Topological Quantum Computing
via
The Toric Code

by Milo Moses

University of California, Santa Barbara

April 20, 2023

Abstract

One of the most exciting forms of quantum computation proposed today is topological quantum computation. In this manuscript we give a detailed introduction to topological quantum computation, with special focus on the simplest non-trivial example: 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

0   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 the microscopic world has proved quite challenging in large part due to thermal fluctuations which cause quantum states to decohere 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 most recent such models is "topological quantum computation" (TQC), proposed formally in a 2008 paper of Freedman-Kitaev-Larsen-Wang [FKLW03]. 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.

There are already a few good surveys of TQC. The relevant mathematics is described in [BK01] and [RW18]. Physics oriented people will get more out of [Pre99] and [NSS+08]. Wang's book [Wan10] gives a relatively complete picture of the subject. The research article by 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 grounded as possible, we put front-and-center the simplest example of TQC: the toric code. This special case is used as motivation for the general theory. 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 to the students of the class without whom this manuscript would not have been possible.

The primary reference for the toric code is the seminal work of Kitaev [Kit03]. It was there that the idea of computation by braiding anyons was first described.

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 to their being seen as too obvious to be stated explicitly. A secondary goal of this manuscript is to present a formal treatment of these implicit ideas.

---

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

Finally, we end with a terminological clarification. The name "toric code" refers to an example of TQC, but also to a quantum error correction algorithm. Moreover, it is from this use in error correcting that it is dubbed a " code". Famously, Google uses the toric code algorithm for its quantum computer. 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 1 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 is useful.

- Section 2 gives a treatment of the basics of quantum mechanics. The axioms are stated from a mathematical perspective, and are given ample motivation from the theory of probability. The only prerequisite is linear algebra.

- Section 3 gives an elementary mathematical description of the toric code. 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.

- Section 4 gives an introduction to topological quantum field theories (TQFTs), the formal mathematical abstractions of topological quantum phases of matter. Subsection 4.1 gives an overview of the subject. Subsection 4.2 defines the $\mathbb{Z}_2$ Dijkgraaf-Witten theory, the TQFT associated with the toric code. This section has no extra formal prerequisites, but from here on out a significantly stronger mathematical maturity will be assumed.

- Section 5 gives an introduction to the relevant category theory. Subsection 5.1 gives a general treatment of categories, and subsection 5.2 deals with braided monoidal categories.

- 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. Subsection 6.2 gives the more elegant interpretation of MTCs in the language of categories. Subsection 6.3 defines $\mathcal{Z}(\mathbf{Rep}_{\mathbb{Z}_2})$, the MTC associated with the toric code.

- Section 7 gives an introduction to the general TQC methodology, using all of the tools developed in the previous sections. Subsection 7.1 gives a

detailed overview of TQC, including measurement-based algorithms. Subsection 7.2 carries this out explicitly for the toric code. Subsection 7.3 introduces the Fibonacci anyon model, and shows that it gives universal quantum computation via braiding alone.

1 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 general, 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)

There are many proposed methods of quantum computation (superconducting quantum computers [Wen17], trapped ion quantum computers [DLF$^+$16], semiconductor based quantum computers [Kan98], etc...), but they all have roughly similar mathematical descriptions. This common description is known as *universal* quantum computation. TQC has a fundamentally different mathematical formalism. It was a major milestone when TQC was shown to be equivalent to universal quantum computation, in the sense that universal quantum computers can effectively simulate all instances of TQC, and there are instances of TQC that can simulate universal quantum computers [FLW02, FKW02]. It is expected that every reasonable mathematical formalism for quantum computation will be equivalent in this sense: this is the content of the Freedman-Church-Turing thesis [FKLW03].

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 provably 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

---

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

Figure 1.1: A model of a (non-quantum) topological message

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 with. 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 simply read off by counting (as in Figure 1.1)! 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 accidentally 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 1.2. 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 strands being knotted are no longer physical pieces of twine, but *trajectories of quasiparticles through spacetime*. For instance, suppose A and B 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 1.2: An Incan Quipu
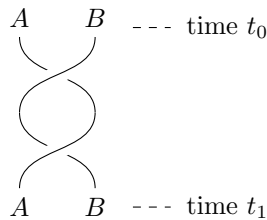
Spooky action at a distance causes non-trivial knots to store non-trivial quantum information. That is, moving one quasiparticle around another will lead to a physically different quantum system than if the particle had not been moved. The resulting physical system doesn't depend on how the first particle moved around the other, however - only the topology of the knot matters.

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 constructed[3]. Things that behave like particles in these 2 dimensional phases of matter are known as quasiparticles, and form non-trivial knots when braided.

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, 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

---

[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.
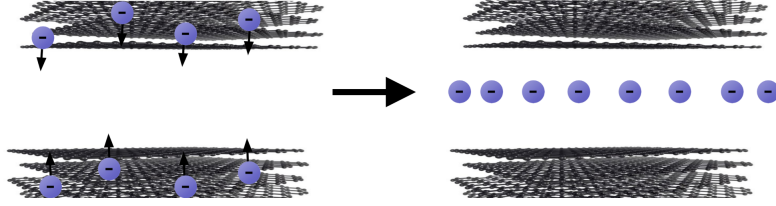
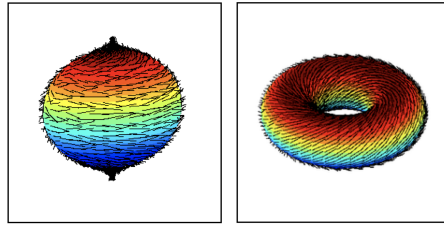Figure 1.3: The formation of an electron gas from graphene.

Figure 1.4: Assigning vector fields (spins) to a sphere, verses to a torus

phase of matter [YZB$^+$21]. A diagram showing this process is found in Figure 1.3

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 entangle 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 the content of the "hairy ball theorem" [EG79].

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 1.4. 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. 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 atoms around it: 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.

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, which will interfere with computation. Compactly, we use the term *ground state* to refer to a state in a system with lowest possible energy.

We now 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.

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.

2   Quantum Foundations

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

Throughout this section we will strongly use analogy with the classical theory of probability, which we now recall in a mathematically rigorous way. 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 analyze probabilities. Assigning a real number to every element in a set S is exactly the same as choosing a vector in $\mathbb{R}[S]$ - the real vector space uniquely defined to have S as a basis. That is, every vector in $\mathbb{R}[S]$ is a linear combination of elements of S. If we have probabilities p_x assigned to every $x \in S$, then this corresponds to the vector $\sum_{x \in S} p_x \ket{x} \in \mathbb{R}[S]$. For example, the previous example of accepting and denying can be concisely summarized as the vector

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

We make a comment about our notation. We use the bars/angle-brackets $\ket{\cdot}$ to formally separate elements of our set S from the numbers used when taking linear combinations. This is necessarily, for if 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 separating with bars/angle-brackets, we arrive at the much more sensible $\frac{2}{3} \ket{0} + \frac{1}{3} \ket{1}$. The symbol $\ket{\cdot}$ us known as a *ket*. Ket 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

$$\ket{\text{start}} \longrightarrow \tfrac{1}{2}\ket{\text{h}} + \tfrac{1}{2}\ket{\text{t}} \longrightarrow \tfrac{1}{2}\left(\ket{\text{hh}}\right) + \tfrac{1}{2}\left(\tfrac{1}{2}\ket{\text{th}} + \tfrac{1}{2}\ket{\text{tt}}\right).$$

$$\rotatebox{90}{$\in$} \qquad\qquad\qquad \rotatebox{90}{$\in$} \qquad\qquad\qquad\qquad \rotatebox{90}{$\in$}$$

$$\mathbb{R}[\{\text{start}\}] \qquad\qquad \mathbb{R}[\{\text{h, t}\}] \qquad\qquad \mathbb{R}[\{\text{hh, ht, th, tt}\}]$$

We introduce the following terminology, for ease of discussion. 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 $\sum_{x \in S} p_x \ket{x}$ 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, $-\frac{1}{2}\ket{\text{heads}} + \frac{1}{2}\ket{\text{tails}}$ 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 $\sum_{x \in S} p_x \ket{x}$, 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 manipulation

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

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 probability 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:

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 finite sets, the system obtained by joining $\mathbb{R}[S]$ and $\mathbb{R}[S']$ is $\mathbb{R}[S \times S']$.

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 collapse into each $x \in S$ with probability p_x.

$\square$

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 quantum states on S. Here, 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 finite sets, the system obtained by joining $\mathbb{C}[S]$ and $\mathbb{C}[S']$ is $\mathbb{C}[S \times S']$.

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 collapse into each $x \in S$ with probability $|c_x|^2$.

$\square$

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]

We now add some physical interpretation to these axioms. 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:

- 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 formally 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 $M : \mathbb{C}[S] \to \mathbb{C}[S]$ by

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

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

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

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

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

---

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

same signs in the $|0\rangle$s causing the probability of measuring 0 to add, and the amplitudes had opposite signs in the $|1\rangle$s, causing the probabilities of measuring 1 to cancel. This linear map M defined is called the Hadamard gate, and it is a very important process for quantum information. It is not immediately clear that H sends all normalized vectors to normalized vectors. For instance, if we had defined $M(|1\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ then applying M to the equal superposition of 0 and 1 would not give a normalized value. The following proposition clarifies exactly what transformations are allowed in quantum mechanics:

Proposition 2.1. *Let S be a finite set, and let $U : \mathbb{C}[S] \to \mathbb{C}[S]$ a linear transformation. The following are equivalent:*

1. *U sends normalized vectors to normalized vectors.*

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

If either of these two equivalent 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 complex conjugation. We find that

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

is the norm square of $|\psi\rangle$. Showing that U preserves norm is thus the same as showing that

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

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 these formulas, we find that U preserving norm implies that $\langle U\phi | U\psi \rangle = \langle \phi | \psi \rangle$ for all $|\psi\rangle, |\phi\rangle \in \mathbb{C}[S]$. Let $UU^\dagger$ be the product of U with its conjugate transpose. This can be represented as a matrix whose rows and columns are labeled by elements of S. The $(x, y) \in S \times S$ entry of $UU^\dagger$ is

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

13

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

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

which gives us the desired conclusion. $\qquad\square$

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. States 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 to choosing a real number as observable.

