Topological Quantum Computing via The Toric Code

by Milo Moses

University of California, Santa Barbara

March 24, 2023

Abstract

One of the most promising forms of quantum computation proposed today is Topological Quantum Computation. In this manuscript, we describe the simplest non-trivial example of Topological Quantum Computation: The toric code. We give explanations in terms of elementary mathematics and physics, as well as the high-power languages of Topological Quantum Field Theory and Modular Tensor Categories.

Contents

1 Preface

Quantum computing has seen massive advances over the last 30 years — prompted in large part by Peter Shor's discovery of an efficient quantum factoring algorithm [Sho94] — and gained notoriety as an emerging technology and area of insight. However, as of yet, nobody has made a usable quantum computer. Precisely controlling this microscopic world has proved quite challenging in large part due to thermal fluctuations of the outside world which cause quantum states to degenerate and scramble. Thus, the current state of quantum computing has been dubbed the "NISQ" era: The noisy intermediate-scale quantum era.

Moving past this era will require some major insights and discoveries, and perhaps an entirely new model of quantum computation. One of the moew recent such models is Topological Quantum Computation (TQC), proposed in a 2008 paper of Freedman-Kitaev-Larsen-Wang. The foremost team working on TQC is Microsoft Station Q, based in Santa Barbara, California. While this team has not been able to reliably perform computations with even a single qubit, they have made significant progress on the underlying theoretical physics since 2008.

There are already a few good surveys of TQC. The relevant mathematics is described in [BK01] and [RW18]. Physics oriented people will more out of [Pre99] and [NSS+08]. Z. Wang's book [Wan10] gives a relatively complete picture of the subject. The research article by M. Freedman et al. [FKW02] gives a good introduction as well. While certainly important references, they all expect the reader to have advanced knowledge of Quantum Mechanics, Algebraic Geometry, and Category Theory. This text serves as a much more elementary entry point into this vast and intricate field.

To remain as accessible as possible, we restrict ourselves to the simplest example of TQC: The toric code. This special case is used as motivation for the general theory. Key concepts for the general picture are left undefined, for even simply stating the main results of general TQC would be too cumbersome, and lead us too far astray. In the words of Alexei Kitaev, the inventor of the Toric Code:

> "Throughout my career I have been successful inventing toy models, some simple models that capture important features of a more complex problem." - Alexei Kitaev[1]

This manuscript is based on lecture notes from a course on TQC taught by Zhenghan Wang, in the winter of 2023 at UC Santa Barbara. The author expresses his sincerest gratitude to Zhenghan Wang and the other students of the class, without whom this manuscript would not have been possible.

The main reference for the description of the toric code as a quantum system on the torus is the seminal work of Kitaev [Kit03]. It was here that the idea

[1] From Kitaev's Simons Foundation interview, *"Alexei Kitaev and the Value of Toy Models"*

of computation by braiding anyons was first described, and much of that paper focuses specifically on the example of the toric code.

Many of the propositions and descriptions offered here are nowhere to be found in literature. This is not due to their being particularly novel, but rather their being seen as too obvious to be stated explicitly and written off as folklore. A secondary goal of this manuscript is to present a formal treatment of these implicit ideas.

Finally, we end with a terminological clarification. The term "toric code" refers to an example of TQC, but also to an error correcting code in universal quantum computation. Moreover, it is from this use as an error correcting code that it gets the name "toric code". Famously, Google uses the toric code error correction algorithm for its quantum computer, which is how it acheives its fantasic results. A readable reference to the surface codes (a generalization of the toric code) as error correction can be found in J. Roffe's article [Rof19]. The takeaway is that TQC is so intrinsically error resistant that its mathematical descriptions immediately give associated error correction algorithms. The widespread use and study of the toric code outside of TQC is a testament to the power of the theory.

The structure of the manuscript is as follows:

- Section 2 gives an introduction to TQC. While great effort is taken to make the treatment as accessible as possible, one is still required to have at least an elementary understanding of mathematics and physics. A passing familiarity with quantum mechanics and quantum computation would be extremely useful.

- Section **??** gives a treatment of the basics of quantum mechanics and quantum computation. In Subsection **??** the axioms of quantum mechanics are stated from a mathematical perspective, as well as ample motiation. Subsection **??** formally defines and describes quantum computation, with an emphasis on the information-theoretic language of computational complexity.

- Section 4 gives a mathematical description of the toric code in terms of undergraduate-level linear algebra. While not strictly necessary, having taken a first course in Algebraic Topology would be preferable. For those unfamiliar with the subject, an introduction is given in Appendix A. Those unfamiliar with the mathematical formalism of quantum mechanics are ad vised to reference Appendix **??**, though the section is entirely readable without this background.

- Section 5 gives an introduction to Topological Quantum Field Theories (TQFTs), the formal mathematical abstractions of topological quantum phases of matter. Subsection 5.1 gives an overview of the subject. Subsection 5.2 defines the $\mathbb{Z}_2$ Dijkgraaf-Witten theory, the TQFT associated with the toric code.

- Section 6 gives an introduction to Modular Tensor Categories (MTCs), the compressed mathematical abstraction of topological quantum phases of matter. Subsection 6.1 gives an overview of the subject, and the equivalence between MTCs and TQFTs. Subsection 6.2 gives the more elegant interpretation of MTCs in the language of categories. For those unfamiliar with the subject of Category Theory, a brief introduction is contained in Appendix B. Subsection 6.3 defines the $\mathcal{Z}(\mathbf{Rep}_{\mathbb{Z}_2})$ MTC, which is the MTC associated with the toric code.

- Section 7 gives an introduction to the general TQC methodology, using all of the tools developped in the previous sections. Subsection 7.1 gives a detailed overview of TQC, including measurement-based algorithms. Subsection 7.2 carries this out explicitely for the toric code. Subsection 7.3 introduces the Fibonacci anyon model, and shows that it gives universal quantum computation via braiding alone.

2 Introduction

Of the many approaches to quantum computation, Topological Quantum Computation (TQC) has the distinction of being both one of the most mathematically complicated and potentially powerful methods. In this manuscript, we describe the simplest non-trivial example of TQC: The toric code. While not particularly useful in itself, a thorough understanding of the toric code undoubtedly elucidates the general TQC methodology.

To describe a theory of Quantum Computation, one must specify the following:

1. How quantum information is stored (i.e. what physical model of qubits[2] one is using)

2. How quantum information is acted on (i.e. what physical actions one can perform on the qubits)

3. How quantum information is measured (i.e. what observables can be physically measured in the system)

A *universal* model of quantum computation is one which can simulate all others. Generally, this will mean that the space of possible physical actions specified by the quantum computation model is dense in the space of all possible transformations on the space of qubits (i.e. can be used to approximate every transformation arbitrarily well).

While there are many proposed methods of quantum computation (superconducting quantum computers [Wen17], trapped ion quantum computers [DLF+16], semiconductor based quantum computers [Kan98], etc...), it is expected that every reasonable model will be essentially equivalent, in the sense that they can

[2]Qubit (or, "quantum bit") is the abstract unit of quantum information

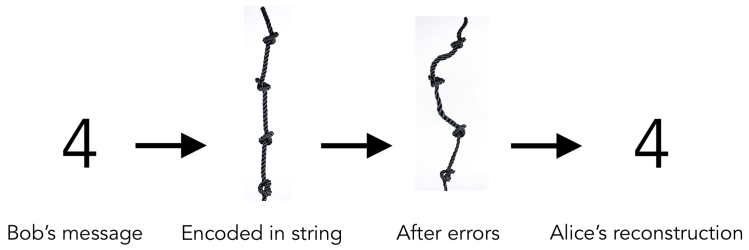


Figure 2.1: A model of a (non-quantum) topological message

all *effectively* simulate each other: This is the content of the Freedman-Church-Turing thesis [FKLW03].

In a a sequence of seminal works by Freedman, Kitaev, Larsen, and Wang, it was shown that universal quantum computers can effectively model any TQC, and conversely that there are models of TQC which can effectively simulate a universal quantum computer [FLW02] [FKW02].

If all forms of quantum computation are roughly equivalent it is reasonable to ask why one would consider TQC to be more promising than other models. This is an especially relevant question seeing as Google's superconducting quantum computer can harness 53 qubits and has demonstrated quantum superiority, while Microsoft's TQC has not been able to reliably harness a single qubit [AAB$^+$19].

The intuition is as follows. The #1 challenge in quantum computation is error correction. While fault tolerant quantum computers (quantum computers that fix errors faster than they arise) can probably exist, the error rate must be unrealistically low [Got98]. *Topology* is the mathematical study of those properties of geometric objects that are invariant under small perturbations. The key insight of TQC is that instead of storing quantum information in the states of individual particles, the information can be stored in topological invariants of geometric objects. As such, even when physical errors happen (e.g. the geometric object is perturbed) the information stored in the qubits remains the same. More than being error correcting, TQC is naturally error resistant!

As a thought experiment to reinforce this idea, suppose that Alice and Bob are placed across the country, and are given only a string to communicate. By "string" we really mean string: This is some physical piece of twine or rope. They can ship this string via train, and through this process there will undoubtedly be errors (e.g. the string will get pushed around during the voyage). How can Alice and Bob effectively communicate, while being relatively confident there are no errors?

The answer is simple: Store the information in knots! By tying a certain number of simple knots in the string Alice can specify an integer that Bob can

Figure 2.2: An Incan Quipu

simply read off by counting (as in Figure 2.1)! The beauty lies in the fact that while the string may be perturbed during the sending process, it would take a very specialized and unlikely error to untie the rope or to accidently re-tie an extra knot. This knotting number is a topological invariant (small perturbations don't change how many knots were tied), and so we can see intuitively that topological invariants are naturally error resistant.

The above situation is more than just a thought experiment: This is exactly the scheme that the ancient South American Incas used over 4000 years ago! The Incas stored all sorts of information in *Quipus*, intricately knotted collections of fibered strings [AA81] as seen in Figure 2.2. Storing information in knot invariants was also common practice in ancient Chinese, Tibetan, and Polynesian cultures [Day21]. In a sense, these are the earliest examples of topological computation.

In TQC, information is still stored in knots. The main difference is that the strings being knotted are no longer physical pieces of twine, but *trajectories of quasiparticles through spacetime*. For instance, suppose X and Z are two quasiparticles (we will elaborate more on this in later). Moving through space from time t_0 to t_1, the trajectories can look something like Figure 2.3. Quantum interactions cause the knotting to yield real differences in physical states, and hence these knots can be used to store quantum information.

Notice that to make 3 dimensional spacetime, we modeled space as being 2 dimensional. While one might initially think this is a quirk of our human incapacity of visualizing 4 dimensional space, there is a deeper mathematical truth at play: There are no knots in 4 dimensional space. The extra dimension always gives the strands space to evade and move past each other without collision. In particular, for TQC to work we must have space be two dimensional. While this task seems initially impossible, phases of matter living entirely in a two dimensional subspace of our three dimensional world have been experimentally constructd[3]. Things that behave like particles in these 2 dimensional phases of matter are known as quasiparticles, and form non-trivial knots when braided.

[3]Of course, these are not *literally* two dimensional. Motion in the third dimension is just so tightly constrained that 3D models break down, and 2D models start to work.

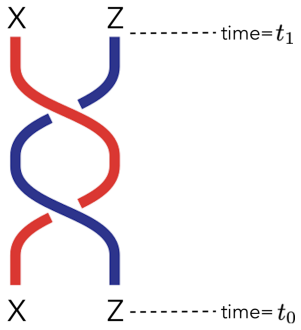


Figure 2.3: Braiding of quasiparticles in spacetime [WORK: do this in tikz]

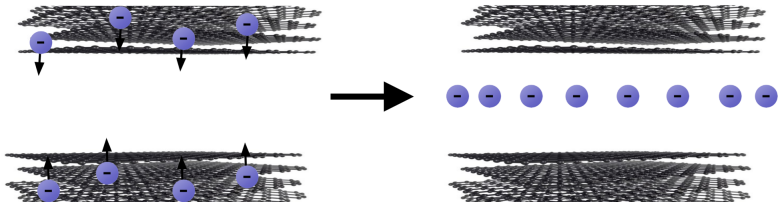


Figure 2.4: The formation of an electron gas from graphene.

The following is a rough description of how these 2 dimensional electron gasses are constructed. One begins by preparing a series of layers of graphene with a small gap in the middle. Upon subjecting the system to extremely cold temperatures and an extremely high magnetic field, the electrons in the graphene begin to move around. To balance the electric charge on both sides, all of the electrons move to the exact center of the setup. This resulting thin layer of electrons is a two dimensional electron gas. In such extreme conditions, all of the electrons will become highly entangled with each other, forming a quantum phase of matter [YZB+21]. A diagram showing this process is found in Figure 2.4

A key insight of Kitaev [Kit03], and one of the motivating pushes towards quantum computation, was that the topological properties of the 2 dimensional phase of matter will determine how the electrons entangled with each other. In other words, 2 dimensional sheets of electrons will form different quantum systems depending on their shape.

To understand this better, suppose that you have a 2 dimensional sphere of electrons. They will want to quantize, and align their spins together in the same direction. This amounts to choosing a unit tangent vector at each point on the sphere. However, there is no coherent way to do this. Every choice of tangent vectors will necessarily have some discontinuity or singularity: This is

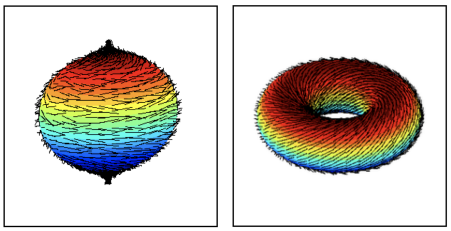


Figure 2.5: Assigning vector fields (spins) to a sphere, verses to a torus

the content of the "Hairy Ball Theorem".

If your sheet of electrons was on a donut, however, the situation is much different. There are several ways to coherently assign unit tangent vectors to each point; thus there are several ways for all of the electrons to quantize their spins together, as seen in Figure 2.5. This is aptly known as a *spin liquid*. In mathematical language a "donut" is called a torus, hence the name *toric code*. The spin liquid associated with this procedure on a torus is called the "$\mathbb{Z}_2$ spin liquid", and it is the physical realization of the toric code. We will spend the body of this manuscript describing the mathematics of the toric code in more detail. Note that generally when making such $\mathbb{Z}_2$ spin liquids in labs one does not make an actual torus; instead, one artificially simulates the boundary conditions of a torus in nanowires, for technical reasons [AHM$^+$16, MZF$^+$12].

We find it illustrative here to make an analogy with classical computing. Consider the following puzzle: Classical bits are stored in the magnetization of small regions on a hard disk. The magnetization of each atom is highly sensitive to thermal fluctuations. So why is it that classical computers seem so resistant to errors? The answer is that since all of the atoms are magnetized in the same direction, any one atom flipping will automatically be corrected back by the normalizing influence of the other atoms: magnets are naturally error resistant. It is exactly the same with these spin liquids that quantize together: Any one electron's spin decohering will immediately be corrected by the normalizing influence of all of its neighbors.

Before moving on to an in-depth treatment of the toric code, we offer a general description of the TQC process, in the style of the three points listed in the beginning of the introduction:

1. Information is stored in the ground states of topological quantum materials.

2. Ground states are acted on by braiding of quasiparticles, that is, by generating pairs of quasiparticles and knotting them in spacetime.

3. Measurements are performed by observing the topological properties of the resulting ground state.

Here, *ground state* refers to a state in the system with lowest possible energy. Note that in the previous description of spin liquids, all electrons having the same spin is a result of them being in the lowest energy state. An "excited" electron with deviant spin will raise the energy of the system. These excited electrons are quasiparticles. In this way, quasiparticles can be interpreted as excitations of a topological quantum material. This motivates the fact that (topological) quantum computers must be exceptionally cold to function: Any extra energy will correspond to extra excitations, causing the computer to malfunction, since information is only stored in ground states.

The possibilities for topological quantum materials and TQC are extremely exciting, and we are eager to see where the field will go in the coming years.

3 Quantum foundations

In this appendix we introduce quantum mechanics and quantum computation, from a mathematical perspective. Namely, we state the axioms of quantum mechanics, the relevant definitions and theorems from linear algebra, and a short discussion of information theory. The goal of quantum mechanics is to describe the microscopic world, where physical phenomina are wholy different than in the macroscopic world. Probabilities don't work in the usual sense (leading to phenomina like *interference*), and objects are modeled simultaneously as particles and waves (leading to phenomina like *superposition* and *entanglement*). This endows quantum information theory with a number of number of counter-intuitive phenomina, like *no-cloning theorems* and *quantum teleportation*.

Throughout this appendix, we will strongly use analogy with the classical theory of probability, which we recall in a mathematically rigorous way now. Let S be a finite set of states. For example, when modelling the flipping of a coin, we might let $S = \{\text{heads, tails}\}$. When modeling the positions of pieces on a chessboard, S could be the 64 element set of chessboard squares. A probability distribution on S is an assignment of positive real numbers (probabilities) p_x for each $x \in S$, such that that the total probability $\sum_{x \in S} p_x$ is 1. For example, if we have two states $S = \{\text{accept, deny}\}$ and there is a 90% chance we will accept, then $p_{\text{accept}} = .9$ and $p_{\text{deny}} = .1$.

It is now clear why linear algebra is the correct field of study to analyse probabilities. Assigning a real number to every element in a set S is exactly the same as choosing a vector in the vector space $\mathbb{R}[S]$, the real vector space defined to have S as a basis. That is, every vector in vector space is uniquely defined as a linear combination of basis elements. If we have probabilities p_x assigned to every $x \in S$, then this corresponds to the vector $\sum_{x \in S} p_x |x\rangle \in \mathbb{R}[S]$. For example, the previous example of accepting and denying can be conciesely summarized as the equation

$$.9 |\text{accept}\rangle + .1 |\text{deny}\rangle \in \mathbb{R}[S] = \mathbb{R}[\{\text{accept, deny}\}].$$

We make a comment about our notation. We use the bars/angle-brackets $|\cdot\rangle$ to formally seperate elements of our set S from the numbers used when taking

linear combinations. This is neccecarily, for if S the elements of S were numbers there would be immediate confusion otherwise. For instance, if $S = \{0, 1\}$, then the distribution with probability $\frac{2}{3}$ given to 0 and probability $\frac{1}{3}$ given to 1 would be notated $\frac{2}{3}0 + \frac{1}{3}1$. Upon seperating with bars/angle-brackets, we arrive at the much more sensible $\frac{2}{3}|0\rangle + \frac{1}{3}|1\rangle$. The symbol $|\cdot\rangle$ us known as a *ket*. This notation is ubiquitous across quantum mechanics for representing states.

Now, suppose we want to model the following process using this language of vector spaces. We start by flipping a coin. Then, we take a second coin. If the result of the first coin was heads, then we set the second coin to heads. If the result of the first coin was tails, then we flip the second coin randomly. Symbolically, writing h for heads and t for tails, this is seen as

$$\begin{array}{ccccc} |\text{start}\rangle & \longrightarrow & \frac{1}{2}|\text{h}\rangle + \frac{1}{2}|\text{t}\rangle & \longrightarrow & \frac{1}{2}(|\text{hh}\rangle) + \frac{1}{2}\left(\frac{1}{2}|\text{th}\rangle + \frac{1}{2}|\text{tt}\rangle\right). \\ \cap & & \cap & & \cap \\ \mathbb{R}[\{\text{start}\}] & & \mathbb{R}[\{\text{h}, \text{t}\}] & & \mathbb{R}[\{\text{hh},\ \text{ht},\ \text{th},\ \text{tt}\}] \end{array}$$

We introduce the following terminology, for ease of dicsussion. A *pure state* is an element of S, and a *mixed state* is a general element of $\mathbb{R}[S]$. General probability distributions are mixed states. When the probabilistic system is measured, a mixed state $\sum_{x \in S} p_x |x\rangle$ will "collapse" onto a pure state, going to each x with probability p_x. In light of this terminology, it makes sense to refer to $\mathbb{R}[S]$ as a state space. Not all mixed states are realistic. That is, $-\frac{1}{2}|\text{heads}\rangle + \frac{1}{2}|\text{tails}\rangle$ can never occur because one cannot have negative probabilities. A *normalized vector* (or, *normalized state*) in $\mathbb{R}[S]$ is a vector which can be written as $\sum_{x \in S} p_x |x\rangle$, where $p_x \geq 0$ and $\sum_{x \in S} p_x = 1$.

General probabilistic processes can be described very simply now. A process that goes from probability distribution on a finite set S to a probability distribution on a finite set S' can be described as a linear map $\mathbb{R}[S] \to \mathbb{R}[S']$, sending normalized vectors to normalized vectors. The fact that map is linear is a direct consequence of the basic rules of probability. In our above example, linearity is the fact one gets the correct answer from using the maniputation

$$\frac{1}{2}(|\text{hh}\rangle) + \frac{1}{2}\left(\frac{1}{2}|\text{th}\rangle + \frac{1}{2}|\text{tt}\rangle\right) = \frac{1}{2}|\text{hh}\rangle + \frac{1}{4}|\text{th}\rangle + \frac{1}{4}|\text{tt}\rangle.$$

We now discuss what happens when one joins two systems together. That is, let S and S' be two finite sets. We wish to speak of joint proability distributions over S and S'. That is, distributions where one samples over elements of S and S'. This corresponds to choosing probabilities $p_{(s,s')}$ for each pair of elements $(s, s') \in S \times S'$, living in the Cartesian product of S and S'. While physically trivial, this observation has important mathematical consequences. We can now state our axioms in a complete way:

Definition (Axioms of probability theory)**.**

1. (Systems) A probabilistic system is a real vector space of the form $\mathbb{R}[S]$, where S is a finite set. The normalized vectors in $\mathbb{R}[S]$ correspond to probability distributions on S.

2. (Processes) A probabilistic process going from a system S to a system S' is a linear map $\mathbb{R}[S] \to \mathbb{R}[S']$, which sends normalized vectors to normalized vectors.

3. (Joining systems) If S and S' are two probabilistic systems, the system obtained by joining S and S' is equal to the system $S \times S'$.

4. (Measuring systems) Given a normalized vector $\sum_{x \in S} p_x |x\rangle \in \mathbb{R}[S]$, measurement corresponds to collapsing into a pure state, where we observe each $x \in S$ with probability p_x.

□

We can state quantum mechanics in exactly the same way:

Definition (Axioms of quantum mechanics, basis dependent version)**.**

1. (Systems) A quantum system is a complex vector space of the form $\mathbb{C}[S]$, where S is a finite set. The normalized vectors in $\mathbb{C}[S]$ correspond to complex states on S. A *normalized* vector $v = \sum_{x \in S} c_x |x\rangle$ is one for which $\sum_{x \in S} |c_x|^2 = 1$, where $|c_x|^2$ denotes the norm square.

2. (Processes) A quantum process going from a system S to a system S' is a linear map $\mathbb{C}[S] \to \mathbb{C}[S']$, which sends normalized vectors to normalized vectors.

3. (Joining systems) If S and S' are two quantum systems, the system obtained by joining S and S' is equal to the system $S \times S'$.

4. (Measuring systems) Given a normalized vector $\sum_{x \in S} c_x |x\rangle \in \mathbb{C}[S]$, measurement corresponds to collapsing into a pure state, where we observe each $x \in S$ with probability $|c_x|^2$.

□

The quantity $\sum_{x \in S} |c_x|$ is called the 1-norm, and $\sqrt{\sum_{x \in S} |c_x|^2}$ is called the 2-norm. The following quote summarizes the above definition:

> "What happens if you try to come up with a theory that's *like* probability theory, but based on the 2-norm instead of the 1-norm?... Quantum mechanics is what inevitably results." - Scott Aaronson[4]

While fully mathematically rigorous, we now add some physical interpretation to the axioms of quantum mechanics. Let $|\psi\rangle = \sum_{x \in S} c_x |x\rangle \in \mathbb{C}[S]$ be a normalized vector in a quantum system. We call $|\psi\rangle$ a quantum state. Wave-particle duality can be understood as follows:

[4]Page 112 of Aaronson's "Quantum Computing since Democritus" [Aar13]

- Particle = Single position; definite = pure state = $|x\rangle$, $x \in S$
- Wave = Multiple positions; spread-out = mixed state = $|\psi\rangle \in \mathbb{C}[S]$.

We can thus say that quantum states are waves, but when they are measured they collapse into a particle. A mixed state is said to be in a *superposition* of the pure states it is a linear combination of. We call the expression $\sum_{x \in S} c_x |x\rangle$ the wave function of $|\psi\rangle$, with c_x being the amplitudes.

