omega Y \rho_\beta) - \sum_\omega h(-\omega) \text{Tr} (X^\dagger A_\omega^\dagger Y \rho_\beta A_\omega).$$

Since A_ω is a Fourier transform of a Hermitian operator $A(t)$ in Eq. (8.2), we apply $A_\omega^\dagger = A_{-\omega}$ to conclude

$$\begin{aligned} &= \sum_{\omega} h(\omega) \text{Tr} (A_\omega^\dagger X^\dagger A_\omega Y \rho_\beta) - \sum_{\omega} h(-\omega) \text{Tr} (X^\dagger A_{-\omega} Y \rho_\beta A_{-\omega}^\dagger) \\ &= 0. \end{aligned}$$

The last equality is because ω is a dummy variable. □

8.4 Analysis of thermal errors

We now analyze the relation between \mathcal{L} and Φ_{ec} . Recall the following terminology and notations. A ground state of the memory Hamiltonian will be referred to as a *vacuum*. It will be convenient to perform an overall energy shift such that the vacuum has *zero energy*. A *Pauli operator* is an arbitrary tensor product of single-qubit Pauli operators X, Y, Z and the identity operators I . We will say that a Pauli operator creates m *defects* iff P anticommutes with exactly m stabilizer generators G_c^X, G_c^Z . Equivalently, applying P to the vacuum one obtains an eigenvector of H with energy m . For example, using the explicit form of the generators, see Figure 5.1, one can check that single-qubit X or Z errors create 4 defects, while Y errors create 8 defects. See Figure 7.2. We will say that a Pauli error P is corrected by the decoder if $P_{ec}(S(P)) = \pm PG$, where $S(P)$ is the syndrome of P and G is a product of stabilizer generators. Let $N = 2L^3$ be the total number of qubits. Note that N is also the number of stabilizer generators for the cubic code.

Let $\Gamma = (P_0, P_1, \dots, P_t)$ be a finite sequence of Pauli operators such that the operators P_i and P_{i+1} differ on at most one qubit for all $0 \leq i < t$. We say that Γ is an **error path** implementing a Pauli operator P when $P_0 = I$ and $P_t = P$. Let m_i be the number of defects created by P_i . The maximum number of defects

$$m(\Gamma) = \max_{0 \leq i \leq t} m_i$$

will be called an **energy cost** of the error path Γ . Given a Pauli operator P , we define its **energy barrier** $\Delta(P)$ as the minimum energy cost of all error paths implementing P ,

$$\Delta(P) = \min_{\Gamma} m(\Gamma).$$

Although the set of error paths is infinite, the minimum always exists because the energy cost is a nonnegative integer. In fact, it suffices to consider paths in which P_i are all distinct. The number of such paths is finite since there are only finitely many Pauli operators for a given system size.

It is worth emphasizing that an operator P may have a very large energy barrier even though P itself creates only a few defects or no defects at all. Consider as an example the 2D Ising model,

$H = -\frac{1}{2} \sum_{\langle uv \rangle} Z_u Z_v$, where the sum runs over all pairs of nearest neighbor sites on the square lattice of size $L \times L$ with open boundary conditions. Then the logical- X operator $P = \bigotimes_u X_u$ has an energy barrier $\Delta(P) = L$ since any sequence of bit-flips implementing P must create a domain wall across the lattice. It is clear that a Pauli operator P acting nontrivially on n qubits has energy barrier at most $O(n)$.

A naive intuition suggests that a stabilizer code Hamiltonian is a good candidate for being a self-correcting memory if there exists an error correction algorithm, or a decoder, that corrects all errors with a sufficiently small energy barrier. Errors with a high energy barrier can confuse the decoder and cause it to make wrong decisions, but we expect that such errors are unlikely to be created by the thermal noise. We make this intuition more rigorous.

Let f be the maximum energy barrier of Pauli operators that appear in the expansion of the quantum jump operators $A_{\alpha,\omega}$ or $A_{\alpha,\omega}^\dagger A_{\alpha,\omega}$ of Eq. (8.3). Since $A_{\alpha,\omega}$ act on a constant number of qubits by Proposition 8.3.1, we have $f = O(1)$. Below m is an arbitrary energy cutoff. Let $\mathcal{D} = \ker \hat{H}$ be the set of all operators that are commuting with the Hamiltonian H . Every operator in \mathcal{D} is block-diagonal in the energy eigenstate basis. Since $\rho(0)$ is supported on the ground subspace of H , we have $\rho(0) \in \mathcal{D}$. Below we only consider states from \mathcal{D} and linear maps preserving \mathcal{D} . Define an orthogonal identity decomposition

$$I = \Pi_- + \Pi_+$$

where Π_- projects onto the subspace with energy $< m + f$ and Π_+ projects onto the subspace with energy $\geq m + f$. Introduce auxiliary Lindblad generators

$$\mathcal{L}_-(\rho) = \sum_{\alpha} \sum_{\omega} h(\alpha, \omega) \left(B_{\alpha,\omega} \rho B_{\alpha,\omega}^\dagger - \frac{1}{2} \{ \rho, B_{\alpha,\omega}^\dagger B_{\alpha,\omega} \} \right), \quad \text{where } B_{\alpha,\omega} = \Pi_- A_{\alpha,\omega} \quad (8.8)$$

and

$$\mathcal{L}_+(\rho) = \sum_{\alpha} \sum_{\omega} h(\alpha, \omega) \left(C_{\alpha,\omega} \rho C_{\alpha,\omega}^\dagger - \frac{1}{2} \{ \rho, C_{\alpha,\omega}^\dagger C_{\alpha,\omega} \} \right), \quad \text{where } C_{\alpha,\omega} = \Pi_+ A_{\alpha,\omega}. \quad (8.9)$$

Simple algebra shows that \mathcal{L}_- and \mathcal{L}_+ preserve \mathcal{D} and their *restrictions on \mathcal{D}* satisfy

$$\mathcal{L} = \mathcal{L}_- + \mathcal{L}_+. \quad (8.10)$$

It is useful to note that any $X \in \mathcal{D}$ commutes with Π_{\pm} . By abuse of notations, we shall apply Eq.(8.10) as though it holds for all operators.

Lemma 8.4.1. *Suppose that an error correction algorithm $s \mapsto P_{ec}(s)$ corrects any Pauli error P with the energy barrier smaller than $m + 2f$. Let Φ_{ec} be the corresponding decoder defined by*

Eq.(8.6). For any time $t \geq 0$ and for any state ρ_0 supported on the ground subspace of H one has

$$\Phi_{ec}(e^{\mathcal{L}-t}(\rho_0)) = \rho_0.$$

Proof. Since all maps are linear, we may assume $\rho_0 = |g\rangle\langle g|$ is a pure state. Then, $e^{\mathcal{L}-t}(\rho_0)$ is in the span of states of form $|\psi\rangle = \Pi_- E_n \cdots \Pi_- E_2 \Pi_- E_1 |g\rangle$, where E_i are Pauli operators that appears in the expansion of $A_{\alpha,\omega}$ or $A_{\alpha,\omega}^\dagger A_{\alpha,\omega}$. This follows from the Taylor expansion of $e^{\mathcal{L}-t}$. Since Pauli errors map eigenvectors of H to eigenvectors of H , we conclude that either $|\psi\rangle = 0$, or $|\psi\rangle = E_n \cdots E_2 E_1 |g\rangle$. Furthermore, the latter case is possible only if the Pauli operator $E \equiv E_n \cdots E_2 E_1$ has energy barrier smaller than $m + 2f$. Indeed, definition of Π_- implies that $E_j E_{j-1} \cdots E_1$ creates at most $m + f - 1$ defects for all $j = 1, \dots, n$. By assumption, each operator E_j can be implemented by an error path with energy cost at most f . Taking the composition of all such error paths one obtains an error path for E with energy cost at most $m + 2f - 1$ and thus Φ_{ec} will correct E . Since $\Phi_{ec} \circ e^{\mathcal{L}-t}$ is a TPCP map, we must have $\Phi_{ec}(e^{\mathcal{L}-t}(\rho_0)) = \rho_0$. \square

For any decomposition $\mathcal{L} = \mathcal{L}_- + \mathcal{L}_+$ one has the following identity:

$$e^{\mathcal{L}t} = e^{\mathcal{L}_- t} + \int_0^t ds e^{\mathcal{L}_- (t-s)} \mathcal{L}_+ e^{\mathcal{L}_+ s}, \quad (8.11)$$

which follows from the identity

$$\frac{d}{ds} e^{\mathcal{L}_- (t-s)} e^{\mathcal{L}_+ s} = e^{\mathcal{L}_- (t-s)} (-\mathcal{L}_- + \mathcal{L}_+) e^{\mathcal{L}_+ s} = e^{\mathcal{L}_- (t-s)} \mathcal{L}_+ e^{\mathcal{L}_+ s}.$$

Lemma 8.4.2. *Assume the supposition of Lemma 8.4.1. Let Q_m be the projector onto the (high energy) subspace with at least m defects. Then*

$$\epsilon(t) \equiv \|\Phi_{ec}(\rho(t)) - \rho(0)\|_1 \leq O(tN) \text{Tr} Q_m e^{-\beta H} \quad (8.12)$$

for any initial state $\rho(0)$ supported on the ground subspace of H . The time evolution of $\rho(t)$ is governed by the Lindblad equation, Eq. (8.1), with the inverse temperature β of the bath.

Proof. Write $\rho_0 \equiv \rho(0)$. First, Proposition 8.3.3 says $\rho(t) = e^{\mathcal{L}t}(\rho_0)$. Applying Lemma 8.4.1 and Eq. (8.11) one arrives at

$$\epsilon(t) \leq \int_0^t ds \|e^{\mathcal{L}_- (t-s)} \mathcal{L}_+ e^{\mathcal{L}_+ s}(\rho_0)\|_1 \leq t \cdot \max_{0 \leq s \leq t} \|\mathcal{L}_+ e^{\mathcal{L}_+ s}(\rho_0)\|_1. \quad (8.13)$$

We shall use an identity

$$\mathcal{L}_+(X) = \mathcal{L}_+(Q_m X Q_m) \quad (8.14)$$

valid for any $X \in \mathcal{D}$. Indeed, any quantum jump operator $A_{\alpha,\omega}$ changes the energy at most by f , so that $\mathcal{L}_+(Q_m^\perp X) = \mathcal{L}_+(X Q_m^\perp) = 0$ for any $X \in \mathcal{D}$ (note that any $X \in \mathcal{D}$ commutes with Q_m). We arrive at

$$\epsilon(t) \leq t \cdot \|\mathcal{L}_+(Q_m e^{\mathcal{L}s}(\rho_0) Q_m)\|_1 \leq t \cdot \|\mathcal{L}_+\|_1 \cdot \|Q_m e^{\mathcal{L}s}(\rho_0) Q_m\|_1 \leq O(tN) \text{Tr} Q_m e^{\mathcal{L}s}(\rho_0), \quad (8.15)$$

where the maximization over s is implicit. We used Proposition 8.3.1 and the positivity of $\mathcal{L}(\rho_0)$ in the last inequality. Since the ground-state energy of H is zero, one has

$$\rho_0 = \mathcal{Z}_\beta \rho_\beta \rho_0, \quad (8.16)$$

where \mathcal{Z}_β is the partition function. It yields

$$\text{Tr} Q_m e^{\mathcal{L}s}(\rho_0) = \text{Tr} \rho_0 e^{\mathcal{L}^*s}(Q_m) = \mathcal{Z}_\beta \text{Tr} \rho_\beta \rho_0 e^{\mathcal{L}^*s}(Q_m) = \mathcal{Z}_\beta \langle \rho_0, e^{\mathcal{L}^*s}(Q_m) \rangle_\beta, \quad (8.17)$$

Proposition 8.3.4 implies that the map $e^{\mathcal{L}^*s}$ is also self-adjoint with respect to the Liouville inner product. Hence, we have

$$\text{Tr} Q_m e^{\mathcal{L}s}(\rho_0) = \mathcal{Z}_\beta \langle \rho_0, e^{\mathcal{L}^*s}(Q_m) \rangle_\beta = \mathcal{Z}_\beta \langle e^{\mathcal{L}^*s}(\rho_0), Q_m \rangle_\beta = \text{Tr} e^{\mathcal{L}^*s}(\rho_0) Q_m e^{-\beta H} \leq \text{Tr} Q_m e^{-\beta H}, \quad (8.18)$$

where the last inequality is because $e^{\mathcal{L}^*s}$ is a unital completely positive map and $\rho_0 \leq I$. \square

8.5 Correctability of errors with an energy barrier

Let P be an unknown Pauli error. Suppose we are promised that P has a sufficiently small energy barrier, namely, $\Delta(P) \leq c \log L$, for some constant c that will be chosen later. In this section we prove that any such error P will be corrected by the RG decoder.

Assume throughout this section that a family of topological stabilizer codes $\{\mathcal{C}_L\}_L$ defined in Section 6.1 with $L_{tqo} \geq L^\gamma$ obey the no-strings rule with some constant α as in Definition 5.1. The ℓ_∞ -metric d is used; $d((x, y, z), (x', y', z')) = \max\{|x - x'|, |y - y'|, |z - z'|\}$. We use

$$\xi(p) = (10\alpha)^p$$

for notational convenience as in the previous chapter, as well as the notion of *level- p sparseness* of Definition 6.3 and *level- p syndrome history*. When P_0, P_1, \dots, P_t form an error path, the corresponding sequence of syndromes $S(j)$ caused by P_j acting on a vacuum is called a level-0 syndrome history. A level- p syndrome history, inductively defined, discards all level- $(p-1)$ sparse syndromes from level- $(p-1)$ syndrome history, but keeps the initial and final syndromes.

Let $\Gamma = (P_0, P_1, \dots, P_t)$ be an error path implementing P with the energy cost $m(\Gamma) = m$. Here $P_0 = I$, $P_t = P$, while $E_j \equiv P_j P_{j-1}$ are single-qubit Pauli operators for all j . Lemma 6.1.1 implies that there is a level $p_{max} < m$ such that in the level- p_{max} syndrome history only the initial empty syndrome $S(0) = 0$ and the final syndrome $S(t) = S$ are possibly non-sparse.

Lemma 8.5.1. *Let P be any Pauli error, $S = S(P)$ be its syndrome, and $m = \Delta(P)$ be its energy barrier. Suppose*

$$16m(10\alpha)^m < L_{tqo}. \quad (8.19)$$

Then, there exists a stabilizer $G \in \mathcal{G}$ such that $P \cdot G$ has support on the $\xi(m)$ -neighborhood of S . Any R -connected component of S is neutral for $2\xi(m) < R \leq 4\xi(m)$.

Proof. Let us apply Lemma 6.1.3 to the level p_{max} , the smallest integer such that the level- p_{max} syndrome history has the initial and final syndrome, and level- p_{max} -sparse syndromes. Since $p_{max} < m$, the condition $16m\xi(p_{max}) < L_{tqo}$ in Lemma 6.1.3 is satisfied. We have $S' = 0$, $S'' = S$, and $E = P$. Hence, there exists a stabilizer $G \in \mathcal{G}$ such that $P \cdot G$ is supported on the $\xi(p_{max})$ -neighborhood of S . It proves the first statement of the lemma.

Let $r = \xi(m) = (10\alpha)^m$. Choose any R such that $2r < R \leq 4r$ and let C_a be any R -connected component of S . Since C_a contains at most m defects, the diameter of C_a is at most mR . Restricting $P \cdot G$ on the r -neighborhood of C_a , we obtain a Pauli operator P_a supported on a cube of linear size at most $mR + 2r \leq 4rm + 2r < L_{tqo}$ by assumption. Furthermore, the support of P_a is separated from $(P_a)^{-1}(P \cdot G)$ by distance at least $R - 2r > 0$. Hence, P_a creates the cluster C_a from the vacuum. Therefore, C_a is neutral. \square

We wish to have a well-separated cluster decomposition.

Lemma 8.5.2. *Let S be any cluster of $m > 0$ defects. For any integer $\mu \geq 1$, there exists a nonnegative integer $p < m$ and a decomposition*

$$S = C_1 \cup \dots \cup C_n \quad \text{such that} \quad d(C_a) \leq 4^p \mu \quad \text{and} \quad d(C_a, C_b) > \frac{1}{2} \cdot 4^{p+1} \mu \quad \text{for } a \neq b. \quad (*)$$

Proof. The only nontrivial part is that p can be chosen as $p < m$. Let us say that a partition of S into clusters is p -good if it satisfies (*). By grouping all defects occupying the same elementary cube into a cluster, one obtains a partition $S = C_1 \cup \dots \cup C_g$. Obviously, $g \leq m$, and $d(C_a) \leq \mu$. If this partition is not 0-good, then $g \geq 2$ and there is a pair, say, C_1, C_2 such that $d(C_1, C_2) \leq 2\mu$. Merging C_1 and C_2 into a single cluster C'_2 , one obtains a partition $S = C'_2 \cup C_3 \cup \dots \cup C_g$ where $d(C'_2) \leq 4\mu$. If this partition is not 1-good, then $g \geq 3$ and one can repeat the merging again. After at most $g - 1$ iterations, one arrives at a good partition. \square

Note that the minimal enclosing boxes of distinct cluster do not overlap, since

$$d(b(C_a), b(C_b)) > 2 \cdot 4^p \mu - 4^p \mu - 4^p \mu = 0.$$

The following is the desired property of the RG decoder.

Lemma 8.5.3. *Let P be any Pauli error with energy barrier $m = \Delta(P)$. Suppose*

$$(160\alpha)^m < L_{tqo}.$$

Then calling the RG decoder on the syndrome $S(P)$ returns a correcting operator P_{ec} such that PP_{ec} is a stabilizer. Thus, the RG decoder corrects P if $\Delta(P) < \frac{\gamma}{\log(160\alpha)} \log L$.

Proof. Let $S = S(P)$ be the syndrome. Let p be the integer such that $2\xi(m) < 2^p \leq 4\xi(m)$. Setting $\mu = 2^p$ in Lemma 8.5.2, S is decomposed into $S = C_1 \cup \dots \cup C_n$ such that $d(C_a) \leq 2^{p'}$ and $d(C_a, C_b) > 2^{p'+1}$ for all $a \neq b$, where p' is an integer such that $p \leq p' < 2m + p$. Since $16m(10\alpha)^m \leq (160\alpha)^m$, Lemma 8.5.1 implies that each C_a is neutral for being a disjoint union of neutral 2^p -connected components. The RG subroutines $EC(s)$ with $s = 0, 1, \dots, p-1$, can only annihilate some neutral 2^s -connected components of C_a , which does not alter the neutrality of C_a . Therefore, the RG decoder from level-0 to p will annihilate each cluster C_a , and hence S at last.