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 (observables) to correspond to each pure state, collapsing into a particle, 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 pure 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 2.2 (Spectral theorem)**.** *Let S be a finite set, and let $H : \mathbb{C}[S] \to \mathbb{C}[S]$ be a linear transformation. The following are equivalent:*

1. *H can be written in the form UDU^{-1} for a unitary matrix U and a real diagonal matrix D.*

2. *$H = H^\dagger$.*

If either of the two equivalent 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.

We now prove the converse. We consider the map $\langle \cdot | \cdot \rangle$ as defined in the proof of Proposition 2.1. Since $\mathbb{C}$ is algebraically complete the characteristic polynomial of H must have a root, hence we know that H has some eigenvector e, with eigenvalue λ. Scaling e if neccecary, we can assume without loss of generality that $\langle e|e \rangle = 1$. Let V be the subspace of vectors $x \in \mathbb{C}[S]$ such that $\langle e|x \rangle = 0$. This is an $|S| - 1$ dimensional subspace. Exercise 2.2 says that $H = H^\dagger$ implies

$$
\langle x|H(y) \rangle = \langle H(x)|y \rangle \ \ \forall x, y \in \mathbb{C}[S].
$$

In particular, if $\langle e|x \rangle = 0$ then

$$
\langle e|H(x) \rangle = \langle H(e)|x \rangle = \lambda \langle e|x \rangle = 0.
$$

Thus, H restricts to a map on V. Continuing this proccess of picking eigenvectors and restricting H to the subspace of vectors for which $\langle \cdot | \cdot \rangle = 0$, we find that $\mathbb{C}[S]$ has a basis of normalized eigenvectors, such that $\langle \cdot | \cdot \rangle$ for any distinct pair. Moreover, all of these eigenvectors satisfy

$$
\lambda \langle e|e \rangle = \langle H(e)|e \rangle = \langle e|H(e) \rangle = \overline{\lambda} \langle e|e \rangle,
$$

so their eigenvalues $\lambda = \overline{\lambda}$ are real. Label these eigenvectors $\{e_s\}_{s \in S}$ arbitrarily by elements of S. We can define a unitary matrix U by $U(|s\rangle) = e_s$. Letting D be the diagonal matrix whose (s, s) entry is the eigenvalue of e_s, we find that $H = UDU^{-1}$, completing the proof. $\square$

The conditions on unitary and Hermitian matrices we have obtained are independent of unitary change of basis, in the sense that unitary (resp. Hermitian) matrices will stay unitary (resp. Hermitian) under a unitary change of basis. Additionally, unitary matrices are defined to send normalized vectors to normalized vectors, and hence the notion of normalized vector is unitary basis-independent 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 arbitrary change

of basis. The solution to this problem is to introduce *Hilbert spaces*. Roughly, Hilbert spaces are vector spaces paired with a notion of normalized vectors, which allows one to define unitary and Hermitian matrices. Abstractly, in the same way that there is a canonical identification

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

there is an identification

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

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 $\langle \cdot | \cdot \rangle : V \times V \to \mathbb{C}$

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 $\overline{\cdot}$ 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 $\psi = 0$.

$\square$

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 unitary change of basis:

Proposition 2.3. *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*

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

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 identify equivalence classes of based vector spaces up to unitary change of basis with Hilbert spaces.

Proof. We demonstrate the claims one by one.

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 of 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 $j \leq k - 2$

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

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 the axioms is immediate, and is left as an exercise to the reader (Exercise 2.1)

3. Suppose two bases are related by a unitary transformation. Since unitary transformations preserves norm, 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.

$\square$

We can now state everything in a basis independent fashion. Let $(V, \langle \cdot | \cdot \rangle)$ be a Hilbert space. A normalized vector is one in which the norm square $\langle \psi | \psi \rangle$ equals one. A unitary matrix is a matrix which preserves norm. That is, $\langle U\psi | U\phi \rangle = \langle \psi | \phi \rangle$ for all $|\phi\rangle, |\psi\rangle \in V$. 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 2.2).

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

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

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 an inner product 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 $x_0, x_1 \in V$, $y_0, y_1 \in W$. (see Exercise 2.3). 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 a unitary 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 $V \otimes W$.

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

$\square$

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 basic 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 the language of Hilbert spaces adds unnecessary confusion and subtlety, which we postpone to Appendix B.

We now conclude with a 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 generic 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 $\mathbb{Z}_2 = \{0, 1\}$ is the two element group, and $\mathbb{Z}_2^n$ is the n-fold cartesian product, consisting of length-n bit strings. All classical processes can be modeled 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 preferred 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 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 $\left(\mathbb{C}^2\right)^{\otimes n}$.

2. How quantum information is acted on. That is, what physical actions one will do to perform the function f.

3. How quantum information is measured. That is, what 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 mechanics. A good reference for this sort of linear algebra, with a special focus on quantum mechanics, is Hall's book [Hal13].

Exercises:

2.1. Verify Proposition 2.3 part (2).

2.2. Let S, S' be finite sets, and let $T : \mathbb{C}[S] \to \mathbb{C}[S']$ be a linear transformation. Show that the conjugate transpose $T^\dagger$ can be characterized as the unique transformation such that

$$\langle \psi | T\phi \rangle = \langle T^\dagger \psi | \phi \rangle$$

for all $\phi \in \mathbb{C}[S]$, $\psi \in \mathbb{C}[S']$. Thus, the conjugate transpose is well defined up to unitary change of basis. In particular, given a linear $T : V \to W$ of (finite dimensional) Hilbert spaces there is a well defined conjugate transpose $T^\dagger : W \to V$.

2.3. Given Hilbert spaces $(V, \langle \cdot | \cdot \rangle_V)$ and $(W, \langle \cdot | \cdot \rangle_W)$, we define a Hilbert 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.

2.4. Let $|\psi\rangle, |\phi\rangle \in V$ be states in a Hilbert space. Show that $|\psi\rangle$ and $|\phi\rangle$ give the same observable under every measurement if and only if there exists a number $t \in \mathbb{R}$ such that $|\psi\rangle = e^{it} \cdot |\phi\rangle$. Physically, this has the following interpretation. Every complex number can be uniquely written as the product of a real number (*amplitude*) with a complex number on the unit circle (*phase*). Multiplying an entire state by e^{it} is a *global phase shift*. This exercise can be read as saying that all quantum states are distinguishable, up to global phase shift.

Figure 3.1: Celluation of the torus, obtained by gluing opposite sides together.

3   The Toric Code

Consider a torus. We will imagine the torus as being a quantum system, corresponding physically to the quantum system one would observe 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 codespace 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" observable of a quantum system. Namely, the eigenvalue of an eigenstate of the Hamiltonian is its total energy. The code space will thus be the lowest eigenvalue 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 3.1. We will work with the understanding that the real physical system is the limit as $n \to \infty$ (see Exercise 3.3). We define the quantum system associated with the n by n celluated torus to be the vector space

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

obtained by "putting a qubit 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. The letters v, e, p will refer to vertices, edges, and faces[5] respectively. 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]Standard practice is to refer to faces with the French term *plaquettes*, hence the letter p

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

The Hamiltonian on $\mathbb{N}$ 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 recovers the σ_X operators, and exponentiating the electric field recovers 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.

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

Proposition 3.1. *We have that*

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

(ii) *All A_vs and B_ps have half eigenvalues $+1$ and half eigenvalues -1*

(iii) *All A_vs and B_ps commute*

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

Proof. We demonstrate the points one by one.

(i). Multiplying tensor product matrices corresponds to simply multiplying component-wise. 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

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

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

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

(*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 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 twice, since each edge touches exactly two 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 $\sigma_X^2 = 1$. $\qquad\square$

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 3.2. *All eigenvalues of H are of the form $-2n^2 + 4q$, for an integer $q \leq n^2/2$. The $-2n^2 + 4q$ eigenspace 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 respects 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 3.1 (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

$$H\,|\psi\rangle = (-\sum_v A_v - \sum_p B_p)\,|\psi\rangle$$

$$= \left(\sum_{\substack{v,p \\ -1 \text{ eigenvalue}}} 1 - \sum_{\substack{v,p \\ 1 \text{ eigenvalue}}} 1\right)|\psi\rangle$$

$$= (q - (n^2 - q))$$

$$= -n^2 + 2q.$$

To complete the initial description of 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. If there were an odd number of such v, then Proposition 3.1 (iv) says 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, yielding the desired result.