We now demonstrate interference. Consider the quantum system with pure states $S = \{0, 1\}$. This is called a qubit. More generally, a qubit is the term used for any two-dimensional quantum system. Define the transformation $H : \mathbb{C}[S] \to \mathbb{C}[S]$ by

$$H(|0\rangle) = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle ,$$

$$H(|1\rangle) = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle .$$

Applying H to $|0\rangle$ and measuring gives 0 and 1 with equal probability, and same with applying H to $|1\rangle$. When we apply H to the equal superposition of 0 and 1, however, results in

$$H\left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle\right) = \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle\right) + \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle\right) = |0\rangle .$$

We can summarize this as saying that there was *constructive interference* in the $|0\rangle$s, and *destructive interference* in the $|1\rangle$s. The amplitudes had the same signs in the $|0\rangle$s causing the proabability of measuring 0 to add, and the amplitudes had opposite signs in the $|1\rangle$s, causing the probabilities of measuring 1 to cancel and give 0. This linear map H defined is called the Hadamard gate, and it is a very important process in quantum information theory. It is not immediately clear that H sends all normalized vectors to normalized vectors. For instance, if we had defined $H(|1\rangle) = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$ then applying H to the equal superpositoin of 0 and 1 would not give a normalized value. The following proposition clarifies exactly what transformations are allowed in quantum mechancis:

Proposition 3.1. *Let S be a finite set, and let $U : \mathbb{C}[S] \to \mathbb{C}[S]$ a linear transformation. The following are equivilant:*

1. *U sends normalized vectors to normalized vectors.*
2. *$U^\dagger = U^{-1}$, where $\dagger$ denotes the conjugate transpose.*

If either of the two equivilant conditions are met, we call U a unitary matrix.

Proof. Given $|\phi\rangle = \sum_{x\in S} c_x |x\rangle$ and, $|\psi\rangle = \sum_{x\in S} d_x \in \mathbb{C}[S]$, define

$$\langle\phi|\psi\rangle = \sum_{x\in S} c_x \overline{d_x},$$

where $\bar{\cdot}$ denotes the complex conjugate, We find that

$$\langle\psi|\psi\rangle = \sum_{x\in S} |c_x|^2$$

is equal to the norm square of $|\psi\rangle$. The statement that U preserves norm is exactly the statement

$$\langle U\psi|U\psi\rangle = \langle\psi|\psi\rangle .$$

For complex numbers $a, b \in \mathbb{C}$, expanding linearly the definition it is clear that

$$\langle a\phi_0 + b\phi_1|\psi\rangle = a\langle\phi_0|\psi\rangle + b\langle\phi_1|\psi\rangle$$

and

$$\langle\phi|a\psi_0 + b\psi_1\rangle = \overline{a}\langle\phi|\psi_0\rangle + \overline{b}\langle\phi_1|\psi_1\rangle .$$

Extending with this formula, we find that U preserving norm implies $\langle U\phi|U\psi\rangle = \langle\phi|\psi\rangle$ for all $|\psi\rangle, |\phi\rangle$. Let $UU^\dagger$ be the product of U with its conjugate transpose. This can be represented as a matrix whose rows and collumns are labeled by elements of S. Given $(x, y) \in S$, then (x, y) entry is

$$\sum_{z\in S} u_{x,z}\overline{u_{y,z}} = \langle Ux|Uy\rangle ,$$

where $u_{x,z}$ is the (x, z) entry of U. We thus follow through the equivilance

$$\begin{aligned}
&\left(UU^\dagger = I\right)\\
\iff &\left(\langle Ux|Uy\rangle = \begin{cases} 1 & x = y \\ 0 & \text{otherwise} \end{cases} \quad \forall x, y \in S\right)\\
\iff &\left(\langle Ux|Uy\rangle = \langle x, y\rangle ,\ \forall x, y \in S\right)\\
\iff &\left(U \text{ preserves norms}\right)
\end{aligned}$$

which gives us the desired conclusion. □

We now comment on measurement. A big component glossed over in the previous discussion is *observables*. When a quantum system is measured, one typically will have an associated observable. For example, let S be the set of possible energy levels of a hydrogen atom. Typically, states $|\psi\rangle$ will be in superpositions of possible energies. Measuring energy results in collapsing the wavefunction onto a given energy level. The observed quantity is a number - the

energy of the level that was collapsed to. Thus, a realistic model of measurement should correspond to not only collapsing onto a pure state, but also choosing a real number to be observed.

In the most general form of measurement, one might want to measure in a basis other than the canonical basis. Thus, the process can be described as starting with a state $|\psi\rangle \in \mathbb{C}[S]$, applying a change of basis matrix $U^{-1} : \mathbb{C}[S] \to \mathbb{C}[S]$, choosing real numbers (ovservables) to correspond to each state, collapsing onto a pure state, observing the observable, then reversing the change of basis with a matrix $U : \mathbb{C}[S] \to \mathbb{C}[S]$. In terms of linear algebra, this can be concisely written as follows. Let D be the diagonal matrix, whose entires on the diagonal correspond to the real numbers chosen as observables for each pute state. Let

$$H = UDU^{-1}$$

be a matrix. The pure states in the U-basis are now the eigenvectors of H, and the observables are the eigenvalues. The following proposition clarifies exactly what measurements are allowed in quantum mechanics:

Proposition 3.2. *Let S be a finite set, and let $H : \mathbb{C}[S] \to \mathbb{C}[S]$ be a linear transformation. The following are equivilant:*

1. *H can be written in the form UDU^{-1} for a unitary matrix U and a diagonal matrix D.*
2. *$H = H^\dagger$.*

If either of the two equivilant conditions are met, we call H a Hermitian matrix.

Proof. We begin by showing the first direction. Suppose $H = UDU^{-1}$. Since $U^{-1} = U^\dagger$, we may write $H = UDU^\dagger$. Expanding $H^\dagger$, we find

$$\begin{aligned} H^\dagger &= (UDU^\dagger)^\dagger \\ &= U^{\dagger\dagger} D^\dagger U^\dagger \\ &= UDU^\dagger \\ &= H. \end{aligned}$$

Here, we used that $D^\dagger = D$ since it is real symmetric, hence fixed under both taking transpose and complex conjugate. We also used that $U^{\dagger\dagger} = U$, which comes from the fact that taking two complex conjugates and two transposes takes a matrix back to itself.

The converse is much more difficult. This is the so called *spectral theorem* of linear algebra, and its proof would take us too far away. A good reference for this sort of linear algebra, with a special emphasis on spectral theorems, is Hall's book [Hal13]. □

The conditions on untitary and Hermitian matricies we have obtained are independent of unitary change of basis, in the sense that unitary (resp. Hermitian) matricies will stay unitary (resp. Hermitian) under a unitary change of basis. Additionally, unitary matricies are defined to send normalized vectors to normalized vectors, and hence normalized vectors are a unitary basis-independent notion as well. This almost allows us to state the axioms of quantum mechanics in a basis independent way. The trouble is that the notations of unitary, Hermitian, and normalized are not invariant under arbitarary change of basis. The solution to this problem is to introduce *Hilbert spaces*. Roughly, Hilbert spaces are vector spaces paired with a notion of normalization, which allows one to define unitary and Hermitian matricies. Abstractly, in the same way that there is a canonical identification

$$\text{(Vector spaces with basis) / (change of basis)} \cong \text{(Vector spaces)}\,,$$

there is an identification

$$\text{(Vector spaces with basis) / (orthogonal change of basis)} \cong \text{(Hilbert spaces)}\,.$$

Formally, we have the following:

Definition (Hilbert space)**.** A Hilbert space is the following data:

1. A vector space V
2. (Inner product) A map $\langle\cdot|\cdot\rangle : V \times V \to V$

Additionally, a Hilbert space is required to satisfy the following properties:

1. (Conjugate symmetric) $\langle\phi|\psi\rangle = \overline{\langle\psi|\phi\rangle}$, for all $|\psi\rangle, |\phi\rangle \in V$, where $\bar{\cdot}$ denotes the complex conjugate.
2. (Linearity in first component) $\langle a\phi_0 + b\phi_1|\psi\rangle = a\langle\phi_0|\psi\rangle + b\langle\phi_1|\psi\rangle$, for all $a, b \in \mathbb{C}$, and $|\phi_0\rangle, |\phi_1\rangle, |\psi\rangle \in V$.
3. (Positive definite) The real number $\langle\psi|\psi\rangle$, $|\psi\rangle \in V$, is always non-negative, and is 0 if and only if $\psi = 0$.

□

It follows from these axioms that $\langle\cdot|\cdot\rangle$ is conjugate linear in the second component:

$$\langle\phi|a\psi_0 + b\psi_1\rangle = \overline{a}\langle\phi|\psi_0\rangle + \overline{b}\langle\phi|\psi_1\rangle\,.$$

The point of this definition is that we can define the norm of $|\psi\rangle \in V$ to be $\sqrt{\langle\psi|\psi\rangle}$, and thus by forcing $\langle\psi|\psi\rangle = 1$ we have a well-defined notion of normalized vector. We now show that Hilbert spaces have the desired property of characterizing vector spaces up to orthogonal change of basis:

Proposition 3.3. *Let V be a an n dimensional vector space. The following statements are true:*

1. *If $\langle\cdot|\cdot\rangle$ is an inner product on V, there exists an orthonormal basis with respect to $\langle\cdot|\cdot\rangle$. That is, a basis $|x_k\rangle$, $k \in \{0...n-1\}$ such that*

$$\langle x_k|x_j\rangle = \begin{cases} 1 & k = j \\ 0 & \text{otherwise.} \end{cases}$$

2. *Suppose $|x_k\rangle$, $k \in \{0...n-1\}$ is a basis for V. Define the map $\langle\cdot|\cdot\rangle : V \times V \to V$ as follows. Given $|\phi\rangle = \sum_{k=0}^{n-1} c_k |x_k\rangle$ and $|\psi\rangle = \sum_{k=0}^{n-1} d_k |x_k\rangle$,*

$$\langle\phi|\psi\rangle = \sum_{k=0}^{n-1} c_k \overline{d}_k.$$

   This is an inner product, and gives V the structure of a Hilbert space. $(|x_k\rangle)_{k=0}^{n-1}$ is an orthonormal basis with respect to this inner product.

3. *Two bases induce the same Hilbert space structure on V if and only if they can be related to each other by a unitary matrix.*

In this sense, one can canonically identitify equivilance classes of based vector spaces up to orthogonal change of basis with Hilbert spaces.

Proof.

1. We proceed by induction on n. When $n = 1$, let $|\tilde{x}_0\rangle$ be any non-zero vector. By positive definiteness, $\langle\tilde{x}_0|\tilde{x}_0\rangle \neq 0$. Letting

$$|x_0\rangle = \langle\tilde{x}_0|\tilde{x}_0\rangle^{-1/2} \cdot |\tilde{x}_0\rangle$$

   we get a normalized basis vector for V. For the inductive step, suppose that every $n-1$ dimensional Hilbert space has an orthonormal basis. Choose an $n-1$ dimensional subspace V' of V. The inner product on V restricts to an inner product on V'. Hence, by the inductive step there is an orthonormal basis $(|x_k\rangle)_{k=0}^{n-2}$ of V'. Choose any vector $|\psi\rangle \notin V'$. Set

$$|\tilde{x}_{n-1}\rangle = |\psi\rangle - \sum_{k=0}^{n-1} \langle\psi|x_k\rangle \cdot |x_k\rangle .$$

   We compute for any $j \leq k-2$

$$\begin{aligned} \langle\tilde{x}_{n-1}|x_j\rangle &= \langle\psi|x_j\rangle - \sum_{k=0}^{n-1} \langle\psi|x_k\rangle \cdot \langle x_k|x_j\rangle \\ &= \langle\psi|x_j\rangle - \langle\psi|x_j\rangle = 0. \end{aligned}$$

The vector $|x_{n-1}\rangle = \langle \tilde{x}_{n-1}, \tilde{x}_{n-}\rangle^{-1/2} \cdot |\tilde{x}_{n-1}\rangle$ thus completes the construction of an orthonormal basis for $\langle \cdot | \cdot \rangle$.

2. Verifying thee axioms is immediate, and is left as an exercise to the reader (Exercise 3.3)

3. Suppose two bases are related by a unitary transformation. Since the unitary transformation preserves the inner product, the inner product induced by the two bases are the same. Conversely, suppose that two bases induce the same inner product. This means that the change of basis matrix preserves the inner product, hence is unitary, and hence the two bases are related by a unitary change of basis.

□

We can now state everything in a basis independent fashion. A normalized vector is one in which the norm square $\langle \psi | \psi \rangle$ equals one. A unitary matrix is a matrix which preserves the norm. That is, $\langle U\psi | U\phi \rangle = \langle \psi | \phi \rangle$ for all $|\phi\rangle, |\psi\rangle$. A Hermitian matrix is one which is a diagonal matrix with real entries in some orthonormal basis. In terms of the inner product, this can be characterized as saying that $\langle \psi, H\phi \rangle = \langle H\psi, \phi \rangle$ (see Exercise 3.1).

Our last task for a basis independent statement of quantum mechanics is joining systems. Here, we use the following observation. For finite sets S and S', there is a canonical isomorphism

$$\begin{gathered} \mathbb{C}[S] \otimes \mathbb{C}[S'] \xrightarrow{\sim} \mathbb{C}[S \times S']. \\ |x\rangle \otimes |x'\rangle \mapsto |(x, x')\rangle \end{gathered}$$

The basis-independent version of taking the Cartesian products of underlying sets is hence taking the tensor product. Given Hilbert spaces $(V, \langle \cdot | \cdot \rangle_V)$ and $(W, \langle \cdot | \cdot \rangle_W)$, we define a space structure on $V \otimes W$ by

$$\langle x_0 \otimes x_1 | y_0 \otimes y_1 \rangle = \langle x_0 | x_1 \rangle_V \otimes \langle y_0 | y_1 \rangle_W ,$$

where $x_0, x_1 \in V$, $y_0, y_1 \in W$. We verify in Exercise 3.2 that this is indeed an inner product. Thus, we can state the axioms of quantum mechanics as follows:

Definition (Axioms of quantum mechanics, basis independent version)**.**

1. (Systems) A quantum system is a complex Hilbert space V

2. (Processes) A quantum process going from a system V to a system W is an orthogonal transformation from V to W

3. (Joining systems) If V and W are two quantum systems, the system obtained by joining V and W is equal to the system $V \otimes W$.

4. (Measuring systems) Given a normalized vector in $|\psi\rangle \in V$, measurement corresponds to Hermitian matricies H. Namely, writting $|\psi\rangle = \sum_{k=0}^{n-1} c_k |x_k\rangle$ where $(|x_k\rangle)_{k=0}^{n-1}$ is an orthonomal basis of eigenvectors of H, measurement will collapse $|\psi\rangle$ onto one of the pure states, going to the state $|x_k\rangle$ with probability $|c_k|^2$. One additionally will physically observe the number corresponding to the eigenvalue of H at $|x_k\rangle$.

□

While Hilbert spaces are more technically accurate, we will often be thinking of quantum systems as simple vector spaces. This is done for two reasons.

1. In simple situations we will often be extremely explicit with choosing bases, and hence we will not need the basis independent language of Hilbert spaces

2. In complex situations keeping track of inner products is too complicated, and hence we work in the simpler situation of vector spaces. When this becomes an issue we will add conditions to simulate Hilbert space structure (for example, adding a unitarity condition to Modular Tensor Categories), though this is often unnececary.

We now conclude with a more percise treatment of quantum computation. The goal of computer science is to perform computations on information. A computation is a way of taking in information, transforming it, and returning information. Information is a very broad term, but one of the greatest successes of information theory is the universal language of *bits*. That is, we represent general information as finite collections of 1s and $0s$. Abstractly, a classical computation is a function

$$f : \mathbb{Z}_2^n \to \mathbb{Z}_2^m,$$

where $\mathbb{Z}_2 = \{0, 1\}$, and $\mathbb{Z}_2^n$ is the n-fold cartesian product, consisting of length-n bit strings. All classical processes can be modeles as first writing your information as an element of $\mathbb{Z}_2^n$ for large enough n, writing a function form $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^m$ which performs the desired task, and reading out elements of $\mathbb{Z}_2^m$ in the correct way. A randomized algorithm is thus exactly the same thing, except with random processes instead of deterministic ones. Namely, a randomized computation is a probabilistic process

$$f : \mathbb{R}[\mathbb{Z}_2^n] \to \mathbb{R}[\mathbb{Z}_2^m].$$

A quantum computation is a quantum process

$$f : \mathbb{C}[\mathbb{Z}_2^n] \to \mathbb{C}[\mathbb{Z}_2^m].$$

This can be seen as taking superpositions of length-n bit strings to superpositions of length-m bit strings. It is often more pleasant to consider quantum computations in a basis-independent language. Namely, we have a canonical

isomorphism $\mathbb{C}[\mathbb{Z}_2^n] \cong \mathbb{C}[\mathbb{Z}_2]^{\otimes n}$, where $\otimes n$ dentoes the n-fold tensor product of a space with itself. We can now identify $\mathbb{C}[\mathbb{Z}_2]$ with $\mathbb{C}^2$, where $\mathbb{C}^2$ is given the Hilbert space structure inherited by the prefered basis $\{|0\rangle, |1\rangle\}$. Thus, a basis-independent quantum computation is a unitary transformation

$$f : \left(\mathbb{C}^2\right)^{\otimes n} \to \left(\mathbb{C}^2\right)^{\otimes m}.$$

The two dimensional quantum system $\mathbb{C}^2$ is called a qubit. It is now clear that specifying a theory of quantum computation requires specifying

1. How quantum information is stored. That is, what physically object will have associated quantum state-space which we identity with $\left(\mathbb{C}^2\right)^{\otimes n}$.
2. How quantum informatoin is acted on. That is, what physical actions one will do to perform the function f.
3. How quantum information is measured. That is, how one can observables one can measure to reliably read information about quantum states from $\left(\mathbb{C}^2\right)^{\otimes m}$.

This concludes our introduction of quantum mechancis.

Exercises:

3.1. Let $(V, \langle\cdot|\cdot\rangle)$ be a Hilbert space. Let $H : V \to V$ be a linear transformation. Verify that H is Hermitian if and only if

$$\langle\psi|H\phi\rangle = \langle H\psi|\phi\rangle$$

for all $|\psi\rangle, |\phi\rangle \in V$.

3.2. Given Hilbert spaces $(V, \langle\cdot|\cdot\rangle_V)$ and $(W, \langle\cdot|\cdot\rangle_W)$, we define a space structure on $V \otimes W$ by

$$\langle x_0 \otimes x_1 | y_0 \otimes y_1\rangle = \langle x_0|x_1\rangle_V \otimes \langle y_0|y_1\rangle_W,$$

where $x_0, x_1 \in V$, $y_0, y_1 \in W$. Show that $\langle\cdot|\cdot\rangle$ is an inner product.

3.3. Verify Proposition 3.3 part (2).

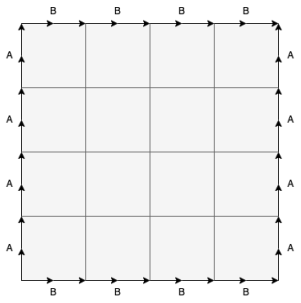


Figure 4.1: Celluation of the torus, obtained by gluing opposite sides together [WORK: add "=donut" visual].

4 The Toric Code

Consider a torus. We will be imagining the torus as a whole as being a quantum system, corresponding physically to the quantum system one would observe when the torus is in the $\mathbb{Z}_2$ spin liquid topological quantum phase of matter. The *code space* of the torus is the space of states on which we will be building our quantum computer, i.e., those states we will be using to store quantum information. In general Topological Quantum Computing (TQC) fashion, the code space of the toric code will be its ground states.

Our mathematical priorities are thus as follows: To define the quantum system, and to define a Hamiltonian operator on it. A Hamiltonian is an operator corresponding to the total energy of a quantum system. Namely, the eigenvalue of an eigenstate of the Hamiltonian corresponds to the total energy of that state. The code space will thus be the lowest eigenspace of the Hamiltonian.

Working with a continuous torus and the corresponding infinite dimensional vector spaces is cumbersome and unnecessary. Instead, we celluate the torus into an n by n square lattice with opposing sides identified, as in Figure 4.1. We will work with the understanding that the real physical system is the limit as $n \to \infty$. We define the quantum system associated with the n by n celluated torus to be the vector space

$$\mathcal{N} = \bigotimes_{\substack{\text{edges of} \\ \text{torus}}} \mathbb{C}^2,$$

obtained by "putting a qubit[5] on every edge". Here and throughout, *vertices*, *edges*, and *faces*, when used as indexing sets, will refer to the set of *vertices*, *edges*, and *faces* of our celluated torus. We will choose a canonical basis $\{|0\rangle, |1\rangle\}$ for $\mathbb{C}^2$, reflecting our information theoretic intentions. To more forward with defining the Hamiltonian, we introduce the Pauli matrices

[5] A qubit is the quantum-computing term for "two dimensional quantum system", i.e., $\mathbb{C}^2$.

$$\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ \sigma_Z = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

The Hamiltonian is defined by

$$H = -\sum_{\text{vertices } v} A_v - \sum_{\text{faces } p} B_p,$$

where

$$A_v = \bigotimes_{\substack{\text{edges} \\ \text{touching } v}} \sigma_Z,\ B_p = \bigotimes_{\substack{\text{edges} \\ \text{touching } p}} \sigma_X.$$

All of the power of the toric code comes from this highly non-obvious choice of Hamiltonian. The physical interpretation for this choice of Hamiltonian comes from gauge theory. Namely, the $U(1)$ Lattice Gauge Theory has two fields: The Compact Gauge Field and the Electric Field. Exponentiating the Compact Gauge Field we get the σ_X operators, and exponentiating the Electric Field we get the σ_Z operators. Thus, the A_v contribute a "Gauss' Law" term, and the B_p contribute a "Magnetic Field" term to the Hamiltonian [OKMH22]. While potentially physically illuminating, this discussion of gauge theory will have no influence on the rest of the mathematics presented in this manuscript, and does not need to be understood to appreciate the toric code.

Letting I denote the identity matrix, the key facts about the A_vs and B_ps are summarized in the following proposition:

Proposition 4.1. *We have that*

(i) $A_v^2 = B_p^2 = I$ *for all* v, p

(ii) All A_v*s and* B_p*s have half eigenvalues* $+1$ *and half eigenvalues* -1

(iii) All A_v*s and* B_p*s commute*

(iv) $\prod_{vertices\ v} A_v = I$ *and* $\prod_{faces\ p} B_p = I$

Proof. (i). Multiplying tensor product matrices corresponds to simply multiplying componentwise. Hence, this part follows immediately from the relations $\sigma_X^2 = \sigma_Z^2 = I$.

(ii). We define an isomorphism between the $+1$ eigenspace and -1 eigenspace of A_v. Namely, apply σ_X to an edge e touching v. Since $\sigma_X\sigma_Z = -\sigma_Z\sigma_X$, the computation

$$A_v \left(\bigotimes_{\text{edge } e} \sigma_X \right) |\psi\rangle = -A_v \left(\bigotimes_{\text{edge } e} \sigma_X \right) A_v |\psi\rangle$$

show that a $+1$ eigenstate will be transformed into a -1 eigenstate, and a -1 eigenstate will be turned into $+1$ eigenstate. Thus, this defines an isomorphism

between the desired eigenspaces. Applying σ_Z instead of σ_X, we can define a similar isomorphism for B_p.

this will have the effect of turning a $+1$ eigenstate into a -1 eigenstate and vice-versa,

(*iii*). All the A_vs commute with each other since σ_Z commutes with itself, and all the B_ps commute with each other since σ_X commutes with itself. What's left to check is that $A_v B_p = B_p A_v$. Notice that if v is not touching the face p, none of the σ_Zs in the tensor product of A_v will be in the same spots as any of the σ_Xs as the tensor product for B_p. Hence, A_v and B_p commute in this case. If v is touching p, then exactly two of the σ_Zs in the tensor product of A_v will be in the same spots as σ_Xs in the tensor product of B_p. Hence, pulling B_v through A_v corresponds to switching σ_X and σ_Z. Since $\sigma_X \sigma_Z = -\sigma_Z \sigma_X$, this introduces an overall phase shift of $(-1)^2 = 1$. Hence, $A_v B_p = B_p A_v$ as desired!

(*iv*). Applying $\prod_{\text{vertices } v} A_v$, is the same as applying σ_Z to each vertex 2 times, since each edge touches exactly 2 vertices. Hence,

$$\prod_{\text{vertices } v} A_v = \bigotimes_{\text{edges}} \sigma_Z^2 = \bigotimes_{\text{edges}} I = I.$$

Similarly, since every edge touches exactly 2 faces, the fact that $\prod_{\text{faces } p} B_p = I$ follows from $\sigma_X^2 = 1$. □

Using the above facts about the A_vs and B_ps, we can describe the eigenspaces of H well enough to compute their dimension:

Proposition 4.2. *All eigenvalues of H are of the form $-2n^2+4q$, for an integer $q \leq n^2/2$. The $-2n^2 + 4q$ can be described as the space of states $|\psi\rangle$ such that*

$$|\{ v, p |\, A_v |\psi\rangle = -1,\ B_p |\psi\rangle = -1\}| = 2q,$$

that is, the space of states with $2q$ excitations. There will always be an even number of v such that $A_v |\psi\rangle = -1$, as well as an even number of p such that $B_p |\psi\rangle = -1$. The dimension of of this eigenspace is

$$4 \sum_{k=0}^{q} \binom{n^2}{2k} \binom{n^2}{2(q-k)}.$$

In particular, the code space of the toric code is 4 dimensional, and consists of those vectors $|\psi\rangle$ such that $A_v |\psi\rangle = B_p |\psi\rangle = |\psi\rangle$ for all v, p.