We need to show that $P \cdot P_{ec}$ is a stabilizer, where P_{ec} is the returned correcting operator. Let B_a be the $(10\alpha)^m$ -neighborhood of $b(C_a)$. Our assumptions imply that B_a has diameter smaller than L_{tqo} and distinct B_a 's do not intersect. By construction, the operators P_{ec} and $P \cdot G$ have support in the union $B_1 \cup \dots \cup B_n$. Therefore, $P \cdot G \cdot P_{ec} = Q_1 \cdots Q_n$, where Q_a has support on B_a and has trivial syndrome. Topological order condition implies that Q_a are stabilizers, so is the product. \square

The full hierarchy of the RG decoder is not necessary to correct the error with the low energy barrier. A single level- p error correction with p proportional to $\log L_{tqo}$, will be sufficient. We nevertheless include the hierarchy since in practice it corrects errors with slightly higher (although only by a constant factor) energy barrier at a marginal slowdown of the decoder. If one wishes to apply the decoder against random errors, the hierarchy becomes necessary, as we have discussed in Section 7.5.

Remark 8.1. A closer analysis reveals a simplification of TestNeutral defined in Section 7.2 for the 3D Cubic Code. We defined TestNeutral to return the identity operator if a cluster turns out to be charged. The modified TestNeutral' just applies the broom algorithm and returns recorded operator in any case. It gives the *same* characteristic as stated in the Lemma 8.5.3. $EC'(p)$ using TestNeutral' will transform a charged cluster C_a to a *different* cluster C'_a , but C'_a is still contained in $b(C_a)$. Due to Lemma 8.5.2, $b(C_a)$ do not overlap at a high level p , and $EC'(p)$ will eliminate

neutral clusters at last. This specialized version of RG decoder is used in our numerical simulation in Section 8.7.

8.6 A lower bound on memory time

Theorem 8.1. *For a code Hamiltonian in D spatial dimensions that satisfies TQO1, TQO2, and no-strings rule, there exists a decoder Φ_{ec} and a constant $c, c' > 0$ such that for any inverse temperature $\beta > 0$, any state $\rho(0)$ supported on the ground subspace of H , and any evolution time $t \geq 0$ one has*

$$\epsilon(t) \equiv \|\rho(0) - \Phi_{ec}(\rho(t))\|_1 \leq O(t) \cdot 2^{k(L)} \cdot L^{D-c\beta} \quad (8.20)$$

as long as $L \leq e^{c'\beta}$. The error correction algorithm used by the decoder has running time $\text{poly}(L)$.

Proof. We use the renormalization group decoder of Chapter 7. Its running time is $\text{poly}(L)$. Lemma 8.5.3 guarantees that the supposition of Lemma 8.4.2 is satisfied with $m = \Omega(\log L)$. It remains to bound $\text{Tr} Q_m e^{-\beta H}$ from above, where H has ground energy equal to 0 by convention and Q_m is the projector onto the space of energy m or higher. The number of states of exactly n defects, is $2^{k(L)}$ times the number of configurations of n defects, the latter of which is upper bounded by the binomial coefficient $\binom{rL^D}{n}$ where r is the maximum number of terms in the Hamiltonian that acts on an elementary cube. (In case of the cubic code, $r = 2$.) Therefore,

$$\begin{aligned} \epsilon(t) &\leq O(tL^D) 2^k \sum_{n \geq m} \binom{rL^D}{n} e^{-\beta n} \\ &= O(tL^D) 2^k e^{-\beta m/2} \sum_{n \geq m} \binom{rL^D}{n} e^{-\beta n + \beta m/2} \\ &\leq O(tL^D) 2^k e^{-\beta m/2} \sum_{n \geq m} \binom{rL^D}{n} e^{-\beta n/2} \\ &\leq O(tL^D) 2^k e^{-\beta m/2} \left(1 + e^{-\beta/2}\right)^{rL^D} \end{aligned} \quad (8.21)$$

As long as $rL^D \leq e^{\beta/2}$ the entropy contribution is bounded by a constant. Since $m = \Omega(L)$, the proof is complete. \square

Clearly, our bound is most useful when $k(L)$ is small. In the following we shall mostly be interested in the smallest ground-state degeneracy, $k(L) = 2$. This happens for any odd $3 \leq L \leq 200$ such that L is not a multiple of 15 or 63. In fact, there exists an infinite sequence of lattice sizes such that $k(L) = 2$, for example, $k(2^p + 1) = 2$ for all $p \geq 1$ by Corollary 5.3.2.

On the other hand, this requirement seems unnecessary; we believe that the 2^k factor should be removable. A very rough argument is as follows. Once we fix a ground state at $t = 0$, the interaction

with the thermal bath turns the system into an ensemble, which is likely to be supported on the states above the fixed ground state. Eq. 8.20 can be viewed as a probability estimation that the system has visited a high energy state above the logarithmic cutoff, below which topological sectors are unambiguously told. Since quantum tunneling to another sector is highly suppressed by the macroscopic code distance, the system would not be aware of the other topological sectors.

The upper bound on the storage error can be easily translated to a lower bound on the memory time. Indeed, if one is willing to tolerate a fixed storage error ϵ , say $\epsilon = 0.01$, the memory time T_{mem} can be defined as the smallest $t \geq 0$ such that $\epsilon(t) \geq \epsilon$. Assuming that the lattice size is chosen such that $k(L) = 2$, Theorem 8.1 implies that

$$T_{mem} \geq L^{c\beta-3} \quad \text{if } L \leq e^{c'\beta}. \quad (8.22)$$

Here we neglected the overall constant coefficient. It shows that for low temperatures, $\beta \gg 1$, and sufficiently small system size, $L \ll e^{c'\beta}$, the memory time grows with L according to a power law whose exponent is proportional to β . To the best of our knowledge, this provides the first realistic example of a topological memory with a self-correcting behavior. Unfortunately, the bound is not conclusive in the thermodynamic limit. At the optimally chosen lattice size, the maximum memory time $T_{mem}(\beta)$ achievable at a given temperature β is easily found from Eq. (8.22):

$$T_{mem}(\beta) \geq e^{cc'\beta^2} \quad (8.23)$$

for $\beta \gg 1$. For comparison, the memory time of the 2D toric code model grows only exponentially with β [10, 124]. Depending on the value of the constant cc' and the temperatures realizable in experiments, the scaling Eq. (8.23) may be favorable enough to achieve macroscopic memory times.

The restriction $L \ll e^{c'\beta}$ implies that the average number of defects (flipped stabilizers) in the equilibrium Gibbs state $\rho_\beta \sim e^{-\beta H}$ is small, that is, the Gibbs state has most of its weight on the ground subspace of H . This might suggest that the thermal noise is irrelevant in the studied regime. However, this is not the case. If the evolution time is large enough, so that $\rho(t) \approx \rho_\beta$, the encoded information cannot be retrieved from $\rho(t)$, since ρ_β does not depend on the initial state. If a time $t \sim e^{\Omega(\beta^2)}$ has elapsed, the system would have accommodated approximately $tL^3 e^{-\beta} \sim e^{\Omega(\beta^2)}$ defects during the evolution. This implies in particular that the system has endured $e^{\Omega(\beta^2)}$ errors which becomes significant for low temperatures.

8.7 Numerical simulation

Since Theorem 8.1 only provides a lower bound on the memory time, a natural question is whether this bound is tight and, if so, what is the exact value of the constant coefficient c ? To answer this

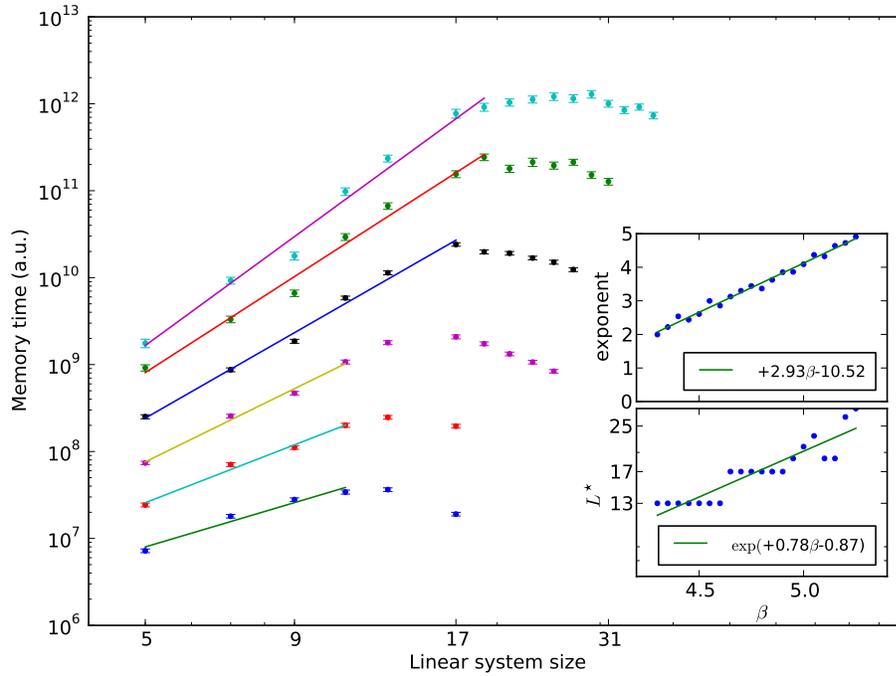


Figure 8.1: The memory time T_{mem} vs. the system size L . In the upper inset is shown the exponent of the power law fit of T_{mem} for the first a few system sizes. It is clear that $T_{mem} \propto L^{2.93\beta-10.52}$ when $L < L^*$, where L^* is the optimal system size where T_{mem} reaches maximum. The data for $\beta = 4.3, 4.5, 4.7, 4.9, 5.1, 5.25$ are shown.

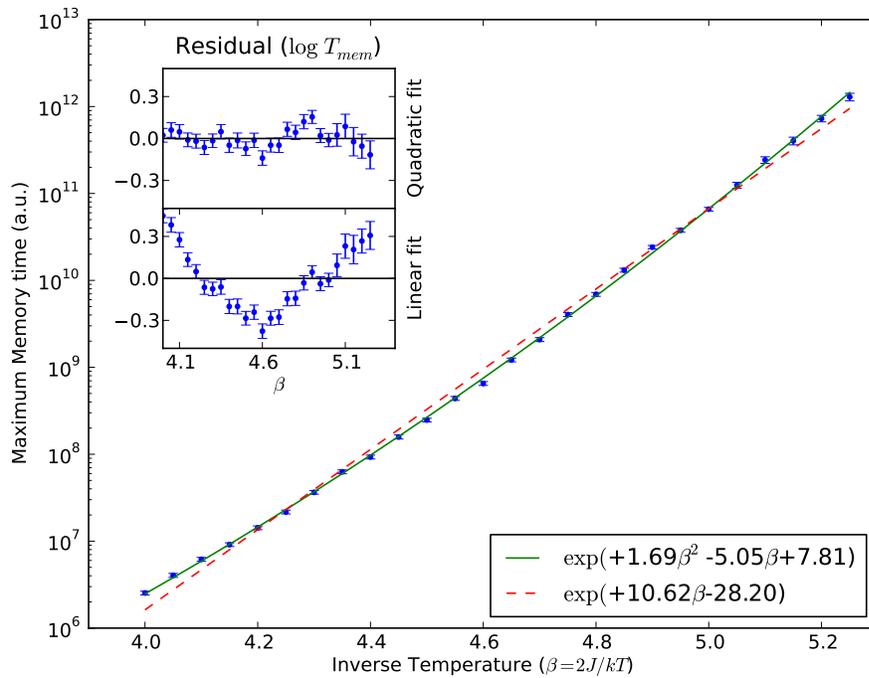


Figure 8.2: The maximum memory time T_{mem} vs. the inverse temperature β . The memory time is maximized with respect to the system size. The logarithm of T_{mem} clearly follows a quadratic relation with β as opposed to a linear one.

question, the memory time of the 3D cubic code has been computed numerically for a range of β 's and L 's. It should be emphasized that both Theorem 8.1 and our numerical simulation use the *same* decoder at the read-out step. The numerical results strongly suggest that our analytical bound is tight up to constant coefficients for our renormalization group decoder. See Figure 8.1,8.2. It suggests that $T_{mem} \approx L^{2.93\beta-10.52}$ as long as $L \leq L^* \approx e^{0.78\beta-0.87}$. The number 0.78 in the estimate of L^* should not be taken too seriously, as one sees in the inset that the dependence of L^* on β is hard to tell quantitatively. It is clear, however, that L^* is increasing with the inverse temperature.

The interaction of the memory system with a thermal bath is simulated by Metropolis evolution. As we wish to observe low temperature behavior we adopt continuous time algorithm by Bortz, Kalos, and Lebowitz (BKL) [132]. A pseudo-random number generation package `RngStream` by L'Ecuyer [133] was used. As before, the coupling constant in the Hamiltonian is set to $J = \frac{1}{2}$ so a single defect has energy 1. Although the cubic code is inherently quantum, it is relevant to consider only X -type errors (bit flip) in the simulation, thanks to the duality of the X - and Z -type stabilizer generators of the cubic code. The simulation thus is purely classical. The errors are represented by a binary array of length $2L^3$, and the corresponding syndrome by a binary array of length L^3 .

The memory time is measured to be the first time when the memory becomes unreliable. There are two cases the memory is unreliable: either the broom algorithm fails to remove all the defects so we have to reinitialize the memory, or a nontrivial logical error is occurred. It is thus necessary in our simulation to keep track of the error operator during the time evolution. In fact, most of the time, it was the broom algorithm's failure that made the memory unreliable. Nontrivial logical errors occurred only for very small system sizes $L = 5, 7$.

It is too costly to decode the system every time it is updated. Alternatively, we have performed a trial decoding every fixed time interval

$$T_{ec} = \frac{e^{4\beta}}{100}$$

where β is the inverse temperature. Although the time evolution of the BKL algorithm is stochastic, a single BKL update typically advances time much smaller than T_{ec} . So it makes sense to decode the system every T_{ec} . The exponential factor appears naturally because BKL algorithm advances time exponentially faster as β increases. It is to be emphasized that we do not alter the system by the trial decodings (a copy of the actual syndrome has been created for each trial decoding).

The system sizes L^3 for the simulation are chosen such that the code space dimension is exactly 2, for which the complete list of logical operators is known. If the linear size L is ≤ 200 , this is the case when L is not a multiple of 2, 15, or 63 by Corollary 5.3.2. For these system sizes, to check whether a logical operator is nontrivial is to compute the commutation relation with the known nontrivial logical operators.

The measured memory time for a given L and β is observed to follow an exponential distribution; a memory system is corrupted with a certain probability given time interval. Specifically, the probability that the measured memory time is t is proportional to $e^{-t/\tau}$. Thus the memory time should be presented as the characteristic time of the exponential distribution. We choose the estimator for the characteristic time to be the sample average $\bar{T} = \frac{1}{n} \sum_i^n T_i$. The deviation of the estimator will follow a normal distribution for large number n of samples. We calculated the confidence interval to be the standard deviation of the samples divided by \sqrt{n} . For each L , 400 samples when $\beta \leq 5.0$ and 100 samples when $\beta > 5.0$ were simulated. The computation was performed on IBM Blue Gene/P using 512 cores located in IBM T. J. Watson Research Center, Yorktown Heights, New York. The result is summarized in Figure 8.1,8.2.

Figure 8.2 clearly supports $\log T_{mem} = c\beta^2 + \dots$. Figure 8.1 demonstrates the power law for small system size:

$$T_{mem} \propto L^{2.93\beta - 10.5}$$

We wish to relate some details of the model with the numerical coefficients. The rigorous analysis of the previous section, gives a relatively small coefficient c of the energy barrier for correctable errors by our RG decoder. However, we expect that the coefficient of β in the exponent is the same as the constant c that appear in the energy barrier

$$E = c \log_2 R$$

to create an isolated defect separated from the other by a distance R . This is based on an intuition that the output P' of the decoder would have roughly the same support as the real error P for the most of the time, provided that the error has energy barrier less than $\Delta = c \log_2 L_{tqo}$. Thus, an error of energy barrier less than Δ would be corrected by the decoder. Our empirical formula supports this intuition. It suggests that $c = 2.93 \log 2 = 2.03 \sim 2$.

Indeed, we can illustrate explicitly an error path that separates a single defect from the rest by distance 2^p during which only $2p + 4$ defects are needed. Consider an error of weight 2 that creates 4 defects as shown in the top of Fig. 8.3. We call it the *level-0 hook*. The bottom sequence depicts a process to create a configuration shown at the bottom-left, which we call *level-1 hook*. One sees that level-1 hook is similar with ratio 2 to level-0, and is obtained from level-0 with extra 2 defects. One defines level- p hooks hierarchically. We claim that a level- p hook can be constructed from the vacuum using $2p + 4$ defects. The proof is by induction. The case $p = 1$ is treated in the diagrams. Suppose we can construct level- p hook using $2p + 4$ defects. Consider the 2^{nd} , 4^{th} , 6^{th} , and 8^{th} steps in Fig. 8.3. They can be viewed as a minuscule version of level- p steps that construct a level- $(p + 1)$ hook from the level- p hooks. It requires at most $2p + 4 + 2$ defects to perform the level- p step; this completes the induction.