We now compute the dimensions of the eigenspaces. Let D denote the dimension of the codespace. 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 would apply the same argument with vertices replaced by faces. Choose two vertices $v_0, v_1 \in \mathbf{v}$. 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 vertices that γ passes through an even number of times. The only vertices 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 $|\mathbf{v} + \mathbf{p}| = q'$.
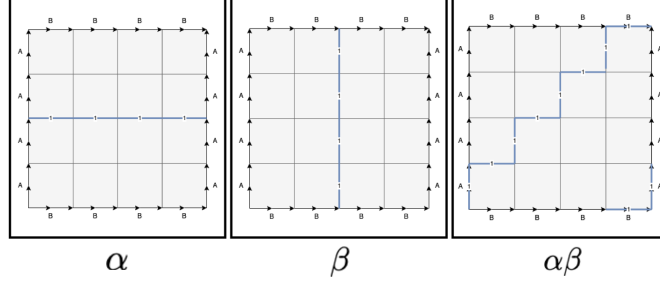
Figure 3.2: The three non-trivial homology classes of a torus

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

$$D \sum_{q=0}^{2n^2} \sum_{k=0}^{q} \binom{n^2}{2k} \binom{n^2}{2(q-k)} = D \left(\sum_{q=0}^{2n^2} \binom{n^2}{2k_0} \right)$$

$$= D \cdot \left(2^{n^2-1} \right)^2 = D \cdot 2^{2n^2-2}.$$

The Hamiltonian is a symmetric matrix with real coefficients. Proposition 2.2 thus says it be diagonalized, so 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. Thus, $D = 2^2 = 4$. $\qquad\square$

The fact that the code space is four dimensional can be motivated as follows. By Proposition 3.1 (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 3.1 (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 3.3. *Let $\mathbf{0}, \alpha, \beta,$ and $\alpha\beta$ be the four $\mathbb{Z}_2$ homology classes on the torus, as in Figure 3.2. Choose $\mathbf{0}_0, \alpha_0, \beta_0,$ and $(\alpha\beta)_0$ respectively to be representatives. Letting γ run over all $\mathbb{Z}_2$ cycles, we have that*

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

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

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

Proof. Choose $\omega \in H_1(T; \mathbb{Z}_2)$. 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. Hence, $|\omega\rangle$ is in the $+1$ eigenspace for each A_v as well.

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. Hence, we conclude that $|\omega\rangle$ is in the codespace.

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 over counts the space of cycles homologous to ω by a factor of 2, since $\prod_{\text{faces } p} B_p = I$ by Proposition 3.1 (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.

We finally observe 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 as desired. $\square$

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 $\mathbb{C}[H_1(T; \mathbb{Z}_2)]$. 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 interpret *quasiparticles* in the toric code as excitations. That is, given an eigenstate $|\psi\rangle$, we say there is a quasiparticle at a vertex v if $A_v|\psi\rangle = -|\psi\rangle$, and there is a quasiparticle at face 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

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

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

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 vertices 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 vertices 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*. If both v_1 and v_1 have quasiparticles, then tensoring with σ_X at e has the effect of *annihilating quasiparticles at the endpoints of e*.

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

We can similarly describe the quasiparticles living on faces. 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 quasiparticle/antiparticle pair if neither of the faces have 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 as follows:

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

| Generate quasiparticle pair | Go around the torus | Annihilate quasiparticles |

Figure 3.3: Topological quantum process implementing the NOT_α gate

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 3.3

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

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

Proposition 3.4. *The following computation, shown in Figure 3.3, 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, create a particle pair at v_0 and v_1, i.e., tensor with σ_X at the edge connecting v_0 and v_1. Then move v_1 along α_0, i.e., tensor with σ_X along the edges in α_0. Then, fuse the X-type quasiparticles at v_0 and v_1 back together, i.e., tensor along the edge connecting v_0 and v_1 again. Since $\sigma_X^2 = 1$, this whole process can be described mathematically as
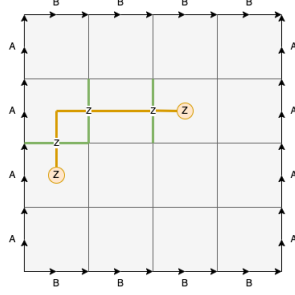
$$\bigotimes_{\text{edges in } \alpha_0} \sigma_X \,.$$

Figure 3.4: Sample trajectory along dual celluation of torus

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$_\alpha$ gate. $\qquad \square$

Similarly, we can implement the "$(-1)_\alpha$" gate, which reverses the sign of 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 3.5. *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 3.4. 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'.

29

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

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

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. $\quad\square$

Sadly for the toric code, 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 think of quantum gates on a system as forming a group, where the group law is given by the composition of processes, and every element has an inverse since unitary matrices are invertible.

Proposition 3.6. *There are exactly 16 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 $\text{NOT}_\beta, \text{NOT}_{\alpha\beta}, (-1)_\beta$, in complete analogy to how we define NOT_α. Namely, NOT_β flips whether or not a state has a 'β' in it, and $\text{NOT}_{\alpha\beta}$ flips whether or not a state has an '$\alpha\beta$' in it, i.e.,

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

We proceed identically for $(-1)_\beta$ and $(-1)_{\alpha\beta}$. 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 quasiparticles, moving them around a loop, then annihilating them. Following the proof of Proposition 3.5, 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: $\{\pm I, \text{NOT}_\omega, (-1)_\omega\}$, where ω runs over homology classes. The relations $\text{NOT}_\alpha\text{NOT}_\beta = \text{NOT}_{\alpha\beta}$ and $(-1)_\alpha(-1)_\beta = (-1)_{\alpha\beta}$ allow one to reduce the generating set further. The relations

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

and

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

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

Before moving to the next section, we make a few final remarks about the behavior of quasiparticles on the toric codes. Consider the simple braiding of adjacent X-type and Z-type quasiparticles around each other, as shown below
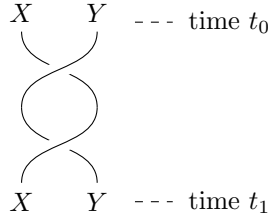
A line going under another corresponds to the particle having passed through that space first, before the other particle. This process corresponds to a transformation $\mathcal{N} \to \mathcal{N}$ by tensoring with the appropriate σ_Xs and σ_Zs. The key observation is that this transformation is *not* 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 parti-
cles should be impossible. The conclusion is that these really are *quasi*particles,
which behave 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 quasiparticles in topological quantum materials
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 such anyons *abelian*. Quasiparticles whose
braiding statistics are not always phase shifts are called *non-abelian*. To create
useful quantum gates, these sorts of interesting braidings are needed. The search
for a topological quantum computer is essentially the search for experimentally-
sound easy-to-braid non-abelian anyons.

Exercises:

3.1. 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 of
H' is 4 dimensional, and the gate group of H' is the Pauli group.

3.2. 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*. Ground states being highly entan-
gle is a more general phenomenon in TQC, and gives the theory much of
its power. (HINT: prove this for ground states first, then lift to general
eigenstates using an induction argument along the lines of the proof of
Proposition 3.2)

3.3. 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: PASS What is the correct definition?]

(a) Show that this map is linear and injective, and hence that $\mathcal{N}_n$ can be realized as a sub vector space of $\mathcal{N}_m$.

(b) Show that $\tilde{H}_m$ restricted to $\mathcal{N}_n$ is equal to $\tilde{H}_n$.

(c) Show that the map $\mathcal{N}_n \hookrightarrow \mathcal{N}_m$ is norm-preserving, in the sense that if $|\phi\rangle, |\psi\rangle$ are states on $\mathcal{N}_n$, the inner product $\langle\phi|\psi\rangle$ is independent of whether or not it was computed in $\mathcal{N}_n$ or $\mathcal{N}_m$

(d) 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].

4 Topological Quantum Field Theories

4.1 The general picture

Topological quantum computation (TQC) is physically based on topological quantum phases of matter. Topological quantum field theories (TQFTs) are the mathematical formalism of topological quantum phases of matter. That is, every topological quantum phase of matter (physical object) has an associated TQFT (mathematical object) to describe it. To make this clearer, we recall classical phases of matter in a more mathematical way. A phase of matter is an assignment

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

---

[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 discretely in a fine enough celluation.

Figure 4.1: The two holed torus (surface of genus of 2)

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

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

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 3.2). If the $\mathbb{Z}_2$ spin liquid is induced on the torus with two holes (see Figure 4.1), 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 topological space is called a *surface*. The surfaces we are interested in are those two dimensional spaces which can be embedded withour intersections into 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 4.2). 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.
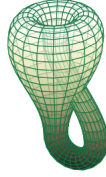
Figure 4.2: A Klein bottle, attempting to be embedded in 3d space

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 4.1. *Consider a connected 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 of g-holed torus, for some integer $g \geq 0$.

Thus, going forward the word 'connected surface' will simply refer to a g-holed torus. 'Surface' will allow for non-connected spaces, that is, collections of multiple torii. 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 ranges over surfaces and $V(S)$ is a finite dimensional complex vector space. This mathematical formalism is known as topological quantum field theory[7]. The assignment $S \rightsquigarrow V(S)$ *is* a TQFT.

However, not every assignment of surfaces to vector spaces will be a TQFT - many will be 'un physical', in the sense that they never could have come from topological phases of matter. For example, the axioms of quantum mechanics

---

[7]This formalism of quantum field theory as function from spaces to systems is known more generally as functional quantum field theory [Sto14, Sch09]. Creating non-topological functional quantum field theories in this language is possible (e.g. [Seg88] for conformal field theories), but it is more complicated and other formalisms are preferred.
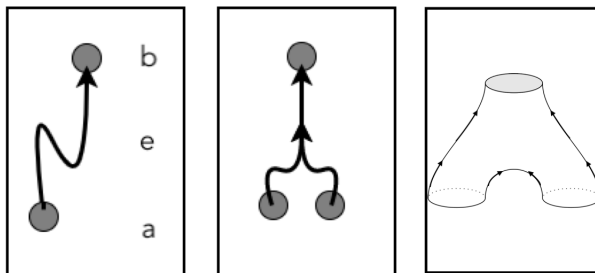
Figure 4.3: First box - A path in spacetime from a to b by e, i.e., a path e with $\partial e = a \sqcup b$. Second box - The fusion of two particles in spacetime. Third box - the fusion of two circles in spacetime, known informally as a "Pair of Pants".

tell us 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 "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 4.3.

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 4.3. This corresponds to the fusion and annihilation of particles.