Proof. To begin, we observe the following general fact from linear algebra. If M and N are commuting matrices and $|\psi\rangle$ is an eigenvector for N with eigenvalue λ, then

$$N(M |\psi\rangle) = M(N |\psi\rangle) = \lambda(M |\psi\rangle).$$

Hence, M respect the eigenspaces of N, and vice versa. This implies that the eigenspaces for H will be simultaneous eigenspaces for all of the A_vs and B_ps, since all of the A_vs and B_ps commute by Proposition 4.1 (iii).

Suppose that $|\psi\rangle$ is an eigenstate with

$$|\{\, v, p |\, A_v \,|\psi\rangle = -1,\ B_p \,|\psi\rangle = -1\}| = q.$$

Then, we find that

$$\begin{aligned} H\,|\psi\rangle &= (-\sum_v A_v - \sum_p B_p)\,|\psi\rangle \\ &= \left(\sum_{\substack{v,p \\ -1 \text{ eigenvalue}}} 1 - \sum_{\substack{v,p \\ 1 \text{ eigenvalue}}} 1 \right) |\psi\rangle \\ &= (q - (n^2 - q)) \\ &= -n^2 + 2q. \end{aligned}$$

Thus, to complete the initial description of the eigenstates, we must show that the number of v such that $A_v\,|\psi\rangle = -1$ and the number of p such that $B_p\,|\psi\rangle = -1$ is even. This follows from the computation that is this number where odd, then we would have by Proposition 4.1 (iv) that

$$|\psi\rangle = \left(\prod_v A_v \right) |\psi\rangle = -\,|\psi\rangle\,,$$

which is a contradiction since we are supposing that $|\psi\rangle \neq 0$. The exact same argument applies to the B_p. We now compute the dimensions of the eigenspaces. Let D denote the dimension of the group space. We show that given any even sized sets $\mathbf{v}, \mathbf{p}$ of vertices and faces respectively, the space

$$\mathcal{N}_{\mathbf{v},\mathbf{p}} = \{\, |\psi\rangle |\, (A_v\,|\psi\rangle = -1 \iff v \in \mathbf{v})\,,\ (B_p\,|\psi\rangle = -1 \iff p \in \mathbf{p})\}$$

is D dimensional. We proceed by induction on $|\mathbf{v} + \mathbf{p}|$. If $|\mathbf{v} + \mathbf{p}| = 0$, then this is the definition of D. Without loss of generality, suppose $|\mathbf{v}| \geq 2$. If $|\mathbf{p}| \geq 2$, we apply the same arguement with verticies replaced by faces. Choose two verticies $v_0, v_1 \in \mathbf{v}$. Choose a path γ along the edges of the torus that connect v_0 and v_1. We show that $\bigotimes_{\text{edges in } \gamma} \sigma_X$ gives an isomorphism between $\mathcal{N}_{\mathbf{v},\mathbf{p}}$ and $\mathcal{N}_{\mathbf{v}-\{v_0,v_1\},\{p\}}$. Namely it is clear from $\sigma_X^2 = \sigma_X$, so this map is its own inverse, so it is sufficient to show that the image is in the desired space. To prove this, we observe that $\bigotimes_{\text{edges in } \gamma} \sigma_X$ commutes with all the B_ps, and commutes with all of the A_vs at verticies that γ passes through an even number of times. The only verticies that γ passes through an odd number of times are its endpoints (by definition), and hence A_v has exactly the effect of flipping the

eigenvalues at A_{v_0} and A_{v_1}. Thus, the image of a point in $\mathcal{N}_{\mathbf{v},\mathbf{p}}$ is in $\mathcal{N}_{\mathbf{v}-\{v_0,v_1\},\mathbf{p}}$, as desired.

Combining, we find that the $-2n^2 + 2q'$ eigenstate can be decomposed as direct sums of $\mathcal{N}_{\mathbf{v},\mathbf{p}}$, where $\mathbf{v}$ and $\mathbf{p}$ range over even sized sets with $|\mathbf{v}+\mathbf{p}| = q'$. In particular, $q' = 2q$ must be even. The dimension of this space is equal to D times the number of way of choosing the sets $\mathbf{v}$ and $\mathbf{q}$, i.e.,

$$D\sum_{k=0}^{q}\binom{n^2}{2k}\binom{n^2}{2(q-k)}.$$

The total dimension of eigenspaces of H can be computed as

$$\begin{aligned} D\sum_{q=0}^{2n^2}\sum_{k=0}^{q}\binom{n^2}{2k}\binom{n^2}{2(q-k)} &= D\left(\sum_{q=0}^{2n^2}\binom{n^2}{2k_0}\right) \\ &= D\cdot\left(2^{n^2-1}\right)^2 = D\cdot 2^{2n^2-2}. \end{aligned}$$

The Hamiltonian is a symmetric matrix with real coefficients, since it is the tensor product of such matrices. It is a standard fact from linear algebra that such matrices can be diagonalized, and hence the total dimension H is equal to the dimension of $\mathcal{N} = \bigotimes_{\text{edges}}\mathbb{C}^2$. Seeing as there are $2n^2$ edges this space is 2^{2n^2} dimensional, and hence we must have $D = 2^2 = 4$. □

The fact that the code space is four dimensional can be motivated as follows. By Proposition 4.1 (ii), being in the $+1$ eigenspace for each A_v and B_p will impose a condition that decreases the dimension of your space by $1/2$. Since $\mathcal{N}$ is 2^{2n^2} dimensional, imposing all n^2 of these conditions decreases the code space to 1 dimension. However, the fact that $\prod_{\text{vertices } v} A_v = I$ and $\prod_{\text{faces } p} B_p = 1$ from Proposition 4.1 (iv) shows that two of these conditions imposed were redundant, brining the code space dimension back up to $2^2 = 4$ dimensions.

To describe the generators of the codespace explicitly we will need to use the basics of homology theory with $\mathbb{Z}_2$ coefficients, where $\mathbb{Z}_2 = \{0, 1\}$ is the additive group modulo 2. For those unfamiliar, a brief introduction is included in Appendix A.

A pure state on $\mathcal{N}$ is specified by a pure state on each qubit, namely, a choice of $|0\rangle$ and $|1\rangle$ for each edge. This is exactly the data to specify a $\mathbb{Z}_2$-chain. Given a $\mathbb{Z}_2$-chain γ, we write $|\gamma\rangle$ for the associated pure state. Given any γ, γ', we write $\gamma \sim \gamma'$ to mean that γ and γ' are homologous. The following elucidates the meaning of the codespace of the toric code:

Proposition 4.3. *Let $\mathbf{0}, \alpha, \beta$, and $\alpha\beta$ be the four $\mathbb{Z}_2$ homology classes on the torus, as in Figure 4.2. Choose $\mathbf{0}_0$, α_0, β_0, and $(\alpha\beta)_0$ respectively to be representatives. Then, letting γ run over all $\mathbb{Z}_2$-cycles, we have that*

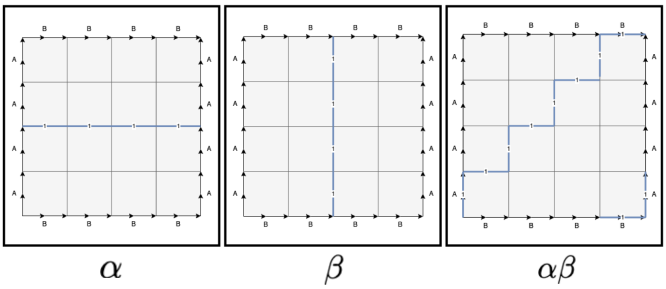


Figure 4.2: The three non-trivial homology classes of a torus

$$|\mathbf{0}\rangle = \frac{1}{\sqrt{2^{n^2-1}}} \sum_{\gamma \sim \mathbf{0}_0} |\gamma\rangle\,, \;\; |\alpha\rangle = \frac{1}{\sqrt{2^{n^2-1}}} \sum_{\gamma \sim \alpha_0} |\gamma\rangle\,,$$
$$|\beta\rangle = \frac{1}{\sqrt{2^{n^2-1}}} \sum_{\gamma \sim \beta_0} |\gamma\rangle\,, \;\; |\alpha\beta\rangle = \frac{1}{\sqrt{2^{n^2-1}}} \sum_{\gamma \sim (\alpha\beta)_0} |\gamma\rangle\,,$$

are all normalized eigenstates of that Hamiltonian H, and serve as a canonical orthonormal basis of the codespace.

Proof. Choose $\omega \in H_1(T; \mathbb{Z}_2)$. To show that $|\omega\rangle$ is in the codespace, we observe that it is in the $+1$ eigenspace of every A_v and B_p. Since σ_Z sends $|0\rangle$ to $|0\rangle$ and $|1\rangle$ to $-|1\rangle$, A_v has the effect of sending a pure state $|\gamma\rangle$ to $\pm|\gamma\rangle$, depending on whether γ has an odd or even count of edges touching the vertex v. In particular, because γ is running over cycles, we have that each $|\gamma\rangle$ is in the $+1$ eigenspace of all the A_v, and hence the same applies to $|\omega\rangle$.

For B_ps, we observe that applying B_p to a pure state $|\gamma\rangle$ has the effect of flipping all of the qubits around the face p. By definition of being $\mathbb{Z}_2$ homologous, B_p maps the space of all cycles homologous to $|\omega\rangle$ back into the space of all cycles homologous to $|\omega\rangle$. In particular, $|\omega\rangle$ is in the $+1$ eigenspace of B_p for every p.

To show that $|\omega\rangle$ is normalized, we observe that there are exactly that there are exactly 2^{n^2-1} cycles homologous to ω. This is proved as follows. Starting with a fixed representative ω_0 of ω, cycles homologous to ω correspond to flipping qubits around the edges, i.e., applying B_ps at faces. Since there are n^2 faces, this gives 2^{n^2} cycles. This overcounts the space of cycles homologous to ω by a factor of 2, since $\prod_{\text{faces } p} B_p = I$ by Proposition 4.1 (iv). The fact that the codespace is 4 dimensional says that this is the *only* relation between the B_ps. Hence, there are 2^{n^2-1} cycles.

To show that these states are mutually orthogonal, we observe simply that no cycle can be homologous to two of the $\{\mathbf{0}, \alpha, \beta, \alpha\beta\}$, hence $\{|\mathbf{0}\rangle, |\alpha\rangle, |\beta\rangle, |\alpha\beta\rangle\}$ have disjoint support, hence they are orthogonal. □

Letting T denote the torus, the above shows that we can view the codespace of the toric code as a physical realization of the vector space $\mathbb{C}[H_1(T;\mathbb{Z}_2)]$. Here, $\mathbb{C}[A]$ for some set A denotes the vector space generated by A, i.e., the unique complex vector space which has a basis given by A. Quantum physics gives the physical analogue of the abstract mathematical notation of an equivalence class, namely, an equivalence class is realized as the superposition over all possible representatives. This can be compared with the path integral formulation of quantum mechanics, where one integrates over all possible paths between two points.

We now give *quasiparticle* interpretation of the toric code. A quasiparticle is an excitation in the toric code. Namely, given an eigenstate $|\psi\rangle$, we say that there is a quasiparticle at a vertex v if $A_v |\psi\rangle = -|\psi\rangle$, and get a face p we say that there is a quasiparticle at p if $B_p |\psi\rangle = -|\psi\rangle$.

Let $|\psi\rangle$ be an eigenstate, and let v_0, v_1 be adjacent vertices connected by an edge e. Suppose that there is a quasiparticle at v_0, and that there is not a quasiparticle at v_1. Let $|\psi'\rangle$ be the state obtained by applying σ_X to the edge e. We observe that

$$A_{v_0} |\psi'\rangle = A_{v_0} \left(\bigotimes_{\text{edge } e} \sigma_X \right) |\psi\rangle = -A_{v_0} |\psi\rangle = |\psi\rangle ,$$

$$A_{v_1} |\psi'\rangle = A_{v_1} \left(\bigotimes_{\text{edge } e} \sigma_X \right) |\psi\rangle = -A_{v_1} |\psi\rangle = -|\psi\rangle ,$$

where we used the key fact that $\sigma_X \sigma_Z = -\sigma_Z \sigma_X$. Additionally, $A_v |\psi'\rangle = A_v |\psi\rangle$ for $v \neq v_0, v_1$, since applying σ_X to e only affects the verticies v_0 and v_1. We can interpret this computation as saying the following: Applying σ_X has the effect of *moving the quasiparticle along* e, from v_0 to v_1. Applying longer chains of σ_Xs, we see in general that applying σ_X corresponds to moving quasiparticles at verticies along the edges. If neither v_0 nor v_1 had quasiparticles, then again tensoring with σ_X at e would have the effect of flipping the eigenvalues at v_0 and v_1, i.e., the effect of *creating quasiparticles at the endpoints of* e, at v_0 and v_1. If both v_1 and v_1 has quasiparticles, then tensoring with σ_X at e would have the effect of *anhilating quasiparticles at the endpoints of* e.

In summary, the quasiparticles at edges are their own antiparticle. Creating particle/antiparticle pairs, moving the quasiparticles, and annihilating particle/antiparticle pairs all are mathematically realized by the simple operation of tensoring edges with σ_X.

Similarly, we can describe the quasiparticles sitting at faces, corresponding to faces with an excitation $B_p |\psi\rangle = -|\psi\rangle$. Tensoring with σ_X has no effect on these quasiparticles, since tensoring with σ_X at any edge commutes with all the B_p: σ_X commutes with itself. However, it is now tensoring with σ_Z that causes the motion of particles. Given faces p_0, p_1 with common edge e, tensoring with σ_Z at e has the effect of moving a quasiparticle from p_0 to p_1 if exactly one of the faces had a quasiparticle, has the effect of creating a particle/antiparticle

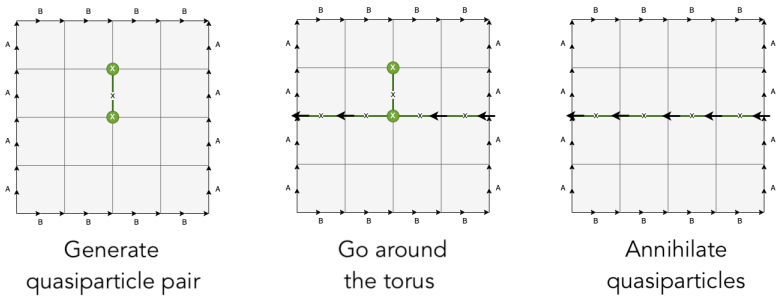


Figure 4.3: Topological quantum process implementing the NOT_α gate

pair if neither of the faces has quasiparticles, and has the effect of annihilating a particle/antiparticle pair if both faces have quasiparticles.

Summarizing, we find that the toric code naturally have two types of quasiparticles, an X-type that lives on vertices which moves by tensoring by σ_X, and a Z-type that lives in faces and moves by tensoring with σ_Z. This allows us to mathematically implement a topological quantum computer. Namely:

1. Quantum information is stored in the ground state of the toric code, i.e., the lowest eigenvalue eigenspace of the Hamiltonian.

2. Ground states are acted on by generating and manipulating quasiparticles, moving them around the torus, and annihilating them. Mathematically, this is realized by repeatedly tensoring with σ_X and σ_Z along edges, until one returns to a ground state.

3. Quantum information is measured by observing the ground state with respect to the canonical orthonormal basis of the codespace, given in Proposition 4.3

As an example, we implement the "NOT_α" gate, which flips the input state depending on whether it has an α component, namely

$$|\mathbf{0}\rangle \mapsto |\alpha\rangle\,,\ |\beta\rangle \mapsto |\alpha\beta\rangle$$
$$|\alpha\rangle \mapsto |\mathbf{0}\rangle\,,\ |\alpha\beta\rangle \mapsto |\beta\rangle\,.$$

A diagram visualizing the process described in the following proposition is shown in Figure 4.3.

Proposition 4.4. *The following computation has the effect of performing the NOT_α gate. First, generate a particle/antiparticle pair of X-type particles. Then, move one of the particles around the torus via a path homologous to α. Finally, fuse your two adjacent X-type particles together.*

Proof. Let v_0 and v_1 be adjacent vertices. Let α_0 be a cycle homologous to α going from v_1 to itself. The process described in the statement of the proposition can be reworded as saying the following. First, we create a particle pair at v_0 and v_1, i.e., we tensor with σ_X at the edge connecting v_0 and v_1. Then we move v_1 along α_0, i.e., we tensor with σ_X along the edges in α_0. Then, we fuse the X-type quasiparticles at v_0 and v_1 back together, i.e., we tensor along the edge connecting v_0 and v_1 again. Since $\sigma_X^2 = 1$, this whole process can be described mathematically as

$$\bigotimes_{\text{edges in } \alpha_0} \sigma_X.$$

Seeing as σ_Xs corresponds to flipping $|0\rangle$s to $|1\rangle$s in pure states, this process has the effect of flipping all of the qubits along α_0. On the level of cycles, this means that we take $|\gamma\rangle$ to $|\gamma + \alpha_0\rangle$, where addition is in the group of cycles. Seeing as adding a cycle homologous to α to a cycle homologous to ω results in a cycle homologous to $\omega + \alpha$ we find thus that this process has the effect of sending $|\omega\rangle$ to $|\omega + \alpha\rangle$. Seeing as $\alpha + \alpha = 0$ in $H_1(T; \mathbb{Z}_2)$, this process is exactly the NOT_α gate. □

Similarly, we can implement the "$(-1)_\alpha$" gate, which flips the input state depending on whether it has an α component, namely

$$|\mathbf{0}\rangle \mapsto |\mathbf{0}\rangle\,,\ |\beta\rangle \mapsto |\beta\rangle$$
$$|\alpha\rangle \mapsto -|\alpha\rangle\,,\ |\alpha\beta\rangle \mapsto -|\alpha\beta\rangle\,.$$

Proposition 4.5. *The following computation has the effect of performing the (-1)$_\alpha$ gate. First, generate a particle/antiparticle pair of Z-type particles. Then, move one of the particles around the torus via a path homologous to β. Finally, fuse your two adjacent Z-type particles together.*

Proof. Let p_0 and p_1 be adjacent faces. Let β_0 be a cycle homologous to β going from p_1 to itself. Note that since Z-type particles live on faces, β_0 does not consist of a series of edges. Instead, it is a path going through the centers of faces. We take $\widehat{\beta}_0$ to be the set of edges that β_0 passes through. Tensoring with σ_Z along $\widehat{\beta}_0$ corresponds to motion of a particle from p_1 along β_0 back to itself.

These cycles that go through faces of the torus are called *dual cycles*, and are standard practice in the theory of homology. Namely, they are cycles in the dual celluation, as seen in Figure 4.4. Whereas the edges associated with a normal cycle satisfy the property 'every vertex touches an even number of 1s', the edges associated with a cycle in the dual celluation satisfy the dual condition 'every face touches an even number of 1s'.

As before, we find that the whole process can be described mathematically as

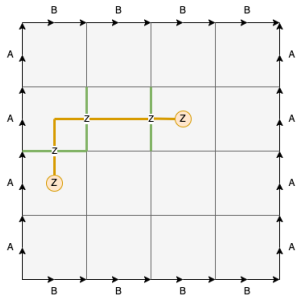


Figure 4.4: Sample trajectory along dual celluation of torus

$$\bigotimes_{\text{edges in } \widehat{\beta}_0} \sigma_Z.$$

The matrix σ_Z acts on pure states by sending $|0\rangle$ to itself, and $|1\rangle$ to $-|1\rangle$. Thus, this process has the effect of introducing a -1 global phase shift for every 1 in states along $\widehat{\beta}_0$. Thus, when acting on a pure state γ, the definition of $\widehat{\beta}_0$ shows that this process has the effect of introduce a phase shift of -1 to the power of the number of intersection between γ and $\widehat{\beta}_0$.

It is a well known fact that this signed intersection number (-1 to the power of the number of intersections) is an invariant in $\mathbb{Z}_2$ homology. To see this, observe that changing representatives of a homology class correspond to flipping qubits around a face. By the 'dual cycle' condition, this flipped face will touch an even number of elements in the dual cycle. Hence, the intersection number will change by an even amount, leaving -1 to the power of that number invariant.

In particular, $\mathbf{0}$ doesn't intersect β, β doesn't intersect β (representatives can be chosen to be parallel), α intersects β (horizontal loops and vertical loops meet at exactly one point), and $\alpha\beta$ intersects β. Thus, this process has the effect of adding a -1 phase shift to those states which include an 'α', as desired. □

Sadly for the toric codes, these are essentially the only gates that can be implemented. No matter how one moves around particles, there is not enough complexity in the system to generate interesting gates. We formalize this by writing out the *group of gates* of the toric codes. We can think of quantum gates on a system as forming a group, where the group law is given by the composition of gates, and every element has an inverse since unitary matrices are invertible. For the toric codes, we have the following:

Proposition 4.6. *There are exactly 8 possible computations in the toric codes. The group of gates is (non canonically) isomorphic to the Pauli group, i.e., the group whose objects are*

$$\{\pm I, \pm iI, \pm\sigma_X, \pm i\sigma_X, \pm\sigma_Y, \pm i\sigma_Y, \pm\sigma_Z, \pm i\sigma_Z\}$$

and whose group operation is given by matrix multiplication. A minimal generating set is given by $\{NOT_\alpha, NOT_\beta, (-1)_\alpha\}$.

Proof. To begin, we define $\mathrm{NOT}_\beta, \mathrm{NOT}_{\alpha\beta}, (-1)_\beta$, and $(-1)_{\alpha\beta}$ in complete analogy to how we define NOT_α and $(-1)_\alpha$. Namely, NOT_β flips whether or not a state has a 'β' in it, and $\mathrm{NOT}_{\alpha\beta}$ flips whether or not a state has an '$\alpha\beta$' in it, i.e.,

$$|\mathbf{0}\rangle \mapsto |\alpha\beta\rangle\,,\ |\beta\rangle \mapsto |\alpha\rangle$$
$$|\alpha\rangle \mapsto |\beta\rangle\,,\ |\alpha\beta\rangle \mapsto |\mathbf{0}\rangle\,.$$

The relation $\sigma_X\sigma_Z = -\sigma_Z\sigma_X$ implies that we can switch the order of operations between first applying all our σ_Xs and then applying all our σ_Zs, up to an operator-wise phase shift -1. Any process of creating and annihilating X-type quasiparticles can be modeled in sequence as repeatedly creating particles, moving them around a loop, then annihilating them. Following the proof of Proposition 4.5, this is the same as repeatedly applying NOT_ω gates, for homology classes ω. Similarly, the processes on Z-type particles will be compositions of $(-1)_\omega$ gates.

Hence, we now have a full set of generators for our gate group: $\{\pm I, \mathrm{NOT}_\omega, (-1)_\omega\}$, where ω runs over homology classes. The relations $\mathrm{NOT}_\alpha\mathrm{NOT}_\beta = \mathrm{NOT}_{\alpha\beta}$ and $(-1)_\alpha(-1)_\beta = (-1)_{\alpha\beta}$ allow one to reduce the generating set further. The relations

$$\mathrm{NOT}_\alpha(-1)_\alpha\mathrm{NOT}_\alpha = (-1)_\beta$$

and

$$(-1)_\alpha\mathrm{NOT}_\alpha(-1)_\alpha = -I$$

reduce the generating set to $\{\mathrm{NOT}_\alpha, \mathrm{NOT}_\beta, (-1)_\alpha\}$. Verifying simple relations gates, it is simple to see that the gate group is isomorphic to the Pauli group, as desired.

□

Before moving on to the next section, we make a few final remarks about the behavior of quasiparticles on the toric codes. Namely, we observe the following. Consider the full vector space $\mathcal{N}$, and adjacent two adjacent X-type and Z-type quasiparticles. Consider the simple braiding of these particles around each other, as in Figure 2.3. A line going under another corresponds to the particle having passed through that space first, before the other particle. This braiding can be obtained by first performing a twist halfway around the circle by X, then a twist all the way around the circle by Z, then finally moving the second half of the circle by X. This process corresponds to a transformation $\mathcal{N} \to \mathcal{N}$

(i.e. tensoring with the appropriate σ_Xs and σ_Zs). The observation is that this transformation is *not* the identity on the codespace. Namely, since $\sigma_Z\sigma_X = -\sigma_X\sigma_Z$, this operation corresponds to a global phase shift of -1 on the system.