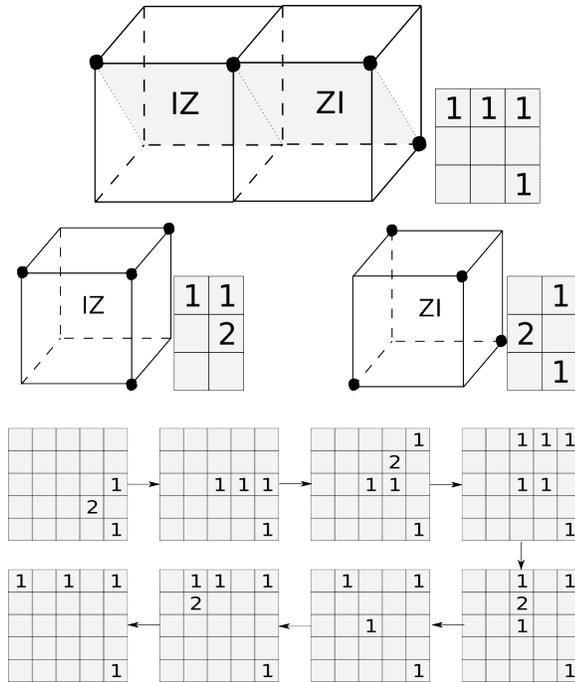


Figure 8.3: Construction of a hook of level 2 from the vacuum. The grid diagram represents the position and the number of defects in the $(x = z)$ -plane. For each transition, an operator of weight 1 is applied. The total number of defects never exceeds 6. From a level-0 hook (the second diagram in the sequence), a level-1 hook (the last in the sequence) is constructed using extra 2 defects.

It may not be obvious whether a high level hook corresponds to a nontrivial logical operator, but such a large hook is bad enough to make our decoder to fail.

Appendix A

Commutative algebra

We briefly review algebraic concepts and tools used in this thesis, mainly in Chapter 3 and 4. There are many nice textbooks including those by Lang [60], Atiyah and MacDonald [80], and Eisenbud [76]. The book by Lang is a comprehensive textbook covering a wide range of topics in abstract algebra. The book by Atiyah and MacDonald explains commutative algebra that may look too concise, but precisely for this reason it is very useful as a reference. Examples are rare but essential. The book by Eisenbud is also on commutative algebra and is extensive. It covers more material than Atiyah-MacDonald. In particular, our summary of Gröbner basis follows Eisenbud. The chapter on Gröbner basis appears in the middle of the book, but is relatively self-contained and elementary. Here, we will omit many proofs and not try to be fully rigorous. We explain theorems to the point where intuition can be developed. Rigorous proofs can be found in one of the three books.

We start by recalling definitions for abelian groups. An abelian group G with the identity element denoted by 0 is a set with an operation $+$: $G \times G \rightarrow G$ such that $g + g' = g' + g$ and $0 + g = g$. It is required for G to have inverses of g denoted by $-g$ such that $g + (-g) = 0$. n -fold sum of g is simply denoted as ng , where $n \in \mathbb{Z}$. Given two abelian groups G and H , we can form a direct sum $G \oplus H$. It is the set of all tuples (g, h) , where $g \in G$, $h \in H$, and the group operation $+$ is defined as $(g, h) + (g', h') = (g + g', h + h')$. We can form a **direct sum** $\bigoplus_{\alpha} G_{\alpha}$ of arbitrary family $\{G_{\alpha}\}$ of groups. It is the set of all indexed collections of group elements (g_{α}) where only *finitely many* g_{α} are nonzero. The group operation is again defined component-wise. Thus, any element in the direct sum is a sum of finitely many $g_{\alpha} \in G_{\alpha}$. A sum of two abelian groups can be defined if they are subgroups of a parent group. If $A, B \leq C$ are subgroups, the **sum** $A + B$ is the group of all elements of C of form $a + b$ where $a \in A$ and $b \in B$. Note that $A + B \cong A \oplus B$ if and only if $A \cap B = 0$. Given a subgroup $N \leq G$, we can form a quotient group G/N , the set of all equivalent classes under the equivalence relation $[g] = [g']$ iff $g - g' \in N$. In commutative algebra, almost everything is an abelian group. On top of the abelian (additive) group structure, a new “multiplication” is added.

A.1 Rings and homomorphisms

The set of integers $\dots, -2, -1, 0, 1, \dots$ admits two operations, addition and multiplication. There is 0 that has no effect under addition, and 1 that has no effect under multiplication. One can always undo the addition because one can subtract a number. However, the multiplication is not invertible within the set of integers because fractions are not integers. One convenient thing is that the multiplication does not care about the order. A commutative ring is an abstraction of this structure. It is a set, in which one can add and subtract. A multiplication exists but is not in general invertible. An additive identity 0 exists, and a multiplicative identity 1 exists. The distribution law $a(b+c) = ab+ac$ is assumed, and the multiplication is commutative $ab = ba$. A ring R can consist of a single element, in which case R is called a zero ring, if and only if $0 = 1$. Indeed, if $a \in R$ and $1 = 0 \in R$, then $a = a \cdot 1 = a \cdot 0 = a \cdot (0+0) = a \cdot (1+1) = a+a = 0$. Examples of rings are abundant: The set of all integers, the set of all complex numbers, the set of all square diagonal matrices of a fixed size, the set of polynomials, the set of all differentiable functions on a real line, the set of all continuous real-valued functions on a manifold, etc. Is the set of all even integers a ring? No. Some authors define rings to include this case where the multiplicative identity 1 is not provided, but we avoid this case. Any ring is with 1. Note that 1 is unique; if $1'$ is also a multiplicative identity, then $1 = 1 \cdot 1' = 1'$. The same is true for 0.

A ring is always understood in terms of relations with other rings. Given two rings A and B we consider a restricted class of maps between them. That is, we require that the map obeys the ring structure of the rings. $f : A \rightarrow B$ is a **homomorphism** if $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in R$. In addition, we assume $f(0) = 0$ and $f(1) = 1$. (“morph” means “shape.”) The $+$ or the omitted \cdot between a and b in ab on the left-hand side are the operations defined in A , whereas those in the right-hand side are in B . The **image** of a homomorphism f is the subset of B written as $f(A)$ defined by $\{f(a) \mid a \in A\}$. Is the image of a homomorphism a ring? Yes.

There is no point to speak of a map between two rings A, B that is not a homomorphism. If we are going to ignore the ring structure, we would rather say the map between the “sets” A, B . We will simply say a **map between rings** to mean a homomorphism. We note more terminologies: An **endomorphism** is a map from a ring into itself. An **isomorphism** is a map between two rings with a unique inverse. An **automorphism** is an isomorphism that is an endomorphism.

The ring of integers is so primitive in the following sense. Let A be an arbitrary ring. Consider a map $f : \mathbb{Z} \rightarrow A$. $f(n) = \sum_{i=1}^n f(1)$ and $f(-n) = \sum_{i=1}^n (-f(1))$ where $n > 0$. But, $f(1) = 1$ is the unique multiplicative identity. Therefore, f is completely determined, though we just required f be a homomorphism; there is a unique nonzero map from \mathbb{Z} into any ring. How many endomorphisms are there for \mathbb{Z} ?

The **kernel** of a map (homomorphism!) f is the subset of A written as $\ker f$ defined by $\{a \in A \mid f(a) = 0\}$. It is easy to see that the kernel is closed under the addition and multiplication. Here, the closeness means that the result of the operation using two elements in a subset lies in the subset. (It is pointless to speak of the closedness of an operation without reference to a subset.) There is one more important property as we discuss below.

A.2 Ideals and modules

The kernel I of a map f between rings $R \rightarrow S$ has the following property:

$$\forall r \in R, \forall x \in I : rx \in I \tag{A.1}$$

This is easily verified since $f(rx) = f(r)f(x) = f(r) \cdot 0 = 0$. When a subset I of a ring R is closed under the multiplication and addition, and satisfies the above property, we call I to be an **ideal** of R . For example, in \mathbb{Z} , the set of all even numbers is an ideal denoted as (2) . The property (A.1) is trivial, because it reads a multiple of an even number is even. This ideal is the kernel of the map $\mathbb{Z} \rightarrow \mathbb{Z}/(2)$, where the latter is the ring of integers modulo 2. Remember that there is a unique nonzero map from \mathbb{Z} to any ring. In fact, any ideal arises in this way: An ideal is the kernel of a ring homomorphism.

To understand this, we need to formalize how to construct **quotient rings** or **factor rings**. Let R be a ring and I be an ideal. They are both abelian groups; they are closed under the addition with identity 0, and contains additive inverses, the minus elements. The quotient ring R/I as a set is the same as the quotient group as an abelian group. R/I is the family of equivalence classes under the equivalence relation that $[a] = [b] \in R/I$ iff $a - b \in I$. The multiplication in R/I is as expected: $[a] \cdot [b] = [ab]$. Using the property (*) one can verify that it is well-defined. Consider a map $R \rightarrow R/I$ defined by $a \mapsto [a]$. It should be straightforward that it is a ring homomorphism. What is the kernel? Precisely, I . Now it is an almost tautology that an ideal is a kernel of a ring homomorphism. Often, we just write a in place of the equivalence class notation $[a]$. In this lazy notation, “the map $R \rightarrow R/I$ is defined by $a \mapsto a$.” This map is so important that it has its own name: **canonical map** or **quotient map**.

In leisurely words, an ideal extends what we treat as zeros; any element of I is zero in R/I . Zero plus zero or zero times zero must be zero, so I is closed under the addition and multiplication. Zero times any element must be zero, so the property (A.1) should hold. How do we specify an ideal in a real calculation? Consider a polynomial ring $\mathbb{Q}[x]$, the set of all polynomials (of finitely many terms) in x with coefficients in the rational numbers. Suppose we decided that x must be equal to $\frac{1}{2}$. In other words, we decided that $x - \frac{1}{2}$ must be “zero” in $\mathbb{Q}[x]/I$. Then, as zero times anything

must be zero, any element $(x - \frac{1}{2}) \cdot f(x)$ must be zero in $\mathbb{Q}[x]/I$, too; it must be an element of the ideal we are defining. We require no more elements are identified as zeros. That is, we define $I = \{f(x)(x - \frac{1}{2}) \mid f(x) \in \mathbb{Q}[x]\}$ as our ideal, and carry out any computation in the quotient ring $\mathbb{Q}[x]/I$. We write I as $(x - \frac{1}{2})$ by putting the **generator** inside the parenthesis. Computing in $\mathbb{Q}[x]/I$ is the same as computing in $\mathbb{Q}[x]$ and evaluate the polynomial at $x = \frac{1}{2}$.

In general, if we write an ideal I of R as (a, b, c) , then we mean

$$I = \{ax + by + cz \mid x, y, z \in R\}.$$

I is said to be **generated by** a, b, c . A quick exercise: What is $\mathbb{Q}[x]/(x - \frac{1}{2}, x - 1)$? It is a zero ring. Since $x - \frac{1}{2}$ and $x - 1$ are “zeros,” their difference $\frac{1}{2}$ is zero. Zero times 2 is zero, so 1 is zero. Therefore, everything is zero. We proved an ideal equality $(x - \frac{1}{2}, x - 1) = (1)$. The whole ring R viewed as an ideal is called the **unit ideal** denoted by (1) . In fact, when there is any invertible element in an ideal, it is the unit ideal. For this reason, an invertible element in a ring is called a **unit**. Note that computing the minimal set of generators is in general a hard problem. For instance, I do not know any algorithmic answer to questions like “can this ideal be generated by three elements?” However, the Gröbner basis gives a *canonical* set of generators for an ideal of a polynomial ring, and we can algorithmically compare two ideals.

Prime, maximal

There is a very important class of ideals that generalizes prime numbers in \mathbb{Z} . A prime number p has a property that if p divides a product of two integers ab then p divides either a or b . A **prime**¹ ideal \mathfrak{p} of R is an ideal not equal to (1) such that

$$ab \in \mathfrak{p} \text{ implies } a \in \mathfrak{p} \text{ or } b \in \mathfrak{p} \text{ for any } a, b \in R. \tag{A.2}$$

The condition is rephrased as $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$ imply $ab \notin \mathfrak{p}$. Is the ideal $(0) = \{0\}$ prime? It depends. In \mathbb{Z} the zero ideal is prime because the product of two nonzero integers is nonzero. In the polynomial ring $\mathbb{Q}[x]$, (0) is prime because the degree of nonzero polynomial does not decrease under any nonzero multiplication. If any nonzero elements of a nonzero ring R has a multiplicative inverse, in which case R is called a **field**, then (0) is prime because $ab = 0$ means $a = 0$ or $b = 0$. However, in the ring of diagonal 2×2 matrices, (0) is not prime because nonzero matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ multiply to zero. The ring in which (0) is prime has a special name, **(integral) domain**. It is easy to verify that R/\mathfrak{p} is an integral domain if and only if \mathfrak{p} is prime, applying the picture that \mathfrak{p} defines zeros in R/\mathfrak{p} .

¹Do not use “primary” in place of “prime.” The adjective “primary” has a slightly different technical meaning.

There is one more important property of prime ideals. Let $f : A \rightarrow B$ be a map between two rings. If $\mathfrak{p} \subseteq B$ is a prime ideal, then $I = f^{-1}(\mathfrak{p}) \subseteq A$ is prime. Proof: $aa' \in I \Rightarrow f(a)f(a') \in \mathfrak{p} \Rightarrow f(a) \in \mathfrak{p} \vee f(a') \in \mathfrak{p} \Rightarrow a \in I \vee a' \in I$.

A subclass of prime ideals consists of maximal ideals. A **maximal ideal** $\mathfrak{m} \neq (1)$ is defined by the maximal property:

$$\mathfrak{m} \subsetneq \mathfrak{m}' \text{ implies } \mathfrak{m}' = (1) \text{ for any ideal } \mathfrak{m}'. \quad (\text{A.3})$$

It is a priori not vivid why maximal ideals are prime. But it is easy to see. Consider R/\mathfrak{m} . If $a \in R/\mathfrak{m}$ is nonzero, that is $a \notin \mathfrak{m}$, then $I = (\mathfrak{m}, a) \supsetneq \mathfrak{m}$ and therefore $I = (1)$, which means there is an element $b \in R$ such that $ba + m = 1$ for some $m \in \mathfrak{m}$. By the canonical map, b maps to a multiplicative inverse of a in R/\mathfrak{m} . (The converse is also true. $\mathfrak{m} \neq (1)$ is a maximal ideal if and only if R/\mathfrak{m} is a field.) In other words, R/\mathfrak{m} is a field, and therefore an integral domain. In particular, \mathfrak{m} is prime.

Modules

Ideals admit another viewpoint. Let us forget the multiplication within an ideal I , and treat I as a separate set from the mother ring R . It is still an abelian group, and satisfies (A.1). The condition (*) looks very similar to the scalar multiplication on vector spaces. Indeed, consider a direct sum $R \oplus R$ of abelian groups, the set of all tuples (r, r') where $r, r' \in R$ are any elements. There is an operation on $R \oplus R$ similar to (A.1); we can define $r \cdot (s, s')$ to be (rs, rs') , similar to the scalar multiplication for a vector space. Indeed, a two-dimensional vector space is precisely obtained in this way by setting $R = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, etc.

Let us define an abstract notion. Let M be an abelian group with a *bilinear* operation \cdot such that

$$\forall r \in R, \forall m \in M : r \cdot m \in M. \quad (\text{A.4})$$

The “multiplication” \cdot here is not the same thing as the multiplication within the ring. We assume expected formulas $(rs) \cdot m = r \cdot (s \cdot m)$, and simply write $(rs) \cdot m = rsm$ where $r, s \in R$ and $m \in M$. We call M an **R -module** or a **module over R** . It is general than the notion of vector spaces. A vector space is a module over a **field**, a commutative ring in which multiplication by a nonzero element has an inverse. An ideal is a subset of R such that it is a module over R .² Note that R itself is an R -module via the multiplication within R . The above example $R \oplus R$ is an R -module.

For an R -module M if there exist finitely many elements $m_1, \dots, m_n \in M$ such that

$$M = \{r_1 m_1 + \dots + r_n m_n \mid r_1, \dots, r_n \in R\}, \quad (\text{A.5})$$

² Although an ideal is a valid module, often it is treated differently than a module. One should sometimes be careful to apply things defined for modules, especially when one reads the dimension theory of Eisenbud [76].

then we say M is **finitely generated**. All of our modules in the thesis are finitely generated. An ideal is finitely generated if it is finitely generated as a module.

There is a confusingly similar terminology that one must distinguish. Suppose A is a subring of B . That is, A is a ring by itself and contained in a bigger ring B . Or slightly more generally, suppose we are given a ring map $A \rightarrow B$. The subring case is precisely when the map is an inclusion. We say B is a **finitely generated A -algebra** if there exists finitely many elements $b_1, \dots, b_n \in B$ such that any element of b can be written as a polynomial in b_1, \dots, b_n with coefficients in the image of A . In this case, B is sometimes written as $B = A[b_1, \dots, b_n]$. A typical situation is when A is a field such as \mathbb{Q}, \mathbb{C} and B is a polynomial ring over A . For example, $B = \mathbb{Q}[x, y]$. The reason it is a confusing terminology is because B is not necessarily finitely generated A -module. $\mathbb{Q}[x]$, a finitely generated \mathbb{Q} -algebra, has infinitely many generators $\{1, x, x^2, \dots\}$ as a \mathbb{Q} -module. Is \mathbb{Q} a finitely generated \mathbb{Z} -algebra? No, because multiplying by integers cannot produce large denominators.

As the rings are understood in relation to others, the modules should be understood via maps. We required the ring homomorphisms to preserve the defining operations of the rings. The same is true for the module maps. Given two modules M and N over R , we define an **R -linear map** or **R -module homomorphism** $f : M \rightarrow N$ to satisfy

$$f(m + m') = f(m) + f(m') \quad \text{and} \quad f(r \cdot m) = r \cdot f(m) \quad \text{for any } r \in R, m, m' \in M. \quad (\text{A.6})$$

Note that the \cdot on the left-hand side is the operation (A.4) for M whereas that on the right-hand side is the operation for N .³ The notions of kernel, image, endomorphism, automorphism, and isomorphism apply to module maps, too. A simple exercise: Let A, B be two R -algebras; there are ring maps $R \rightarrow A$ and $R \rightarrow B$. The two algebras are naturally R -modules, when a map $A \rightarrow B$ becomes R -linear? Answer: It becomes R -linear when the following diagram commutes.

$$\begin{array}{ccc} A & \xrightarrow{\quad} & B \\ & \swarrow \quad \searrow & \\ & R & \end{array}$$

Free

An R -module isomorphic to $\bigoplus_{\alpha} R$ is called a **free module**. When there are finitely many summands, it is called **finitely generated free module**. It is the most convenient type of modules. In particular, a module map between finitely generated free R -modules is simply given by a matrix with entries in R , just as linear map between finite dimensional vector space can be described by a matrix with entries in a field. Note that elements of a finitely generated free R -module $M = R^{\oplus n}$ can

³ In group representation theory, the R -linear maps are called equivariant maps, where R is the group algebra which may not be commutative. The representation space is a module, the subrepresentation space is a submodule, and the irreducible representation space is a simple submodule.

be expressed by column matrices. Let e_i ($i = 1, \dots, n$) denote the canonical basis column matrices. (We could say “column vectors” instead of column matrices. However, an element of a module is not a vector in general.) A map f from M to any module is specified if we specify the image $f(e_i)$ because the image of other elements $a_1e_1 + \dots + a_n e_n$ is must be $a_1f(e_1) + \dots + a_n f(e_n)$ by R -linearity. Writing $f(e_i)$ in columns, we have a matrix representation of f . An un-redundant set of generators of a free module is called a **basis**. The cardinality of a basis is called **rank**. (One can show that rank is independent of the choice of a basis.) Only for free modules can we speak of bases. The crucial difference between general modules and vector spaces is that a module is in general not free, while a vector space, a module over a field, is always free. That nonzero elements are invertible makes such a huge difference.