Working one dimension higher, we can imagine the trajectory of particle loops through spacetime. The merging of two loops 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 4.3.

We now 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 orientation. 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*[8] from S_0 to S_1. In summary, 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. We can now formally define a TQFT:

Definition ($(2+1)$-TQFT). A $(2+1)$ topological quantum field theory is the following data.

1. A choice of finite dimensional $\mathbb{C}$ vector space $V(S)$ for every surface S.

2. A choice of linear transformation $Z(X) : V(S_0) \to V(S_1)$ 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.

---

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

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 unit real 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 between 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 surfaces S_0, S_1 and moving them around each other.

$\square$

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 some 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 braided monoidal functor from the category of bordisms to the category of vector spaces"[9]. For those unfamiliar with category theory, a short introduction is found in Appendix 5. 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 3. The difficult part is often showing that the object you defined is independent of the choice of celluation. For the toric code, this was Exercise 3.3. In general, one resorts to the following theorem:

Theorem 4.2 (Pachner, [Pac91, Lic99]). *Let X be A manifold with triangulations Δ_X and Δ'_X (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 4.4. The naming convention is that the "n-m" move is the move that takes n cells to m cells.*

---

[9]braided=axiom 4, monoidal=axiom 1, functor=axiom 3, bordism category=axiom 2

Figure 4.4: The Pachner moves.

This massively facilitates the verification of whether or not a definition is independent of celluation. 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 Pachner moves. Typically, this verification is entirely elementary and does not require any great show of cleverness. As such, our standard practice for subsection 4.2 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.

4.2 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 3, 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. 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 3.5. 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

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

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 vertices, 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 pairs of 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 4.1. *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, $(\omega_{S_0}, \omega_{S_1})$ is extendable in Δ_X if and if it is extendable in Δ'_X. By Theorem 4.2 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 invariant under the process of applying Pachner moves. Drawing out the diagrams, these are straightforward computations. We leave the verification as an exercise to the reader (Exercise 4.1). □

Lemma 4.1. *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) $\left| \left\{ \omega_{S_1} \in C^1(\Delta_{S_1}; \mathbb{Z}_2) \text{ s.t. } (\omega_{S_0}, \omega_{S_1}) \text{ extendable} \right\} \right|$ *is independent of choice of ω_{S_0}*

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

WORK: fix this proof. How do I know I can pick such ω_{S_1} *in the first place?* We prove (i), and leave (ii) as an exercise (Exercise 4.2) since its proof is identical. Fix ω_{S_1} and ω_{S_1} 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). $\square$

Proposition 4.2. *Letting* X_0, X_1 *be as in Lemma 4.1, 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 $N_{X_1 \cup X_0}^{-1}$ if $(\omega_{S_0}, \omega_{S_2})$ extendable, and 0 otherwise. Multiplying through, we find the equality we are trying to prove is [WORK: $\omega_{S_0}, \omega_{S_2}$ currently undefined. Fix proof structure!]

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

Fix ω_{S_0}. We claim both sides of the above expression are equal to the number of extendable pairs $(\omega_{S_1}, \omega_{S_2})$ such that $(\omega_{S_0}, \omega_{S_1})$ is also 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 4.1 for assuming values are equal. This completes the proof.

$\square$

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. 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 orientation on $[0,1]$.
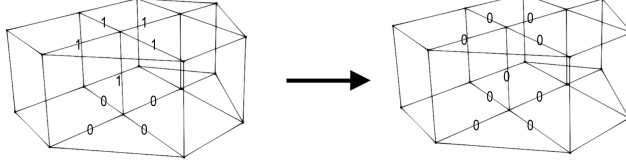
Figure 4.5: Removing the 1s from the central edges in $S \times [0, 1]$

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 passively decrease in energy. Thus, $Z(S \times [0, 1])$ should act by the identity on ground states, and send higher energy states down to ground states. 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 thus says that $V(S)$ is the ground state space:

Proposition 4.3. *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 $V(S)$. That is, 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 4.5.

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 $|Z^1(\Delta_S; \mathbb{Z}_2)|$, so

the stated formula is correct. 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 4.4. *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 4.3, and then extending $(\omega_{S_0}, \omega_{S_1})$.

Thus, the equal superposition $|\omega_{S_0}\rangle$ of every cocycle cohomologous 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 claim 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 Pachner moves and is left as an exercise (Exercise 4.3). □

The main result of our section is as follows:

Theorem 4.3. *The assignments $S \mapsto V(S)$ and $X \mapsto Z(X)$ give a TQFT, 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 4.3.

3. This follows immediately from Proposition 4.2.

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.

$\square$

Seeing that the $\mathbb{Z}_2$ Dijkgraaf-Witten TQFT applied to the torus yields the toric code as defined in section 3 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 not an issue. We decided to work with homology in section 3 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. It is for this reason that even though ground states are complicated maximally entangled objects (Exercise 3.2) 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 takes classical computers a long time to simulate the process. This gives a sort of quantum computation, known as an adiabatic quantum computation [AL18]. It is interesting to note that the original definition of the toric code did not include a Hamiltonian [Kit97], and one was only introduced later to facilitate the study. A more general study of TQFTs via Hamiltonians was conducted by Levin-Wen [LW05].

In the the language of TQFTs 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 1-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. This is in marked contrast to Modular Tensor Categories, where anyons are placed front and center of the theory.

Exercises:

4.1. Complete the proof of Proposition 4.1.

4.2. Complete the proof of Lemma 4.1.

4.3. Complete the proof of Proposition 4.4.

5 Category Theory

5.1 Objects, morphisms, and composition

Category theory is the mathematical abstraction of things, and relationships between them. It is a language in which almost all other mathematical fields can be expressed, with often fruitful consequences.

Definition (Category). A category is the following data:

1. (Objects) A set $\mathscr{C}$.

2. (Morphisms) A set $\mathrm{Hom}(A, B)$ for all $A, B \in \mathscr{C}$

3. (Composition) Functions

$$\circ : \mathrm{Hom}(B, C) \times \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C)$$

for all $A, B, C \in \mathscr{C}$.

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

1. $(h \circ g) \circ f = h \circ (g \circ f)$, for all morphisms $f \in \mathrm{Hom}(A, B)$, $g \in \mathrm{Hom}(B, C)$, $h \in \mathrm{Hom}(C, D)$, and objects $A, B, C, D \in \mathscr{C}$.

2. (Identity) For all objects $A \in \mathscr{C}$ there exists a morphism $\mathrm{id}_A : A \to A$ such that for all $B \in \mathscr{C}$, $f \in \mathrm{Hom}(A, B)$,

$$f \circ \mathrm{id}_A = f,$$

and for all $f \in \mathrm{Hom}(B, A)$

$$\mathrm{id}_B \circ f = f.$$

□

The intuition is that the set of objects $\mathscr{C}$ includes everything that we are interested in studying. That is $\mathscr{C}$ could be the set of sets, set of groups, set of vector spaces, set of topological spaces, etc... . The set $\mathrm{Hom}(A, B)$ is viewed as being the set of allowable functions from A to B. That is, functions (morphisms[10]) which respect the structures at hand. For instance, given G, H in the set **Grp** of groups, the space $\mathrm{Hom}(G, H)$ consists of all group homomorphisms from G to H. Given V, W in the set **Vec** of finite dimensional complex vector spaces, $\mathrm{Hom}(V, W)$ consists of all linear maps from V to W. Given X, Y living in the set **Top** of topological spaces, $\mathrm{Hom}(X, Y)$ consists of all continuous maps from X to Y. Given A, B living in the set **Set** of sets, $\mathrm{Hom}(A, B)$ should consist of all maps from A to B.

The composition operation "$\circ$" is the fundamental operation of category theory. Given two transformations, it is a deep truth that doing one after the other gives another transformation. The axiom $(h \circ g) \circ f = h \circ (g \circ f)$ makes sure that composition works properly. Every category that one naturally considers has identity elements. That is, the "do-nothing" transformation on an object should always be allowed. The identity map from a topological space/vector space/group is always a continuous map/linear map/homomorphism. In particular, the above descriptions give us *categories* **Set**, **Top**, **Vec**, and **Grp**.

The power of category theory lies in its generality. For example, one might consider the Cartesian product of sets (i.e. $A \times B = \{(a, b),\ a \in A,\ b \in B\}$). The product of vector spaces has a natural vector space space structure, giving a product $V \times W$ in **Vec**. The product of groups has a natural group structure, giving a product $G \times H$ in **Grp**. The product of topological spaces has a natural product topology, giving a product $X \times Y$ in **Top**. All of these examples and more can be generalized as products in a category. We now work out this illustrative example in detail.

Definition (Product). A product of two elements A, B in a category $\mathscr{C}$ is the following data:

1. An object $A \times B \in \mathscr{C}$.

2. A morphism $\pi_A \in \mathrm{Hom}(A \times B, A)$.

3. A morphism $\pi_B \in \mathrm{Hom}(A \times B, B)$.

Additionally, a product is required to satisfy the following property. For every $C \in \mathscr{C}$ paired with morphisms $\tau_C : C \to A$ and $\tau_C : C \to B$, there exists a unique morphism $f : C \to A \times B$ such that $f \circ \pi_A = \tau_A$ and $f \circ \pi_B = \tau_B$.

□

This definition motivates a lot of the key concepts, benefits, and drawbacks of category theory. For instance:

---

[10] "Hom" is short for "Homomorphism", coming from the greek *homos* (meaning 'same') and *morphe* (meaning 'shape')

- While the goal is often to define objects (in this case, the product $A \times B$), one realizes that the important subtleties lie in the implicit morphisms. In this case, the projection maps π_A, π_B turn out to be the key parts of the definition. In the case of **Set** we have maps $\pi_A : A \times B \to A$ sending (a, b) to a, and $\pi_B : A \times B \to B$ sending (a, b) to b. These maps are continuous in the case of **Top**, homomorphisms in the case of **Grp**, and linear in the case of **Vec**, and from them we recover the standard definitions of product.