Thus, the braiding of X type and Z type particles corresponds to a phase shift of -1. This is in contrast to braiding two identical X type or Z type particles, which corresponds to the identity since σ_X and σ_Z commute with themselves. All particles in the standard model of physics are *fermions*, which give a phase shift of -1 when you braid them with themselves, or *bosons*, which act by the identity when you braid them with themselves. Seeing as X type and Z type particles in the toric code braid by the identity with themselves, one would expect them to be bosons. However, bosons always braid by the identity with each other and hence the -1 phase shift from braiding X and Z type particles should be impossible. The conclusion is that these really are *quasi*particles, which behave much differently than particles in the standard model. Quasiparticles with simultaneously non-bosonic and non-fermionic braiding rules are known as *anyons*. The name comes from the fact that they can have "any " braiding rules, hence "any"-on. All interesting particles in topological quantum phases of matter will be anyons.

In the case of the toric code, the braiding will always be trivial or give a global phase shift (i.e. -1). We call anyons *non-abelian* if they can braid in such a way to create transformations that are not phase shifts. To create interesting quantum gates, these sort of non-phase shift braidings are what we need. The search for a topological quantum computer is essentially the search for experimentally-sound easy-to-braid non-abelian anyons.

Exercises:

4.1. For edges v and faces p, define

$$A'_v = \bigotimes_{\substack{\text{edges}\\ \text{touching } v}} \sigma_X,\ B'_p = \bigotimes_{\substack{\text{edges}\\ \text{touching } p}} \sigma_Z,$$

$$H' = -\sum_{\text{vertices } v} A'_v - \sum_{\text{faces } p} B'_p.$$

Let $M = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ be the Hadamard matrix. Using the relations

$$\sigma_X = M\sigma_Z M^{-1},\ \sigma_Z = M\sigma_X M^{-1},$$

show that H and H' are similar, in the sense that $H' = MHM^{-1}$. Use this to conclude that all basis independent properties of the toric code are formally symmetric by replacing X with Z. In particular, the codespace (lowest eigenspace) of H' is 4 dimensional, and the gate group of H'.

4.2. Show that eigenvectors of the Hamiltonian are equally likely to give 0 or 1 when measured at every qubit. This implies that the eigenvectors of the Hamiltonian are *maximally entangled*, which is a more general phenomenon in TQC. (HINT: Prove this for ground states first, then lift to general eigenstates using an induction argument along the lines of the proof of Proposition 4.2)

4.3. Let $\mathcal{N}_n$ denote the vector space associated to the n by n grid on the torus. Let

$$\tilde{H}_n = H_n + (2n^2)I,$$

so that the ground states have eigenvalue 0. This is more physically realistic, since systems cannot have negative energy. When n divides m, we have a natural map

$$\mathcal{N}_n \hookrightarrow \mathcal{N}_m$$

defined by [WORK: What is the correct definition?]. Show that this map is linear and injective, and hence that $\mathcal{N}_n$ can be realized as a sub vector space of $\mathcal{N}_m$. Show that $\tilde{H}_m$ restricted to $\mathcal{N}_n$ is equal to $\tilde{H}_n$. Show that the map $\mathcal{N}_n \hookrightarrow \mathcal{N}_m$ is norm-preserving, in the sense that if $|\chi\rangle, |\psi\rangle$ are states on $\mathcal{N}_n$, the inner product $\langle\chi|\psi\rangle$ is independent of whether or not it was computed in $\mathcal{N}_n$ or $\mathcal{N}_m$. Define

$$\mathcal{N}_\infty = \bigcup_{n=3}^{\infty} \mathcal{N}_n,$$

and define $\tilde{H}_\infty$ to be the operator on $\mathcal{N}_\infty$ which acts on vectors in $\mathcal{N}_n$ by $\tilde{H}_n$. Show that these are well defined objects, that $\mathcal{N}_\infty$ is naturally a Hilbert space. It is in this sense that we can speak of a limiting continuous model formed by the discrete grid celluations[6].

5 Topological Quantum Field Theories

5.1 The general picture

Topological Quantum Computation (TQC) is physically based on topological quantum phases of matter. Topological Quantum Field Theories are the mathematical formalism of topological quantum phases of matter. Namely, every topological quantum phase of matter (physical object) has an associated Topological Quantum Field Theory (mathematical object) to describe it. To make

[6]Note that objects in $\mathcal{N}_\infty$ themselves aren't continuous paths; they are just discrete cycles in $\mathcal{N}_n$ for some n. This is not an issue, since the *simplicial approximation theorem* says that every continuous phenomenon can be modeled discreetly in a fine enough celluation.

Figure 5.1: The two holed torus (surface of genus of 2)

this clearer, we recall classical phases of matter in a more mathematical way. Namely, a phase of matter is an assignment

$$\begin{pmatrix}\text{Collections of}\\ \text{particles}\end{pmatrix} \rightsquigarrow \begin{pmatrix}\text{Physical}\\ \text{systems}\end{pmatrix},$$

taking a set of particles to the way it would behave under the phase of matter. The "gas" phase of matter will take a collection of particles and make the physical system of having them all bounce around each other really fast. The "solid" phase of matter will take that same collection of particles and have them move less freely, forming a more crystalline structure. A quantum phase of matter should do the exact same thing, but now your physical system is replaced by a quantum system. Namely, a quantum phase of matter is an assignment

$$\begin{pmatrix}\text{Collections of}\\ \text{particles}\end{pmatrix} \rightsquigarrow \begin{pmatrix}\text{Quantum}\\ \text{systems}\end{pmatrix}.$$

Topological quantum phases of matter arise from the understanding that the topology of a shape (i.e. the physical invariants of the shape invariant under deformation) will affect the quantum system arising from inducing that shape with a given phase of matter. For example, consider the "$\mathbb{Z}_2$ spin liquid" topological quantum phase of matter described in the introduction. When this phase of matter is induced by a torus, the resulting quantum system will be the four dimensional codespace of the toric code (Proposition 4.2). If the $\mathbb{Z}_2$ spin liquid is induced on the torus with two holes (see Figure 5.1), the ground space will instead be sixteen dimensional. Thus, a topological quantum phase of matter is an assignment

$$\begin{pmatrix}\text{Topological}\\ \text{spaces}\end{pmatrix} \rightsquigarrow \begin{pmatrix}\text{Quantum}\\ \text{systems}\end{pmatrix}.$$

All of the interesting quantum systems are in two dimensional spaces. This can be seen as follows. TQC is performed by braiding quasiparticles through spacetime. When space is two dimensional, spacetime is three dimensional. When space is three dimensional, spacetime is four dimensional. It is a theorem that there are no knots in four dimensions: The extra dimension gives the knot room to move around and untangle. Thus, to have nontrivial knots, space must be two dimensional. A two dimensional space is called a *surface*. The surfaces we are interested in are those two dimensional spaces which can be embedded

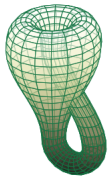


Figure 5.2: A Klein bottle, attempting to be embedded in 3d space

into three dimensional space, i.e., those surfaces which can be realized physically in our three dimensional world. Note that there are some weird surfaces which can not be embedded into three dimensional space, such as the Klein bottle (shown in Figure 5.2). While the 'true' surface does not intersect itself, any way of placing it in three dimensions will self intersect. One needs an extra dimension to avoid this intersection.

This condition on embeddability into three dimensional space makes our study of surfaces much simpler. Namely we have the following well-known theorem from topology:

Theorem 5.1. *Consider a surface that*

1. *Is finite in area (for example, an infinitely stretched flat plane would not count)*
2. *Has no boundary (for example, a unit disk would not count, since its boundary is the circle)*
3. *Can be embedded into three dimensional space.*

Then, this surface must be a collection of g-holed torii, for some integers $g \geq 0$.

Thus, going forward the word 'surface' will simply refer to a collection of g-holed torii. A connected surface is one which can not be decomposed as the union of two other smaller surfaces. Every connected surface will be the g-holed torus for some $g \geq 0$, and more general surfaces can all be uniquely written as a union of connected surfaces. A two dimensional topological quantum phase of matter is thus an assignment

$$\begin{pmatrix}\text{Surfaces}\\ \text{in space}\end{pmatrix} \rightsquigarrow \begin{pmatrix}\text{Quantum}\\ \text{systems}\end{pmatrix}.$$

Mathematically, a quantum system is a complex vector space. Hence, a topological quantum phase of matter is an assignment

$$S \rightsquigarrow V(S),$$

where S is a surface and $V(S)$ is a finite dimensional vector space over the complex numbers. This mathematical formalism is known as Topological

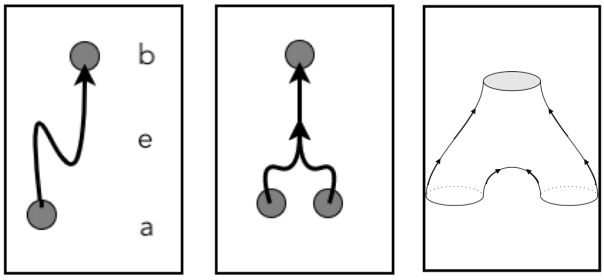


Figure 5.3: First box - A path in spacetime from a to b by e, i.e., a path e with $\partial e = a \sqcup b$. Second box - The fusion of two particles in spacetime. Third box - the fusion of two circles in spacetime, known informally as a "Pair of Pants".

Quantum Field Theory. Namely, the assignment $S \rightsquigarrow V(S)$ *is* a Topological Quantum Field Theory. To ease terminology, we will from now on use the acronym TQFT.

Not every assignment of surfaces to vector spaces will be a TQFT. Namely, many will be 'un physical', meaning that they never could have come from topological phases of matter. For example, the axioms of quantum mechanics say that putting two quantum systems together should correspond to the tensor product of those systems. Formally, we should have

$$V(S_0 \sqcup S_1) = V(S_0) \otimes V(S_1).$$

Here, $\sqcup$ denotes the disjoint union. The disjoint union is the same as a union, but it specifies that the union should be taken in a way such that S_0 and S_1 do not intersect (i.e. that they are disjoint). The disjoint union can be intuitively read as simply putting two spaces next to each other.

Additionally, by the axioms of quantum mechanics, transformations of a surface through spacetime should correspond to linear maps on quantum systems. We think mathematically about what a trajectory through spacetime looks like. In the one dimensional case, suppose we have two particles a and b. A trajectory through spacetime from a to b is a path e connecting a and b. Thinking deeply, one observes that the condition of "connecting" a and b can be mathematically stated as $\partial e = a \sqcup b$, where ∂e denotes the boundary of e. This is shown in Figure 5.3.

We observe however an ambiguity: Time has direction, but our edge a-priori does not. Hence, it is impossible to distinguish a path from a to b and a path from b to a. For this reason we have to introduce the concept of *orientation*. An oriented path is a path with a choice of direction. This can be visualized by putting a consistent set of arrows on the path. The points at the back end of the arrow correspond to the particles at the start of the process, and the points at the front end of the arrow correspond to the particles at the end of the process.

Note that the paths can join and split, as seen in the second box of Figure 5.3. This corresponds to the fusion and annihilation of particles.

Working one dimension higher, we can imagine the trajectory of circles of particles - loops - through spacetime. The merging of two circles will look exactly like it did before, except that now instead of tracing a path through spacetime it will trace a surface with boundary. The boundary components correspond exactly to the particles at the start and end of the process, as seen in the third box of Figure 5.3.

We now try to generalize this picture to the case of surfaces. Remember, our goal is to mathematically describe a trajectory of surfaces through spacetime, which will be key to our theory since these will correspond to linear transformations on quantum systems. The key insight is as follows. Given two sets of A and B (still representing particles), we saw a trajectory through spacetime was a path E such that $\partial E = A \sqcup B$. Given two collections of circles A and B, we saw a trajectory through spacetime was a surface E such that $\partial E = A \sqcup B$. Given two surfaces S_0 and S_1 (with no boundary, as usual), a trajectory through spacetime should be a three dimensional object X whose boundary is $\partial X = S_0 \sqcup S_1$.

Defining what we mean exactly by three dimensional object is very technical. Namely, these objects should be 3-manifolds, in the same way that a surface is a 2-manifold, a path is a 1-manifold, and a set of points is a 0-manifold. An introduction to the theory of manifolds can be found in Spivak's textbook [Spi18]. We leave the notion vague. One can think of 3-manifolds as being filled in surfaces. For instance, the torus is a surface (2-manifold), but the filled in solid torus is a 3-manifold. Let X be the solid torus with a smaller solid torus removed from inside it. Then the boundary ∂X will be equal to the disjoint union of the outside torus and the smaller inside torus. We can see that X forms a trajectory through spacetime, as the bigger torus contracts onto the smaller one. There is still one ambiguity. How do we know that X is a contraction big to small? Instead, it could have been an expansion small to big. To fix this issue we will again have to speak of oriented 3-manifolds. Oriented manifolds are (loosely) manifolds with a coherent system of arrows giving direction at every point. For example, a series of arrows in X all pointing from the big outside torus toward the smaller inside torus is an orientation.

We introduce a piece of notation. When $\partial X = S_0 \sqcup S_1$ is the disjoint union of two surfaces, one of those surfaces (say, S_0) will always be the stuff going in, and one of those surfaces (say, S_1) will always be the stuff going out. We call this a *bordism*[7] from S_0 to S_1. Namely, a bordism from a surface S_0 to a surface S_1 is an oriented 3-manifold X such that $\partial X = S_0 \sqcup S_1$, where all of the arrows in the orientation of X are pointing away from S_0 and towards S_1 . With this out of the way, we can formally define a TQFT:

Definition ((2 + 1)-TQFT)**.** A (2 + 1) Topological Quantum Field Theory (TQFT) is the following data.

1. A choice of finite dimensional complex vector space $V(S)$ for every surface

[7]Sometimes called a cobordism; the difference is immaterial.

S.

2. A choice of linear transformation $Z(X) : S_0 \to S_1$ for every bordism X from S_0 to S_1.

Additionally, a $(2+1)$-TQFT is required to satisfy the following properties:

1. (Union = tensor product). $V(S_0 \sqcup S_1) = V(S_0) \otimes V(S_1)$. Here, S_0 and S_1 are any two surfaces.

2. (Do nothing = identity) $Z(S \times [0,1]) = \mathrm{id}_{V(S)}$. Here, $S \times [0,1]$ is the Cartesian product of S with the interval, treated as a bordism from S to itself. Concretely $\partial(S \times [0,1]) = S \times \{0\} \sqcup S \times \{1\}$, and we identify $S \times \{0\}$ and $S \times \{1\}$ both with S.

3. (Composing bordisms = composing maps). $Z(X_1 \cup X_0) = Z(X_1) \circ Z(X_0)$. Here, X_0 is a bordism from two surfaces S_0 and S_1 and X_1 is a bordism from surfaces S_1 to S_2. One easily verifies that their union $X_1 \cup X_0$ is a bordism between S_0 and S_2, whose induced map we can compare with the composition of the induced maps of X_0 and X_1.

4. (Swap spaces = swap tensor factors) $Z(X)(v_0 \otimes v_1) = v_1 \otimes v_0$ for all $v_0 \in V(S_0)$, $v_1 \in V(S_1)$. Here, X is the bordism from $S_0 \sqcup S_1$ to $S_1 \sqcup S_0$ defined by taking S_0, S_1 and moving them around each other.

□

We offer a few remarks. The term "$(2+1)$" refers to the fact that there are two space dimensions, plus one time dimension. More generally, an $(n+1)$-TQFT is an assignment of n-manifolds to vector spaces, and of $(n+1)$-manifolds to linear transformations. We also remark on the structure of the definition. We first defined a few assignments of objects of one type to objects of another type, and then we defined a laundry list of properties that those assignments should satisfy. This is extremely standard practice in higher mathematics. The abstraction of this practice is known as Category Theory. The assignments of one type of object to another type of object are known as functors, and the properties to satisfy are known as axioms. The category theory definition of a TQFT is "a symmetric monoidal functor from the category of bordisms to the category of vector spaces"[8]. For those unfamiliar with category theory, a short introduction is found in Appendix B. While we will not be using any categories in this section, a familiarity of the subject is required for the following section on Modular Tensor Categories.

Often, TQFTs will be defined in terms of celluations. A celluation is a way of splitting up a space into vertices, edges, and faces. The utility of celluations is that they turn continuous objects into discrete ones, which allows for simple computations - this was the entire point of modeling the torus as an n by n grid in Section 4. The difficult part is often showing that the object you defined is

[8] symmetric=axiom 4, monoidal=axiom 1, functor=axiom 3, bordsism category=axiom 2

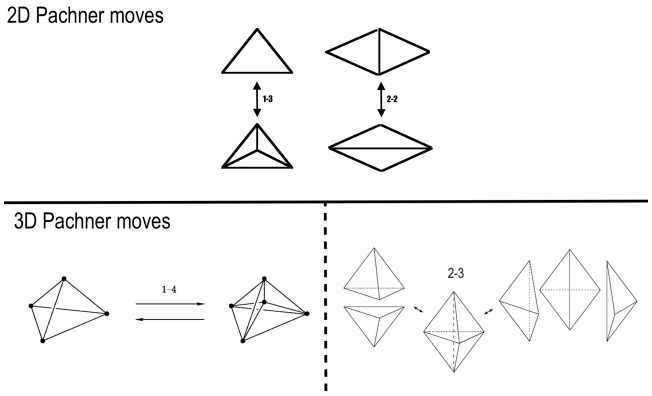


Figure 5.4: The Pachner moves.

independent of the choice of celluation. For the toric code, this was Exercise 4.3. In general, one resorts to the following theorem:

Theorem 5.2 (Pachner, [Pac91], [Lic99])**.** *Let (X, Δ_X) and (X, Δ'_X) be two manifolds with triangulations (i.e. celluations in which every face has three edges). There exists a finite sequence of so-called Pachner moves relating Δ_X to Δ'_X. In two dimensions (i.e. when X is a surface) and three dimensions, the full list of Pachner moves is given in Figure 5.4. The naming convention is that the "a-b" move is the move that takes a cells to b cells.*

This massively facilitates the verification of whether or not a definition is independent of celluation. Namely, first you show that the definition is invariant under adding/removing edges (allowing you to turn the celluation into a triangulation), and then you check that the definition is invariant under applying the Pachner moves. Typically, this verification is entirely elementary and does not require any great show of cleverness. As such, our standard practice for Subsection 5.2 will be to state theorems, reduce the problem to the verification of invariance under Pachner moves, and assign the rest as an exercise to the reader.

5.2 The $\mathbb{Z}_2$ Dijkgraaf-Witten TQFT

We now define the Topological Quantum Field Theory (TQFT) associated with the toric code, and describe how TQC can be performed in this framework. We could also call it the "$\mathbb{Z}_2$ spin liquid TQFT", since it is the mathematical realization of the $\mathbb{Z}_2$ spin liquid topological quantum phase of matter. The original reference for this subject is [DW90], but our presentation follows more closely [QW21].

As with the definition of the toric codes in Section 4, the definition of the $\mathbb{Z}_2$ Dijkgraaf-Witten TQFT is in the language of $\mathbb{Z}_2$ homology. Seeing as our

definition of homology requires a celluation we first define $\tilde{V}(S, \Delta)$, where S is a surface and Δ_S is a celluation of S. That is, Δ_S is a representation of S as a collection of vertices, edges, and faces, with some edges and vertices identified. For example, $S = T$ could be the torus, and Δ could be the n by n lattice with opposite edges identified. For every surface S and celluation Δ_S, we define

$$\tilde{V}(S, \Delta_S) = \mathbb{C}\left[C^1(\Delta_S; \mathbb{Z}_2)\right].$$

Here $C^1(\Delta_S; \mathbb{Z}_2)$ denotes the group $\mathbb{Z}_2$ cocycles on the celluation Δ_S, and $\mathbb{C}[-]$ is notation for "complex vector space generated by", i.e., $\tilde{V}(S)$ is the unique complex vector space having $C^1(\Delta_S; \mathbb{Z}_2)$ as a basis. A $\mathbb{Z}_2$ cocycle is an assignment of 0s and 1s to every edge, such that every face touches an even number of 1-labeled edges.

Notice that a $\mathbb{Z}_2$ cocycle is the same thing as a $\mathbb{Z}_2$ cycle in the dual celluation, as discussed in the proof of Proposition 4.5. That is, every $\mathbb{Z}_2$ cocycle on S specifies a cycle on S, by drawing lines between the centers of two faces whenever the edge connecting them is labeled by a 1. This process of identifying cocycles on Δ_S and cycle in the dual celluation is known as Poincaré Duality. It is important to note that in higher dimensions the process breaks down, because generically loops will fail to intersect in three dimensions (they can just be shifted past each other). Thus, when discussing 3-manifold bordisms there is a real distinction between cycles and cocycles.

The reason we call this $\tilde{V}$ instead of V is that it depends on the choice of celluation Δ_S, and we want $V(S)$ to only depend on S. The invariant subspace $V(S)$ is defined like so:

$$V(S) = \mathbb{C}[H^1(S; \mathbb{Z}_2)],$$

where $H^1(S; \mathbb{Z}_2)$ is the cohomology of S. Cohomology is defined by

$$H^1(S; \mathbb{Z}_2) = C^1(S; \mathbb{Z}_2)/Z^1(S; \mathbb{Z}_2),$$

where $Z^1(S; \mathbb{Z}_2)$ is the subgroup of $C^1(S; \mathbb{Z}_2)$ generated by the cocycles consisting of 1s at every edge touching a vertex. Assigning 1s and 0s this way really does give a cocycle: Every face has either 0 or 2 edges in its boundary that touch a given vertex, and both 0 and 2 are even numbers. It is a standard fact that the cohomology of a space does not depend on the choice of celluation.

To view $V(S)$ and a subspace of $\tilde{V}(S, \Delta_S)$, we define a linear injection

$$\begin{aligned} V(S) &\hookrightarrow \tilde{V}(S, \Delta_S). \\ |\alpha\rangle &\mapsto \frac{1}{\sqrt{|Z^1(S; \mathbb{Z}_2)|}} \sum_{\gamma \sim \alpha} |\gamma\rangle \end{aligned}$$

Here, α is a cohomology class (an element of $H^1(S; \mathbb{Z}_2)$), $|\alpha\rangle$ is the corresponding vector in $V(S)$, $|Z^1(S; \mathbb{Z}_2)|$ denotes the number of elements in $Z^1(S; \mathbb{Z}_2)$,

and $\sim$ denotes the equivalence relation of being cohomologous. That is, two cocycles are cohomologous if they give the same element in $H^1(S;\mathbb{Z}_2)$. This map can be summarized by saying that a cohomology class sends to the equal superposition of all of its representatives. The normalizing factor $|Z^1(S;\mathbb{Z}_2)|^{-1/2}$ is introduced to make sure that the norm is preserved.

We now define the action of bordisms. Let (S_0, Δ_{S_0}) and (S_1, Δ_{S_1}) be two surfaces with celluations. Let X be a bordism from S_0 to S_1. Let Δ_X be a celluation on X compatible with the celluations on S_0 and S_1. By compatible we mean that if we restrict Δ_X to ∂X then we will recover the celluations Δ_{S_0} and Δ_{S_1}. This restriction process can be described visually as dropping all verticies, edges, and faces, from Δ_X that aren't part of $\partial X = S_0 \sqcup S_1$. We call a pair of cocycles $(\omega_{S_0}, \omega_{S_1})$ extendable if there is a cocycle in $\omega_X \in C^1(X, \Delta_X)$ which gives ω_{S_0} when restricted to S_0 and ω_{S_1} when restricted to S_1. Let N_X be the number of cocycles in $C^1(S_1;\mathbb{Z}_2)$ with which the 0 cocycle on S_0 can be extended. We define

$$\tilde{Z}(X, \Delta_X) = \frac{1}{N_X} \begin{pmatrix} 1 \text{ if } (\omega_{S_0}, \omega_{S_1}) \text{ extendable} \\ 0 \text{ otherwise} \end{pmatrix}_{\substack{\omega_{S_0} \in C^1(S_0;\mathbb{Z}_2) \\ \omega_{S_1} \in C^1(S_1;\mathbb{Z}_2)}}.$$

We now elaborate on the meaning of this expression. Linear algebra tells us that to specify a linear transformation between two spaces, all we need to do is specify the entries of a matrix. The entries of a matrix are labeled by basis vectors. Namely, the matrix entries of a map from $\mathbb{C}[C^1(S_0;\mathbb{Z}_2)]$ to $\mathbb{C}[C^1(S_1;\mathbb{Z}_2)]$ are labeled by ordered pairs of basis vectors $(|\omega_{S_0}\rangle, |\omega_{S_1}\rangle)$, where $\omega_{S_0} \in C^1(S_0;\mathbb{Z}_2)$ and $\omega_{S_1} \in C^1(S_1;\mathbb{Z}_2)$. The $(|\omega_{S_0}\rangle, |\omega_{S_1}\rangle)$ entry in $\tilde{Z}(X;\Delta_X)$ is equal to 1 if $(\omega_{S_0}, \omega_{S_1})$ is extendable, and 0 otherwise.