Note that any module can be described by free modules. Take a **generating** set $\{m_\alpha\}$ of a module M ; any element of M is a *finite* R -linear combination $\sum_i r_{\alpha_i} m_{\alpha_i}$. A trivial and useless choice would be to take whole M as a generating set. Let F be a free R -module whose rank is the same as the cardinality of the generating set, i.e., there is a surjective module map $F \rightarrow M$. The kernel N is a submodule of F , not necessarily free, and $M \cong F/N$. One can carry the same process for the module N . That is, one finds a free module F' such that $\phi : F' \rightarrow N$ is a surjection. Now M is expressed as $M \cong F/\text{im } \phi$. This is conceptually important observation, but not too useful because we do not have any control over the ranks of F and F' . We need some finiteness conditions. An R -module M is said to be **finitely presented** if there is a map $\phi : F' \rightarrow F$ between finitely generated free modules such that $M \cong F/\text{im } \phi$. The latter expression $F/\text{im } \phi$ is often abbreviated as $\text{coker } \phi$. The map ϕ is called a **finite presentation** of M . As we have seen above, ϕ is a matrix with entries in R , and M is expressed by a single matrix ϕ . In case of a finite dimensional vector space, ϕ can always be brought to a diagonal matrix with entries of 0 or 1, after basis change of F and F' . We will discuss more on a finite presentation in Section A.5.

Noetherian

A technically very important and convenient adjective is Noetherian. It is as important as vector spaces having finite dimensions. A **module M is Noetherian** if every increasing sequence of submodules is stationary, i.e., if $M_1 \leq M_2 \leq \dots \leq M_n \leq \dots$ is a sequence of submodules of M , then for all sufficiently large n one has $M_n = M_{n+1}$. Often this condition is referred to as the **ascending chain condition** or **a.c.c.** *A module M is Noetherian if and only if any submodule is finitely generated.* If a submodule cannot be generated by finitely many elements, one can construct a strictly increasing infinite sequence of submodules using an infinite subset of generators. Conversely, if any submodule of M is finitely generated, then the union $\cup_{i=1}^{\infty} M_i$ of any increasing sequence of submodules M_i of M is also finitely generated, say, by m_1, \dots, m_r . Since m_j is contained in some $M_{j'}$, there must be some k such that $m_1, \dots, m_r \in M_k$. It follows that $M_k = M_{k'}$ for all $k' \geq k$. A

Noetherian module over a field is just a finite dimensional vector space. A **Noetherian ring** R is a ring that is Noetherian as an R -module, i.e., the a.c.c is satisfied with respect to the ideals of R . In a Noetherian ring, any ideal is finitely generated.

Being Noetherian is preserved in many cases. Loosely speaking, it says that a module carries a finite amount of data. A module with a finite amount data manipulated finitely many times would still have a finite amount of data. The following are facts:

- *A homomorphic image of Noetherian ring (module) is a Noetherian ring (module).*
- *A submodule of Noetherian module is Noetherian.*
- *A finitely generated algebra over a Noetherian ring is a Noetherian ring.*
- *In particular, a polynomial ring over a field with finitely many variables is a Noetherian ring.*
- *A finitely generated module over a Noetherian ring is Noetherian.*

There are more to mention about being Noetherian using tensor products and localization. See Section A.4.

Remark that a finitely generated module M over a Noetherian ring R always admits a finite presentation $\phi : F' \rightarrow F$. Since M is finitely generated, the module F is of finite rank. F is Noetherian, and therefore, $\text{im } \phi$ is finitely generated, which means F' can be taken to be of finite rank. The “matrix” ϕ is of finite size.

Is the ring of all differentiable functions $\mathbb{R} \rightarrow \mathbb{R}$ Noetherian? No. Is the ring of all trigonometric functions $\mathbb{R} \rightarrow \mathbb{R}$ of period $1/n$, where n are positive integers, Noetherian? Yes.

A.3 Gröbner basis

Gröbner basis is a special generating set for ideals and modules. It provides canonical presentations of modules and ideals, from which any concrete computational commutative algebra is built. In all notions in the previous section, I cannot imagine any systematic way to compute things concretely without Gröbner basis. It is theoretically important too because it tells what is actually constructible. A nice application of the Gröbner basis is a sharp version of Hilbert syzygy theorem [76, Corollary 15.11]. In this section we *assume the (base) ring is a polynomial ring over a field \mathbb{F} with finitely many variables; $R = \mathbb{F}[x_1, \dots, x_n]$* . Since R is Noetherian, for any ideal there is a finite set of generators.

How do ideals look like in \mathbb{F} ? There are only (0) and (1) because any nonzero element is a unit. How about $\mathbb{F}[x]$? It is only slightly more complicated. By the Euclidean algorithm, the gcd of two

polynomials $f(x)$, $g(x)$ can be expressed as

$$\gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x) \in (f(x), g(x))$$

An ideal generated by $f(x)$ and $g(x)$ is thus the same as an ideal generated by a single element $\gcd(f(x), g(x))$, in which case the ideal is called **principal**. By induction, one can always reduce the number of generators of an ideal in $\mathbb{F}[x]$ if it is greater than 1. Since $\mathbb{F}[x]$ is Noetherian, this is enough to imply that *any ideal of $\mathbb{F}[x]$ is generated by a single element*, i.e., *any ideal of $\mathbb{F}[x]$ is principal*. The principal generator $p(x)$ is important, not only because it is simple, but also because it gives a criterion whether an arbitrary polynomial $h(x)$ is contained in $(p(x))$: Divide the $h(x)$ by $p(x)$. The remainder is zero if and only if $h(x) \in (p(x))$. Put differently, we can find a canonical representative in the quotient ring $\mathbb{F}[x]/(p(x))$ to be the remainder $r(x)$ where $\deg r < \deg p$. The $p(x)$ is the Gröbner basis for the ideal $(p(x))$ in $\mathbb{F}[x]$.

In case of two or more variables, it is no more true that any ideal is principal. Let us examine the **division algorithm**. Let $f(x)$ be a dividend and $p(x)$ be a divisor. We first compare degrees of them. If $\deg f < \deg p$, then the division is completed, and f is the remainder. Otherwise, we match the leading coefficients and then subtract a multiple $a(x)p(x)$ from $f(x)$. $a(x)$ is a monomial such as $3x^2$. The purpose is of course to have $\deg(f - ap) < \deg f$. And then we iterate. Essential is a total ordering among terms such that the ordering is preserved under multiplication by a monomial. Now we consider a problem of computing the remainder of f modulo $G = \{g_1, \dots, g_k\}$. Equipped with the ordering, given a dividend f and a set G of divisors, (Step-1) one should be able to match the leading term and kill it, thereby “reduce” the leading term of the dividend. (Step-2) One stops when the reduction becomes impossible. A question arises. During Step-1, there would be many possible choices among the divisors from G . How do we guarantee that the remainder is independent of the choices? This is a sound question, and the answer is no in general. Even in the one variable case, the answer is no in general. Consider $f = x^2 - 1$, $g = x^3 - 1$ in $\mathbb{Q}[x]$. The division by the set $\{f, g\}$ of a dividend x^3 gives 1 if we kill the leading term by $x^3 - 1$, or x by $x^2 - 1$.

We formulate the problem as finding a generating set of an ideal I that gives rise to a unique remainder under the division. A solution is that we include more and more elements of I into a generating set G so that any leading term l of a dividend can be removed where l appears as a leading term of some elements of I . In the one variable case, it is enough to include the gcd of all (finitely many) generators of I . We have given enough motivation and technical problems to smooth out.

Definitions

A monomial is a product of variables. A **monomial order** on the set of all monomials of $R = \mathbb{F}[x_1, \dots, x_n]$ is a total ordering \succ , under which any two monomials are comparable, such that

$$x_i m \succ x_i m' \succ m' \quad \text{whenever} \quad m \succ m' \quad (\text{A.7})$$

for any monomial m, m' and any variable x_i . Since a monomial $x_1^{a_1} \cdots x_n^{a_n}$ is uniquely given by a n -tuple of nonnegative integers $(a_i) = (a_1, \dots, a_n)$, a monomial order is a total order on the hyper-octant of \mathbb{Z}^n of nonnegative coordinates. Note that under any monomial order, 1 is the least monomial.

Two examples at least are important. The first one is the **lexicographic order**, under which $(a_i) \succ (b_i)$ if and only if $a_i > b_i$ for the least i such that $a_i \neq b_i$. For example,

$$x_1 \succ_{\text{lex}} x_2^5 \succ_{\text{lex}} x_2 x_3^{100}.$$

The second example is the **degree reverse lexicographic order**, under which $(a_i) \succ (b_i)$ if and only if ‘ $\sum a_i > \sum b_i$ ’ or ‘ $\sum a_i = \sum b_i$ and $a_i < b_i$ for the largest i such that $a_i \neq b_i$.’ For example,

$$\begin{aligned} x_1 \succ_{\text{revlex}} x_2 \succ_{\text{revlex}} \cdots \succ_{\text{revlex}} x_n \\ x_3^{100} \succ_{\text{revlex}} x_2^{50} \succ_{\text{revlex}} x_1^{49} x_3. \end{aligned}$$

The degree reverse lexicographic order is the most commonly used in computer software.

Any monomial order is a well-order, i.e., every set of monomials has a minimal element. This statement is at the core of any finiteness proof regarding Gröbner basis. The proof is very simple. Let X be any set of monomials of R . The submodule (ideal) generated by X is finitely generated by G because R is Noetherian. It means X consists of multiples of a finitely many monomials of G . Therefore, the minimal element of G , a finite set, is the minimal element of X . The statement can be rephrased as *any decreasing sequence of monomials is stationary* or as *any strictly decreasing sequence of monomials is finite*.

With a monomial order, we can define the **leading term** or **initial term** of a polynomial f which is the greatest term of f with respect to the monomial order. (We are distinguishing “term” and “monomial.” A monomial is a product of variables only, and a term is \mathbb{F} -multiple of a monomial.) Let us denote the leading term of f by $\text{lt}(f)$. Given any set S of R , let the ideal generated by all leading terms of element of S be denoted by $\text{lt}(S)$. Now, a **Gröbner basis** G of I is a generating set of I such that $\text{lt}(I) = \text{lt}(G)$. Since R is Noetherian, $\text{lt}(I)$ is finitely generated. Therefore, G can be chosen to be a finite set.

Buchberger criterion

The division by a Gröbner basis results in a unique remainder. In particular, a polynomial is in I if and only if the division by a Gröbner basis yields the zero remainder. To see this, let f be an arbitrary polynomial. Let r be a remainder obtained by killing large terms of f by elements of G . Let r' be another remainder. We must show $r = r'$. It is clear that $r - r'$ belongs to I . If nonzero, the leading term of $r - r'$ belongs to $\text{lt}(I) = \text{lt}(G)$. However, r or r' has by construction no leading term that belongs to $\text{lt}(G)$. Therefore, $r - r'$ must be zero.

It is not clear yet how G can be computed from given generators of I , though we know a solution in the case where the generators of I are in a single variable. A strategy is hinted from one-variable case:

- (1) Start with any generating set S of I .
- (2) Try to produce new polynomials whose initial terms are not contained in $\text{lt}(S)$.
- (3) Update S by adjoining the new polynomials.
- (4) Iterate.

It will end after finitely many iterations because the new initial terms form a descending sequence of monomials. It remains to find an effective method to produce new initial terms. Let us work with an example first. Consider $I = (x^2, xy + y^2) \subset \mathbb{Q}[x, y]$. We will compute Gröbner basis with respect to two monomial orders. The first one is the lexicographic order under which $x \succ y$. We have $\text{lt}(x^2) = x^2$ and $\text{lt}(xy + y^2) = xy$. Neither of them is a multiple of the other. However, $y(x^2) - x(xy + y^2) = -xy^2$ has the leading term divisible by xy . This combination is called “S-polynomial” of x^2 and $xy + y^2$. So, $y(x^2) - x(xy + y^2) + y(xy + y^2) = y^3$. We see that y^3 is a new initial term of I . The generating set is expanded as $G = \{x^2, xy + y^2, y^3\}$. We then again form S-polynomials using any two among G , but fail to produce any new initial term. Indeed, G is a Gröbner basis of I . The second monomial order is the lexicographic order under which $x \prec y$. Then, $\text{lt}(x^2) = x^2$ and $\text{lt}(xy + y^2) = y^2$. We form an S-polynomial, $y^2(x^2) - x^2(xy + y^2) = -x^3y$. It is a multiple of x^2 , and we do not get anything new. Indeed, $\{x^2, xy + y^2\}$ is a Gröbner basis.

Given two polynomials f, g let us fix the leading coefficient of gcd to be 1. The **S-polynomial** of two polynomials f and g is the polynomial

$$\sigma(f, g) = \frac{\text{lt}(g)}{\text{gcd}(\text{lt}(f), \text{lt}(g))}f - \frac{\text{lt}(f)}{\text{gcd}(\text{lt}(f), \text{lt}(g))}g.$$

Dividing an S-polynomial by a set of generators will give a non-unique remainder, but we can hope that the calculation would find a new initial term. Buchberger showed that *the process is sufficient*

to find all initial terms of an ideal. The **Buchberger algorithm** to find a Gröbner basis is given by the above “algorithm,” where the step (2) is now well-defined by (2’):

(2’) For each pair f, g of polynomials of S , compute $\sigma(f, g)$ and its remainder r after division by S .

$$\frac{\text{lt}(g)}{\text{gcd}(\text{lt}(f), \text{lt}(g))}f - \frac{\text{lt}(f)}{\text{gcd}(\text{lt}(f), \text{lt}(g))}g = \sum_k h_k s_k + r$$

where $s_k \in S$, $h_k \in R$, and $\text{lt}(r) \notin \text{lt}(S)$ or $r = 0$.

In other words, the algorithm terminates with a correct answer, a Gröbner basis G , if the remainder of any S-polynomial computed from a pair of polynomials in G is zero. This is called the **Buchberger criterion**. It follows that if G is a Gröbner basis for the ideal (G) , then any subset $G' \subseteq G$ is a Gröbner basis for the ideal (G') .

A Gröbner basis $G = f_1, \dots, f_t$ is **reduced** if any term of f_i is not divisible by any $\text{lt}(f_j)$ where $i \neq j$, and the leading coefficients of all f_i are 1. The reduced Gröbner basis can be obtained from any Gröbner basis. *Given a monomial order, a reduced Gröbner basis is unique for an ideal.* Therefore, *two ideals are the same if and only if their reduced Gröbner bases are the same.*

Applications

An immediate application is to decide whether a set of polynomial equations $\{f_i(x_1, \dots, x_n) = 0\}$ admits a common solution. If one obtains $1 = 0$ while manipulating f_i , then certainly there is no solution, and this is the only case. That is, the ideal I generated by f_i contains 1, i.e., I is the unit ideal, if and only if there is no common solution to $f_i = 0$. Since the ideal membership can be tested by the division algorithm using a Gröbner basis, we can algorithmically answer this question by computing a Gröbner basis in any monomial order and looking for 1.

Note that known algorithms for Gröbner basis is not efficient in a computation complexity sense. Any significant improvement seems impossible because if one can compute Gröbner basis efficiently, then one can also solve, for example, Boolean satisfiability problem (SAT) efficiently. A SAT is a decision problem that asks whether there exists an assignment to Boolean variables x_1, \dots, x_n such that a given formula using AND, OR, and parenthesis evaluates to 1. Any SAT can be formulated as a finding a solution to a system of polynomial equations. Being Boolean can be expressed as $x_i(x_i - 1) = 0$. The OR of two binary variables x, y can be expressed as $1 - (1 - x)(1 - y)$. The AND of two binary variables x, y is the product xy . In particular, the 3-SAT, the SAT where all the expressions are given by conjunctive normal form with 3 variables per clause, is equivalent to finding a solution to systems of polynomial equations, each of which has degree at most 3. The 3-SAT is known to be NP-complete. However, finding Gröbner basis for a fixed number of variables is efficient, i.e., *the number of calculation steps increases as a polynomial in the degree of the generating*

polynomials.

We can also compute the intersection of an ideal with a subring. The foundational case is when the subring is given by $T = \mathbb{F}[x_1, \dots, x_n]$ contained in $R = \mathbb{F}[x_1, \dots, x_n, y_1, \dots, y_m]$. If an ideal I of R is given, we wish to compute the intersection $T \cap I$, which is an ideal of T . We should use an **elimination monomial order** under which $\text{lt}(f) \in T$ implies $f \in T$. The lexicographic order in which $x_a \prec y_b$ is an elimination order. The following statement is true. *If a Gröbner basis $G = \{f_1, \dots, f_u, g_1, \dots, g_v\}$ of I under elimination order is such that f_i do not involve any variable y_b ($b = 1, \dots, m$) but g_j do, then $G' = \{f_1, \dots, f_u\}$ is a Gröbner basis of $I \cap T$.* The ideal J generated by G' is certainly contained in $I \cap T$. It is clear that G' is a Gröbner basis for J because it satisfies the Buchberger criterion. If $J \subsetneq I \cap T$, then there would be $f \in (I \cap T) \setminus J$ with the least leading term. In particular, $\text{lt}(f) \notin \text{lt}(J)$. Since G is a Gröbner basis, $\text{lt}(f) \in \text{lt}(G)$. Since $\text{lt}(g_j)$ involve y_b due to the elimination order, but $\text{lt}(f) \in T$, we must have $\text{lt}(f) \in \text{lt}(G') = \text{lt}(J)$, a contradiction.