- The definitions are abstract, and get to the conceptual core of the relevant theory. In this case, the product of A and B can be summarized as "the most general object which admits morphisms to both A and B". This condition of being the "most general object" satisfying a condition is known as a *universal property*. Universal properties are how many notions in category theory are defined.

- Category theoretic definitions can often be hard to read. It is for this reason we use diagrams to elucidate ideas. Instead of writing $f \in \operatorname{Hom}(A, B)$, we write $f : A \to B$. This makes our intuition of f as a function from A to B clear. We package conditions like "$f \circ \pi_A = \tau_A$ and $f \circ \pi_B = \tau_B$" as *commutative diagrams*. That is, consider the series of objects and morphisms below:

$$
\begin{array}{ccc}
 & A & \\
\tau_A \nearrow & \big\uparrow \pi_A & \\
A \times B & \xrightarrow{\pi_B} & B \\
f \nearrow & \searrow \tau_B & \\
C & &
\end{array}
$$

  The fact that $f \circ \pi_A = \tau_A$ and $f \circ \pi_B = \tau_B$ is exactly the statement that composing all of the functions along any two paths between any two objects gives the same function. We call a diagram with this property a commutative diagram. The product condition is thus the statement is that there exists a function $f : C \to A \times B$ such that the above diagram commutes. The diagrammatic language is often easier to read, and leaves room ease-of-use features. For instance, we made the line under f dotted to differente it from the others - f exists only conditionally, whereas $\pi_A, \tau_A, \pi_B, \tau_B$ are given.

One might want to show that the product $A \times B$ of two elements is unique, however, this is not the case. What is true that all products will be *isomorphic*. An isomorphism between an object A and an object B is a function $f : A \to B$ such that there exists $f^{-1} : B \to A$, such that $f^{-1} \circ f = \operatorname{id}_A$ and $f \circ f^{-1} = \operatorname{id}_B$. This recovers bijection in the case of **Set**, group isomorphisms in case of **Grp**, vector space isomorphisms in case of **Vec**, and homeomorphisms in the case of **Top**.

Proposition 5.1. *Let $\mathscr{C}$ be a category, and let $A, B \in \mathscr{C}$ be objects. Let $(A \times_0 B, \pi_A^{(0)}, \pi_B^{(0)})$ and $(A \times_1 B, \pi_B^{(1)}, \pi_B^{(1)})$ be products of A and B. There is a unique isomorphism $i : A \times_0 B \to A \times_1 B$ such that*

$$
\begin{array}{c}
A \\
\nearrow \quad \uparrow \pi_A^{(0)} \\
\pi_A^{(1)} \qquad A \times_0 B \xrightarrow{\pi_B^{(0)}} B \\
\nearrow \quad i \quad \nearrow \\
A \times_1 B \qquad \pi_B^{(1)}
\end{array}
$$

commutes.

Proof. By the universal property of $A \times_0 B$, there is a unique map $i : A \times_1 B \to A \times_0 B$ making the diagram commute. The only issue is showing that i is an isomorphism. By the universal property of $A \times_1 B$, there exists a map $i^{-1} : A \times_0 B \to A \times_1 B$ making the same map commute. Now, we observe the commutative diagram

$$
\begin{array}{c}
A \\
\nearrow \quad \uparrow \pi_A^{(0)} \\
\pi_A^{(0)} \qquad A \times_0 B \xrightarrow{\pi_B^{(0)}} B \\
\nearrow \quad i \circ i^{-1} \quad \nearrow \\
A \times_0 B \qquad \pi_B^{(0)}
\end{array}
$$

The universal property of $A \times_0 B$ says that there is a unique choice of function $A \times_0 B \to A \times_0 B$ making the diagram commute. Seeing as $\mathrm{id}_{A \times_0 B}$ also preserves commutativity, uniqueness thus tells us that $i \circ i^{-1} = \mathrm{id}_{A \times_0 B}$. Considering the diagram corresponding to $i^{-1} \circ i$, we find similarly that $i^{-1} \circ i = \mathrm{id}_{A \times_1 B}$. Thus, i is an isomorphism as desired. $\qquad\square$

Observe that not only do we get an isomorphism between $A \times_0 B$ and $A \times_1 B$, but we get one which respects the relevant projection maps. There are many products, but they all have unique isomorphisms between each other which respect structure. Hence, we say that the product of two elements in a category is *unique up to unique isomorphism*. We say in this situation that $A \times_0 B$ and $A \times_1 B$ are *canonically* isomorphic. A structure is canonical if it is uniquely "natural". Generally, the canonical choice is the one which makes the most diagrams commute. It is the goal of much of category theory to formalize the notions of constructions being canonical. It is the goal of many mathematicians to develop the most canonical possible constructions:

"I can assure you, at any rate, that [...] my results are invariant,

probably canonical, [and] perhaps even functorial." - Rudolf Lipschitz[11]

The term *functorial* in the above quote makes reference to one of the most systematic measures of canonicalness in category theory. Suppose one has two categories $\mathscr{C}$ and $\mathscr{D}$, and an assignment of objects from $\mathscr{C}$ to $\mathscr{D}$. For instance $\mathscr{C} = \mathbf{Top}$, $\mathscr{D} = \mathbf{Grp}$, and the assignment sends a space X to its first homology group with $\mathbb{Z}_2$ coefficients $H_1(X; \mathbb{Z}_2)$. Or perhaps $\mathscr{C} = \mathbf{Set}$, $\mathscr{D} = \mathbf{Vec}$, and the assignment sends a set[12] S to the vector space $\mathbb{C}[S]$ which has distinguished basis S. These assignments are very natural, and one would want a measure of the fact that they are canonical. In this case, we say they are *functorial*. This means they can be extended to functors, as defined below:

Definition (Functor). A functor between two categories $\mathscr{C}$ and $\mathscr{D}$ is the following data:

1. An object $F(A) \in \mathscr{D}$ for every object $A \in \mathscr{C}$.

2. A morphism $F(f) : F(A) \to F(B)$ for every morphism $f : A \to B$, $A, B \in \mathscr{C}$.

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

1. (Preserves composition) $F(g \circ f) = F(g) \circ F(f)$, for all $f : A \to B$, $g : B \to C$, $A, B, C \in \mathscr{C}$.

2. (Preserves identity) $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ for all $A \in \mathscr{C}$.

$\square$

We verify that the mappings $\mathbb{C}[-]$ and $H_1(-; \mathbb{Z}_2)$ are functorial in Exercise 5.3. This abstracted language of functors gives the following meta-fact:

Proposition 5.2. *Define the following data for a category:*

1. *(Objects) Categories.*

2. *(Morphisms) Functors.*

3. *(Composition) $G \circ F : \mathscr{C} \to \mathscr{E}$ is the functor sending an object $A \in \mathscr{C}$ to $G(F(A)) \in \mathscr{E}$, and sending $f \in \mathrm{Hom}(A, B)$ to the map*

$$G(F(f)) \in \mathrm{Hom}(G(F(A)), G(F(B))),$$

for $F \in \mathrm{Hom}(\mathscr{C}, \mathscr{D})$, $G \in \mathrm{Hom}(\mathscr{D}, \mathscr{E})$.

---

[11]This quote appears in a correspondence between Lipschitz and André Weil, which was documented in the collection [Wei09], on page 558.

[12]To get a finite dimensional vector space, S has to be finite. Thus, this is really a functor $\mathbf{finSet} \to \mathbf{Vec}$ whose source is the category of finite sets.

This is well defined, and gives a category called **Cat***.*

Proof. Verifying that **Cat** satisfies the composition axiom is trivial. The identity element of $\mathscr{C}$ is the functor $\mathrm{id}_{\mathscr{C}} : \mathscr{C} \to \mathscr{C}$, when sends objects and functions to themselves. It is again trivial to verify that this is a functor, and that it is an identity element. $\square$

This gives a notion of isomorphism between two categories. Namely, two categories $\mathscr{C}$ and $\mathscr{D}$ are isomorphic if there is an invertible functor between them. However, requiring two categories be isomorphic is often too restrictive. For instance, in topological quantum computing, categorical models of quasiparticles correspond to topological quantum phases of matter only up to a weaker notion of equivalence. Hence, we shouldn't force the functors to be equal to the identity, only *isomorphic* to the identity. This requires defining what we mean by isomorphism of functors. The summary is simple: an isomorphism of functors is an isomorphism in the category of functors! We give the definitions below.

Definition (Natural transformation)**.** A natural transformation between two functors $F, G : \mathscr{C} \to \mathscr{D}$, with $\mathscr{C}, \mathscr{D} \in$ **Cat**, is a family or morphisms $\eta_A : F(A) \to G(A)$ for all $A \in \mathscr{C}$. Additionally, a natural transformation is required to satisfy the property that the diagram

$$
\begin{array}{ccc}
F(A) & \xrightarrow{\ \eta_A\ } & G(A) \\
{\scriptstyle F(f)}\big\downarrow & & \big\downarrow{\scriptstyle G(f)} \\
F(B) & \xrightarrow{\ \eta_B\ } & G(B)
\end{array}
$$

commutes for any morphism $f : A \to B$.

$\square$

Proposition 5.3. *Let $\mathscr{C}, \mathscr{D}$ be categories. Define the following data for a category*

$$
\mathbf{Hom}(\mathscr{C}, \mathscr{D}) = \begin{pmatrix} \mathbf{objects} : \textit{Functors } \mathscr{C} \to \mathscr{D} \\ \mathbf{morphisms} : \textit{Natural transformations} \end{pmatrix}.
$$

Along with a canonical choice of composition rule, this forms a category.