The intuition for $\tilde{Z}(X, \Delta_X)$ comes from the path integral formulation of quantum mechanics. When not being observed, a system will transform along an equal superposition of all possible trajectories. There is a spacetime trajectory sending a state (cocycle) $|\omega_{S_0}\rangle$ to a state (cocycle) $|\omega_{S_1}\rangle$ exactly when $(\omega_{S_0}, \omega_{S_1})$ can be extended. The map $\tilde{Z}(X, \Delta_X)$ can be described as the transformation that takes a state to the equal superposition of all possible states it could go to.

Our goal is to show that $\tilde{Z}(X, \Delta_X)$ restricts to a map $V(S_0) \to V(S_1)$, and that this restriction is independent of our choice of $\Delta_{S_0}, \Delta_{S_1}$ and Δ_X. Once this has been done we can define $Z(X)$ to be this common restriction. All that will be left to do then is to show that our assignments $V(S)$ and $Z(X)$ satisfy the axioms of a $(2+1)$-TQFT. We work on this overarching plan over the course of a few propositions.

Proposition 5.1. *Let (S_0, Δ_{S_0}) and (S_1, Δ_{S_1}) be surfaces with celluations, X a bordism from S_0 to S_1, and Δ_X a celluation of X compatible with the celluations on S_0 and S_1. Then, the map $\tilde{Z}(X, \Delta_X) : \tilde{V}(S_0, \Delta_{S_0}) \to \tilde{V}(S_1, \Delta_{S_1})$ is independent of the choice of celluation Δ_X. Hence, we can properly omit Δ_X from our notation, and speak of a well defined map $\tilde{Z}(X)$.*

Proof. We need to show that if Δ_X and Δ'_X are two different choices of celluations on X compatible with Δ_{S_0} and Δ_{S_1}, then then $\tilde{Z}(X, \Delta_X) = \tilde{Z}(X, \Delta'_X)$.

That is, $(\omega_{S_0}, \omega_{S_1})$ are extendable in Δ_X if and if they are extendable in Δ'_X. By Theorem 5.2, all we have to do is show that the property of $(\omega_{S_0}, \omega_{S_1})$ being extendable is invariant first under the operation of adding/removing edges (to turn the celluation into a triangulation), and secondly invaraint under the process of applying Pachner moves. Drawing out the diagrams, these are straightforward computations. We leave the verification of the proof as an exercise to the reader (Exercise 5.1). □

Lemma 5.1. *Let (S_0, Δ_{S_0}), (S_1, Δ_{S_1}), (S_1, Δ_{S_2}) be surfaces with celluations, let X_0 be a bordism from S_0 to S_1, and let X_1 be a bordism from S_1 to S_2.*

(i) $|\{\omega_{S_1} \in C^1(\Delta_{S_1}; \mathbb{Z}_2) \text{ s.t } (\omega_{S_0}, \omega_{S_1}) \textit{ extendable}\}|$ *is independent of choice of ω_{S_0}*

(ii) $|\{\omega_{S_1} \in C^1(\Delta_{S_1}; \mathbb{Z}_2) \text{ s.t } (\omega_{S_0}, \omega_{S_1}) \text{ \& } (\omega_{S_1}, \omega_{S_2}) \textit{ extendable}\}|$ *is independent of choice of ω_{S_0}, ω_{S_2}, so long as $(\omega_{S_0}, \omega_{S_2})$ is extendable*

Proof. We prove (i), and leave (ii) as an exercise (Exercise 5.2) since the proof is identical. Let ω_{S_1} and ω_{S_1} be such that $(\omega_{S_0}, \omega_{S_1})$ and $(\omega_{S_0}, \omega'_{S_1})$ are extendable. Then, adding extensions of these pairs together edgewise we get that $(\omega_{S_0} + \omega_{S_0}, \omega_{S_1} + \omega'_{S_1})$ is extendable. Since $\omega_{S_0} + \omega_{S_0} = 0$, we find that there is a 1-to-1 bijection between ω_{S_1} such that $(0, \omega_{S_1})$ is extendable and ω_{S_1} such that $(\omega_{S_0}, \omega_{S_1})$ is extendable, sending ω_{S_1} to $\omega_{S_0} + \omega_{S_1}$ Thus, these sets have the same cardinality, and we conclude (i). □

Proposition 5.2. *Letting X_0, X_1 be as in Lemma 5.1, the composition law*

$$Z(X_1 \cup X_0) = Z(X_1) \circ Z(X_0)$$

holds.

Proof. Expanding by matrix multiplication, we find by the definition of $Z(X)$ that the coefficient of $(\omega_{S_0}, \omega_{S_2})$ in $Z(X_1) \circ Z(X_0)$ is

$$\frac{1}{N_{X_0} N_{X_1}} \sum_{\omega_{S_1}} \begin{pmatrix} 1 \text{ if } (\omega_{S_0}, \omega_{S_1}) \text{ extendable} \\ 0 \text{ otherwise} \end{pmatrix} \begin{pmatrix} 1 \text{ if } (\omega_{S_1}, \omega_{S_2}) \text{ extendable} \\ 0 \text{ otherwise} \end{pmatrix}.$$

The coefficient of $(\omega_{S_0}, \omega_{S_2})$ in $Z(X_1 \cup X_0)$ is $N^{-1}_{X_1 \cup X_0}$ if $(\omega_{S_0}, \omega_{S_2})$ extendable, and 0 otherwise. Multiplying through, we find the equality we are trying to prove is

$$N_{X_0 \cup X_1} |\{\omega_{S_1} \text{ s.t } (\omega_{S_0}, \omega_{S_1}) \text{ \& } (\omega_{S_1}, \omega_{S_2}) \text{ extendable}\}| = N_{X_0} N_{X_1}.$$

Fix ω_{S_0}. We claim that both sides of the above expression are equal to the number of pairs $(\omega_{S_1}, \omega_{S_2})$ such that $(\omega_{S_0}, \omega_{S_1})$ and $(\omega_{S_1}, \omega_{S_2})$ are simultaneously extendable. The left hand side computes this value by first counting the

number of ways of choosing ω_{S_2} (i.e. $N_{X_0 \cup X_1}$), and the by counting the number of ways of filling in ω_{S_1}. The right hand side computes this value by first counting the number of ways of choosing ω_{S_1} (i.e. N_{X_0}) and then counting the number of ways of choosing ω_{S_2} (i.e. N_{X_1}). Note the implicit use of Lemma 5.1, saying that all of these values are equal. This completes the proof.

□

The next proposition has a strong physical meaning, and can be seen as motivation for the fact that $V(S)$ is a ground state space. Namely, let (S, Δ_S) be a surface with celluation and let $S \times [0,1]$ be the product of S with the real interval of numbers between 0 and 1. That is, elements of $S \times [0,1]$ are pairs (s,t) where $s \in S$ and $t \in [0,1]$. This is a 3-manifold, and gives a bordism from S to itself. Namely, $\partial(S \times [0,1])$ is built of the two components $S \times \{0\}$ and $S \times \{1\}$. The orientation on $S \times [0,1]$ is induced by the orienation on $[0,1]$. This can viewed as the identity bordism: S is doing nothing as time increases from 0 to 1. The boundary components correspond to the placement of S at time 0 and S at time 1. When time passes on a system, we expect it to ambiently decrease in energy. Thus, physically $Z(S \times [0,1])$ should act by the identity on ground states, and send higher energy states down to the ground state. This is exactly the statement that $Z(S \times [0,1])$ should be a projection from the full state space to the ground state space. The following proposition in this lens thus says that $V(S)$ are exactly the ground space:

Proposition 5.3. *Let (S, Δ_S) be a surface with celluation. Viewing $S \times [0,1]$ as a bordism from S to itself, we have that $\tilde{Z}(S \times [0,1])$ is a projection from $\tilde{V}(S, \Delta_S)$ to $V(S)$. Namely, the image of $\tilde{Z}(S \times [0,1])$ is $V(S)$, and $\tilde{Z}(S \times [0,1])$ acts by the identity on $V(S)$. Explicitly, $\tilde{Z}(S \times [0,1])$ is given by the map*

$$|\omega\rangle \mapsto \frac{1}{|Z^1(\Delta_S; \mathbb{Z}_2)|} \sum_{\gamma \sim \omega} |\gamma\rangle .$$

Proof. Let ω_S, ω'_S be two cocycles on Δ_S. We show that (ω_S, ω'_S) is extendable if and only if ω_S and ω'_S are cohomologous. Consider the celluation $\Delta_{S \times [0,1]}$ obtained by adding an edge connecting each vertex in $S \times \{0\}$ to the corresponding vertex in $S \times \{1\}$.

We proceed by induction on the number of central edges in $S \times [0,1]$ (i.e. edges of $S \times [0,1]$ not in the boundary) which are assigned the value 1 in the extension ω_X of (ω_S, ω'_S). If there are no such edges, then clearly we must have $\omega_S = \omega'_S$, and so our proof is complete. Suppose there is a nonzero amount of such edges. Choose a central edge e assigned 1 in ω_X. Let ω'_X the the cocycle obtained by flipping e to as 0, as well as flipping all of the edges touching e in $S \times \{1\}$. ω'_X satisfies the cocycle condition since faces in the center touching e will also touch exatly one of the edges flipped in $S \times \{1\}$, and hence the sum 1s around the edges of those faces will change an even amount. By our inductive hypothesis, we conclude that ω'_S and ω_S are cohomologous. This process is demonstrated in Figure 5.5.

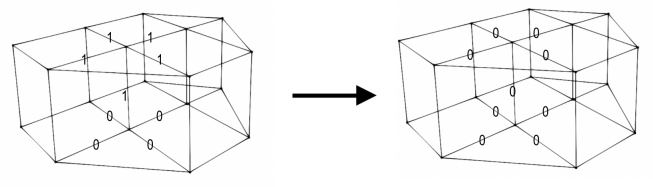


Figure 5.5: Removing the 1s from the central edges in $S \times [0,1]$

The number of ways $N_{S\times[0,1]}$ of extending the 0 cocycle is thus equal to the number of cocycles cohomologous to 0, which is by definition $|Z^1(\Delta_S;\mathbb{Z}_2)|$. Thus, the stated formula is correct. It is straightforward to see that the rest of the proposition follows immediately from this formula. □

This allows us to prove the full independence of our theory from choice of celluation:

Proposition 5.4. *Let (S_0, Δ_{S_0}) and (S_1, Δ_{S_1}) be surfaces with celluations, and let X be a bordism from S_0 to S_1. The image of $\tilde{Z}(X)$ is contained in $V(S_1)$. In particular, $\tilde{Z}$ restricts to a map $V(S_0) \to V(S_1)$. This map is independent of our choice of Δ_{S_0} and Δ_{S_1}. We define $Z(X) : V(S_0) \to V(S_1)$ to be this common restriction.*

Proof. To begin, we observe that if $(\omega_{S_0}, \omega_{S_1})$ is extendable, then so is $(\omega'_{S_0}, \omega_{S_1})$ for any ω'_{S_0} homologous to ω_{S_0}. This follows by precomposing X with $S_0 \times [0,1]$, which does not change X, first extending $(\omega'_{S_0}, \omega_{S_0})$ by Proposition 5.3, and then extending $(\omega_{S_0}, \omega_{S_1})$.

Thus, the equal superposition $|\omega_{S_0}\rangle$ of every cocycle homologous to ω_{S_0} will map under $\tilde{Z}(X, \Delta_X)$ to a sum of equal superpositions of cohomologous classes in $H^1(S_1;\mathbb{Z}_2)$, i.e., an element of $V(S_1)$. What is left to check is whether or not a cohomology class in S_0 can be lifted to a cohomology class in S_1 is independent of the choices of celluations.

To prove this, we consider the identity bordism $S \times [0,1]$ with $S \times \{0\}$ given a celluation Δ_S and $S \times \{1\}$ given a celluation Δ'_S. We show that a cocycle in $C^1(\Delta_S;\mathbb{Z}_2)$ can be lifted to a class in $C^1(\Delta'_S;\mathbb{Z}_2)$ if and only if they are homologous. Applying this with $S = S_0$ and precomposing with $S_0 \times [0,1]$ gives the desired independence of choice of celluation on S_0, and applying this with $S = S_1$ and postcomposing with $S_1 \times [0,1]$ gives the desired independence of choice of celluation on S_1.

The above claim again follows from applying induction with respect to the moves in Theorem 5.2, and thus is left as an exercise (Exercise 5.3). □

The main result of our section is as follows:

Theorem 5.3. *The assignments $S \mapsto V(S)$ and $X \mapsto Z(X)$ give a Topological Quantum Field Theory, called the $\mathbb{Z}_2$ Dijkgraaf-Witten TQFT.*

Proof. We check that our choices of $V(S)$ and $Z(X)$ satisfy the four axioms.

1. Specifying a cohomology class on $S_0 \sqcup S_1$ amounts to specifying a cohomology class on S_0, and a cohomology class on S_1. In other words, we have a natural equality

$$H^1(S_0 \sqcup S_1; \mathbb{Z}_2) = H^1(S_0; \mathbb{Z}_2) \times H^1(S_1; \mathbb{Z}_2).$$

   Additionally, for any sets A and B we have $\mathbb{C}[A \times B] = \mathbb{C}[A] \otimes \mathbb{C}[B]$, where we identity $[(a, b)]$ with $[a] \otimes [b]$, $a \in A$, $b \in B$. Thus,

$$\begin{aligned} V(S_0 \sqcup S_1) &= \mathbb{C}\left[H^1(S_0 \sqcup S_1; \mathbb{Z}_2)\right] \\ &= \mathbb{C}\left[H^1(S_0; \mathbb{Z}_2) \times H^1(S_1; \mathbb{Z}_2)\right] \\ &= \mathbb{C}\left[H^1(S_1; \mathbb{Z}_2)\right] \otimes \mathbb{C}\left[H^1(S_1; \mathbb{Z}_2)\right] \\ &= V(S_0) \otimes V(S_1). \end{aligned}$$

2. This follows immediately from Proposition 5.3.

3. This follows immediately from Proposition 5.2.

4. The bordism X has the effect of swapping S_0 and S_1, hence sends $H^1(S_0; \mathbb{Z}_2) \times H^1(S_1; \mathbb{Z}_2)$ to $H^1(S_1; \mathbb{Z}_2) \times H^1(S_0; \mathbb{Z}_2)$, sending $(\omega_{S_0}, \omega_{S_1})$ to $(\omega_{S_1}, \omega_{S_0})$. Tracing through the series of equalities in part 1, we get the desired result.

□

Seeing that the $\mathbb{Z}_2$ Dijkgraaf-Witten TQFT applied to the torus yields the toric code as defined in Section 4 is simple. The only difficulty comes from the fact that as defined, the toric code is generated by homology classes and the $\mathbb{Z}_2$ Dijkgraaf-Witten TQFT is generated by cohomology classes. However, as mentioned before, there is a duality between homology classes and cohomology classes which arises from considering the dual celluation, and so this discrepancy is really not an issue. We decided to work with homology in Section 4 for pedagogical reasons: homology is more intuitive than cohomology. However, for 3-manifolds there is a discrepancy between homology and cohomology, which is why the $\mathbb{Z}_2$ Dijkgraaf-Witten TQFT has to use the less intuitive concept.

In general, there is no Hamiltonian in TQFTs. The lowest energy states are those which will naturally occur after time passes, namely, those in the image of the "do nothing" bordism $\tilde{Z}(X)$. It is for this reason that even though ground states are complicated maximally entangled objects (Exercise 4.2) they are easy to make in the lab. All one has to do is make a cold enough system and allow it to relax. As time passes, it will naturally go into a ground state. In some quantum

systems, these relaxed states are already interesting enough that it would take a long time to simulate the process on a classical computer. This gives a sort of quantum computer, known as an Adiabatic quantum computation. It is interesting to note that the original definition of the toric code did not include a Hamiltonian, and this was only introduced later to facilitate the study [Kit97]. A more general study of TQFTs with Hamiltonians was conducted by Levin-Wen [LW05], but is still not the norm.

In the TQFT language it is hard to see what anyons and quantum computations correspond to. How do I do braiding in a TQFT? How do I see how many particle types there are? The intriguing fact is that this information is present, but hidden. Namely, one has to pass to a *1-extended TQFT* to engage with anyons explicitly. This extension allows us to define $V(S)$ whenever S is a surface with punctures. These punctures correspond to anyons, and moving the punctures around each other corresponds to braiding. Not every TQFT can be 1-extended, but those that can (like the $\mathbb{Z}_2$ Dijkgraaf-Witten theory) keep that anyon information in their structure. A more complete introduction to TQC would have defined 1-extensions, but we omitted the topic for clarity. All of this is in marked contrast to Modular Tensor Categories, where anyons are placed front and center of the theory.

Exercises:

5.1. Complete the proof of Proposition 5.1.

5.2. Complete the proof of Lemma 5.1.

5.3. Complete the proof of Proposition 5.4.

6 Modular Tensor Categories

6.1 Anyon models

To describe Topological Quantum Computation (TQC), one has to describe topological quantum phases of matter. Topological Quantum Field Theories (TQFTs) are the most immediate way of doing this, as described in Section 4. However, there are a few problems with this method:

1. There is a large amount of data that needs to be specified to define a TQFT. Namely, one needs to keep track of what vector spaces are assigned to every surface, and what morphisms are assigned to every bordism. As was seen in subsection 5.2, this can make defining TQFTs very difficult, and can lead to the verification of even basic axioms being difficult.

2. It is hard to deal directly with anyons (quasiparticles), which can make describing TQC (the braiding of anyons) very difficult. This is resolved in

part by the consideration of *extended* TQFTs, where we allow punctures in surfaces to represent anyons, but this results in even more data to carry around.

To summaraize, what we want is a mathematical desciption of topological quantum phases of matter that puts anyons and their motions/behaviors front and center. This is what Modular Tensor Categories give us. The objects and morphisms of a Modular Tensor Category (MTC) are thought of abstractly as

$$\begin{pmatrix} \textbf{objects} : \text{finite collections of anyons} \\ \textbf{morphisms} : \text{motions/behaviors of anyons} \end{pmatrix}.$$

For those needing a refresher on Category Theory, Appendix B contains the neccecary prerequisites. For this subsection, however, no knowledge of categories will be needed. This is becasue MTCs also have an elementary description as a finite collection of numbers representing physical properties of anyons.

It should not be seen as too surprising that topological quantum phases of matter can be described with a finite set of numbers. At the end of the day, when measuring physical phenomina all one will get is a number - wavelength, spin, energy etc... Thus, any practical physical theory should be able to be boiled down to a collection of numbers.

The most fundamental operation on anyons is *fusion*, which we have up to now seldom discussed. The reason for this is that the elementary description of the toric code given in Section 4 works perfectly well without introducting fusion, so the notion was ommited for clarity. We now revisit the picture of Section 4, with our eyes towards fusion. Fusion is the process in which two elementary particles collide, and output other types of particles.

In the context of the toric code, we have discussed two types of quasiparticles: X-type and Z-type. When they fuse together, we get a third Y-type particle. Seeing as X-type particles move along edges and Z-type particles move along faces, we observe that the intersection of the trajectory of an X-type particle and a Z-type particle must occur at the center of an edge. Moving the X-type particle along that edge corresponds to tensoring that edge with σ_X, and moving the Z-type particle corresponds to tensoring with σ_Z. Hence, creating two pairs of X and Z type particles and fusing them together corresponds to tensoring with $\sigma_X\sigma_Z$. Seeing as $\sigma_X\sigma_Z = i\sigma_Y$, we call these new particles Y-type particles.

Visualizing Y-type particles is cumbersome - hence the desire to stick with simply writing X and Z particles and to ignore the fact that they can fuse into a Y. One practice could be to place the Y type particle halfway betwen the X and Z type particles that fused to make it. Tensoring with $i\sigma_Y$ will move the particle in a stange fashion, keeping it halfway between faces and edges, as seen in Figure 6.1.

To write out the full set of fusion rules for the toric code, we need one last particle type. Namely, the "do-nothing" particle that one gets when fusing a particle with its own antiparticle. While physically trivial, this particle is neccecary to make our mathematical descriptions. Seeing as the do-nothing particle moves by doing nothing, we call it the I-type particle since it moves by

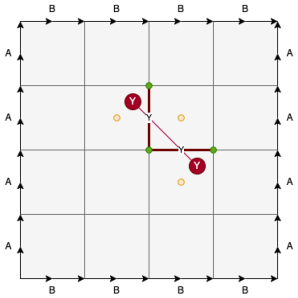


Figure 6.1: Movement of Y-type particles in toric code

tensoring with I. We denote $a \otimes b$ for the fusion of two particles a and b. It will become clear in the category theoretic notation why the tensor product symbol is used. The fusion rules are given as a table below:

	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	$-Z$	I	X
Z	Z	$-Y$	$-X$	I

We make a few observations. The fact that X fused with Z is Y is by definition. The fact that Z and X fuse to $-Y$ comes from the fact that fusing the opposite direction means applying $\sigma_Z \sigma_X$ to the edge instead of $\sigma_X \sigma_Z$. Seeing as σ_X and σ_Z anticommute, this gives a -1 sign. All of the other boxes in the table can be checked similarly. For example, $Z \otimes Y = -X$ becasue $\sigma_Z(i\sigma_Y) = -\sigma_X$. We observe that fusion essentially gives a group law on the space of anyon types. However, this is not exactly the case: Sometimes the output is positive, and sometimes the output is negative.

In general, fusion will have the following structure. We let $\mathscr{L}$ be a finite set, which we think of as being the possible anyon types. For any $a, b \in \mathscr{L}$, we will have the formal equality

$$a \otimes b = \sum_{c \in \mathscr{L}} N_c^{a,b} c.$$

This formula intuitively says that when a and b are fused this will result in a collection of particles, constisting of $N_c^{a,b}$ copies of c for each $c \in \mathscr{L}$. This can be thought of as the generalization of a finite group, where now the group law is allowed to output formal linear combinations of elements in the group. These generalizations of groups are called *fusion systems*. Those fusion systems which satisfy a generalization of commutivity are called *braided fusion systems*, and correspond to braided fusion categories. Modular Tensor Categories are braided fusion categories which satisfy a certain non-degeneracy and symmetry

condition. In this way, one can think of MTCs as being vast "non-degenerate" generalizations of finite abelian groups. We now formally state the definition of fusion system:

Definition (Fusion system)**.** A fusion system is the following data.

1. (Anyon types) A finite set $\mathscr{L}$.
2. (Fusion coefficients) Integers $N_c^{a,b} \in \{0,1\}$ for all $a,b,c \in \mathscr{L}$.

Additionally, a fusion system is required to satisfy the following properties:

1. (Identity/Do-nothing) There is a unique element $1 \in \mathscr{L}$ such that

$$1 \otimes a = a \otimes 1 = a$$

for all $a \in \mathscr{L}$. In other words,

$$N_b^{a,1} = N_b^{1,a} = \begin{cases} 1 & a = b \\ 0 & \text{otherwise} \end{cases}$$

for all $a,b \in \mathscr{L}$.

2. (Inverse/anti-particle) There is a unique element $a^* \in \mathscr{L}$ such that

$$a \otimes a^* = 1 \oplus [\text{other terms}],$$

for all $a \in \mathscr{L}$. For all $b \neq a^*$, $a \otimes b$ has no 1 term. In other words,

$$N_1^{a,b} = N_1^{b,a} = \begin{cases} 1 & b = a^* \\ 0 & \text{otherwise} \end{cases}$$

for all $a,b \in \mathscr{L}$.

3. (Associativity) We have

$$(a \otimes b) \otimes c = a \otimes (b \otimes c)$$

for all $a,b,c \in \mathscr{L}$. In other words, for all $a,b,c,d \in \mathscr{L}$ we have that

$$\sum_{e \in \mathscr{L}} N_e^{a,b} N_d^{e,c} = \sum_{e \in \mathscr{L}} N_e^{b,c} N_d^{a,e}.$$

□

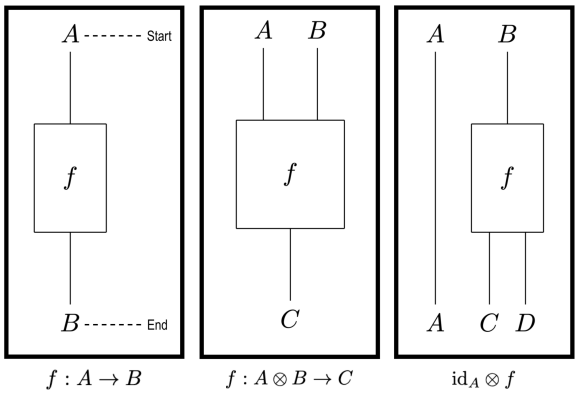


Figure 6.2: Examples of the quantum algebraic graphical language

Observe that in the above definition we required that $N_c^{a,b}$ always be 0 or 1. That is, when two particles are fused they will not create multiple copies of the same particle. This condition is not strictly neccecary, but we included it here as it greatly simplifies the theory. Many authors do not put this stipulation, and refer to examples with $N_c^{a,b}$ always equal to 0 or 1 as multiplicity free.