More generally, suppose we are given with a subring $T \subseteq \mathbb{F}[y_1, \dots, y_m]$ generated by some polynomials $h_i(y_1, \dots, y_m)$ ($i = 1, \dots, n$) over \mathbb{F} . We wish to find $T \cap I$ for an ideal I of $\mathbb{F}[y_1, \dots, y_m]$. Introduce new variables x_1, \dots, x_n , and consider

$$T' = \mathbb{F}[x_1, \dots, x_n] \xrightarrow{\phi} \mathbb{F}[y_1, \dots, y_m] \xrightarrow{\pi} \mathbb{F}[y_1, \dots, y_m]/I,$$

where ϕ is defined by $x_i \mapsto h_i(y_1, \dots, y_m)$ and π is the canonical map. ϕ maps onto T . If we knew $K = \ker \pi \circ \phi$, the image $\phi(K)$ would be precisely $T \cap I$. Let $R = \mathbb{F}[x_1, \dots, x_n, y_1, \dots, y_m]$. Note that R contains T' and $\mathbb{F}[y_1, \dots, y_m]$ as subrings. Thus ϕ can be extended to $\tilde{\phi}$ as

$$\tilde{\phi} : R = \mathbb{F}[x_1, \dots, x_n, y_1, \dots, y_m] \rightarrow \mathbb{F}[y_1, \dots, y_m] \quad \text{defined by} \quad \begin{cases} x_i \mapsto h_i(y), \\ y_j \mapsto y_j. \end{cases}$$

The kernel of $\pi \circ \tilde{\phi}$ is the ideal $J = (x_1 - h_1(y), \dots, x_n - h_n(y)) + I$. We have $K = J \cap T'$, which can be computed by the method above. For example, let $I = (1 + x + y + z, 1 + xy + yz + zx) \subseteq \mathbb{F}_2[x, y, z]$. If a subring is $T = \mathbb{F}_2[x^3, y^3, z^3]$, then an auxiliary ring is $T' = \mathbb{F}_2[x', y', z']$. The intersection $I \cap T$ can be found by computing

$$(1 + x + y + z, 1 + xy + yz + zx, x' - x^3, y' - y^3, z' - z^3) \cap \mathbb{F}[x', y', z'].$$

In the end, one has to replace x' with x^3 , y' with y^3 , and z' with z^3 .

The Gröbner basis is also useful to compute the vector space dimension of R/I , where $R = \mathbb{F}[x_1, \dots, x_n]$. The remainder r after division by a Gröbner basis of I is unique and has a property that $\text{lt}(r)$ is not divisible by any leading term of the Gröbner basis elements. The remainders are unique representatives for elements of R/I . It follows that there is a one-to-one correspondence as

sets between R/I and $R/\text{lt}(I)$. In particular, they are isomorphic as vector spaces. The generators of $\text{lt}(I)$ are monomials m_1, \dots, m_t computed by the Gröbner basis. Recall that monomials are in one-to-one correspondence with the hyper-octant H of nonnegative coordinates of \mathbb{Z}^n . Therefore, the vector space basis of $R/\text{lt}(I)$ is labeled by points of H that are not contained in any cone whose vertex, the least element with respect to the monomial order, is m_i ($1 \leq i \leq t$). For example, let $I = (x^2, xy + y^2) \subset \mathbb{F}[x, y] = R$. The reduced Gröbner basis under a lexicographic order in which $x \succ y$ is $\{y^3, xy + y^2, x^2\}$. Therefore, $R/\text{lt}(I)$ has a vector space basis $\{1, x, y, y^2\}$. In a different lexicographic order in which $x \prec y$, the reduced Gröbner basis of I is $\{x^2, y^2 + xy\}$. A vector space basis of $R/\text{lt}(I)$ is $\{1, x, y, xy\}$.

Syzygies and generalization to free modules

So far we have discussed only ideals and generators. It is straightforward to generalize the notions to submodules of free modules over polynomial rings $R = \mathbb{F}[x_1, \dots, x_n]$. We first need to generalize the monomial order. Let e_1, \dots, e_r be a basis of free module $F = R^r$. A **monomial** of F is a product of variables times one of the basis, e.g., $x_1x_2^5e_3$ and $x_1^3x_3e_1$ are monomials. A **monomial order** on F is defined in the same way as (A.7). The well-ordering property holds with the same proof. The leading terms are defined the same way, as well as the ideal generated by leading terms. The division algorithm does not need to be restated. The Buchberger criterion and algorithm make sense with a minor change that *if two leading terms involve different basis elements, then the S-polynomial is defined to be zero*. The elimination order are still applicable, and the calculation techniques are valid with respect to submodules.

Nontrivial relations between polynomials are called syzygies. (Here, polynomials include basis elements, so they are really elements of a free module.) More formally, if a submodule is defined by the image of a module map $\phi : F' \rightarrow F$ between finitely generated *free* modules, the kernel of ϕ is called **syzygy**. For instance, the syzygies of x and y can be described by a submodule M of $\mathbb{F}[x, y]^2$ generated by $\begin{pmatrix} y \\ -x \end{pmatrix}$, since the ideal (x, y) with generators x and y is the image of the map $\phi : R^2 \xrightarrow{\begin{pmatrix} x & y \end{pmatrix}} R$ and $M = \ker \phi$. The relation between x and y is thus $y(x) - x(y) = 0$. We have implicitly seen how to obtain nontrivial relations from the Buchberger algorithm. We formed an S-polynomial of two polynomials and ran the division algorithm with respect to a set $G = \{g_i\}$ of polynomials:

$$\sigma(g_i, g_j) = \frac{\text{lt}(g_j)}{\gcd(\text{lt}(g_i), \text{lt}(g_j))} g_i - \frac{\text{lt}(g_i)}{\gcd(\text{lt}(g_i), \text{lt}(g_j))} g_j = \sum_k h_k^{ij} g_k + r,$$

where $h_k^{ij} \in R$. If G were a Gröbner basis, then by Buchberger criterion we would have $r = 0$, and

the expression would be a nontrivial relation among g_i . More formally, let the module be generated by a Gröbner basis $\{g_i\}$. That is, module is the image of the map $\phi : F' \rightarrow F$ where the basis $\{\epsilon_i\}$ of F' is mapped as $\epsilon_i \mapsto g_i$. Then,

$$\tau_{ij} = \frac{\text{lt}(g_j)}{\text{gcd}(\text{lt}(g_i), \text{lt}(g_j))} \epsilon_i - \frac{\text{lt}(g_i)}{\text{gcd}(\text{lt}(g_i), \text{lt}(g_j))} \epsilon_j - \sum_k h_k^{ij} \epsilon_k$$

is mapped to zero under ϕ . It is a theorem that $\ker \phi$ is generated by τ_{ij} . $\{\tau_{ij}\}$ is often a redundant generating set for $\ker \phi$. Be warned that τ_{ij} is defined to be identically zero if $\text{lt}(g_i)$ and $\text{lt}(g_j)$ involve different basis elements of F .

Given a finite presentation of a module $F_0/\text{im } \phi_1$ where $\phi_1 : F_1 \rightarrow F_0$ is a module map between finitely generated free modules, we can algorithmically find $\ker \phi_1$. This kernel is a finitely generated submodule of F_1 , so it can be identified with the image of a map $\phi_2 : F_2 \rightarrow F_1$ between finitely generated free modules. We can continue this as many times as we want, and obtain a sequence of maps

$$\cdots \rightarrow F_n \xrightarrow{\phi_n} F_{n-1} \rightarrow \cdots \rightarrow F_2 \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0.$$

This sequence is called a **free resolution** of $F_0/\text{im } \phi_1$. A particularly interesting case is when the resolution is finite, i.e., $F_n = 0$ for some n .

A.4 Localization

Tensor product

Operations of modules include direct sum and quotient, both of which are automatic from the fact that modules are abelian groups. Here we introduce another operation on modules called tensor product. It is perhaps best defined by a categorical characterization, which is the most useful to prove things. Here we define it in a colloquial way.

Let us first review a familiar case of vector spaces over a field \mathbb{F} . The tensor product $V \otimes W$ of two vector spaces V, W is a collection of formal finite linear combinations $\sum_{i,j} a_{ij} v_i \otimes w_j$ of “products” $v_i \otimes w_j$ where $v_i \in V$, $w_j \in W$ and $a_{ij} \in \mathbb{F}$. The “product” \otimes is multilinear since

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w \quad \text{and} \quad v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2.$$

The scalar multiplication floats around \otimes as

$$(av) \otimes w = v \otimes (aw)$$

for any $a \in \mathbb{F}$. In physics literature, it is sometimes said that a tensor is a multi-indexed object

that transforms in a certain way under transformations for “indices.” This phrasing focuses on the coefficients a_{ij} and captures the multilinearity, as

$$\sum_{ij} a_{ij} v_i \otimes w_j = \sum_{ij} a_{ij} \left(\sum_a A_{ia} v'_a \right) \otimes \left(\sum_b B_{jb} w'_b \right) = \sum_{ab} \left(\sum_{ij} a_{ij} A_{ia} B_{jb} \right) v'_a \otimes w'_b.$$

The **tensor product of two modules** is defined in a similar way. For an R -module M and N , we build a formal abelian group out of all possible expressions $x \otimes_R y$ for $x \in M$ and $y \in N$, with the following equalities *imposed*:

$$\begin{aligned} (x + x') \otimes_R y &= x \otimes_R y + x' \otimes_R y, \\ x \otimes_R (y + y') &= x \otimes_R y + x \otimes_R y', \\ rx \otimes_R y &= x \otimes_R ry. \end{aligned} \tag{A.8}$$

The resulting abelian group is denoted by $M \otimes_R N$. It is an R -module by defining an action $r \cdot (x \otimes_R y) = rx \otimes_R y$. This is the tensor product of M and N . When there is no confusion about the base ring R , we write \otimes instead of \otimes_R .

Note that any abelian group M is a module over \mathbb{Z} by action $n \cdot m = \sum_{i=1}^{|n|} \text{sgn}(n)m$ for any $n \in \mathbb{Z}$ and any $m \in M$. Hence, we can take the tensor product of any abelian groups as \mathbb{Z} -modules. Since any R -module is an abelian group, one realizes that there are at least two ways to form tensor products of two R -modules M and N ; $M \otimes_{\mathbb{Z}} N$ and $M \otimes_R N$. All but one equations of (A.8) remain unchanged. The last equation declaring R -linearity of \otimes_R depends on R . It makes a huge difference. For instance, $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \cong \mathbb{C}$ is one dimensional, but $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{C}$ is infinite dimensional since there are infinitely many irrational numbers. $\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{C}$ is even larger. When the subscript is omitted, *the tensor product of two R -modules is taken over R by convention*.

Since the tensor product of two modules is a module, it makes sense to take the tensor product of three or more modules. Fortunately, the order of the tensor product does not matter.

$$(L \otimes_R M) \otimes_R N \cong L \otimes_R (M \otimes_R N) \quad M \otimes_R N \cong N \otimes_R M$$

There are (unwelcome) phenomena for general modules that never occur for vector spaces. The tensor product of two nonzero modules may be zero. For example, the tensor product of two \mathbb{Z} -modules $\mathbb{Z}/(2)$ and \mathbb{Q} is zero because $[a] \otimes b = [a] \otimes 2\frac{a}{2} = 2[a] \otimes \frac{a}{2} = 0 \otimes \frac{a}{2} = 0$. An expression $x \otimes y$ may be zero in $M \otimes N$ but may not be zero in $M' \otimes N'$ where $M' \leq M$ and $N' \leq N$ are submodules. For example, let $M = \mathbb{Z}$ and $N = \mathbb{Z}/(2)$ be \mathbb{Z} -modules. Choose $M' = 2\mathbb{Z}$ and $N' = N$. Now $2 \otimes [1]$ is nonzero in $M' \otimes N'$, but in $M \otimes N$, it is equal to $2 \cdot 1 \otimes [1] = 1 \otimes [2] = 0$.

Below we explain a “safe” and powerful tensor product.

Ring of fractions

The ring of rational numbers \mathbb{Q} is constructed from \mathbb{Z} by inverting nonzero elements. We wish to do a similar thing for general rings. Let U be a **multiplicatively closed** subset of a ring R , i.e., $1 \in U$ and any product of two elements of U lies in U . U needs not be closed under addition. For example, the set of all nonzero numbers in \mathbb{Z} is a multiplicatively closed set. More important is the complement of a prime ideal \mathfrak{p} . 1 is included in $R \setminus \mathfrak{p}$ because $\mathfrak{p} \neq (1)$. If $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$, then $ab \notin \mathfrak{p}$. This is the defining property of the prime ideal.

We construct “fractions” by putting elements of $U \subseteq R$ in denominators and elements of R in numerators. The set of all fractions becomes a ring with the “usual” additions and multiplications

$$\frac{a}{p} + \frac{b}{q} = \frac{aq + bp}{pq}, \quad (\text{A.9})$$

$$\frac{a}{p} \cdot \frac{b}{q} = \frac{ab}{pq}. \quad (\text{A.10})$$

Moreover, the elements of U are invertible!

$$\frac{1}{p} \cdot p = \frac{p}{p} = 1, \quad \frac{qa}{qp} = \frac{a}{p}.$$

The new **ring of fractions**⁴ is denoted by $U^{-1}R$ or $R[U^{-1}]$. Two special cases are so important that they deserve separate notations.

- If $U = R \setminus \mathfrak{p}$, the ring of fractions is called the **localization of R at \mathfrak{p}** and denoted by $R_{\mathfrak{p}}$.
- If $U = \{1, f, f^2, f^3, \dots\}$ for some $f \in R$, the ring of fractions is denoted by R_f .

The original ring R lives in $U^{-1}R$ via a canonical map $r \mapsto \frac{r}{1}$. With this canonical map, we omit 1 in the denominators. Note that $U^{-1}R$ is an R -module. For example, $\mathbb{Z}_2 = \mathbb{Z}[\frac{1}{2}]$ is a ring of fractions with denominators are powers of 2. (Yes, this is a confusing notation since \mathbb{Z}_n is used to mean $\mathbb{Z}/(n)$.) $\mathbb{Z}_{(2)}$ is a ring of fractions with odd denominators. $\mathbb{Q}[x]_{(x)}$ is a ring of fractions of polynomials where denominators does not vanish at $x = 0$. What is $\mathbb{Q}[x, y]_{xy}$? It is a ring of fractions of polynomials where denominators are powers of xy . Since $\frac{1}{x} = \frac{y}{xy}$ and $\frac{1}{y} = \frac{x}{xy}$, we notice that $\mathbb{Q}[x, y]_{xy}$ is really the ring of Laurent polynomials.

Modules can be fractionalized as well. Let M be an R -module. Choose a multiplicatively closed set U of the base ring R , and define $U^{-1}M$ as the set of all fractions with elements of M in the numerators and elements of U in the denominators. The addition within $U^{-1}M$ is defined by (A.9). $U^{-1}M$ becomes an $U^{-1}R$ -module using (A.10). In fact, $U^{-1}M \cong (U^{-1}R) \otimes_R M$ as $U^{-1}R$ -modules.

⁴ Rigorously, the ring of fractions is a collection of equivalence classes of $R \times U$; $(a, p) = (b, q)$ if and only if there exists $s \in U$ such that $s(aq - bp) = 0$. The reason we do not define the equivalence using “ $aq = bp$ ” is that there could be zero-divisors in R . Interested readers might want to check that $U^{-1}R$ indeed becomes a ring using (A.9) and (A.10) as definitions.

Moreover,

- $U^{-1}M \otimes_{U^{-1}R} U^{-1}N = U^{-1}(M \otimes_R N)$ for any R -modules M, N .

The **localization**, the process passing to fractional rings and modules, is so well behaving under nearly all conceivable operations. Let $A, B \leq M$ be submodules.

- $U^{-1}A$ is a submodule of $U^{-1}M$, i.e., $U^{-1}A$ injects into $U^{-1}M$.
- $U^{-1}A \cap U^{-1}B = U^{-1}(A \cap B)$.
- $U^{-1}A + U^{-1}B = U^{-1}(A + B)$.
- $U^{-1}(M/A) = (U^{-1}M)/(U^{-1}A)$.

They all originate from the following. A sequence of maps among modules A, B, C

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

is a **short exact sequence** if

- $\ker(A \rightarrow B) = 0$,
- $\operatorname{im}(A \rightarrow B) = \ker(B \rightarrow C)$,
- $\operatorname{im}(B \rightarrow C) = C$.

The localization preserves short exact sequence, i.e., if $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is a short exact sequence, then

$$0 \rightarrow U^{-1}A \rightarrow U^{-1}B \rightarrow U^{-1}C \rightarrow 0$$

is also a short exact sequence. For example, the first and the fourth statement above follows from localizing the short exact sequence

$$0 \rightarrow A \rightarrow M \rightarrow M/A \rightarrow 0.$$

The localizations at prime ideals are useful because *an R -module M is zero if and only if $M_{\mathfrak{p}} = 0$ for every prime ideal \mathfrak{p} of R* . In fact, $M = 0$ if and only if $M_{\mathfrak{m}} = 0$ for every maximal ideal \mathfrak{m} of R . This can be understood as follows. The **annihilator** denoted by $\operatorname{ann}_R M$ of an R -module M is an ideal of R defined by

$$\operatorname{ann}_R M = \{r \in R \mid rm = 0 \text{ for any } m \in M\} \quad (\text{A.11})$$

It is an ideal because $(a+b)m = am+bm = 0+0 = 0$ and $(ra)m = r(am) = 0$ if $a, b \in \operatorname{ann}_R M$. Note that *any R -module M becomes a module over $R/(\operatorname{ann}_R M)$* . What is to be proved for this statement

is the well-definedness of the defining operation (A.4), i.e., one needs to check that $[a] \cdot m = [b] \cdot m$ if $[a] = [b] \in R/(\text{ann}_R M)$ for any $m \in M$. Note that if R is a polynomial ring over a field, there is an algorithm to compute $\text{ann}_R M$ for a finitely presented module M using pull-backs and Gröbner basis techniques. Now, it is easy to see that *a module $M_{\mathfrak{p}}$ (the localization of M at a prime \mathfrak{p}) is zero if and only if the annihilator is not contained in \mathfrak{p}* , since a module is zero if and only if 1 or any unit is an annihilator, but the localized ring at \mathfrak{p} anything outside \mathfrak{p} is a unit. If M becomes zero at the localization at any maximal ideal, it means that the annihilator is not contained in any maximal ideal. The only elements of R that lie outside of any maximal ideal are units. Therefore, $M = 0$.