Proof. Let $\eta^{(0)} : F_0 \to F_1$, $\eta^{(1)} : F_1 \to F_2$, $\eta^{(2)} : F_2 \to F_3$ be natural transformations, with $F_1, F_1, F_2, F_3 : \mathscr{C} \to \mathscr{D}$ functors. We define the composition $\eta^{(1)} \circ \eta^{(0)} : F_0 \to F_2$ by

$$
\left(\eta^{(1)} \circ \eta^{(0)} \right)_A = \eta_A^{(1)} \circ \eta_A^{(0)}.
$$

This satisfies the composition law, since

$$\left(\left(\eta^{(2)} \circ \eta^{(1)}\right) \circ \eta^{(0)}\right)_A = \left(\eta^{(2)} \circ \eta^{(1)}\right)_A \circ \eta_A^{(0)}$$
$$= \eta_A^{(2)} \circ \eta_A^{(1)} \circ \eta_A^{(0)}$$
$$= \eta_A^{(2)} \circ \left(\eta^{(1)} \circ \eta^{(0)}\right)_A$$
$$= \left(\eta^{(2)} \circ \left(\eta^{(1)} \circ \eta^{(0)}\right)\right)_A$$

for all $A \in \mathscr{C}$. The identity map on a functor F is the natural transformation $\mathrm{id}_F : F \to F$ defined by $(\mathrm{id}_F)_A = \mathrm{id}_{F(A)}$. It is trivial to check that this is a well defined natural transformation, and that it gives an identity element in the category. $\qquad\square$

The fact that the hom-spaces in the category **Cat** can themselves be realized as categories is not unique to **Cat**. There are many sets which not only have morphisms (category structure), but also morphisms of morphisms (category structure on hom-spaces). These are known as 2-categories. Those categories with morphisms of morphisms of morphisms and so on n-times recursively are known as n-categories. While we do not explicitly use the higher category theory in this manuscript, many topological quantum computing related authors strongly use n-categories. For instance, this is the founding philosophy of the nLab, the largest repository of mathematical physics:

> "It is believed that [...] higher category theory provide[s] a point of view on Mathematics, Physics and Philosophy which is a valuable unifying point of view for the understanding of the concepts involved" - nLab[13]

We now give such a story where category theory helps unify concepts. Let V be a vector space, and let V^* denote the dual vector space, consisting of morphisms $V \to \mathbb{C}$. Both V and V^* have the same dimension, hence choosing bases we get an isomorphism $V \xrightarrow{\sim} V^*$. However, this is non-canonical: there is no "correct" choice of basis. However, there *is* a canonical isomorphism $V \xrightarrow{\sim} V^{**}$, given by

$$V \to V^{**}.$$
$$v \mapsto (\varphi \mapsto \varphi(v))$$

This can be seen as saying that points are functions on functions. It is an important fact that this map is an isomorphism, and the proof relies on the key fact that V is finite dimensional - it fails in general, where we only get injections $V \hookrightarrow V^{**}$. We state this formally below as a proposition, leaving out details in the statement, which we fill in during the proof. Definitions in category theory are all often similar, so leaving exact detail implicit is standard practice. Stating everything explicitly becomes quickly untenable, so this is a necessary measure.

---

[13]This is the first line of the nLab's "nPOV" page.

Proposition 5.4. *Define the functor* $(-)^{**} : \mathbf{Vec} \to \mathbf{Vec}$ *sending* V *to* V^{**}. *The double dual maps* $V \to V^{**}$ *defined above gives a natural isomorphism between* $\mathrm{id}_{\mathscr{C}}$ *and* $(-)^{**}$.

Proof. We first show that $(-)^{**}$ is functorial. Given $f : V \to W$, we define $f^* : W^* \to V^*$ by sending φ to $\varphi \circ f$. Applying this construction twice, this gives a well defined map $f^{**} : V^{**} \to W^{**}$. It is trivial to show that this respects composition, and thus gives $(-)^{**}$ the structure of a functor. To show that the maps $V \to V^{**}$ give a natural transformation, we must show that for all $f : V \to W$ the square

$$
\begin{array}{ccc}
V & \longrightarrow & V^{**} \\
\downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f^{**}} \\
W & \longrightarrow & W^{**}
\end{array}
$$

commutes. Choose $v \in V$. Going around the bottom of the diagram, we get $(\varphi \mapsto \varphi(f(v))) \in W^{**}$. Going around the top of the diagram, we get $f^{**}(\varphi \mapsto \varphi(v)) \in W^{**}$. Unraveling definitions we find that

$$
\begin{aligned}
f^{**}(\varphi \mapsto \varphi(v)) &= (\varphi \mapsto f^*(\varphi)(v)) \\
&= (\varphi \mapsto \varphi(f(v)))
\end{aligned}
$$

as desired. Now, we check that this natural transformation is invertible. Since all of the maps $V \to V^{**}$ are isomorphisms, so we can define a natural transformation $(-)^{**} \to \mathrm{id}_{\mathscr{C}}$ whose component $(-)^*_V$ is the inverse of the double dual $V \to V^{**}$. It is trivial to check that this is an inverse in the category $\mathbf{Hom}(\mathbf{Vec}, \mathbf{Vec})$, so we are done. $\square$

This fundamental duality of vector spaces is something that one desires to emulate, since switching perspectives from points to functions can be illuminating. Yoneda's Lemma is the general category theoretic duality which allows one to switch perspectives from objects to functions[14]. We state it below, after a lemma.

Lemma 5.1. *Let* $\mathscr{C}$ *be a category. Define the category* $\mathscr{C}^{\mathrm{op}}$ *whose objects are symbols of the form* A^{op}, *for* $A \in \mathscr{C}$, *and whose hom-set* $\mathrm{Hom}(A^{\mathrm{op}}, B^{\mathrm{op}})$ *consists of symbols* f^{op}, *for* $f \in \mathrm{Hom}_{\mathscr{C}}(B, A)$. *Along with a canonical composition law,* $\mathscr{C}^{\mathrm{op}}$ *is a well defined category.*

Proof. Given $f : A^{\mathrm{op}} \to B^{\mathrm{op}}$, $g : B^{\mathrm{op}} \to C^{\mathrm{op}}$, $h : C^{\mathrm{op}} \to D^{\mathrm{op}}$ with $A, B, C, D \in \mathscr{C}$, we define $g^{\mathrm{op}} \circ f^{\mathrm{op}} = (f \circ g)^{\mathrm{op}}$. The composition axioms are verified by a straightforward computation. It is trivial to check that $(\mathrm{id}_A)^{\mathrm{op}}$ serves as an identity element for A^{op}, so we are done. $\square$

---

[14]The category-theoretic duality literally most similar to vector space duality is Tannaka-Krein duality. While this duality is useful (specifically, even, in our setting of quantum algebra [JS06]), Yoneda's lemma is far more universal.

Theorem 5.1 (Yoneda's Lemma). *Let $\mathscr{C}$ be a category. The functor*

$$\mathscr{C} \to \mathbf{Hom}(\mathscr{C}^{\mathrm{op}}, \mathbf{Set}).$$
$$A \mapsto (B^{\mathrm{op}} \mapsto \mathrm{Hom}_{\mathscr{C}}(B, A))$$

it is injective on the level of objects, injective on the level of morphisms ("faithful"), and surjective on the level of morphisms ("full"). This is summarized as saying the assignment above is a fully faithful embedding of categories.

Proof. To begin, we check that the assignment $B^{\mathrm{op}} \mapsto \mathrm{Hom}_{\mathscr{C}}(B, A)$ is functorial. Suppose we are given a morphism $f^{\mathrm{op}} : B^{\mathrm{op}} \to C^{\mathrm{op}}$, coming from a morphism $f : C \to B$, $B, C \in \mathscr{C}$. This induces a set morphism $\mathrm{Hom}_{\mathscr{C}}(f, A)$ by precomposition,

$$\mathrm{Hom}_{\mathscr{C}}(B, A) \xrightarrow{\mathrm{Hom}_{\mathscr{C}}(f, A)} \mathrm{Hom}_{\mathscr{C}}(C, A).$$
$$\varphi \mapsto \varphi \circ f$$

Now, choose $g^{\mathrm{op}} : C^{\mathrm{op}} \to D^{\mathrm{op}}$. The statement that $\mathrm{Hom}_{\mathscr{C}}(g, A) \circ \mathrm{Hom}_{\mathscr{C}}(f, A) = \mathrm{Hom}_{\mathscr{C}}(f \circ g, A)$ is exactly the statement that $(\varphi \circ f) \circ g = \varphi \circ (f \circ g)$, which follows from the fact that $\mathscr{C}$ is a category. Precomposition with the identity does not affect the map on hom, hence $\mathrm{Hom}_{\mathscr{C}}(\mathrm{id}_B, A) = \mathrm{id}_{\mathrm{Hom}_{\mathscr{C}}(B,A)}$ as desired.

Next we show that the assignment $A \mapsto (B^{\mathrm{op}} \mapsto \mathrm{Hom}_{\mathscr{C}}(B, A))$ is functoral. Suppose we are given $f : A \to B$. We need to show that this induces a natural transformation $\eta^{(f)}$ between the functors $(C \mapsto \mathrm{Hom}_{\mathscr{C}}(C, A))$ and $(C \mapsto \mathrm{Hom}_{\mathscr{C}}(C, B))$. We define this transformation by postcomposition,

$$\mathrm{Hom}_{\mathscr{C}}(C, A) \xrightarrow{\eta^{(f)}_C} \mathrm{Hom}_{\mathscr{C}}(C, B).$$
$$\varphi \mapsto f \circ \varphi$$

It is trivial to verify that this is a natural transformation, and that the assignment is thus functorial. We now check that the functor has all the stated properties. Injectivity on the level of objects follows from the observation that if $A \neq B$, then the functors $(C^{\mathrm{op}} \mapsto \mathrm{Hom}_{\mathscr{C}}(C, A))$ and $(C^{\mathrm{op}} \mapsto \mathrm{Hom}_{\mathscr{C}}(C, B))$ will be literally different assignments. For instance, when $C = A$, then $\mathrm{Hom}(A, A)$ contains id_A but $\mathrm{Hom}(A, B)$ does not.