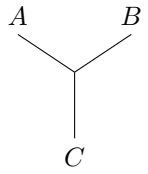
The next piece of the puzzle is based on one of the key ideas from category theory: Equal versus isomorphic. Given quasiparticles a, b, c fusing via $(a \otimes b) \otimes c$ or $a \otimes (b \otimes c)$ will result in the same particles. However, just because the particles present are the same does not mean that the quantum systems are the same. A huge theme in Section 4 is that changing order in processes like braiding might result in the same particles, but different states. Namely, different states in the same eigenspace. The processes $(a \otimes b) \otimes c$ and $a \otimes (b \otimes c)$ need only be equal up to an invertable linear transformation, i.e., isomorphism. We will define a $6j$ fusion system to be a fusion system in which we have chosen isomorphisms between all $(a \otimes b) \otimes c$ and $a \otimes (b \otimes c)$.

The visualization of this is best suited to a graphical language. As we will see next section, it is really best suited to a category-theoretic graphical language. The idea behind the graphical language is to make rigorous the sorts of diagrams that one will obviously draw when explaining the subject, as to clarify often messy conditions one will impose on objects. The general policy for these diagrams is as follows.

1. The diagrams are to be read from top to bottom.
2. Strands correspond to anyons.
3. Operations on strands correspond to operations on anyons.

Some examples can be found in Figure 6.2. Some special functions are encoced via special graphical diagrams. For example, suppose we choose a

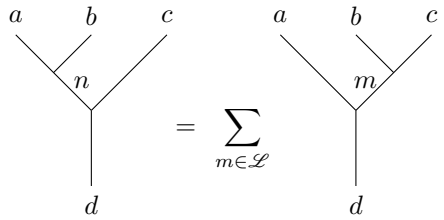
distinguished function $a \otimes b \to c$ to represent $a \otimes b$ fusing into c. In general the choice is mostly arbitrary, and changing our choices of such functions is *gauge symmetry*, as will be formally defined later. Our informal notion of function will be put in firmer footing in Subsection 6.2 when we use category theory. We graphically write our distinuished function $a \otimes b \to c$ as



Consider a function $(a \otimes b) \otimes c \to d$. This can be decomposed as taking a function $a \otimes b \to n$, then $n \otimes c \to d$, i.e., as

$$(a \otimes b) \otimes c \to n \otimes c \to d.$$

Similarly, functions $a \otimes (b \otimes c) \to d$ can decomposed by taking functions $b \otimes c \to m$ and $a \otimes m \to d$. These two processes can be represented in terms of each other by a linear combination. In the graphical language, this is expressed as



These values $F^{a,b,c}_{d;n,m} \in \mathbb{C}$ are known as $6j$ symbols. They clearly depend on the choice of functions ($a \otimes b \to n$ and such). Understanding the real intuition behind these $6j$ symbols without any handwaiving will have to wait until next section. However, for our purposes, this is really not neccecary: These can be treated simply as complex numbers, with as much or as little intuition behind them as one desires. All that is required is that they satisfy some axioms, as in the following definition:

Definition ($6j$ Fusion system)**.** A $6j$ fusion system is the following data.

1. A fusion system $(\mathscr{L}, N_{-}^{-,-})$
2. Complex numbers $F^{a,b,c}_{d;n,m}$ for all $a, b, c, d, n, m \in \mathscr{L}$.

Additionally, a $6j$ fusion system is required to satisfy the following properties:

1. (Admissibility) We call a triple $(a,b,c) \in \mathscr{L}^3$ admissible if $N_c^{a,b} \neq 0$. We call a sextuple $(a,b,c,d,n,m) \in \mathscr{L}^6$ admissible if (a,b,m), (m,c,d), and (b,c,n) are all admissible. We write $F_d^{a,b,c}$ to be the matrix whose coefficients are $F_{d;n,m}^{a,b,c}$, where n,m run over pairs making (a,b,c,d,n,m) admissible. We have that

   - $F_{d;n,m}^{a,b,c} = 0$ if (a,b,c,d,n,m) is not admissible
   - $F_d^{a,b,c}$ is invertible

   for all a,b,c,d,n,m.

2. (Associativity trivial on two inputs) $F_d^{a,b,c}$ is the identity matrix, whenever one of a, b, or c is 1.

3. (Pentagon) For all $a,b,c,d,e,f,p,q,m \in \mathscr{L}$,

$$\sum_{n \in \mathscr{L}} F_{q;p,n}^{b,c,d} F_{f;q,e}^{a,n,d} F_{e;n,m}^{a,b,c} = F_{f;q,m}^{a,b,p} F_{f;p,e}^{m,c,d}.$$

4. (Time reversal symmetry) $\left[\left(F_{a^*}^{a^*,a,a^*}\right)^{-1}\right]_{1,1} = \left[F_a^{a,a^*,a}\right]_{1,1}$, where $[\cdot]_{n,m}$ denotes the $[n,m]$th entry of a matrix.

□

Seeing as these axioms are more complicated, we explain them all in detail. Admissibility of the triple (a,b,c) says that when $N_c^{a,b} \neq 0$, which is equivilant to saying that when a and b fuse, a c particle is created. In the language of functions, this is saying that there is a nonzero map $a \otimes b \to c$, i.e., a nonzero physical process taking as input $a \otimes b$ and outputting c. Thus, when we think about decomposing $a \otimes b \otimes c$ as maps $a \otimes b \to n$, $m \otimes c \to d$, and $b \otimes c \to n$, it makes sense that if any of these pairs is not admissible then $F_{d;n,m}^{a,b,c} = 0$. One of those tripes being nonadmissible would mean that one of the functions in one of the compositions $a \otimes b \otimes c \to d$ is 0, and hence the function itself is zero, and hence will contribute nothing to the change of basis. Similarly, the matrix $F_d^{a,b,c}$ should give an equivilance between functions $(a \otimes b) \otimes c \to d$ and functions $a \otimes (b \otimes c) \to d$. Equvilance means isomorphism, which means that $F_d^{a,b,c}$ should be invertible.

If one of a,b,c is 1, then $F_d^{a,b,c}$ should surely be the identity. Imagine, for instance, $c = 1$. Then, we will be relating $(a \otimes b) \otimes 1$ and $a \otimes (b \otimes 1)$. Tensoring with 1 should not only leave you isomorphic with where you started, but it should really leave you equal. That is, we should be able to suppress $\otimes 1$ from notation and things should still work. Upon removing the $\otimes 1$, we find that we are relating $a \otimes b$ and $a \otimes b$, two equal objects, and hence the transformation $F_d^{a,b,c}$ should be the identity.

The pentagon identity is exactly the sort of identity for which graphical language is useful. As stated, it is quite non-obvious to decipher meaning from

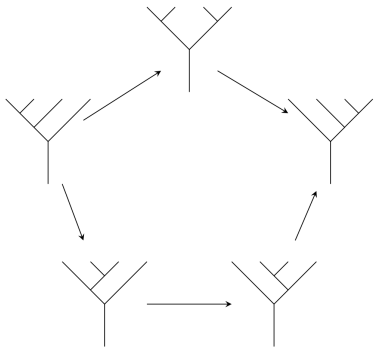


Figure 6.3: The pentaon axiom for $6j$ symbols

the expression. It becomes the statement that applying associativity in two diffent ways is identical. In graphical language, it becomes the fact that going either way around the 5-term diagram in Figure 6.3 gives the same answer (hence the name pentagon). All of terms in the pentagon are maps $a \otimes b \otimes c \otimes d \to e$. Each of the arrows corresponds to applying the approproate F-matrix.

[WORK: Explain time reversal symmetry]

A natural question about the definition of $6j$ symbols could be as follows: The goal was to define an isomorphism $a \otimes (b \otimes c)$ to $(a \otimes b) \otimes c$. Instead, one defined how morphisms $a \otimes (b \otimes c) \to d$ and $(a \otimes b) \otimes c \to d$ relate for every d. While this does indeed give some connection between $a \otimes (b \otimes c)$ and $(a \otimes b) \otimes c$, it is not immediately clear that tells us the two objects are isomorphic or, if so, what that isomorphism would be. While seemingly counterintuitive, this switch from studying objects to studying the functions between objects is extremely fruitful. This forms the heart of the Yoneda lemma, the most important result in category theory: Objects should be understood by their relationship with each other. According to Ravi Vakil:

> You work at a particle accelerator. You want to understand some particle. All you can do are throw other particles at it and see what happens. If you understand how your mystery particle responds to all possible test particles at all possible test energies, then you know everything there is to know about your mystery particle - Ravi Vakil[9].

In this context, Vakil's quote is very literal - we are studying particles by looking at their fusion rules. Fusion, as a process, generally happens when things hit each other very fast in a particle accelerator. By knowing that $a \otimes (b \otimes c)$ and $(a \otimes b) \otimes c$ can go to d in all the same ways (with the relationship being those ways being specified by the matrix $F_d^{a,b,c}$), we can conclude an isomorphism

[9] This quote is folklore, relayed by a MathOverflow post of Theo Johnson-Freyd

between $a \otimes (b \otimes c)$ and $(a \otimes b) \otimes c$. A formal treatment of the Yoneda lemma insofar as it relates to our study is given in the next section.

We now define braided $6j$ fusion systems. A braiding should give the relashionship between $a \otimes b$ and $b \otimes a$. These objects will be isomorphic, but not equal. For example, the fact that X and Z anticommute in the toric code is exactly the statement that isomorphism $X \otimes Z \to Z \otimes X$ should be -1 times the identity. Keeping with our Yoneda perspective, instead of giving an isomorphism $a \otimes b$ and $b \otimes a$ we give isomorphism between the spaces $a \otimes b \to c$ and $b \otimes a \to c$ for every c. Graphically, this can be seen in Figure [WORK: make figure]. The formal definition is as follows:

Definition (Braided $6j$ Fusion system)**.** A braided $6j$ fusion system is the following data.

1. A $6j$ fusion system $(\mathscr{L}, N_{-}^{-,-}, F_{-;-,-}^{-;-,-})$.
2. Complex numbers $R_c^{a,b}$ for all $a, b, c \in \mathscr{L}$.

Additionally, a braided $6j$ fusion system is required to satisfy the following properties:

1. (Admissibility) $R_c^{a,b} \neq 0$ if $(a, b, c) \in \mathscr{L}^3$ is admissible
2. (Hexagon) For all $a, b, c, d, e, m \in \mathscr{L}$,

$$\left(R_e^{a,c}\right)^{\pm 1} F_{d;e,m}^{b,a,c} \left(R_m^{a,b}\right)^{\pm 1} = \sum_{n \in \mathscr{L}} F_{d;e,n}^{b,c,a} \left(R_d^{a,n}\right)^{\pm 1} F_{d;n,m}^{a,b,c}.$$

□

Again, the hexagon is a mess of symbols when written out explicitely. In graphical language, we can [WORK: what does braiding look like]. The hexagon identity is thus the condition that going either way around the following 6-term diagram gives the same answer:

[WORK: Make hexagon]

With all this, we can finally define an MTC:

Definition (Modular tensor fusion system)**.** A modular tensor fusion system is a braided $6j$ fusion system satsifying the following conditions

1. (Spherical) $F_{1;a^*,c}^{a,b,c} F_{1;a^*a,a}^{b,c^*,a} F_{1;b^*,b}^{c^*,a,b} = 1$ for all $a, b, c \in \mathscr{L}$.
2. (Non-degenerate) For $a \in \mathscr{L}$, if $B_c^{a,b} = B_c^{b,a}$ for all $b, c \in \mathscr{L}$, then $a = 1$.

□

In graphical language, the spherical condition looks like [WORK: make diagram, explain why its neccecary.]

The non-degeneracy condition says that every non-trival particle should braid non-trivially with at least one other particle. Graphically, this is shown in [WORK: make diagram].

It is important to remember that even though the definition is long, at the end of the day these are still just finite collections of numbers satisfying a finite number of polynomial equations. This makes many things simple. For instance, we can define a morphism between fusion systems $(\mathscr{L}, N)$ and $(\mathscr{L}', N')$ to be a function $f : \mathscr{L} \to \mathscr{L}'$ such that $N_c^{a,b} = N'^{f(a),f(b)}_{f(c)}$. For $6j$ fusion sytems and braided $6j$ fusion systems, we simply require that f should respect F symbols and R symols as well. We can thus properly speak of fusion systems up to equivilance. We will see in the next section, however, that the correct notion of equivilance is a weaker *gauge equivilance*. This corresponds to keeping the same label set, but performing a local change of basis on F matricies.

Definition (Gauge equivilance of $6j$ symbols)**.** A gauge equivilance of $6j$ symbols $F_{-}^{-,-,-}$ and $\tilde{F}_{--}^{-,-,-}$ on a fusion sytem $(\mathscr{L}, N_{-}^{-,-})$ is the following data:

1. Complex numbers $f_c^{a,b}$ for all $a, b, c \in \mathscr{L}$.

Additionally, a gauge equivilance of $6j$ symbols is required to satisfy the following properties:

1. $f_c^{a,b} \neq 0$ if and only if $(a, b, c) \in \mathscr{L}^3$ is admissible.
2. $f_a^{1,a} = f_a^{a,1} = 1$ for all $a \in \mathscr{L}$.
3. (Rectangle axiom) For all $a, b, c, d, n, m \in \mathscr{L}$,

$$f_n^{b,c} f_d^{a,n} F_{d;n,m}^{a,b,c} = \tilde{F}_{d;n,m}^{a,b,c} f_m^{a,b} f_d^{m,c}.$$

□

If $(\mathscr{L}, N, F)$ and $(\mathscr{L}', N', F')$ are $6j$ fusion systems with different label sets, then a gauge equivilance between $\mathscr{L}$ and $\mathscr{L}'$ is a guage equivilance of $(\mathscr{L}, N, F)$ to some system $(\mathscr{L}, N, \tilde{F})$, followed by a standard equivilance of fusion systems between $(\mathscr{L}, N, \tilde{F})$ and $(\mathscr{L}', N', F')$.

.[WORK: Give explination of rectangle axiom, preferably with graphical language]

In the case of the toric code we summarize the relevant data. The label set is $\mathscr{L} = \{I, X, Y, Z\}$. The nonzero fusion coefficients are given by

	I	X	Y	Z
I	$N_I^{I,I} = 1$	$N_X^{I,X} = 1$	$N_Y^{I,Y} = 1$	$N_Z^{I,Z} = 1$
X	$N_X^{X,I} = 1$	$N_I^{X,X} = 1$	$N_Z^{X,Y} = 1$	$N_Y^{X,Z} = 1$
Y	$N_Y^{Y,I} = 1$	$N_Z^{Y,X} = 1$	$N_I^{Y,Y} = 1$	$N_X^{Y,Z} = 1$
Z	$N_Z^{Z,I} = 1$	$N_Y^{Z,X} = 1$	$N_X^{Z,Y} = 1$	$N_I^{Z,Z} = 1$

All of the F matricies are the identity. The non-unit non-zero braiding coefficients are given by

	I	X	Y	Z
I				
X			$R_Z^{X,Y} = -1$	$R_Y^{X,Z} = -1$
Y		$R_Z^{Y,X} = -1$		$R_X^{Y,Z} = -1$
Z		$R_Y^{Z,X} = -1$	$R_X^{Z,Y} = -1$	

This gives a full definition of the toric code as modular tensor fusion system. All that is left is to show is that all of the axioms of are satisfied - this is Exercise 6.3.

6.2 The category-theoretic viewpoint

In this subsection, we give the category theoretic perspective on Modular Tensor Categories (MTCs). As with subsection 6.1, we will build up to the definition of a MTC slowly. Thinking of MTCs as corresponding to "non-degenerate" finite abelian groups, we will start with the category-theory analogues of monoids[10], groups, finite groups, finite abelian groups, and then end with non-degenerate finite abelian group. The category theory analogues are as below:

Algebraic structure	Categorification
Set	Category
Monoid	Monoidal category
Finite group	Fusion category
Finite abelian group	Braided fusion category
"non-degenerate" finite abelian group	Modular Tensor Category

. We begin with the generalization of monoid:

Definition (Monoidal category)**.** A monoidal category is the following data:

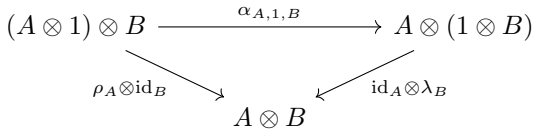
1. A category $\mathscr{C}$.
2. A functor $\otimes : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$.
3. (Identity) A distinguished element $1 \in \mathscr{C}$.
4. (Associativity) A natural equivilance $\alpha : - \otimes (- \otimes -) \to (- \otimes -) \otimes -$, where $- \otimes (- \otimes -)$ denotes the functor $\mathscr{C} \times \mathscr{C} \times \mathscr{C} \to \mathscr{C}$ sending (A, B, C) to $A \otimes (B \otimes C)$, and similarly for $(- \otimes -) \otimes -$.
5. (Left unitor) A natural equivilance $\lambda : 1 \otimes - \to -$, where $1 \otimes -$ denotes the functor $\mathscr{C} \to \mathscr{C}$ sending A to $1 \otimes A$, and $-$ denotes the identity.

[10] A monoid is a set equipped with an associative binary operation and an identity element

6. (Right unitor) A natural equivilance $\rho : - \otimes 1 \to -$, where $- \otimes 1$ is the functor $\mathscr{C} \to \mathscr{C}$ sending A to $A \otimes 1$.

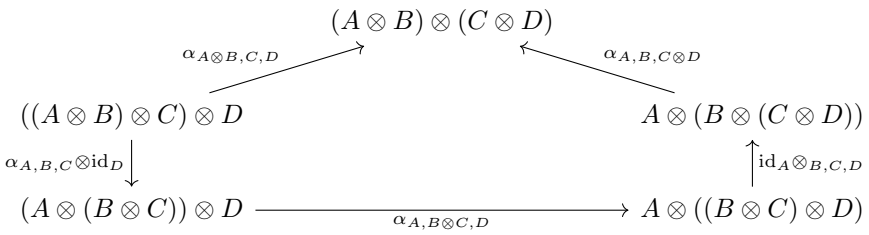
Additionally, a monoidal category is required to satisfy the following properties:

1. (Triangle identity) For all $A, B \in \mathscr{C}$, the diagram



   commutes.

2. (Pentagon identity) For all $A, B, C, D \in \mathscr{C}$, the diagram



   commutes.

□

Observe the parallels between the propreties of monoidal categories and the prerties of $6j$ fusion systems. The triangle identity can be seen as analagous to the fact that associativity being trivial on two inputs, and the pentagon is analagous to the pentagon. We will make this explicit when we show how to make fusion systems from categories.

In the definition of fusion systems, the identity, associativity, and inverse are properties instead of structures. They are unique if they exist. While the identity will be unique up to isomorphism, one still must make a choice of object. There are possibly multiple different choices of natural equivilances for the unit. In category theory, the difference between equal and isomorphic is very pronounced, and one needs to choose an isomorphism. The following theorem answers in what sense we really do get mileage out of considering categories in which we make strange choices of α, λ, ρ, and in what sense we really do get mileage out of considering categories with multiple objects in the same equivilance class. The notion of monoidal equivilance is used in the theorem; we postpone the definition until after the statement.

Theorem 6.1 ([HH09])**.** *Let $(\mathscr{C}, \otimes_{\mathscr{C}}, \alpha_{\mathscr{C}}, \lambda_{\mathscr{C}}, \rho_{\mathscr{C}})$ be a monoidal category. Then*

1. *(MacLane) $\mathscr{C}$ is monoidally equivilant to a category $(\mathscr{D}, \otimes_{\mathscr{D}}, \alpha_{\mathscr{D}}, \lambda_{\mathscr{D}}, \rho_{\mathscr{D}})$ in which $A \otimes_{\mathscr{D}} (B \otimes_{\mathscr{D}} C) = (A \otimes_{\mathscr{D}} B) \otimes_{\mathscr{D}} C$, $1 \otimes_{\mathscr{D}} A = A \otimes_{\mathscr{D}} 1 = 1$, and $\alpha_{\mathscr{D}}, \lambda_{\mathscr{D}}, \rho_{\mathscr{D}}$ are identity functors, for all $A, B, C \in \mathscr{D}$.*
2. *$\mathscr{C}$ is monoidally equivilant to a category in $\mathscr{D}$ in which all objects which are isomorphic are equal.*

*However, $\mathscr{C}$ is **not** in general equivilant to a category which is both at the same time.*

This theorem really says that you cannot have your cake and eat it too. You can forget about non-trivial maps or you can forget about non-equal isomorphic obects, but you can't do both at once. Authors will often assume either one condition or the other (known as *strict* and *skeletal* respectively), and this will sometimes lead to confusion across the literature. A monoidal equivilance is a monoidal functor which has an inverse.

Definition (Monoidal functor)**.** A monoidal functor between monoidal categories $(\mathscr{C}, \otimes_{\mathscr{C}}, \alpha_{\mathscr{C}}, \lambda_{\mathscr{C}}, \rho_{\mathscr{C}}, 1_{\mathscr{C}})$ and $(\mathscr{D}, \otimes_{\mathscr{D}}, \alpha_{\mathscr{D}}, \lambda_{\mathscr{D}}, \rho_{\mathscr{D}}, 1_{\mathscr{D}})$ is the following data:

1. A functor $F : \mathscr{C} \to \mathscr{D}$.
2. A morphism $\epsilon : 1_{\mathscr{D}} \to F(1_{\mathscr{C}})$.
3. A natural transformation μ between the functors $F(-) \otimes_{\mathscr{D}} F(-)$ and $F(- \otimes_{\mathscr{C}} -)$.

Additionally, a monoidal functor is required to satisfy the following properties:

1. (Associativity) For all $A, B, C \in \mathscr{C}$, the diagram

$$\begin{array}{ccc}
(F(A) \otimes_{\mathscr{D}} F(B)) \otimes_{\mathscr{D}} F(C) & \xrightarrow{\alpha_{\mathscr{D};F(A),F(B),F(C)}} & F(A) \otimes_{\mathscr{D}} (F(B) \otimes_{\mathscr{D}} F(C)) \\
\downarrow{\scriptstyle \mu_{A,B} \otimes \mathrm{id}_{F(C)}} & & \downarrow{\scriptstyle \mathrm{id}_{F(A)} \otimes \mu_{B,C}} \\
F(A \otimes_{\mathscr{C}} B) \otimes_{\mathscr{D}} F(C) & & F(A) \otimes_{\mathscr{D}} F(B \otimes_{\mathscr{C}} C) \\
\downarrow{\scriptstyle \mu_{A \otimes_{\mathscr{C}} B, C}} & & \downarrow{\scriptstyle \mu_{A, B \otimes_{\mathscr{C}} C}} \\
F((A \otimes_{\mathscr{C}} B) \otimes_{\mathscr{C}} C) & \xrightarrow{F(\alpha_{\mathscr{C};A,B,C})} & F(A \otimes_{\mathscr{C}} B \otimes_{\mathscr{C}} C)
\end{array}$$

   commutes.

2. (Unitality) The diagrams

$$\begin{array}{ccc} 1_{\mathscr{D}} \otimes_{\mathscr{D}} F(A) & \xrightarrow[\epsilon \otimes \mathrm{id}_{F(A)}]{} & F(1_{\mathscr{C}}) \otimes F(A) \\ \downarrow{\scriptstyle \lambda_{\mathscr{C};F(A)}} & & {\scriptstyle \mu_{1_{\mathscr{C}},A}}\downarrow \\ F(A) & \xleftarrow[F(\lambda_{\mathscr{C};A})]{} & F(1_{\mathscr{C}} \otimes A) \end{array}$$

and

$$\begin{array}{ccc} F(A) \otimes_{\mathscr{D}} 1_{\mathscr{D}} & \xrightarrow[\mathrm{id}_{F(A)} \otimes \epsilon]{} & F(A) \otimes_{\mathscr{D}} F(1_{\mathscr{C}}) \\ \downarrow{\scriptstyle \rho_{\mathscr{C};F(A)}} & & {\scriptstyle \mu_{A,1_{\mathscr{C}}}}\downarrow \\ F(A) & \xleftarrow[F(\rho_{\mathscr{C};A})]{} & F(1_{\mathscr{C}} \otimes A) \end{array}$$

commute for all $A \in \mathscr{C}$.