Recall that there exists a canonical map ϕ from R to a ring of fractions $U^{-1}R$, sending r to $\frac{r}{1}$. The image under ϕ of any ideal I of R is not in general an ideal. However, we may consider the ideal of $U^{-1}R$ generated by $\phi(I)$. This ideal is denoted by $I^e \subseteq U^{-1}R$, called an **extended ideal**. In fact, *any ideal of $U^{-1}R$ is an extended ideal*. To see this, consider any ideal J of $U^{-1}R$, and its **contraction** $\phi^{-1}(J) \subseteq R$. An element of J is $\frac{x}{s}$. Since J is an ideal, $\frac{s}{1} \frac{x}{s} = \frac{x}{1} \in J$. That is, $x \in \phi^{-1}(J)$. We have shown $(\phi^{-1}(J))^e = J$. Note that *every prime ideal of $U^{-1}R$ is an extended ideal of a prime ideal of R that do not intersect U* . We have seen that the inverse image of a prime ideal \mathfrak{p} is prime; the contraction $\mathfrak{p}^c = \phi^{-1}(\mathfrak{p})$ of a prime ideal of $U^{-1}R$ is prime. Since prime ideal is not (1) , it cannot contain any unit. Hence \mathfrak{p}^c cannot meet the set of units U . Conversely, for any prime ideal \mathfrak{q} of R that do not intersect U , \mathfrak{q}^e is a prime ideal of $U^{-1}R$, since $\frac{ab}{ss'} \in \mathfrak{q}^e \iff \frac{ab}{1} \in \mathfrak{q}^e$.

It is clear that if $\phi^{-1}(J)$ is generated by n elements of R , then J is generated by n elements of $U^{-1}R$. More importantly, *if R is a Noetherian ring, then any localization is a Noetherian ring*.

A **local ring** is a ring with a unique maximal ideal. Typically, maximal ideals are not unique. In the ring of integers, every prime number generates a distinct maximal ideal. Let $R_{\mathfrak{p}}$ be a localized ring at a prime ideal \mathfrak{p} of R . By definition of $R_{\mathfrak{p}}$, the set of all denominators do not meet \mathfrak{p} . Hence, $\mathfrak{p}_{\mathfrak{p}}$ is a prime ideal of $R_{\mathfrak{p}}$. If \mathfrak{m} is any ideal of $R_{\mathfrak{p}}$, we must have $\mathfrak{m} \subseteq \mathfrak{p}_{\mathfrak{p}}$. Otherwise, \mathfrak{m} contains an element outside $\mathfrak{p}_{\mathfrak{p}}$, which is invertible, and hence $\mathfrak{m} = (1)$. The localized ring $R_{\mathfrak{p}}$ at a prime ideal is a local ring with a unique maximal ideal $\mathfrak{p}_{\mathfrak{p}}$. One thing to remember about a local ring is that *any element outside the unique maximal ideal is a unit, i.e., it is invertible*.

Geometry

Why is it called “localization?” Here we briefly introduce the algebro-geometric point of view on rings.

The (only) algebraic structure that we should start with for a geometric object is a function space. By a function we mean a set-theoretical map from the geometric object to numbers. We can impose certain conditions such as continuity or differentiability on the function space to study deeper and interesting aspects of the geometric object. In classical algebraic geometry, the geometric

object, called variety, is defined by one or more polynomial equations, and the functions are defined by polynomials.

Roughly speaking, there are two interesting types of functions: globally defined functions and locally defined functions. The locally defined ones may not be well-defined for some regions far from the point of interest. In the algebraic setting, the global functions are given by polynomial expressions without denominators. There may be several polynomial expressions for the same function. This happens when two polynomials differ by the equations of the variety. For example, the global function space, called **coordinate ring** of a parabola on \mathbb{R}^2 defined by $y = x^2$ is a quotient ring $R = \mathbb{R}[x, y]/(y - x^2)$.

Locally defined functions at a point p , if they are given as a fraction of two polynomials, are precisely those whose the denominators are not zero at p . For example, the fraction $\frac{1}{x+1}$ is a locally defined function at a point $(0, 0)$ of the parabola, but $\frac{x-1}{y}$ is not. Collecting all locally defined functions at $\mathfrak{m} = (0, 0)$, we obtain a **local ring** $R_{\mathfrak{m}} = (\mathbb{R}[x, y]/(y - x^2))_{(x, y)}$, which is consisted of fractions whose denominators are not contained in the maximal ideal (x, y) . The global function ring R is *localized at \mathfrak{m} to be a local ring $R_{\mathfrak{m}}$* . Note that we have identified a point on the parabola with a maximal ideal \mathfrak{m} . This makes sense because the set of all solutions of the equations $f(x, y) = 0$ where $f(x, y) \in \mathfrak{m}$ is exactly $(0, 0)$.

One might ask what it means geometrically to localize at a prime ideal \mathfrak{p} . A prime ideal defines a subvariety by equations $f = 0$ where $f \in \mathfrak{p}$. The localization reveals the set of “functions” that are locally defined “around” the subvariety. (The notion of neighborhood can be made rigorous by defining a topology using polynomials.)

A.5 Determinantal ideal

When is a square matrix with integer entries invertible? A naive answer is that it is when the determinant is nonzero. It is true when the matrix is viewed as a matrix over \mathbb{Q} . If we insist that the inverse matrix must be expressed over \mathbb{Z} , then the answer is that it is when the determinant is ± 1 . That is, the determinant must be invertible within the ring. Put differently, it is when the ideal generated by the determinant is the unit ideal. The determinant has another use. The rank of a matrix is the largest k such that there exists a $k \times k$ submatrix whose determinant is a nonzero. Put differently, it is when the ideal generated by determinants of all $k \times k$ submatrices is nonzero.

These observations motivate us to define a determinantal ideal over an arbitrary commutative ring R . Consider a rectangular matrix \mathbf{M} with entries in R . A k^{th} **minor** is the determinant of a $k \times k$ submatrix. (There are quite many k^{th} minors if k is about half of the matrix size.) Note that to define the minor we do not have to assume that the full matrix \mathbf{M} is square. When k is larger than the number of rows or columns, k^{th} minor is, by definition, zero. k^{th} **determinantal ideal**

$I_k(\mathbf{M})$ of \mathbf{M} is the ideal of R generated by all k^{th} minors of \mathbf{M} . By convention, 0^{th} determinantal ideal is taken as $I_0(\mathbf{M}) = (1) = R$. If \mathbf{M} is $n \times n$, then n^{th} determinantal ideal is generated by a single element, the determinant of \mathbf{M} . The first determinantal ideal is generated by all entries of \mathbf{M} . A $(k+1)^{\text{st}}$ minor is a linear combination of k^{th} minors, as it has a cofactor expansion. Therefore, the determinantal ideals form a decreasing chain:

$$R = I_0(\mathbf{M}) \supseteq I_1(\mathbf{M}) \supseteq I_2(\mathbf{M}) \supseteq \cdots \supseteq I_{\min(\#row, \#col)}(\mathbf{M}) \supseteq (0)$$

The **rank** of \mathbf{M} is the largest k such that $I_k(\mathbf{M})$ is nonzero.

The determinantal ideals are invariants of \mathbf{M} under invertible matrix multiplications on the right or on the left.

$$I_k(\mathbf{M}\mathbf{D}) = I_k(\mathbf{E}\mathbf{M}) = I_k(\mathbf{M}) \quad \text{if } \mathbf{D}, \mathbf{E} \text{ are square and invertible.}$$

To understand this, it is enough to see $I_k(\mathbf{E}\mathbf{M}) \subseteq I_k(\mathbf{M})$ for arbitrary matrix E . Then, for invertible \mathbf{E} , we would have $I_k(\mathbf{E}^{-1}\mathbf{E}\mathbf{M}) \subseteq I_k(\mathbf{E}\mathbf{M})$. We need to see that a k^{th} minor of $\mathbf{E}\mathbf{M}$ is a linear combination of k^{th} minors of \mathbf{M} . Fix a $k \times k$ submatrix \mathbf{K} of $\mathbf{E}\mathbf{M}$.

$$\mathbf{K}_{il} = \sum_j e_{ij} \mathbf{M}_{jl}$$

where $e_{ij} = \mathbf{E}_{ij}$ is written with small letter to emphasize it is merely an element of R . Now the determinant of \mathbf{K} is vividly expressed by minors of \mathbf{M} , since the determinant is multilinear over R in rows K_i of \mathbf{K} .

$$\begin{aligned} \det \mathbf{K} &= \det(K_1, \dots, K_k) = \det \left[\sum_{j_1} e_{1j_1} M_{j_1}, \dots, \sum_{j_k} e_{kj_k} M_{j_k} \right] \\ &= \sum_{j_1, \dots, j_k} e_{1j_1} \cdots e_{kj_k} \det [M_{j_1}, \dots, M_{j_k}] \end{aligned}$$

where M_j is the row j of the submatrix of \mathbf{M} that is consisted of entries contributing to \mathbf{K} .

Suppose R be a local ring with a maximal ideal \mathfrak{m} , and consider a matrix \mathbf{M} over R of rank k . If $I_k(\mathbf{M}) = (1)$, how would \mathbf{M} look like after row and column operations? The operations are invertible, and therefore do not change the determinantal ideals. Since the determinantal ideals form a descending chain, it follows that $I_1(\mathbf{M}) = (1)$. It means that at least one entry must lie outside \mathfrak{m} and is invertible. Bringing that entry to $(1, 1)$ position by permuting rows and columns, we can

eliminate other entries in the first row and column, by row and column additions. So

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

where \cong means the equivalence up to invertible matrix multiplication on the left or right. Now we use the fact that $I_2(\mathbf{M}) = (1) = I_1(\mathbf{M}')$. By a similar process we can extract 1 from \mathbf{M}' . After k steps, we have

$$\mathbf{M} \cong \begin{pmatrix} \text{id}_k & 0 \\ 0 & 0 \end{pmatrix}. \quad (\text{A.12})$$

Here, observe that R is not necessarily a field. It is just a local ring where some nonzero elements may not be invertible. The smallest nonzero determinantal ideal being a unit ideal was strong enough to imply the structure of the matrix.

Smith normal form

Beyond the “easy” local ring case, there is one more easy case of **principal ideal domains**, in which every ideal is generated by a single element. It is not necessarily local. *The ring of integers and the ring of polynomials in one variable over a field are principal ideal domains*; given finitely many generators of an ideal, one can find the greatest common divisor (gcd) by the Euclidean algorithm.

Let R be a principal ideal domain. We ask what normal forms of matrices we may have, after invertible matrix multiplication on the left or right. In other words, we seek for invariants of the matrices. Observe that the gcd of two elements⁵ f and g can be expressed as a linear combination of f and g

$$\text{gcd}(f, g) = af + bg$$

for some $a, b \in R$. To see this, consider the ideal (f, g) . It must be generated by a single element, say, d , i.e., $(d) = (f, g)$. Then, $f \in (d) \iff f = df'$ and $g \in (d) \iff g = dg'$. So d is a common divisor of f and g . In addition, $(d) = (f, g) \subseteq (\text{gcd}(f, g))$ implies that $\text{gcd}(f, g)$ divides d . Thus, $\text{gcd}(f, g)$ and d are the same up to units, and $\text{gcd}(f, g) \in (f, g)$. We thus obtain the above expression. Now, consider the following matrix equation

$$\begin{pmatrix} \text{gcd}(f, g) \\ 0 \end{pmatrix} = \begin{pmatrix} a & b \\ -g' & f' \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix}$$

⁵To speak of gcd, it must be first proved that in R any element has a unique factorization. It is true that in any principal ideal domain, any element is a product of irreducible factors that are unique up to units. If the latter is satisfied, the ring is called a **unique factorization domain**. Note that an arbitrary ring may not be a unique factorization domain. For example, in $\mathbb{Z}[\sqrt{-5}]$, we have $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, which are two different factorizations of 6 into irreducible factors.

The 2×2 matrix has determinant $af' + bg' = \gcd(f, g)/d$, a unit. We have transformed a 2×1 matrix by an invertible left multiplication such that there is only a single nonzero entry left. A similar thing can be done for an $n \times 1$ matrix.

$$\left(\gcd(f_1, \dots, f_n) \ 0 \ \dots \ 0 \right)^T = \mathbf{E} \left(f_1 \ \dots \ f_n \right)^T$$

where \mathbf{E} is invertible.

If we are given with a rectangular matrix \mathbf{M} , we can perform this transformation by looking at the first column of \mathbf{M} . The transformed matrix M' will have a nonzero entry on the first row in the first column. Perform a similar transformation by right multiplication, focusing on the first row of M' . The new matrix M'' has unique nonzero entry at $M''_{1,1}$ in the first row, but the first column may be screwed up. We can iterate these transformations as many times as we want. Will this process eventually terminate? Yes. For example, if we are working in the ring of integers, the absolute value of the entry $M''_{1,1}$ is smaller than $|M'_{1,1}|$, which is $\leq |M_{1,1}|$. Positive integers cannot decrease forever, and the process must terminate. More generally, the ascending chain condition makes the proof smooth. The ideals generated by the $(1, 1)$ -entries will form an increasing sequence of ideals. Our ring R , being a principal ideal domain, is Noetherian. The sequence must become stationary after finitely many iterations. If one is not too familiar with Noetherian rings, one can rely on the fact that there are finitely many factors of a given element. If $(d_1) \subseteq (d_2) \subseteq \dots$ is an increasing sequence of ideals, we have $d_{i+1} | d_i$. Since there are only finitely many factors in d_1 , one cannot have an infinite and strictly increasing sequence of ideals.

The matrix $\mathbf{M}^{(n)}$ obtained from \mathbf{M} by iterating the gcd-computations n -times, has a unique nonzero entry d at $(1, 1)$ in its row and column.

$$\mathbf{M}^{(n)} = \begin{pmatrix} d & 0 \\ 0 & M_1 \end{pmatrix}$$

We can claim a bit more. If there is any entry at (u, v) of M_1 that is not divisible by d , we can add the row u to the first row and run the gcd-computation again. The ideal generated by $(1, 1)$ -entry will become larger. Iterating, we eventually find the largest possible ideal generated by $(1, 1)$ -entry. Therefore, we can obtain M_1 whose entries are all divisible by d .

The above algorithm applied to M_1 , and to its submatrix, and so on, will produce a diagonal matrix. This diagonal matrix is called the **Smith normal form** of \mathbf{M} . The nonzero diagonal entries d_1, \dots, d_k have a property that

$$d_1 | d_2 | \dots | d_k.$$

Here, the number k is precisely the rank of the matrix \mathbf{M} . Moreover, the determinantal ideals are

$$I_t(\mathbf{M}) = (d_1 \cdots d_t).$$

This immediately proves that d_i 's are uniquely determined by \mathbf{M} . The invariants d_i 's are called **elementary divisors** of \mathbf{M} . Since any matrix, not necessarily square, can be brought to the Smith normal form by invertible transformations, it follows that the elementary divisors are **complete invariants**, i.e., the elementary divisors are the same for two matrices if and only if two matrices are related by invertible matrix multiplication on the left and right.

Finitely generated modules and Fitting ideals

We briefly noted about finite presentations of modules when we discussed free modules. We say that an R -module M is finitely presented by a matrix $\phi : R^m \rightarrow R^n$ if M is isomorphic to $R^n / \text{im } \phi$. This is more commonly denoted as $M = \text{coker } \phi$.

To get some feeling, let us consider a simple case where $R = \mathbb{Z}$. The matrix $\phi : R^m \rightarrow R^n$ is an $n \times m$ matrix with integer entries. Any basis change in R^n amounts to an invertible left multiplication on ϕ . Any basis change in R^m amounts to an invertible right multiplication on ϕ . We know a very convenient canonical form of ϕ — the Smith normal form. Let ϕ be in the Smith normal form with the diagonal elements d_1, \dots, d_k . In the simplest case $k = m = n = 1$, the module M is $R / \text{im } \phi = \mathbb{Z} / (d_1)$. If $m = n = 2$ and $d_2 = 0$, the module M is $R^2 / \text{im } \phi = \mathbb{Z} / (d_1) \oplus \mathbb{Z}$.

In fact, we can prove the structure theorem for finitely generated abelian groups very easily. Let M be a finitely generated abelian group. It can be viewed as a finitely generated \mathbb{Z} -module. Let n be the number of generators. We have a module map $\tilde{\phi} : \mathbb{Z}^n \rightarrow M$, which is surjective. The kernel K is also finitely generated since \mathbb{Z}^n is Noetherian. Hence, we have another map $\phi : \mathbb{Z}^m \rightarrow K \subseteq \mathbb{Z}^n$ where m is the number of generators of K . We have constructed a finite presentation of M by ϕ , i.e., $M = \mathbb{Z}^n / \text{im } \phi$. Bring ϕ to the Smith normal form by basis changes in \mathbb{Z}^n and \mathbb{Z}^m . If $d_1 | \cdots | d_k$ are elementary divisors of ϕ , we define $d_{k+1} = \cdots = d_n = 0$. Then we have an isomorphism of \mathbb{Z} -modules $M \cong \mathbb{Z} / (d_1) \oplus \cdots \oplus \mathbb{Z} / (d_n)$. Viewed as a group, the notation will be

$$M = \mathbb{Z} / d_1 \mathbb{Z} \times \cdots \times \mathbb{Z} / d_k \mathbb{Z} \times \mathbb{Z}^{n-k}.$$

This is the most general form of a finitely generated abelian group. Note that the rank $n - k$ and the elementary divisors $d_1 | d_2 | \cdots | d_k \neq 0$ are uniquely determined by the group M . Any finite abelian group is obviously finitely generated.