We now verify injectivity on the level of morphisms. Suppose $f, g : A \to B$ are two morphisms, which induce the same natural transformations $\eta^{(f)}$ and $\eta^{(g)}$. We find that $f = g$ by simply unravelling definitions:

$$f = \eta^{(f)}_A(\mathrm{id}_A) = \eta^{(g)}_A(\mathrm{id}_A) = g.$$

We now verify surjectivity on the level of morphisms. Suppose η is a natural transformation between the functors $(C^{\mathrm{op}} \mapsto \mathrm{Hom}_{\mathscr{C}}(C, A))$ and $(C^{\mathrm{op}} \mapsto \mathrm{Hom}_{\mathscr{C}}(C, B))$. Let $f = \eta_A(\mathrm{id}_A)$. We need to show that $\eta = \eta^{(f)}$. That is, that $\eta_C(\varphi) = f \circ \varphi$

for all $C \in \mathscr{C}$, $\varphi \in \mathrm{Hom}(C, A)$. Since η is a natural transformation, the square corresponding to φ commutes:

$$
\begin{array}{ccc}
\mathrm{Hom}_{\mathscr{C}}(A, A) & \xrightarrow{\eta_A} & \mathrm{Hom}_{\mathscr{C}}(A, B) \\
{\scriptstyle \mathrm{Hom}_{\mathscr{C}}(\varphi, A)} \downarrow & & \downarrow {\scriptstyle \mathrm{Hom}_{\mathscr{C}}(\varphi, B)} \\
\mathrm{Hom}_{\mathscr{C}}(C, A) & \xrightarrow{\eta_C} & \mathrm{Hom}_{\mathscr{C}}(C, B)
\end{array}
$$

Starting with $\mathrm{id}_A \in \mathrm{Hom}(A, A)$, going around the bottom gives $\eta_C(\varphi)$, and going around the top gives $\mathrm{Hom}(\varphi, B)(\eta_A(\mathrm{id}_A)) = \mathrm{Hom}(\varphi, B)(f) = f \circ \varphi$. This demonstrates the desired claim, and completes the proof of the theorem. $\square$

Yoneda's lemma is considered one of the most fundamental results in category theory. While seemingly abstract it quickly becomes very useful. It can be loosely read as saying that if two source objects have the "same" (i.e. naturally isomorphic) hom-sets into every target, then the source objects must be the "same" (i.e. isomorphic).

Yoneda's lemma can be stated in an alternatively in the language of pairings. There is a natural map $V \times V^* = V \times \mathrm{Hom}(V, \mathbb{C}) \to \mathbb{C}$, sending (v, φ) to $\varphi(v)$. Vector space duality is exactly the fact that this pairing is non-degenerate, in the sense that if $\varphi(v) = 0$ for all v then $\varphi = 0$, and if $\varphi(v) = 0$ for all φ then $v = 0$. There is a pairing $\mathscr{C} \times \mathscr{C}^{\mathrm{op}} \to \mathbf{Set}$ on the level of categories, and the Yoneda lemma is exactly the statement that it is non-degenerate (see Exercises 5.1 - 5.2). Observe that to make this statement formal, we will have to define the product $\times$ of categories. In some sense, we already have: $\times$ is just the product in the category of categories! Explicitly, we can describe the product as follows:

Proposition 5.5. *Let $\mathscr{C}, \mathscr{D}$ be categories. We define the following data for a category:*

1. *(Objects) Pairs (A, B), $A \times B \in \mathscr{C} \times \mathscr{D}$*

2. *(Morphisms) We set*

$$
\mathrm{Hom}((A_0, B_0), (A_1, B_1)) = \mathrm{Hom}(A_0, A_1) \times \mathrm{Hom}(B_0, B_1),
$$

   for all $(A_0, B_1), (A_1, B_1) \in \mathscr{C} \times \mathscr{D}$.

3. *(Composition) We define $(f_1, g_1) \circ (f_0, g_0) = (f_1 \circ f_0, g_1 \circ g_0)$, for all $(f_0, g_0) \in \mathrm{Hom}((A_0, B_0), (A_1, B_1))$, $(f_1, g_1) \in \mathrm{Hom}((A_1, B_1), (A_2, B_2))$, and $(A_0, B_0), (A_1, B_1), (A_2, B_2) \in \mathscr{C} \times \mathscr{D}$.*

This gives a well defined category $\mathscr{C} \times \mathscr{D}$. This category is the product in the category of categories.

Proof. Verifying that $\mathscr{C} \times \mathscr{D}$ forms a category is trivial, so we omit the details. Defining the functors

$$\pi_{\mathscr{C}} : \mathscr{C} \times \mathscr{D} \to \mathscr{C}$$
$$(A, B) \mapsto A$$

and

$$\pi_{\mathscr{D}} : \mathscr{C} \times \mathscr{D} \to \mathscr{D},$$
$$(A, B) \mapsto B$$

we show that the triple $(\mathscr{C} \times \mathscr{D}, \pi_{\mathscr{C}}, \pi_{\mathscr{D}})$ is a product. Suppose we are given a category $\mathscr{E}$ and functors $\tau_{\mathscr{C}} : \mathscr{E} \to \mathscr{C}$, $\tau_{\mathscr{D}} : \mathscr{E} \to \mathscr{D}$. This induces a functor

$$F : \mathscr{E} \to \mathscr{C} \times \mathscr{D}.$$
$$E \mapsto (\tau_{\mathscr{C}}(E), \tau_{\mathscr{D}}(E))$$
$$f \mapsto (\tau_{\mathscr{C}}(f), \tau_{\mathscr{D}}(f))$$

It is clear that the diagram

commutes. Seeing a $(\mathscr{E}, \tau_{\mathscr{C}}, \tau_{\mathscr{D}})$ was chosen arbitrarily, this completes the proof. $\square$

This concludes our basic introduction to category theory. The canonical reference is Mac-Lane's foundational text [ML13]. As a readable way to begin learning the theory, however, there are modern sources which do a better job. For instance, Fong and Spivak's book [FS19] gives a very well-motivated and grounded approach to the subject.

5.2 Braided monoidal categories

The tensor product is an extremely important operation in linear algebra, especially in its applications to topological quantum computing. Braided monoidal categories are categories in which there is a generalization of the tensor product. Physically, this will represent "fusion". More precisely, a braided monoidal category is a category $\mathscr{C}$ along with a functor $\otimes : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$ satisfying axioms

reminiscent of the tensor product. Namely, there is tensor unit 1 such that for all $A, B, C \in \mathscr{C}$

$$1 \otimes A \cong A \otimes 1 \cong A \text{ (unit axiom)}$$
$$(A \otimes B) \otimes C \cong A \otimes (B \otimes C) \text{ (associativity axiom)}$$
$$A \otimes B \cong B \otimes A \text{ (commutivity axiom)}.$$

The key subtelty in the theory is that these isomorphisms are *not* equalities - $1 \otimes A$ and A for instance need not be equal, only isomorphic. The above thus aren't just axioms - they're structures. One must make a *choice* of isomorphism. These choices should be all be coherent, in the sense that applying the unit, associativity, and commutivity axioms in different orders should give the same results. It was not at all clear in the early days of the theory exactly what the correct conditions should be. MacLane's first definition included more conditions than the treatment below (see Exercise 5.5).

The condition that $A \otimes B \cong B \otimes A$ does not hold in every reasonable theory of tensor products. Hence, we first define a monoidal category to be a category with a possibly non-commutative tensor product, and then we define a braided monoidal category to be a commutative monoidal category.

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 isomorphism $\alpha : - \otimes (- \otimes -) \to (- \otimes -) \otimes -$, 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 isomorphism $\lambda : 1 \otimes - \to -$, where $1 \otimes -$ denotes the functor $\mathscr{C} \to \mathscr{C}$ sending A to $1 \otimes A$, and $-$ denotes the identity.

6. (Right unitor) A natural isomorphism $\rho : - \otimes 1 \to -$, 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) The diagram

$$
\begin{array}{ccc}
(A \otimes 1) \otimes B & \xrightarrow{\ \alpha_{A,1,B}\ } & A \otimes (1 \otimes B) \\
& \searrow^{\rho_A \otimes \mathrm{id}_B} \quad \swarrow_{\mathrm{id}_A \otimes \lambda_B} & \\
& A \otimes B &
\end{array}
$$

commutes for all $A, B \in \mathscr{C}$.

2. (Pentagon identity) The diagram

$$
\begin{array}{ccc}
& (A \otimes B) \otimes (C \otimes D) & \\
\alpha_{A \otimes B, C, D} \nearrow & & \nwarrow \alpha_{A, B, C \otimes D} \\
((A \otimes B) \otimes C) \otimes D & & A \otimes (B \otimes (C \otimes D)) \\
\alpha_{A, B, C} \otimes \mathrm{id}_D \downarrow & & \uparrow \mathrm{id}_A \otimes_{B, C, D} \\
(A \otimes (B \otimes C)) \otimes D \xrightarrow{\quad \alpha_{A, B \otimes C, D} \quad} & & A \otimes ((B \otimes C) \otimes D)
\end{array}
$$

commutes for all $A, B, C, D \in \mathscr{C}$.