□

We now define fusion categories. One key difficulty is deciding what category-theorertical object should correspond to the label set $\mathscr{L}$ of a fusion system. The answer is as follows. We want general elements of $\mathscr{C}$ to be uniquely representable as direct sums of the elements in the label set. The elements of $\mathscr{C}$ which cannot be broken down further as direct sums of smaller objects are known as indecomposable objects.

There are a few difficulties in trying to formalize this idea. For one, you might be in the strange case that there are indecomposable objects that still have smaller subjects. For example, consider the category of abelian groups. The group $\mathbb{Z}_4$ has the subject $\mathbb{Z}_2$. However, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \neq \mathbb{Z}_4$. Formally, this example is saying that the exact sequence

$$0 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 0$$

does not split. An introduction to exact sequences is found in Appendix B. What we really want is that every object should be the direct sum of objects which themselves have no subjects. Objects with no subobjects are called irriducible objects. This discrepency between irriducible and indecomposable forms one of the key themes of representation theory, and leads to a great deal of subtledy. Irrididucible objects are also called simple objects. Categories in which there is no discrepency between irrididuble and indecomposable are called semisimple, i.e., semisimple categories are those categories in which every object is the direct sum of simple objects.

This discussion above strongly uses the notion of *subobject*. However, it is not clear in general what subobject should mean. The classic intuation is that A is a subobject of B if there is an injective map $f : A \hookrightarrow B$. Being injective is the statement that the kernel of f is 0, but in arbitarary categories there is no good notion of kernel. Thus, we restrict our attention to *abelian* categories.

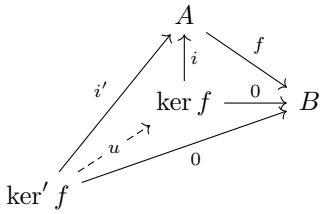
Being abelian comes with a large amount of desirable properties, and most categories people consider are abelian. In abelian categories, we require that all hom sets are given the structure of abelian groups. This is done for various reasons [WORK: what are those reasons?]. Seeing as our eyes are towards quantum physics, all hom sets will be $\mathbb{C}$ vector spaces. Linear combinations of morphisms will correspond to superpositions. To preserve space, we combine "abelian" and "$\mathbb{C}$-linear" into one definition:

Definition ($\mathbb{C}$-linear abelian category)**.** A $\mathbb{C}$-linear abelian category is the following data:

1. A category $\mathscr{C}$.
2. The structure of a $\mathbb{C}$ vector space on $\mathrm{Hom}(A, B)$ for all $A, B \in \mathscr{C}$.

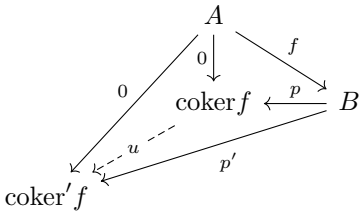
Additionally, a semisimple linear category is required to satisfy the following properties:

1. (Linearity) The composition map $\mathrm{Hom}(A, B) \times \mathrm{Hom}(B, C) \to \mathrm{Hom}(A, C)$ is bilinear for all $A, B, C \in \mathscr{C}$.
2. (Has a zero object) There is an object $0 \in \mathscr{C}$ such that for every $A \in \mathscr{C}$ there is a unique morphism $0 \to A$.
3. (Has binary biproducts) For all $A, B \in \mathscr{C}$ the biproduct of A and B exists. This biproduct is denoted $A \oplus B$, and refered to as the direct sum. Recall that the biproduct of A and B is an object $A \oplus B$, paired with morphisms $p_A, p_B : A \oplus B \to A, B$, and $i_A, i_B : A, B \to A \oplus B$, such that
   - $p_X \circ i_Y$ is id_X when $X = Y$, and 0 otherwise,
   - $i_A \circ p_A + i_B \circ p_B = \mathrm{id}_{A \oplus B}$.
4. (Has kernels and cokernels) For all $A, B \in \mathscr{C}$ and $f : A \to B$, we have objects $\ker f, \mathrm{coker} f$, and morphisms $i : \ker f \to A$, $p : B \to \mathrm{coker} f$. We require that
   - $f \circ i = 0$.
   - For any $i' : \ker' f \to A$ with $f \circ i' = 0$, there is a morphism $u : \ker' f \to \ker f$ such that



   commutes.

- $p \circ f = 0$
- For any $p' : B \to \text{coker}' f$ with $p' \circ f = 0$, there is a morphism $u : \text{coker} f \to \text{coker}' f$ such that



commutes

5. (All monomorphisms and epimorphisms are normal) All monomorphisms are kernels, and all epimorphisms are cokernels. A monomorphism $f : A \to B$ is a map such that for all $g_0, g_1 : C \to A$, $f \circ g_0 = f \circ g_1$ if and only if $g_0 = g_1$. A monomorphism is said to be normal if it is the kernel of some morphism. An epimorphism $f : A \to B$ is a map such that for all $g_0, g_1 : B \to C$, $g_0 \circ f = g_1 \circ f$ if and only if $g_0 = g_1$. An epimorphism is said to be normal if it is the cokernel of some morphism.

□

A general $\mathbb{C}$-linear category is a $\mathbb{C}$-linear abelian category which only needs to satisfy the linearity condition. As always, when defining an object one must define the appropriate morphisms:

Definition ($\mathbb{C}$-linear functor)**.** A $\mathbb{C}$-linear is a functor between $\mathbb{C}$-linear categories $\mathscr{C}, \mathscr{D}$ is a functor $F : \mathscr{C} \to \mathscr{D}$ such that $F : \text{Hom}(A, B) \to \text{Hom}(F(A), F(B))$ is a linear map of vector spaces for all $A, B \in \mathscr{C}$.

Will these definitions out of the way, we can now define fusion categories.

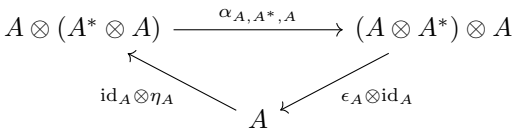
Definition (Fusion category)**.** A fusion category is the following data:

1. A $\mathbb{C}$-linear abelian monoidal category $\mathscr{C}$.
2. (Duals) Choices of objects A^* for every object $A \in \mathscr{C}$.
3. (Unit/co-unit)Choices of morphisms $\eta_A : 1 \to A^* \otimes A$ and $\epsilon_A : A \otimes A^* \to 1$ for all $A \in \mathscr{C}$

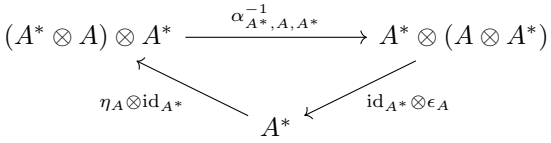
Additionally, a fusion category is required to satisfy the following properties:

1. The tensor product, associativity, left unitor, and right unitor of $\mathscr{C}$ are all $\mathbb{C}$-linear functors.

2. (Rigidity) The diagrams



and



commute for all $A \in \mathscr{C}$.

3. (Semisimpicity) Every object is the direct sum of finitely many simple objects. We call an object simple if it has no proper nontrivial subobjects.
4. All hom spaces are finite dimensional.
5. There are only finitely many isomorphism classes of simple objects
6. The tensor unit 1 is simple.

□

We observe that the definition of rigidity given is not exactly correct. The map $\epsilon_A \otimes \mathrm{id}_A$, for example, has target $1 \otimes A$, not A. In such scenarios, we always implicity apply the left/right unit. For a map like $\mathrm{id}_A \otimes \eta_A$, one first applies to counit, going to $A \otimes 1$, and then one applies η_A on the copy of 1 created. Throughout this text and throughout literature there are many of these implicit maps, and they will generally not be awknowledged. For example, functors between linear categories are always assumed to be linear. It is up to the reader to be cognisent, and to assume what is meant exactly. Additionally, we observe that given any $f : A \to B$ in a fusion category, there is a canonical map $f^* : B^* \to A^*$ defined by the composition

$$f^* : B^* \xrightarrow{\eta_A \otimes \mathrm{id}_{B^*}} A^* \otimes A \otimes B^* \xrightarrow{\mathrm{id}_{A^*} \otimes f \otimes \mathrm{id}_{B^*}} A^* \otimes B \otimes B^* \xrightarrow{\mathrm{id}_{A^*} \otimes \epsilon_A} A^*.$$

We now contrast fusion categories and fusion systems. The first claim is as follows:

Proposition 6.1. *Let $\mathscr{C}$ be a fusion category. Let $\mathscr{L}$ be the set of isomorphism classes of simple objects in $\mathscr{C}$. For any $a, b, c \in \mathscr{L}$ with representatives $A, B, C \in \mathscr{C}$, define*

$$N_c^{a,b} = \dim_{\mathbb{C}} \mathrm{Hom}(A \otimes B, C).$$

The pair $(\mathscr{L}, N_c^{a,b})$ is a fusion system.

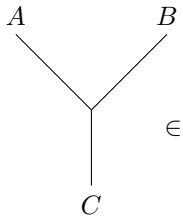
Proof. . [WORK: Prove this!] □

The interesting fact is that one can *not* uniquely go the other direction. Namely, we have the following:

Theorem 6.2 (Ocneanu rigidity,[GHS23])**.** *Let $\mathscr{L}$ be a fusion system. There are finitely many (possibly 0) fusion categories, up to monoidal equivilance, which give systems equivilant to $\mathscr{L}$ under the process described in Proposition 6.1.*

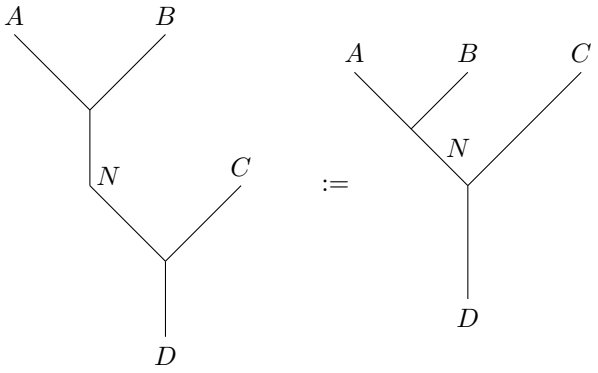
The correct correspondence, in fact, is between fusion categories and $6j$ fusion systems:

Proposition 6.2. *Let $\mathscr{C}$ be a fusion category, with associated fusion system $(\mathscr{L}, N_{-}^{-,-})$. Assume further that $\mathscr{C}$ is multiplicity free, in the sense that all $N_{-}^{-,-} \in \{0,1\}$. For all triples $a,b,c \in \mathscr{L}$, choose representatives $A,B,C \in \mathscr{C}$. Additionally, seeing as each hom space $\mathrm{Hom}(A \otimes B, C)$ is at most one dimensional, we can choose generators*

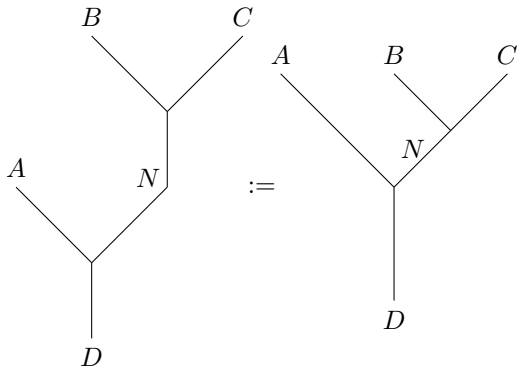


$\in \mathrm{Hom}(A \otimes B, C) \cong \mathbb{C}.$

We find that $\mathrm{Hom}((A \otimes B) \otimes C, D)$ *has a basis*



and $\mathrm{Hom}(A \otimes (B \otimes C), D)$ *has a basis*



In both bases, N ranges over representatives of isomorphism classes of simple objects. Define $F^{a,b,c}_{d;n,m}$ to be $[n,m]$ coefficient of the associativity morphism $\alpha_{A,B,C} : \mathrm{Hom}((A \otimes B) \otimes C, D) \to \mathrm{Hom}(A \otimes (B \otimes C), D)$, expressed as a matrix in the bases above. $(\mathscr{L}, N, F)$ is a $6j$ fusion system.

Theorem 6.3 ([Yam02])**.** *Let $\mathscr{L}$ be a $6j$ fusion system. There is a unique fusion category up to monoidal equivilance which gives $\mathscr{L}$ up to gauge equivilance, under the process described in Proposition 6.2.*

We now give some commentary on Proposition 6.2, through the Yondea perspective. Namely, we elaborate on why it is that we encode associative in terms of the induced map $\mathrm{Hom}((A \otimes B) \otimes C, D) \to \mathrm{Hom}(A \otimes (B \otimes C), D)$ for all D, instead of as the original map $(A \otimes B) \otimes C \to A \otimes (B \otimes C)$. One pragmatic answer is that our hom spaces are vector spaces, not our objects, and so choosing bases of hom spaces is easier. Another pragmatic point is that the induced map on hom spaces for all D uniquely determines the original map, so we aren't losing any information. This is stated formally as follows:

Theorem 6.4 (Yoneda Lemma)**.** *Let $\mathscr{C}$ be a category. Let* **Set** *be the category of sets. For all $A, B \in \mathscr{C}$, consider the functors $\mathrm{Hom}(A, -), \mathrm{Hom}(B, -) : \mathscr{C} \to$* **Set***. There is a canonical isomorphism*

$$\mathrm{Nat}(\mathrm{Hom}(B, -), \mathrm{Hom}(A, -)) \xrightarrow{\sim} \mathrm{Hom}(A, B),$$

where Nat *denotes the space of natural transformations between two functors.*

Proof. Precomposition gives a canonical map

$$\begin{aligned} \mathrm{Hom}(A, B) &\to \mathrm{Nat}(\mathrm{Hom}(B, -), \mathrm{Hom}(A, -)). \\ \varphi &\mapsto (\phi \mapsto \phi \circ \varphi) \end{aligned}$$

We construct an inverse. Let Φ be a natural transformation. Applying Φ to B gives a map

$$\Phi_B : \mathrm{Hom}(B, B) \to \mathrm{Hom}(A, B).$$

We claim $\Phi \mapsto \Phi_B(\mathrm{id}_B)$ gives an inverse to precomposition. This amounts to observing that if $\Phi = (\phi \mapsto \phi \circ \varphi)$ then

$$\Phi_B(\mathrm{id}_B) = \mathrm{id}_B \circ \varphi = \varphi,$$

and that if $\phi = \Phi_B(\mathrm{id}_B)$ then for any $\phi : B \to C$

$$\Phi_C(\phi) = \phi \circ \varphi$$

by naturality of Φ. □

In this case, we systimatically defined F matricies to associate $\mathrm{Hom}((A \otimes B) \otimes C, D)$ with $\mathrm{Hom}(A \otimes (B \otimes C), D)$. Since raning D over simple objects generatres $\mathscr{C}$ by semisimplicity, this means that we have associates $\mathrm{Hom}((A \otimes B) \otimes C, -)$ and $\mathrm{Hom}(A \otimes (B \otimes C), -)$ for all possible choices of target. Since our F matricies were chosen coherently, this assignment is a natural transformation. Thus, by the Yoneda lemma, this canonically specifies an isomorphism in $\mathrm{Hom}((A \otimes B) \otimes C, A \otimes (B \otimes C))$, namely, the associator $\alpha_{A,B,C}$. While encoding $\alpha_{A,B,C}$ as a collection of numbers proves difficult, encoding the associated natural transformation is simpler, since it only requires a finite collection of matricies. We now define our analogues of abelian groups, braided fusion categories:

Definition (Braided fusion category)**.** A braided fusion category is the following data:

1. A fusion category $(\mathscr{C}, \otimes, \alpha)$.
2. A natural isomorphism β between the functor $\mathscr{C} \times \mathscr{C} \to \mathscr{C}$ sending $(A, B) \to A \otimes B$, and the functor sending $(A, B) \to B \otimes A$.

Additionally, a braided fusion category is required to satisfy the following properties:

1. (Hexagon identities) For all $A, B, C \in \mathscr{C}$, the diagrams

$$\begin{array}{ccccc} A \otimes (B \otimes C) & \xrightarrow{\alpha_{A,B,C}} & (A \otimes B) \otimes C & \xrightarrow{\beta_{A\otimes B,C}} & C \otimes (A \otimes B) \\ \downarrow{\scriptstyle \mathrm{id}_A \otimes \beta_{B,C}} & & & & \downarrow{\scriptstyle \alpha_{B,C,A}} \\ A \otimes (C \otimes B) & \xrightarrow[\alpha_{A,C,B}]{} & (A \otimes C) \otimes B & \xrightarrow[\beta_{A,C} \otimes \mathrm{id}_B]{} & (C \otimes A) \otimes B \end{array}$$

and

$$\begin{array}{ccccc} (A \otimes B) \otimes C & \xrightarrow{\alpha^{-1}_{A,B,C}} & A \otimes (B \otimes C) & \xrightarrow{\beta_{A,B\otimes C}} & (B \otimes C) \otimes A \\ \downarrow{\scriptstyle \beta_{A,B} \otimes \mathrm{id}_C} & & & & \downarrow{\scriptstyle \alpha^{-1}_{B,C,A}} \\ (B \otimes A) \otimes C & \xrightarrow[\alpha^{-1}_{B,A,C}]{} & B \otimes (A \otimes C) & \xrightarrow[\mathrm{id}_B \otimes \beta_{A,C}]{} & B \otimes (C \otimes A) \end{array}$$

commute.

□

[WORK: define braided monoidal functor]

We now show that braided fusion categories are indeed equivilant to braided $6j$ fusion systems:

Proposition 6.3. *Let $\mathscr{C}$ be a multiplicity free braided fusion category, with associated $6j$ fusion system $(\mathscr{L}, N_{-}^{-,-}, F_{-}^{-,-,-})$. For all triples $a, b, c \in \mathscr{L}$, choose reprasentatives $A, B, C \in \mathscr{C}$. We define*

[WORK: cool braided symbol: $= \beta$ transformation of original].

[WORK: find correct definition of R-values.]

This process induces a one-to-one correspondance of braided fusion categories up to braided monoidal equivilance and braided fusion systems up to gauge equivilance.

We are now ready to give our final definition:

Definition (Modular Tensor Category)**.** A Modular Tensor Category is the following data:

1. A braided fusion category $\mathscr{C}$.
2. (Twist) A natural equivilance $\theta : \mathscr{C} \to \mathscr{C}$.

Additionally, a Modular Tensor Category is required to satisfy the following properties:

1. $\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$ for all $A, B \in \mathscr{C}$.
2. $\theta_{A^*} = (\theta_A)^*$ for all $A \in \mathscr{C}$.
3. (Non-degeneracy) If $A \in \mathscr{C}$ is a simple object such that for all other simple objects $B \in \mathscr{C}$

$$\mathrm{tr}(\beta_{A,B} \circ \beta_{B,A}) = \mathrm{tr}(\mathrm{id}_{A\otimes B}),$$

then $A \cong 1$. The trace of a morphism $f : A \to A$ is defined as

$$\mathrm{tr}(f) : 1 \xrightarrow{\eta_A} A^* \otimes A \xrightarrow{\mathrm{id}_{A^*} \otimes (\theta_X \circ f)} A^* \otimes A \xrightarrow{\beta_{A^*,A}} A \otimes A^* \xrightarrow{\epsilon_A} 1.$$

The space End(1) is one dimensional, with a canonical generator id_1. Hence, we can canonically identify $\mathrm{tr}(f)$ with a complex number. Graphically, we represent trace as the closed loop [WORK: make diagram].

[WORK: Do I have to do trace? Can I just set these to be equal and have a good day (c.f. [DNO13])]

□

The intuition for the twist is [WORK: what is the intuition?]. The non-degeneracy condition states that only the identity should braid trivially with the other simple objects. [WORK: What is modular equivilance?]

This allows us to state our final equivilance:

Proposition 6.4. *The process in Proposition 6.3 gives a one-to-one correspondance between Modular Tensor Categories up to modular equivilance and modular tensor fusion systems up to gauge equivilance.*

MTCs are called modular because they naturally induce representations of the group of 2 by 2 matricies with unit determinant, $\mathrm{SL}_2(\mathbb{Z})$. The group $\mathrm{SL}_2(\mathbb{Z})$ is known as the modular group, due to its connections with moduli spaces of elliptic curves. We define the modular representation as follows:

Proposition 6.5. *Let $\mathscr{C}$ be an MTC, whose set $\mathscr{L}$ of isomorphism classes of simple objects has n elements. We define the S-matrix of an MTC to be the n by n matrix whose $[a,b]$th coefficient is*

$$S_{a,b} = \mathrm{tr}\left(\beta_{A,B} \cdot \beta_{B,A}\right) = [WORK : make\ graphical\ formula]$$

where a, b are isomorphism classes of simple objects with representatives A, B. Similarly, we define the T-matrix of an MTC to be the n by n diagonal matrix whose $[a,a]$th coefficient is θ_A. Since A is simple, $\mathrm{End}(A)$ is one dimensional, and has a canonical generator given by id_A. Hence, we can identity θ_A with a complex number. The map

$$\rho_{\mathscr{C}} : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Aut}(\mathbb{C}[\mathscr{L}])$$
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \mapsto S,\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto T$$

is a representation of the modular group.

.[WORK: Normalize S and T matricies properly]

These S-matricies and T-matricies are very important invariants of MTCs. They do not, however, uniquely determine the MTC [MS21]. We summarize some important facts about MTCs:

Theorem 6.5. *The follows claims about MTCs are all true:*

- *Suppose $\mathscr{C}$ is a category satisfying all of the conditions of a MTC, except for non-degeneracy (this is called a pre-modular category). Then, $\mathscr{C}$ is modular if and only if the S-matrix is invertible.*
- *([BNRW16]) There are finitely many MTCs, up to braided monoidal equivilance, of a given rank.*
- *.[WORK: think of what other things should go here.]*

6.3 The MTC $\mathcal{Z}(\mathbf{Rep}_{\mathbb{Z}_2})$

In this section we introduce the MTC which corresponds to the toric code, $\mathcal{Z}(\mathbf{Rep}_{\mathbb{Z}_2})$. Intuitively, this can be seen as follows. If fusion categories are generalized groups, then groups should certainly give fusion categories. Namely, a finite group G is assigned its *category of representations* $\mathbf{Rep}_G$. We saw in subsection 6.1 that the modular tensor fusion system associated with the toric code was essentially the group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, except with a non-trivial braiding between the two copies of $\mathbb{Z}_2$. Seeing as the group $\mathbb{Z}_2$ corresponds to the fusion category $\mathbf{Rep}_{\mathbb{Z}_2}$, putting two copies of $\mathbb{Z}_2$ together with a twist corresponds to the category $\tilde{\mathcal{Z}}(\mathbf{Rep}_{\mathbb{Z}_2})$, where $\mathbf{Rep}^*_{\mathbb{Z}_2}$ is the [WORK: what?] category of $\mathbf{Rep}_{\mathbb{Z}_2}$, and $\boxtimes$ is Deligne's tensor product of abelian categories. This section is devoted to a proper treatment of all terms used above, starting with representation theory. [WORK: new definition, new intuition]

One of the only truly "solved" fields of mathematics is linear algebra. Represenation theory can be seen as study of more complicated algebraic objects (groups, rings, algebras) in terms of vector spaces. Namely, instead of looking at an algebraic object we look at all of the ways that it can act on vector spaces. Formally, we define the category of representations of a group G as follows:

$$\mathbf{Rep}_G = \begin{pmatrix} \textbf{objects} : (V, \rho),\ V/\mathbb{C} \text{ a vector space and } \rho : G \to \mathrm{Aut}(V) \text{ a homomorphism} \\ \textbf{morphisms} : \text{linear maps of vector spaces which respect the } G\text{-action} \end{pmatrix}.$$

As usual, $\mathrm{Aut}(V)$ denotes the group of automorphisms of V. Given two representations (V_0, ρ_0) and (V_0, ρ_1), a linear map $f : V_0 \to V_1$ is said to respect the G-action if the diagram

$$\begin{array}{ccc} V_0 & \xrightarrow{f} & V_1 \\ {\scriptstyle \rho_0(g)}\downarrow & & \downarrow{\scriptstyle \rho_1(g)} \\ V_0 & \xrightarrow{f} & V_1 \end{array}$$

commutes for all $g \in G$. A map which respects the G-action is also called G-linear. Observe that representation can be seen as part of the Yoneda perspective: It is better to study an object indirectly by its relation with other objects than it is to study that object in itself. The first big property about the category of representations is that it is abelian:

Proposition 6.6. *Given representations (V_0, ρ_0) and (V_1, ρ_1), the space of G-linear morphisms $f : V_0 \to V_1$ is a subset of the vector space of all linear morphisms, $\mathrm{Hom}_{\mathbf{Vec}}(V_0, V_1)$. Thus, $\mathrm{Hom}_{\mathbf{Rep}_G}((V_0, \rho_0), (V_1, \rho_1))$ can be canonically given the structure of a vector space. This gives $\mathbf{Rep}_G$ the structure of a $\mathbb{C}$-linear abelian category.*

Proof. . [WORK: Do the proof.] □

One can use Proposition 6.6 to get some intuition. One can define a representation of an associative $\mathbb{C}$-algebra[11] R to be a ring homomorphism $R \to \mathrm{End}(V)$, sending R into the algebra of endomorphisms of a vector space V. As such, we can construct of a category $\mathbf{Rep}_R$ for every algebra. These categories are abelian as well. Moreover these are in some sense the only abelian categories, as shown in the following theorem:

Theorem 6.6 (Mitchell's Embedding Theorem)**.** *Let $\mathscr{C}$ be an abelian category. There is some associative algebra R for which there exists a fully faithful exact functor*

$$F : \mathscr{C} \hookrightarrow \mathbf{Rep}_R.$$

Here, we define an exact functor is one which sends short exact sequences

$$0 \to A \xrightarrow{i} B \xrightarrow{q} C \to 0$$

to short exact sequences

$$0 \to F(A) \xrightarrow{F(i)} F(B) \xrightarrow{F(q)} F(C) \to 0.$$

We now introduce a few more structures on $\mathbf{Rep}_G$.