Let R be an arbitrary commutative ring, and M be an R -module with a finite presentation given by a matrix $A : R^m \rightarrow R^n$, i.e., $M \cong R^n / \text{im } A = \text{coker } A$. We define **Fitting ideals** $F_i(M)$ of M

as

$$F_i(M) = I_{n-i}(A), \tag{A.13}$$

so

$$F_0(M) \subseteq F_1(M) \subseteq \cdots \subseteq F_n(M) = R.$$

One should ask: A is one of many possible finite presentations. How can we be sure that $F_i(M)$ is determined by M and is independent of a particular presentation A ? We can be sure. The presentation really consists of two sets of things: a set of generators $x_1, \dots, x_n \in M$ and their relations (syzygies) given by columns of A

$$\sum_i x_i A_{ij} = 0.$$

Thus, we can think of A as the matrix of relations. The isomorphism $M \cong \text{coker } A$ ensures that any possible relations among x_i is generated by columns of A . That is, for any coefficients c_i such that $\sum_i x_i c_i = 0$ we can express c_i as $c_i = \sum_j A_{ij} d_j$. Therefore, if we write a $n \times \infty$ matrix \tilde{A} by collecting *all* relations among x_i , then the k^{th} determinantal ideal of \tilde{A} is exactly $I_k(A)$. In other words, $I_k(A)$ is determined by the chosen generators of M . Our question on the well-definedness of the Fitting ideal concerns, in fact, many possible choices of generators for M . Now, let $y_1, \dots, y_{n'}$ be elements of M . We have $n + n'$ generators $x_i, y_{i'}$ of M , and M is presented as a quotient module of $R^{n+n'}$. The relations among $x_i, y_{i'}$ constitute a matrix

$$W = \begin{pmatrix} A & A' & \# \\ 0 & \text{id} & \# \end{pmatrix} \sim W' = \begin{pmatrix} A & 0 & A' \\ 0 & \text{id} & 0 \end{pmatrix} \sim W'' = \begin{pmatrix} A & 0 & 0 \\ 0 & \text{id} & 0 \end{pmatrix}$$

where \sim means equality up to row or column operations. The first matrix W can be written as shown because $y_{i'}$ can be written as some combination of x_i . W'' is obtained from W' since we know that A generates all relations among x_i . Since determinantal ideals are invariant under invertible matrix multiplications, we see that $I_{k+n'}(W) = I_{k+n'}(W') = I_{k+n'}(W'') = I_k(A)$. Another finite presentation $B : R^{m'} \rightarrow R^{n'}$ of $M \cong \text{coker } B$ gives another set of generators. By the above calculation, $I_{n-k}(A) = I_{n+n'-k}(W) = I_{n'-k}(B)$. Therefore, *the Fitting ideals are well-defined*. We now see clearly why the numbering of the Fitting ideals are given as (A.13). (One might notice that the finite presentation is actually too much than what is needed to define Fitting ideals. They can be defined for any finitely generated module.)

The first nonvanishing Fitting ideal is important because it tells when a finitely generated module becomes free after localization. For example, suppose an R -module M is finitely presented by $\phi : R^m \rightarrow R^3$ and $F_1(M)$ is nonzero. Let \mathfrak{p} be a prime ideal of R such that $F_1(M) \not\subseteq \mathfrak{p}$. Localizing at \mathfrak{p} , we see that $F_1(M) = I_2(\phi)$ becomes the unit ideal, since anything outside \mathfrak{p} is a unit in $R_{\mathfrak{p}}$.

Then, we have seen in (A.12) that the matrix $\phi_{\mathfrak{p}}$ is equivalent to a diagonal matrix with entries 0 or 1. Therefore, $\text{coker } \phi_{\mathfrak{p}}$ is obviously isomorphic to $R_{\mathfrak{p}}^3/R_{\mathfrak{p}}^2 = R_{\mathfrak{p}}^1$, a free module. Conversely, if $\text{coker } \phi_{\mathfrak{p}}$ is free for some prime ideal \mathfrak{p} , then $I_k(\phi_{\mathfrak{p}})$ is either (1) or (0). Therefore, every Fitting ideal of $\text{coker } \phi_{\mathfrak{p}}$ is either (0) or (1). In conclusion, *the localized module $M_{\mathfrak{p}}$ of M at a prime ideal \mathfrak{p} is free if and only if the first nonvanishing Fitting ideal of M is not contained in \mathfrak{p} .*

The initial Fitting ideal $F_0(M)$ is also interesting because it approximates the annihilator of M . Let M be generated by n elements. Then,

$$(\text{ann } M)^n \subseteq F_0(M) \subseteq \text{ann } M. \quad (\text{A.14})$$

Here, the **ideal power** $(\text{ann } M)^n$ means the ideal generated by all products of n elements from $\text{ann } M$. By definition, $F_0(M) = I_n(A)$ where A is a matrix of relations among the n generators x_i of M . If Z is an $n \times n$ submatrix of A , we have $\sum_i x_i Z_{ij} = 0$. Multiplying the adjugate matrix of Z , we see $(\det Z)x_i = 0$ for all $1 \leq i \leq n$. Hence, $\det Z \in \text{ann } M$. Since $F_0(M)$ is generated by these $\det Z$, we have the second inclusion of (A.14). If $a_1, \dots, a_n \in \text{ann } M$, then the diagonal matrix made of a_i expresses relations among x_i . The determinant $a_1 \cdots a_n$ therefore belongs to $F_0(M)$. This proves the first inclusion of (A.14).

A.6 Finite fields

A field is a nonzero commutative ring where every nonzero elements are invertible. There is only one proper ideal, the zero ideal (0). A **finite field** is a field with finitely many elements. If there are q elements in the field, we denote the field by \mathbb{F}_q . The minimum possible number is of course $q = 2$ because we need $0 \neq 1$. In this case it is called **binary field** \mathbb{F}_2 . It may seem quite modest to require for a field to have finitely many elements, but, unlike finite groups, finite fields are particularly simple — *there is a unique field of q elements up to isomorphisms*. Let us see why.

Since any ring is an additive group, \mathbb{F}_q is a finite abelian group. How does it look like as an additive group? Applying the “structure theorem for finitely generated abelian group,” we know $\mathbb{F}_q \cong \bigoplus_{i=1}^k \mathbb{Z}/(d_i)$, where $1 < d_1 | d_2 | \cdots | d_k \neq 0$. It follows that for any element $x \in \mathbb{F}_q$ we have $d_k x = 0$. Here, d_k is the smallest number such that $d_k x = 0$ for any $x \in \mathbb{F}_q$. If d_k is not a prime number, say, $d_k = pp'$ with $p, p' < d_k$, then $p = p \cdot 1 \neq 0$ in \mathbb{F}_q is invertible. Hence, $p' = p' \cdot 1 = 0$, which is a contradiction to the minimality of d_k . Therefore, d_k is prime, and $d_1 = d_2 = \cdots = d_k = p$. It follows that $|\mathbb{F}_q| = q = d_1 d_2 \cdots d_k = p^k$. This conclusion is often phrased as *a finite field has characteristic p for some prime number p and the total number of elements is a power of p* . Note that the image of $\mathbb{Z} \rightarrow \mathbb{F}_q$, as there is a unique ring homomorphism from \mathbb{Z} to any ring, is \mathbb{F}_p , a subfield of \mathbb{F}_q . It is of great importance that \mathbb{F}_q is a k -dimensional vector space over \mathbb{F}_p .

Next, how does the multiplicative group of all nonzero elements of \mathbb{F}_q look like? It is again a finitely generated abelian group. Therefore, its group structure is uniquely determined by elementary divisors $1 < e_1 | e_2 | \cdots | e_m \neq 0$. In a similar logic as above, we have $x^{e_m} = 1$ for any nonzero $x \in \mathbb{F}_q$. It is an equation in the field, so it can be rewritten as $x^{e_m} - 1 = 0$. How many solutions can an equation have? At most the degree. It means that $q - 1 = e_1 e_2 \cdots e_m \leq e_m$. The only possibility is that $m = 1$ and $e_1 = q - 1$. That is, the multiplicative group \mathbb{F}_q^\times consisted of all nonzero elements is isomorphic to the additive group $\mathbb{Z}/(q - 1)$, a **cyclic group** generated by a single element. In other words, there exists an element x in \mathbb{F}_q such that $\{x^n | n \in \mathbb{Z}\}$ is equal to the set of all nonzero elements. Such an element x is called **primitive element** of \mathbb{F}_q . There could be many primitive elements in \mathbb{F}_q .

Finally, let us mix the two operations, the addition and multiplication, and consider the ring structure of \mathbb{F}_q . Before we start analyzing \mathbb{F}_q , remark that for any field \mathbb{F} , not necessarily finite, and an irreducible polynomial $f(x)$ over \mathbb{F} , we can construct a larger field $\mathbb{F}[x]/(f(x))$ that contains \mathbb{F} . A larger field is called an **extension field** over the smaller field.

We noted above that \mathbb{F}_q is a k -dimensional vector space over \mathbb{F}_p . Fix a primitive element α of \mathbb{F}_q . Then, the set of “vectors” $\{1, \alpha, \alpha^2, \dots, \alpha^k\}$ contains $k + 1$ vectors, so it cannot be linearly independent over \mathbb{F}_p . Consider the set I_α of all polynomials $f(t) \in \mathbb{F}_p[t] \subseteq \mathbb{F}_q[t]$ such that $f(\alpha) = 0$. It is clearly a nonzero ideal, and therefore is generated by a single element $f_\alpha(t)$, which divides any element in I_α . $f_\alpha(t)$ is unique if we demand the leading coefficient to be 1. A polynomial with the leading coefficient 1 is called **monic**. The minimality of $f_\alpha(t)$ forces it to be irreducible. $f_\alpha(t)$ is uniquely determined by α , called the **minimal polynomial** of $\alpha \in \mathbb{F}_q$ over \mathbb{F}_p . We have established a ring homomorphism $\mathbb{F}_p[t]/(f_\alpha(t)) \rightarrow \mathbb{F}_q$ such that $t \mapsto \alpha$. Since α is a primitive element, this map is surjective. Moreover, it is injective because of the choice of $f_\alpha(t)$. It follows that the degree of $f(t)$ is actually equal to k , the dimension of \mathbb{F}_q as an \mathbb{F}_p -vector space, and *the ring \mathbb{F}_q is isomorphic to a quotient ring of the polynomial ring $\mathbb{F}_p[t]$.*

Recall the polynomial $h(x) = x^q - x$ becomes zero at any element of \mathbb{F}_q . It means that in the ring $\mathbb{F}_q[x]$, the polynomial $h(x)$ factorized into linear factors as

$$h(x) = x(x - \alpha)(x - \alpha^2)(x - \alpha^3) \cdots (x - \alpha^{q-1}). \quad (\text{A.15})$$

Since $x^q - x \in I_\alpha$, it follows that $f_\alpha(x) \in \mathbb{F}_p[x]$ divides $x^q - x \in \mathbb{F}_p[x]$. Therefore, $f_\alpha(x) \in \mathbb{F}_q[x]$ factorizes into linear factors, too. That is, any root of $f_\alpha(x)$ can be found in \mathbb{F}_q , not only α . Furthermore, *any root of $f_\alpha(x)$ is a primitive element*. Let $\beta \in \mathbb{F}_q$ be any root of $f_\alpha(x)$. The ideal $I_\beta \subseteq \mathbb{F}_p[x]$ contains $f_\alpha(x)$. Hence, the minimal polynomial $f_1(x) \in I_\beta$ divides $f_\alpha(x)$. Since $f_\alpha(x)$ is irreducible in $\mathbb{F}_p[x]$, we must have $f_\alpha(x) = f_\beta(x)$. It means that $\mathbb{F}_q \ni \alpha \mapsto \beta \in \mathbb{F}_q$ is an isomorphism, guaranteeing that β is a primitive element.

The quotient ring presentation of \mathbb{F}_q is not unique because it depends on $f_\alpha(t)$ which is determined by a primitive element. It is thus a relevant question whether two finite fields with the same cardinality \mathbb{F}_q and \mathbb{F}'_q are isomorphic as rings. Let α be a primitive element of \mathbb{F}_q with the minimal polynomial $f(x)$ over \mathbb{F}_p , and β be a primitive element of \mathbb{F}'_q with the minimal polynomial $g(x)$ over \mathbb{F}_p . We know that $f(x)|h(x)$ and $g(x)|h(x)$ where $h(x) = x^q - x$. It follows from (A.15) that $f(\beta^n) = 0$ in \mathbb{F}'_q for some n . Given such n , we can define a ring homomorphism $\mathbb{F}_p[x]/(f(x)) \ni x \mapsto y^n \in \mathbb{F}_p[y]/(g(y))$. It amounts to a ring homomorphism $\mathbb{F}_q \ni \alpha \mapsto \beta^n \in \mathbb{F}'_q$. Note that *any nonzero ring homomorphism from a field is injective* simply because the kernel is a proper ideal. Since both the domain and the target are finite dimensional vector spaces, our homomorphism is bijective, and we obtain a field-isomorphism. In conclusion, *any finite field is uniquely determined up to isomorphisms by its cardinality*.

Let $f(x) \in \mathbb{F}_q[x]$ be any irreducible polynomial over \mathbb{F}_q . We may consider an extension field $\mathbb{E} = \mathbb{F}_q[x]/(f(x))$ over \mathbb{F}_q . It is still a finite field for being a finite dimensional vector space over a finite field. In \mathbb{E} , $f(x)$ factorizes into linear factors by the same reasoning as above. More generally, since any polynomial $g(x)$ is a product of irreducible polynomials, by extending the field, one can factor further some of the irreducible factors. Since there are finitely many irreducible factors, one eventually reaches an extension field where $g(x)$ factorizes into linear factors completely, after finitely many extensions. If we started with a finite field, then the ultimate field will still be finite of cardinality, say, q' . It follows that $g(x)$ is a factor of $(x^{q'} - x)^n$ for some n , where n is to take care of potential multiplicity in $g(x)$. n can be chosen to be large. If one wishes, it may be of form p^m where p is the characteristic of the field. Then, $(x^{q'} - x)^{p^m} = x^{q'p^m} - x^{p^m}$. Summarizing, *any nonzero polynomial $g(x)$ over a finite field divides $x^{p^{m'}} - x^{p^m}$ for some $m' > m$* .

Bibliography

- [1] Feynman, R. P. Simulating physics with computers. *International Journal of Theoretical Physics* **21**, 467–488 (1982).
- [2] Shor, P. W. Fault-tolerant quantum computation. In *Foundations of Computer Science, 1996. Proceedings., 37th Annual Symposium on*, 56–65 (1996). [quant-ph/9605011](#).
- [3] Kitaev, A. Y. Fault-tolerant quantum computation by anyons. *Annals of Physics* **303**, 2–30 (2003). [quant-ph/9707021](#).
- [4] Haldane, F. D. M. Many-particle translational symmetries of two-dimensional electrons at rational landau-level filling. *Phys. Rev. Lett.* **55**, 2095–2098 (1985).
- [5] Wen, X. G. & Niu, Q. Ground-state degeneracy of the fractional quantum Hall states in the presence of a random potential and on high-genus Riemann surfaces. *Phys. Rev. B* **41**, 9377–9396 (1990).
- [6] Bravyi, S., Hastings, M. & Michalakis, S. Topological quantum order: stability under local perturbations. *J. Math. Phys.* **51**, 093512 (2010). [1001.0344](#).
- [7] Dennis, E., Kitaev, A., Landahl, A. & Preskill, J. Topological quantum memory. *J. Math. Phys.* **43**, 4452–4505 (2002). [quant-ph/0110143](#).
- [8] Jiang, L. *et al.* Anyonic interferometry and protected memories in atomic spin lattices. *Nature Physics* **4**, 482–488 (2008). [0711.1365](#).
- [9] Das Sarma, S., Freedman, M. & Nayak, C. Topologically protected qubits from a possible non-abelian fractional quantum Hall state. *Phys. Rev. Lett.* **94**, 166802 (2005).
- [10] Alicki, R., Fannes, M. & Horodecki, M. On thermalization in Kitaev’s 2D model. *Journal of Physics A: Mathematical and Theoretical* **42**, 065303 (2008). [0810.4584](#).
- [11] Bacon, D. Operator quantum error correcting subsystems for self-correcting quantum memories. *Phys. Rev. A* **73**, 012340 (2006). [quant-ph/0506023](#).

- [12] von Klitzing, K., Dorda, G. & Pepper, M. New method for high-accuracy determination of the fine-structure constant based on quantized Hall resistance. *Phys. Rev. Lett.* **45**, 494–497 (1980).
- [13] Prange, R. E. & Girvin, S. M. (eds.) *The Quantum Hall Effect* (Springer-Verlag, 1990), 2nd edn.
- [14] The international system of units (2008). URL <http://physics.nist.gov/Pubs/SP330/sp330.pdf>.
- [15] Laughlin, R. B. Quantized Hall conductivity in two dimensions. *Phys. Rev. B* **23**, 5632–5633 (1981).
- [16] Halperin, B. I. Quantized Hall conductance, current-carrying edge states, and the existence of extended states in a two-dimensional disordered potential. *Phys. Rev. B* **25**, 2185–2190 (1982).
- [17] Thouless, D. J., Kohmoto, M., Nightingale, M. P. & den Nijs, M. Quantized Hall conductance in a two-dimensional periodic potential. *Phys. Rev. Lett.* **49**, 405–408 (1982).
- [18] Tsui, D. C., Störmer, H. L. & Gossard, A. C. Two-dimensional magnetotransport in the extreme quantum limit. *Phys. Rev. Lett.* **48**, 1559–1562 (1982).
- [19] Laughlin, R. B. Anomalous quantum Hall effect: An incompressible quantum fluid with fractionally charged excitations. *Phys. Rev. Lett.* **50**, 1395–1398 (1983).
- [20] Niu, Q., Thouless, D. J. & Wu, Y.-S. Quantized Hall conductance as a topological invariant. *Phys. Rev. B* **31**, 3372–3377 (1985).
- [21] Wilczek, F. Quantum mechanics of fractional-spin particles. *Phys. Rev. Lett.* **49**, 957–959 (1982).
- [22] Willett, R. *et al.* Observation of an even-denominator quantum number in the fractional quantum Hall effect. *Phys. Rev. Lett.* **59**, 1776–1779 (1987).
- [23] Moore, G. & Read, N. Nonabelions in the fractional quantum Hall effect. *Nuclear Physics B* **360**, 362–396 (1991).
- [24] Wen, X. G., Wilczek, F. & Zee, A. Chiral spin states and superconductivity. *Phys. Rev. B* **39**, 11413–11423 (1989).
- [25] Wen, X.-G. Mean-field theory of spin-liquid states with finite energy gap and topological orders. *Phys. Rev. B* **44**, 2664–2672 (1991).

- [26] Read, N. & Sachdev, S. Large- n expansion for frustrated quantum antiferromagnets. *Phys. Rev. Lett.* **66**, 1773–1776 (1991).
- [27] Kitaev, A. & Preskill, J. Topological entanglement entropy. *Phys. Rev. Lett.* **96**, 110404 (2006). [hep-th/0510092](#).
- [28] Levin, M. & Wen, X.-G. Detecting topological order in a ground state wave function. *Phys. Rev. Lett.* **96**, 110405 (2006).
- [29] Kogut, J. B. An introduction to lattice gauge theory and spin systems. *Rev. Mod. Phys.* **51**, 659–713 (1979).
- [30] Wegner, F. J. Duality in generalized ising models and phase transitions without local order parameters. *J. Math. Phys.* **12**, 2259 (1971).
- [31] Elitzur, S. Impossibility of spontaneously breaking local symmetries. *Phys. Rev. D* **12**, 3978–3982 (1975).
- [32] Chesi, S., Loss, D., Bravyi, S. & Terhal, B. M. Thermodynamic stability criteria for a quantum memory based on stabilizer and subsystem codes. *New J. Phys.* **12**, 025013 (2010). [0907.2807](#).
- [33] Levin, M. & Wen, X.-G. Fermions, strings, and gauge fields in lattice spin models. *Phys. Rev. B* **67**, 245316 (2003). [cond-mat/0302460](#).
- [34] Levin, M. A. & Wen, X.-G. String-net condensation: A physical mechanism for topological phases. *Phys. Rev. B* **71**, 045110 (2005). [cond-mat/0404617](#).
- [35] Castelnovo, C. & Chamon, C. Entanglement and topological entropy of the toric code at finite temperature. *Phys. Rev. B* **76**, 184442 (2007).
- [36] Hastings, M. B. Topological order at non-zero temperature. *Phys. Rev. Lett* **107**, 210501 (2011). [1106.6026](#).
- [37] Hasan, M. Z. & Kane, C. L. Topological insulators. *Rev. Mod. Phys.* **82**, 3045 (2010). [1002.3895](#).
- [38] Calderbank, A. R. & Shor, P. W. Good quantum error-correcting codes exist. *Phys. Rev. A* **54**, 1098–1105 (1996). [quant-ph/9512032](#).
- [39] Steane, A. Multiple particle interference and quantum error correction. *Proc. Roy. Soc. Lond. A* **452**, 2551 (1996). [quant-ph/9601029](#).
- [40] Gottesman, D. A class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A* **54**, 1862 (1996). [quant-ph/9604038](#).

- [41] Calderbank, A. R., Rains, E. M., Shor, P. W. & Sloane, N. J. A. Quantum error correction and orthogonal geometry. *Phys.Rev.Lett.* **78**, 405–408 (1997). [quant-ph/9605005](#).
- [42] Kitaev, A. Anyons in an exactly solved model and beyond. *Annals of Physics* **321**, 2–111 (2006). [cond-mat/0506438](#).
- [43] Bravyi, S. & Terhal, B. A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes. *New J. Phys.* **11**, 043029 (2009). [0810.1983](#).
- [44] Haah, J. & Preskill, J. Logical operator tradeoff for local quantum codes. *Phys. Rev. A* **86**, 032308 (2012). [1011.3529](#).
- [45] Landon-Cardinal, O. & Poulin, D. Local topological order inhibits thermal stability in 2D. *Phys. Rev. Lett.* **110**, 090502 (2013).
- [46] Alicki, R., Horodecki, M., Horodecki, P. & Horodecki, R. On thermal stability of topological qubit in Kitaev’s 4d model. *Open Syst. Inf. Dyn.* **17**, 1 (2010). [0811.0033](#).
- [47] Yoshida, B. Feasibility of self-correcting quantum memory and thermal stability of topological order. *Annals of Physics* **326**, 2566–2633 (2011). [1103.1885](#).
- [48] Newman, M. E. J. & Moore, C. Glassy dynamics and aging in an exactly solvable spin model. *Phys. Rev. E* **60**, 5068–5072 (1999). [cond-mat/9707273](#).
- [49] Haah, J. Commuting Pauli Hamiltonians as maps between free modules (2012). [1204.1063](#).
- [50] Haah, J. Local stabilizer codes in three dimensions without string logical operators. *Phys. Rev. A* **83**, 042330 (2011). [1101.1962](#).
- [51] Bravyi, S. & Haah, J. On the energy landscape of 3D spin Hamiltonians with topological order. *Phys. Rev. Lett.* **107**, 150504 (2011). [1105.4159](#).
- [52] Bravyi, S. & Haah, J. Analytic and numerical demonstration of quantum self-correction in the 3D cubic code (2011). [1112.3252](#).
- [53] Preskill, J. Fault-tolerant quantum computation. In Lo, H.-K., Popescu, S. & Spiller, T. P. (eds.) *Introduction to Quantum Computation and Information*, 213 (World Scientific, 1998). [quant-ph/9712048](#).
- [54] Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52**, R2493–R2496 (1995).
- [55] Rains, E. M., Hardin, R. H., Shor, P. W. & Sloane, N. J. A. A nonadditive quantum code. *Phys. Rev. Lett.* **79**, 953–954 (1997).

- [56] Knill, E. Non-binary unitary error bases and quantum codes (1996). [quant-ph/9608048](#).
- [57] Knill, E. Group representations, error bases and quantum codes (1996). [quant-ph/9608049](#).
- [58] Rains, E. Nonbinary quantum codes. *Information Theory, IEEE Transactions on* **45**, 1827–1832 (1999). [quant-ph/9703048](#).
- [59] Gottesman, D. Fault-tolerant quantum computation with higher-dimensional systems. In Williams, C. (ed.) *Quantum Computing and Quantum Communications*, vol. 1509 of *Lecture Notes in Computer Science*, 302–313 (Springer Berlin Heidelberg, 1999).
- [60] Lang, S. *Algebra* (Springer, 2002), revised 3rd edn.
- [61] Kitaev, A. Y., Shen, A. H. & Vyalıy, M. N. *Classical and Quantum Computation* (American Mathematical Society, 2002).
- [62] Calderbank, A., Rains, E., Shor, P. & Sloane, N. J. A. Quantum error correction via codes over $\text{gf}(4)$. *Information Theory, IEEE Transactions on* **44**, 1369–1387 (1998).
- [63] Poulin, D. Stabilizer formalism for operator quantum error correction. *Phys. Rev. Lett.* **95**, 230504 (2005). [quant-ph/0508131](#).
- [64] Yoshida, B. & Chuang, I. L. Framework for classifying logical operators in stabilizer codes. *Phys. Rev. A* **81**, 052302 (2010). [1002.0085](#).
- [65] Bravyi, S. Subsystem codes with spatially local generators. *Phys. Rev. A* **83**, 012320 (2011). [1008.1029](#).
- [66] Wilde, M. M. & Fattal, D. Nonlocal quantum information in bipartite quantum error correction. *Quantum Information Processing* **9**, 591–610, (2010). [0912.2150](#).
- [67] Imai, H. A theory of two-dimensional cyclic codes. *Information and Control* **34**, 1–21 (1977).
- [68] MacWilliams, F. J. & Sloane, N. J. A. *The Theory of Error Correcting Codes* (North-Holland, Amsterdam, 1977).
- [69] Saints, K. & Heegard, C. Algebraic-geometric codes and multidimensional cyclic codes: a unified theory and algorithms for decoding using Gröbner bases. *Information Theory, IEEE Transactions on* **41**, 1733–1751 (1995).
- [70] Güneri, C. & Özbudak, F. Multidimensional cyclic codes and Artin-Schreier type hypersurfaces over finite fields. *Finite Fields and Their Applications* **14**, 44–58 (2008).
- [71] Ollivier, H. & Tillich, J.-P. Quantum convolutional codes: fundamentals (2004). [quant-ph/0401134](#).

- [72] Grassl, M. & Rotteler, M. Non-catastrophic encoders and encoder inverses for quantum convolutional codes. In *Information Theory, 2006 IEEE International Symposium on*, 1109–1113 (2006).
- [73] Wilde, M. M. & Brun, T. A. Quantum convolutional coding with shared entanglement: General structure. *Quantum Information Processing* **9**, 509–540 (2010). [0807.3803](#).
- [74] Michalakis, S. & Pytel, J. Stability of frustration-free Hamiltonians (2011). [1109.1588](#).
- [75] Bravyi, S. & Hastings, M. B. A short proof of stability of topological order under local perturbations. *Communications in Mathematical Physics* **307**, 609–627 (2011). [1001.4363](#).
- [76] Eisenbud, D. *Commutative Algebra with a View Toward Algebraic Geometry* (Springer, 2004).
- [77] Pauer, F. & Unterkircher, A. Gröbner bases for ideals in Laurent polynomial rings and their application to systems of difference equations. *Applicable Algebra in Engineering, Communication and Computing* **9**, 271–291 (1999).
- [78] Buchsbaum, D. A. & Eisenbud, D. What makes a complex exact? *Journal of Algebra* **25**, 259–268 (1973).
- [79] Northcott, D. G. *Finite Free Resolutions* (Cambridge University Press, 1976).
- [80] Atiyah, M. F. & MacDonal, I. G. *Introduction to Commutative Algebra* (Westview, 1969).
- [81] Lang, S. & Weil, A. Number of points of varieties in finite fields. *American Journal of Mathematics* **76**, 819–827 (1954). URL <http://www.jstor.org/stable/2372655>.
- [82] Martin, O., Odlyzko, A. M. & Wolfram, S. Algebraic properties of cellular automata. *Communications in Mathematical Physics* **93**, 219–258 (1984).
- [83] Bruns, W. & Vetter, U. *Determinantal Rings*. Lecture Notes in Mathematics 1327 (Springer-Verlag, 1988). URL <http://www.home.uni-osnabrueck.de/wbruns/brunsw/detrings.pdf>.
- [84] Yoshida, B. Classification of quantum phases and topology of logical operators in an exactly solved model of quantum codes. *Annals of Physics* **326**, 15–95 (2011). [1007.4601](#).
- [85] Beigi, S. Classification of the phases of 1d spin chains with commuting Hamiltonians. *Journal of Physics A: Mathematical and Theoretical* **45**, 025306 (2012).
- [86] Bombin, H., Duclos-Cianci, G. & Poulin, D. Universal topological phase of two-dimensional stabilizer codes. *New Journal of Physics* **14**, 073048 (2012).
- [87] Bombin, H. Structure of 2D topological stabilizer codes (2011). [1107.2707](#).

- [88] Wen, X.-G. Quantum orders in an exact soluble model. *Phys. Rev. Lett.* **90**, 016803 (2003). [quant-ph/0205004](#).
- [89] Chamon, C. Quantum glassiness. *Phys. Rev. Lett.* **94**, 040402 (2005). [cond-mat/0404182](#).
- [90] Bravyi, S., Leemhuis, B. & Terhal, B. M. Topological order in an exactly solvable 3D spin model. *Annals of Physics* **326**, 839–866 (2011). [1006.4871](#).
- [91] Suslin, A. A. On the structure of the special linear group over polynomial rings. *Mathematics of the USSR-Izvestiya* **11**, 221 (1977).
- [92] Park, H. & Woodburn, C. An algorithmic proof of Suslin’s stability theorem over polynomial rings. *Journal of Algebra* **178**, 277–298 (1995). [alg-geom/9405003](#).
- [93] Grunewald, F., Mennicke, J. & Vaserstein, L. On symplectic groups over polynomial rings. *Mathematische Zeitschrift* **206**, 35–56 (1991).
- [94] Kopeyko, V. I. Symplectic groups over Laurent polynomials, and patching diagrams. *Fundam. Prikl. Mat.* **5**, 943–945 (1999). URL <http://www.ams.org/mathscinet-getitem?mr=1806868>.
- [95] Iyengar, S. & Puthenpurakal, T. J. Hilbert-Samuel functions of modules over Cohen-Macaulay rings. *Proc. Amer. Math. Soc.* **135**, 637–648 (2007).
- [96] Wen, X. G. Vacuum degeneracy of chiral spin states in compactified space. *Phys. Rev. B* **40**, 7387–7390 (1989).
- [97] Einarsson, T. Fractional statistics on a torus. *Phys. Rev. Lett.* **64**, 1995–1998 (1990).
- [98] Kane, C. L. & Mele, E. J. z_2 topological order and the quantum spin Hall effect. *Phys. Rev. Lett.* **95**, 146802 (2005). [cond-mat/0506581](#).
- [99] Fu, L., Kane, C. L. & Mele, E. J. Topological insulators in three dimensions. *Phys. Rev. Lett.* **98**, 106803 (2007). [cond-mat/0607699](#).
- [100] Wilson, K. G. The renormalization group: Critical phenomena and the Kondo problem. *Rev. Mod. Phys.* **47**, 773–840 (1975).
- [101] Kadanoff, L. P. The application of renormalization group techniques to quarks and strings. *Rev. Mod. Phys.* **49**, 267–296 (1977).
- [102] Hastings, M. B. & Koma, T. Spectral gap and exponential decay of correlations. *Communications in Mathematical Physics* **265**, 781–804 (2006).

- [103] Verstraete, F., Cirac, J. I., Latorre, J. I., Rico, E. & Wolf, M. M. Renormalization group transformations on quantum states. *Phys. Rev. Lett.* **94**, 140601 (2005). [quant-ph/0410227](#).
- [104] Vidal, G. Entanglement renormalization. *Phys. Rev. Lett.* **99**, 220405 (2007).
- [105] Aguado, M. & Vidal, G. Entanglement renormalization and topological order. *Phys. Rev. Lett.* **100**, 070404 (2007). [0712.0348](#).
- [106] Vidal, G. A class of quantum many-body states that can be efficiently simulated. *Phys. Rev. Lett.* **101**, 110501 (2008). [quant-ph/0610099](#).
- [107] Chen, X., Gu, Z.-C. & Wen, X.-G. Local unitary transformation, long-range quantum entanglement, wave function renormalization, and topological order. *Phys. Rev. B* **82**, 155138 (2010). [1004.3835](#).
- [108] Schuch, N., Cirac, I. & Perez-Garcia, D. Peps as ground states: degeneracy and topology. *Annals of Physics* **325**, 2153 (2010). [1001.3807](#).
- [109] Evenbly, G. & Vidal, G. A class of highly entangled many-body states that can be efficiently simulated (2012). [1210.1895](#).
- [110] Nussinov, Z. & Ortiz, G. Autocorrelations and thermal fragility of anyonic loops in topologically quantum ordered systems. *Phys. Rev. B* **77**, 064302 (2008). [0709.2717](#).
- [111] Binder, K. & Young, A. P. Spin glasses: Experimental facts, theoretical concepts, and open questions. *Rev. Mod. Phys.* **58**, 801–976 (1986).
- [112] Weissman, M. B. What is a spin glass? a glimpse via mesoscopic noise. *Rev. Mod. Phys.* **65**, 829–839 (1993).
- [113] Tsomokos, D. I., Osborne, T. J. & Castelnovo, C. Interplay of topological order and spin glassiness in the toric code under random magnetic fields. *Phys. Rev. B* **83**, 075124 (2011). [1004.4632](#).
- [114] Harrington, J. *Analysis of quantum error-correcting codes : symplectic lattice codes and toric codes*. Ph.D. thesis, California Institute of Technology (2004).
- [115] Duclos-Cianci, G. & Poulin, D. Fast decoders for topological quantum codes. *Phys. Rev. Lett.* **104**, 050504 (2009). [0911.0581](#).
- [116] Gottesman, D. A theory of fault-tolerant quantum computation. *Phys. Rev. A* **57**, 127 (1998). [quant-ph/9702029](#).
- [117] Asano, T. & Tanaka, H. In-place algorithm for connected components labeling. *JPRR* **1**, 10–22 (2010).

- [118] Kiran, B., Ramakrishnan, K., Kumar, Y. & Anoop, K. An improved connected component labeling by recursive label propagation. In *Communications (NCC), 2011 National Conference on*, 1–5 (2011).
- [119] Gray, L. F. A reader’s guide to Gács’s “positive rates” paper. *Journal of Statistical Physics* **103**, 1–44 (2001).
- [120] Gács, P. Reliable computation with cellular automata. *Journal of Computer and System Sciences* **32**, 15–78 (1986).
- [121] Grimmett, G. *Percolation, 2ed* (Springer, 1999).
- [122] van den Berg, J. & Kesten, H. Inequalities with applications to percolation and reliability. *Journal of Applied Probability* **22**, 556–569 (1985).
- [123] Davies, E. B. Markovian master equations. *Communications in Mathematical Physics* **39**, 91–110 (1974).
- [124] Chesi, S., Röthlisberger, B. & Loss, D. Self-correcting quantum memory in a thermal environment. *Phys. Rev. A* **82**, 022305 (2010). [0908.4264](#).
- [125] Hamma, A., Castelnovo, C. & Chamon, C. Toric-boson model: Toward a topological quantum memory at finite temperature. *Phys. Rev. B* **79**, 245122 (2009). [0812.4622](#).
- [126] Wootton, J. R. & Pachos, J. K. Bringing order through disorder: Localisation of errors in topological quantum memories. *Phys. Rev. Lett* **107**, 030503 (2011). [1101.5900](#).
- [127] Stark, C., Imamoglu, A. & Renner, R. Localization of toric code defects. *Phys. Rev. L* **107**, 030504 (2011). [1101.6028](#).
- [128] Bravyi, S. & König, R. Disorder-assisted error correction in Majorana chains. *Communications in Mathematical Physics* **316**, 641–692 (2012). [1108.3845](#).
- [129] Pastawski, F., Clemente, L. & Cirac, J. I. Quantum memories based on engineered dissipation. *Phys. Rev. A* **83**, 012304 (2011). [1010.2901](#).
- [130] Iblisdir, S., Pérez-García, D., Aguado, M. & Pachos, J. Thermal states of anyonic systems. *Nuclear Physics B* **829**, 401–424 (2010). [0812.4975](#).
- [131] Spohn, H. An algebraic condition for the approach to equilibrium of an open n -level system. *Letters in Mathematical Physics* **2**, 33–38 (1977).
- [132] Bortz, A. B., Kalos, M. H. & Lebowitz, J. L. A new algorithm for Monte Carlo simulation of Ising spin systems. *Journal of Computational Physics* **17**, 10–18 (1975).

- [133] L'Ecuyer, P., Simard, R., Chen, E. J. & Kelton, W. D. An object-oriented random-number package with many long streams and substreams. *Operations Research* **50**, 1073–1075 (2002). URL <http://www.jstor.org/stable/3088626>.