Proposition 6.7. *Given representations (V_0, ρ_0) and (V_1, ρ_1), define their tensor product to be the representation whose underlying vector space is $V_0 \otimes V_1$, and whose G-action $\rho_0 \otimes \rho_1$ is defined by the formula*

$$(\rho_0 \otimes \rho_1)(g)(v_0 \otimes v_1) = \rho_0(g)(v_0) \otimes \rho_1(g)(v_1).$$

This naturally induces a functor $\otimes : \mathbf{Rep}_G \times \mathbf{Rep}_G \to \mathbf{Rep}_G$. Define the following structures on $\mathbf{Rep}_G$:

- *The unit element $\mathbb{C}$, whose G-action is given by the 0 map in $G \to \mathrm{Aut}(\mathbb{C})$.*
- *The associator $\alpha : V_0 \otimes (V_1 \otimes V_2) \to (V_0 \otimes V_1) \otimes V_2$ sending $v_0 \otimes (v_1 \otimes v_2)$ to $(v_0 \otimes v_1) \otimes v_2$.*
- *The left unitor $\lambda : \mathbb{C} \otimes V \to V$ sending $x \otimes v$ to $x \cdot v$.*
- *The right unitor $\rho : V \otimes \mathbb{C} \to V$ sending $v \otimes x$ to $x \cdot v$.*

all of these maps extend to functors, and endow $\mathbf{Rep}_G$ with the structure of a monoidal category.

Proof. . [WORK: make proof] □

When G is finite, the situation is very nice. In particuar, we have the following theorem:

[11] A $\mathbb{C}$-algebra is a vector space R, with multiplication $R \otimes R \to R$ and a unit map $\mathbb{C} \to R$

Theorem 6.7 (Maschke's theorem)**.** *Let G be a finite group. [WORK: define duals, unit, counit]. This endows $\mathbf{Rep}_G$ with the structure of a fusion category.*

Proof. . [WORK: make proof] □

We have now introduced enough machinery to answer the following basic question: Does the category of representations of a group (up to the correct notion of equivilance) determine the starting group (up to isomorphism)? The Yoneda perspective gives us an answer in the affermative - studying an object via its interactions with other objects should give you all the information you need to know. It turns out that there is an explicit way of constructing G from $\mathbf{Rep}_G$, though it is more complicated to treat in full generality than Yoneda's lemma. After one definition, we will be able to state this construction and prove its validity in full detail.

Definition (Monoidal natural transformation)**.** .[WORK: make definition]

Theorem 6.8 (Tannaka duality for finite groups)**.** *Let G be a finite group. Let $F : \mathbf{Rep}_G \to \mathbf{Vec}$ be the forgetful functor, sending a representation (V, ρ) to the underlying vector space V. Let $\mathrm{Aut}^{\otimes}(F)$ denote the group of monoidal natural transformation from F to itself, under composition. There is a natural map*

$$G \to \mathrm{Aut}^{\otimes}(F)$$

sending an element $g \in G$ to the automorphism of F acting on (V, ρ) by $\rho(g)$. This is a well defined map, and it induces an isomorphism of groups.

Proof. . [WORK: make proof] □

In the analogy between algebraic structures and their categorifications, finite abelian groups correspond to braided fusion categories. This can be turned into a very percise claim, which we now state:

Proposition 6.8. *Let G be a finite group. The fusion category $\mathbf{Rep}_G$ admits a braiding if and only if G is abelian. If G is abelian, then this braiding is defined explicitely by [WORK: make braiding].*

Proof. . [WORK: make proof] □

We thus observe the following: $\mathbf{Rep}_G$ never has the structure of an MTC. When G is non-abelian then $\mathbf{Rep}_G$ is not braided, but when G is abelian $\mathbf{Rep}_G$ is symmetric, in the sense that $\beta_{A,B} \cdot \beta_{B,A} = \mathrm{id}_A$ for all A, B, so it is degenerate. We are thus in need of a "non-degenerate abelianization", which takes in a good fusion category and spits out a non-degenerate braided fusion category, i.e., an MTC. There is a canonical such construction, known as the Drinfeld center.

Loosely speaking, the Drinfeld center takes in a fusion category $\mathscr{C}$, and looks at all possible ways that objects in $\mathscr{C}$ can braid with other objects. As to avoid making a choice of any specific braiding, objects in $\mathscr{C}$ become pairs (A, Φ), where A is an object and Φ is a possible way A could braid with other elements. This

naturally allows one to be a global braiding on $\mathcal{Z}(\mathscr{C})$. The statement that $\mathcal{Z}(\mathscr{C})$ is non-degenerate is now the statement that choosing the right half-braidings we can make every object briad non-trivially with at least one other object. Formally, we can define the Drinfled center as follows:

Proposition-Definition 6.1 (Drinfeld center)**.** The Drinfeld center of a monoidal category $\mathscr{C}$ is a braided monoidal category defined as follows:

- **objects:** Pairs (A, Φ), where $A \in \mathscr{C}$, and Φ is a natural isomorphism of monoidal natural isomorphism between the two functors $A \otimes -$ and $- \otimes A$ from $\mathscr{C}$ to $\mathscr{C}$, satisfying the additional condition that

$$\Phi_{B\otimes C} = (\mathrm{id}_B \otimes \Phi_C) \circ (\Phi_B \otimes \mathrm{id}_C)\,.$$

- **morphisms:** Given $(A, \Phi), (B, \Psi) \in \mathcal{Z}(\mathscr{C})$, $\mathrm{Hom}_{\mathcal{Z}(\mathscr{C})}((A, \Phi), (B, \Psi))$ is the subspace of morphisms $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ such that for all $C \in \mathscr{C}$,

$$(\mathrm{id}_C \otimes f) \circ \Phi_C = \Psi_C \circ (f \otimes \mathrm{id}_C).$$

- **tensor product:** Given $(A, \Phi), (B, \Psi) \in \mathcal{Z}(\mathscr{C})$, we define

$$(A, \Phi) \otimes (B, \Psi) = (A \otimes B, (\Phi \otimes \mathrm{id}_{\mathscr{C}}) \circ (\mathrm{id}_{\mathscr{C}} \otimes \Psi))\,.$$

- **unit:** The element $(1, \rho \circ \lambda)$
- **braiding:** [WORK: write out braiding correctly]

Along with natural choices of associativity and unitors, this gives $\mathcal{Z}(\mathscr{C})$ the structure of a braided monoidal category.

Proof. . [WORK: do the proof] □

When we input a fusion category to this construction, we get a fusion category out. Moreover, the following condition is neccecary and sufficient to obtain a modular tensor category from this construction:

Definition (Spherical fusion category)**.** . [WORK: fill out definition]

Proposition 6.9. *If $\mathscr{C}$ is a spherical fusion category, then $\mathcal{Z}(\mathscr{C})$ naturally has the structure of a modular tensor category. [WORK: are some of the structures non-trivial? Should I define them?]*

Proof. . [WORK: make proof. Call on some outside references if neccecary] □

Thus, we have arrived at the MTC associated with the toric code: $\mathcal{Z}(\mathbf{Rep}_{\mathbb{Z}_2})$: The Drinfeld center of of the category of representations of $\mathbb{Z}_2$. This is in some sense the simplest MTC. Namely, the simplest MTCs are those which come from spherical fusion categories, as $\mathcal{Z}(\mathscr{C})$ for some $\mathscr{C}$. The simplest fusion categories

are those which come from groups, as $\mathbf{Rep}_G$ for some G. The simplest non-trivial group is $\mathbb{Z}_2$.

Another intuition for $\mathcal{Z}(\mathscr{C})$ is that it is a sort of "quantum double" [WORK: what is the intuition for quantum doubles? There should be good insight in the following thesis: [dF17]]

We now verify that our two definitions of the MTC associated with the toric code are equivilant:

Proposition 6.10. *.[WORK: show that doing the make-it-a-modular-tensor-fusion-system construction on $\mathcal{Z}(\mathscr{C})$ recovers the previously described data]*

[WORK: closing thoughts on MTCs. Maybe mention something about how most of them can be defined relatively easily using a few constructions. In particular, many models are "weakly-group theoretical". Perhaps talk about Morita equivilance, since we have Drinfeld centers already defiened?]

Exercises:

6.1. Define a $(n+1)$-TQFT as a symmetric monoidal functor $\mathrm{Bord}(n+1) \to \mathbf{Vec}$. Show that this agree with our definition in the (2+1)-TQFT case. [WORK: Flesh this out.]

6.2. The original list of axioms for a monoidal category was longer. It was later found by Max Kelly that the smaller set we gave implies the rest. [WORK: State the other axioms, give an outline of the proof, i.e., the diagrams one should show are commutative and have the reader conclude. nLab includes these.]

6.3. Show that the data associated to the toric code forms a modular tensor fusion system.

6.4. .[WORK: Verlinde formula exercise]

7 Topological Quantum Computing

7.1 The TQC framework

[WORK: The big thing is to draw the picture between topological quantum phases of matter, TQFTs, MTCs, and TQC. Show exactly what this looks like in the case of the toric code, i.e., what the topological quantum phase of matter is, the TQFT, the MTC, and the resulting TQC. Add all the connections and insights that I've come up with along this journey, and things I would feel remiss not including. Really, this should be a version of an introduction-to-TQC-for-experts section. Should definitely mention that TQFTs are generally 1-extended with punctures, to visualize anyons. Should mention that literally making torus

bigger will make error rate smaller, since it's harder for things to accidentally interact with each other (exponential decrease). Maybe another thing to add is how the 1st priority is to minimize energy, and the 2nd order is to maximize entanglement.]

[WORK: Give 2nd motivation for topological quantum computing. Namely, that this might be a good avenue for proving that QC can solve NP complete problems, or close to NP problems! Bring up how this is clearly a good theory for computing knot invariants (add reference to examples of knot invariants that were proved to be easy to calculate using this method). Then, mention that computing the Jones polynomial is known to be NP hard! This is in the introduction of Wang and Rowell's "Mathematics of Topological Quantum Computation". This could be a motivation for hybrid computing like

1. Use classical computers to reduce hard problems to the issue of finding the knot invariant of a given knot.
2. Create that knot by braiding the anyons through spacetime.
3. TQC will naturally compute the relevant knot invariant!

]

[WORK: highlight the fact that we can do more TQC when we allow things other than just pure braiding, i.e., measurement based TQC. Let them know that even abelian anyons can be universal, when we're allowed to do this!]

[WORK: define braid group representations + neccecary objects]

[WORK: shoehorn in the quote

> "Folklore, [...] is a technical term for a method of publication in category theory. It means that someone sketched it on the back of an envelope, mimeographed it (whatever that means) and showed it to three people in a seminar in Chicago in 1973, except that the only evidence that we have of these events is a comment that was overheard in another seminar at Columbia in 1976. Nevertheless, if some younger person is so presumptuous as to write out a proper proof and attempt to publish it, they will get shot down in flames."
> - Paul Taylor[12]

]

[WORK: Look at [LP17], an intro-level physics discussion. Is there something to learn from it?]

7.2 Revisiting toric code TQC

.[WORK: compute what everything looks like for the toric code using category theory. Give the big picture triangle correspondance for the toric code.]

[12] [WORK: make description][Aub19]

7.3 Universal TQC with the Fibbonacci anyon

.[WORK: introduce the Fibonacci anyon. Prove that it is universal with braiding alone. Really what I want to do is show that any form of TQC is universal, but I just think Fibonnacci will be simplest. If anyone has a definition it should be here: [TTWL08]]

[WORK: Here are some misc things for the rest of the manuscript.

In the introduction, maybe add something about the number of Nobel prizes associated with the area? Jones also got his fields medal for this stuff, and maybe others. Witten? Right at the end?

I got rid of the unit TQFT axiom, which now includes the degenerate possibility that $V(S) = \emptyset$ for all S. Is that okay?

Why can I always lift celluations? Zhenghan mentioned this in class, but didn't cite a reference.]

A $\mathbb{Z}_2$ Homology Theory

In this appendix we introduce the basic notations of homology theory with $\mathbb{Z}_2$ coefficients, namely, chains, cycles, and homological equivalence. The settings for homology are *simplicial complexes*, which can be loosely thought of as collections of vertices, edges, and faces, with some edges and vertices identified, just as was done for the torus in this text. A $\mathbb{Z}_2$-chain on a space is an assignment of an element of $\mathbb{Z}_2$ to every edge, where $\mathbb{Z}_2 = \{0, 1\}$ is the additive group modulo 2. The set of $\mathbb{Z}_2$-chains forms a group under edge-wise addition. A $\mathbb{Z}_2$-cycle is a $\mathbb{Z}_2$-chain which can be obtained by starting at a vertex and walking along edges, flipping 1s to 0s and vice versa as you go along, and returning back where you started at the end. Equivalently, a $\mathbb{Z}_2$-cycle is a $\mathbb{Z}_2$-chain which has an even number of 1s touching each vertex. The $\mathbb{Z}_2$-cycles form a subgroup of the group of $\mathbb{Z}_2$-chains. Seeing as all chains and cycles discussed in these notes take coefficients in $\mathbb{Z}_2$, we ease notation by simply saying "chain" and "cycle".

The goal of homology theory is to describe cycles on a geometric object, up to deformations. If one cycle can be continuously deformed into another, then they should be considered equivalent. On the sphere, for example, all loops can be contracted away into nothing. On the torus there are four distinct cycles, namely, the zero cycle, the cycle that goes around the torus horizontally, the cycle that goes around the torus vertically, and the cycle that twists around the torus, as in Figure 4.2 These non-trivial cycles correspond exactly to the continuous vector fields described in the introduction [Fra57].

Loosely, we will call two cycles homologically equivalent if they can be continuously deformed one to another. Given any face, the cycle consisting of 1s along the edges touching that face should be 'homologically trivial", i.e., homologically equivalent to the 0 cycle, since it can be contracted away into nothingness. In a strong sense, this is the only condition one needs to impose. WIth X as our simplicial complex, we let $C_1(X; \mathbb{Z}_2)$ be the group of chains. We let $Z_1(X; \mathbb{Z}_2)$ be the subgroup generated by the cycles consisting of 1s the

boundaries of faces. This is the subgroup of homologically trivial cycles. This lets us define the quotient

$$H_1(X;\mathbb{Z}_2) = C_1(X;\mathbb{Z}_2)/Z_1(X;\mathbb{Z}_2),$$

called the (1st) homology group of X. Two elements are called homologically equivalent if they are in the same coset of $H_1(X;\mathbb{Z}_2)$. Alternatively, two elements are homologically equivalent if one can be obtained from the other by repeatedly flipping 1s and 0s along the boundaries of squares.

It is a well known fact that the first homology group of the torus has four elements, corresponding to the zero class, the horizontal cycle around the torus, the vertical cycle around the torus, and the diagonal cycle.

The importance of $H_1(X;\mathbb{Z}_2)$ is that it is *independent of choice of celluation*. Namely, if we start with the same space and chop it up into vertices, edges, and faces, two different ways, $H_1(X;\mathbb{Z}_2)$ will always be the same. This is in stark contrast to $C_1(X;\mathbb{Z}_2)$ and $Z_1(X;\mathbb{Z}_2)$, which will both change wildly depending on the choice of celluation.

The observant reader might find the above discussion frustrating. In particular, we seem to be using the following intuitions interchangeably:

1. Cycles being continuously deformed to each other
2. Cycles that can be obtained from one another by flipping edges along the boundary of faces.

The worry regarding the distinction between these two notions is justified. In general, the group obtained by imposing the equivalence relation of continuous deformations will not be equal to the homology group $H_1(X)$. The group resulting from imposing the continuous deformation restriction is called the *fundamental group* of X, and is denoted $\pi_1(X)$. In general $\pi_1(X)$ can be quite a bit larger than $H_1(X)$, i.e., the equivalence relation can be weaker. The groups are always related by the fact that $H_1(X)$ is canonically isomorphic to the abelianization of $\pi_1(X)$, i.e., the maximal abelian quotient of $H_1(X)$. In the case that $\pi_1(X)$ is abelian (for example, when X is a torus), this means that there is no distinction between these spaces, and one should not make any worry about the discrepancies in intuition.

The canonical reference for this subject (known as *Algebraic Topology*) is Alan Hatcher's textbook [Hat05].

B Category Theory

[WORK: Make appendix. This is to mension for sure; canonical isomorphism between double duals, non canonical isomorphism between first duals. Not only is this super relevant to rigidity, but Zhenghan said that this was one of Eilenberg-MacLane's key motivations. Find a reference to this fact.]

References

[AA81] Marcia Ascher and Robert Ascher. Code of the quipu. *Ann Arbor: University of Michigan Press*, pages 56–74, 1981.

[AAB+19] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[Aar13] Scott Aaronson. *Quantum computing since Democritus*. Cambridge University Press, 2013.

[AHM+16] Sven Marian Albrecht, Andrew P Higginbotham, Morten Madsen, Ferdinand Kuemmeth, Thomas Sand Jespersen, Jesper Nygård, Peter Krogstrup, and CM Marcus. Exponential protection of zero modes in majorana islands. *Nature*, 531(7593):206–209, 2016.

[Aub19] Clément Aubert. Categories for me, and you? *arXiv preprint arXiv:1910.05172*, 2019.

[BK01] Bojko Bakalov and Alexander A Kirillov. *Lectures on tensor categories and modular functors*, volume 21. American Mathematical Soc., 2001.

[BNRW16] Paul Bruillard, Siu-Hung Ng, Eric Rowell, and Zhenghan Wang. Rank-finiteness for modular categories. *Journal of the American Mathematical Society*, 29(3):857–881, 2016.

[Day21] Cyrus Lawence Day. *Quipus and Witches' Knots: The Role of the Knot in Primitive and Ancient Culture, with a Translation and Analysis of" Oribasius de Laqueis"*. University Press of Kansas, 2021.

[dF17] Giovanni de Felice. Hopf algebras in quantum computation. *Unpublished doctoral dissertation*, 2017.

[DLF+16] Shantanu Debnath, Norbert M Linke, Caroline Figgatt, Kevin A Landsman, Kevin Wright, and Christopher Monroe. Demonstration of a small programmable quantum computer with atomic qubits. *Nature*, 536(7614):63–66, 2016.

[DNO13] Alexei Davydov, Dmitri Nikshych, and Victor Ostrik. On the structure of the witt group of braided fusion categories. *Selecta Mathematica*, 19(1):237–269, 2013.

[DW90] Robbert Dijkgraaf and Edward Witten. Topological gauge theories and group cohomology. *Communications in Mathematical Physics*, 129:393–429, 1990.

[FKLW03] Michael Freedman, Alexei Kitaev, Michael Larsen, and Zhenghan Wang. Topological quantum computation. *Bulletin of the American Mathematical Society*, 40(1):31–38, 2003.

[FKW02] Michael H Freedman, Alexei Kitaev, and Zhenghan Wang. Simulation of topological field theories by quantum computers. *Communications in Mathematical Physics*, 227:587–603, 2002.

[FLW02] Michael H Freedman, Michael Larsen, and Zhenghan Wang. A modular functor which is universal for quantum computation. *Communications in Mathematical Physics*, 227:605–622, 2002.

[Fra57] Theodore Frankel. Homology and flows on manifolds. *Annals of Mathematics*, pages 331–339, 1957.

[GHS23] Azat M Gainutdinov, Jonas Haferkamp, and Christoph Schweigert. Davydov-yetter cohomology, comonads and ocneanu rigidity. *Advances in Mathematics*, 414:108853, 2023.

[Got98] Daniel Gottesman. Theory of fault-tolerant quantum computation. *Physical Review A*, 57(1):127, 1998.

[Hal13] Brian C Hall. *Quantum theory for mathematicians*. Springer, 2013.

[Hat05] Allen Hatcher. *Algebraic topology*. Tsinghua University Press, 2005.

[HH09] Tobias J Hagge and Seung-Moon Hong. Some non-braided fusion categories of rank three. *Communications in Contemporary Mathematics*, 11(04):615–637, 2009.

[Kan98] Bruce E Kane. A silicon-based nuclear spin quantum computer. *nature*, 393(6681):133–137, 1998.

[Kit97] A Yu Kitaev. Quantum error correction with imperfect gates. *Quantum communication, computing, and measurement*, pages 181–188, 1997.

[Kit03] A Yu Kitaev. Fault-tolerant quantum computation by anyons. *Annals of physics*, 303(1):2–30, 2003.

[Lic99] William Bernard Raymond Lickorish. Simplicial moves on complexes and manifolds. *Geometry and Topology Monographs*, 2(299-320):314, 1999.

[LP17] Ville Lahtinen and Jiannis Pachos. A short introduction to topological quantum computation. *SciPost Physics*, 3(3):021, 2017.

[LW05] Michael A Levin and Xiao-Gang Wen. String-net condensation: A physical mechanism for topological phases. *Physical Review B*, 71(4):045110, 2005.

[MS21] Michaël Mignard and Peter Schauenburg. Modular categories are not determined by their modular data. *Letters in Mathematical Physics*, 111(3):60, 2021.

[MZF+12] Vincent Mourik, Kun Zuo, Sergey M Frolov, SR Plissard, Erik PAM Bakkers, and Leo P Kouwenhoven. Signatures of majorana fermions in hybrid superconductor-semiconductor nanowire devices. *Science*, 336(6084):1003–1007, 2012.

[NSS+08] Chetan Nayak, Steven H Simon, Ady Stern, Michael Freedman, and Sankar Das Sarma. Non-abelian anyons and topological quantum computation. *Reviews of Modern Physics*, 80(3):1083, 2008.

[OKMH22] Yun-Tak Oh, Jintae Kim, Eun-Gook Moon, and Jung Hoon Han. Rank-2 toric code in two dimensions. *Physical Review B*, 105(4):045128, 2022.

[Pac91] Udo Pachner. Pl homeomorphic manifolds are equivalent by elementary shellings. *European journal of Combinatorics*, 12(2):129–145, 1991.

[Pre99] John Preskill. Lecture notes for physics 219: Quantum computation. *Caltech Lecture Notes*, page 7, 1999.

[QW21] Yang Qiu and Zhenghan Wang. Representations of motion groups of links via dimension reduction of tqfts. *Communications in Mathematical Physics*, 382:2071–2100, 2021.

[Rof19] Joschka Roffe. Quantum error correction: an introductory guide. *Contemporary Physics*, 60(3):226–245, 2019.

[RW18] Eric Rowell and Zhenghan Wang. Mathematics of topological quantum computing. *Bulletin of the American Mathematical Society*, 55(2):183–238, 2018.

[Sho94] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[Spi18] Michael Spivak. *Calculus on manifolds: a modern approach to classical theorems of advanced calculus*. CRC press, 2018.

[TTWL08] Simon Trebst, Matthias Troyer, Zhenghan Wang, and Andreas WW Ludwig. A short introduction to fibonacci anyon models. *Progress of Theoretical Physics Supplement*, 176:384–407, 2008.

[Wan10] Zhenghan Wang. *Topological quantum computation*. Number 112. American Mathematical Soc., 2010.

[Wen17] Göran Wendin. Quantum information processing with superconducting circuits: a review. *Reports on Progress in Physics*, 80(10):106001, 2017.

[Yam02] Shigeru Yamagami. Polygonal presentations of semisimple tensor categories. *Journal of the Mathematical Society of Japan*, 54(1):61–88, 2002.

[YZB+21] Fangyuan Yang, Alexander A Zibrov, Ruiheng Bai, Takashi Taniguchi, Kenji Watanabe, Michael P Zaletel, and Andrea F Young. Experimental determination of the energy per particle in partially filled landau levels. *Physical review letters*, 126(15):156802, 2021.