$\square$

The following theorem answers in what this machinery is neccessary. Do things go wrong if I force these isomorphisms to be equalities? Do things go wrong if I force all isomorphic objects to be equal? The notion of monoidal equivalence is used in the theorem - we postpone the definition until after.

Theorem 5.2 ([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 equivalent to a category $(\mathscr{D}, \otimes_{\mathscr{D}}, \alpha_{\mathscr{D}}, \lambda_{\mathscr{D}}, \rho_{\mathscr{D}})$ in which $A \otimes_{\mathscr{D}} (B \otimes_{\mathscr{D}} C) = (A \otimes_{\mathscr{D}} B) \otimes_{\mathscr{D}} C$, $1 \otimes_{\mathscr{D}} A = A \otimes_{\mathscr{D}} 1 = 1$ for all $A, B, C \in \mathscr{D}$, and $\alpha_{\mathscr{D}}, \lambda_{\mathscr{D}}, \rho_{\mathscr{D}}$ are identity functors.*

2. *$\mathscr{C}$ is monoidally equivalent to a category in $\mathscr{D}$ in which all isomorphic objects are equal.*

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

This theorem says that you can't have your cake and eat it too. You can forget about non-trivial maps or you can forget about non-equal isomorphic objects, but not both. Authors will sometimes assume either one condition or the other (known as *strict* and *skeletal* respectively), though most examples in the wild are neither. A monoidal equivalence between two categories is a pair of monoidal functors[15] between them, such that both compositions are monoidally naturally isomorphic to the identity.

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:

---

[15]What we call "monoidal functor" is sometimes called "lax monoidal functor", by authors who reserve the term monoidal functor for functors in which ϵ and μ are isomorphisms.

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) The diagram

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

commutes for all $A, B, C \in \mathscr{C}$.

2. (Unitality) The diagrams

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

and

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

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

$\square$

Definition (Monoidal natural transformation). A monoidal natural transformation between two monoidal functors (F_0, μ_0, ϵ_0) and (F_1, μ_1, ϵ_1) between monoidal categories $(\mathscr{C}, \otimes_{\mathscr{C}}, 1_{\mathscr{C}})$ and $(\mathscr{D}, \otimes_{\mathscr{D}}, 1_{\mathscr{D}})$ is a natural transformation η between the underlying functors F_0, F_1. Additionally, a monoidal natural transformation is required to satisfy the following properties:

1. (Compatibility with tensor product) For all objects $A, B \in \mathscr{C}$, the diagram

$$
\begin{array}{ccc}
F_0(A) \otimes_{\mathscr{D}} F_1(B) & \xrightarrow{\eta_A \otimes \eta_B} & F_1(A) \otimes_{\mathscr{D}} F_1(B) \\
\downarrow{\mu_{0;A,B}} & & \downarrow{\mu_{1;A,B}} \\
F_0(A \otimes_{\mathscr{C}} B) & \xrightarrow{\eta_{A \otimes B}} & F_1(A \otimes_{\mathscr{C}} B)
\end{array}
$$

commutes.

2. (Compatibility with unit) The diagram

$$
\begin{array}{ccc}
& 1_{\mathscr{D}} & \\
{}^{\epsilon_0}\swarrow & & \searrow^{\epsilon_1} \\
F_0(1_{\mathscr{C}}) & \xrightarrow{\eta_{1_{\mathscr{C}}}} & F_1(1_{\mathscr{C}})
\end{array}
$$

commutes.

$\square$

We comment about our policy on structures/properties. We will often say "Let $\mathscr{C}$ be a monoidal category" instead of "Let $(\mathscr{C}, 1, \otimes, \lambda, \rho, \alpha)$ be a monoidal category". While technically incorrect, listing every structure every time is cumbersome. Hence, we will often only recall the necessary subset of structures we are using, and leave the others implicit. We are now ready to define braiding on our monoidal categories.

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

1. A monoidal 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 monoidal category is required to satisfy the following properties:

1. (Hexagon identities) The diagrams

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

and

$$(A \otimes B) \otimes C \xrightarrow{\alpha^{-1}_{A,B,C}} A \otimes (B \otimes C) \xrightarrow{\beta_{A,B \otimes C}} (B \otimes C) \otimes A$$

with vertical maps $\beta_{A,B} \otimes \mathrm{id}_C$ and $\alpha^{-1}_{B,C,A}$, and bottom row

$$(B \otimes A) \otimes C \xrightarrow{\alpha^{-1}_{B,A,C}} B \otimes (A \otimes C) \xrightarrow{\mathrm{id}_B \otimes \beta_{A,C}} B \otimes (C \otimes A)$$

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

$\square$

We will want to speak of equivalences of braided monoidal categories. That is, pairs of braided monoidal functors whose compositions in either direction have monoidal natural isomorphisms with the identity. We give the definition below:

Definition (Braided monoidal functor). A braided monoidal functor between braided monoidal categories $(\mathscr{C}, \otimes_{\mathscr{C}}, \beta_{\mathscr{C}})$, $(\mathscr{D}, \otimes_{\mathscr{D}}, \beta_{\mathscr{D}})$ is a monoidal functor $(F, \mu) : \mathscr{C} \to \mathscr{D}$ such that the diagram

$$F(A) \otimes_{\mathscr{D}} F(B) \xrightarrow{\beta_{\mathscr{D};F(A),F(B)}} F(B) \otimes_{\mathscr{D}} F(A)$$

with vertical maps $\mu_{A,B}$ and $\mu_{B,A}$, and bottom row

$$F(A \otimes_{\mathscr{C}} B) \xrightarrow{F(\beta_{\mathscr{C};F(A),F(B)})} F(B \otimes_{\mathscr{C}} A)$$

commutes for all $A, B \in \mathscr{C}$.

$\square$

Note that there is no such thing as a "braided monoidal natural transformation" - any monoidal natural transformation between braided functors will automatically respect the braiding. Just as in the general case, braided monoidal categories can also be made strict or skeletal, but not both. A discussion can be found in Joyal and Street's original article [JS86].

Exercises:

5.1. Let $\mathscr{C}$ and $\mathscr{D}$ be categories. A pairing between $\mathscr{C}$ and $\mathscr{D}$ is a functor $\mathscr{C} \times \mathscr{D} \to \mathbf{Set}$. We call a pairing F non-denerate on the right if $F(A,-) \cong F(B,-) \implies A \cong B$, for all $A, B \in \mathscr{C}$. The symbol $\cong$ denotes isomorphism in the respective categories. That is, $F(A, -) \cong F(B, -)$ means that there is a natural isomorphism $F(A, -) \xrightarrow{\sim} F(B, -)$, treated both as functors $\mathscr{D} \to \mathbf{Set}$. Simiarly, a pairing F is called non-degenerate on the left if $F(-, A) \cong F(-, B) \implies A \cong B$ for all $A, B \in \mathscr{D}$.

(a) Show that the map $\mathscr{C} \times \mathscr{C}^{\mathrm{op}} \to \mathbf{Set}$ sending $(A, B^{\mathrm{op}}) \in \mathscr{C} \times \mathscr{C}^{\mathrm{op}}$ to $\mathrm{Hom}(A, B) \in \mathbf{Set}$ is functorial.

(b) Use the Yoneda lemma to show that the above pairing is non-degenerate both on the left and on the right.

5.2. Given a objects A, B in category $\mathscr{C}$, use the Yoneda lemma to show that the mapping

$$\mathrm{Hom}(A, B) \to \mathrm{Hom}_{\mathbf{Hom}(\mathscr{C}^{\mathrm{op}}, \mathbf{Set})}(\mathrm{Hom}_{\mathscr{C}}(B, -), \mathrm{Hom}_{\mathscr{C}}(A, -))$$
$$\varphi \mapsto (f \mapsto f \circ \varphi)$$

is a bijection. Here, $\mathrm{Hom}_{\mathscr{C}}(A, -)$ is considered as a functor in $\mathbf{Hom}(\mathscr{C}^{\mathrm{op}}, \mathbf{Set})$, sending an object $C \in \mathbf{Cat}$ ot the set $\mathrm{Hom}_{\mathscr{C}}(A, C)$, and similarly for $\mathrm{Hom}_{\mathscr{C}}(B, -)$.

5.3. Show that the following are functors, whre **finSet** denotes the category of finite sets.

(a) The assignment $\mathbb{C}[-] : \mathbf{finSet} \to \mathbf{Vec}$, which assigns to each set A the vector space $\mathbb{C}[A]$, and assigns to each function $f : A \to B$ the linear map

$$\mathbb{C}[A] \to \mathbb{C}[B]$$
$$\sum_{a \in A} c_a[a] \mapsto \sum_{a \in A} c_a[f(a)]$$

(b) The assignment $H_1(-; \mathbb{Z}_2) : \mathbf{Top} \to \mathbf{Grp}$ which assigns to each topological space X the homology group $H_1(X; \mathbb{Z}_2)$, and assigns to each continuous map $f : X \to Y$ the group homomorphism $f_* : H_1(X; \mathbb{Z}_2) \to H_1(Y; \mathbb{Z}_2)$, defined as follows. For each function $f : X \to Y$, there exists celluations Δ_X, Δ_Y such that f sends edges in X to edges in Y by the simplicial approximation theorem. We define $f_* : C_1(X; \mathbb{Z}_2) \to C_1(Y; \mathbb{Z}_1)$ by sending ω to the chain $f_*(\omega)$, where an edge e of Y is assigned the (mod 2) sum of ω's values at the edges in $f^{-1}(e)$. Show that this is well defined, and descends to a function $f_* : H_1(X; \mathbb{Z}_2) \to H_1(Y; \mathbb{Z}_2)$, completing the definition of our assignment.

5.4. Let $\mathscr{C}, \mathscr{D}$ be categories. Show that a functor $F : \mathscr{C} \to \mathscr{D}$ induces an equivalence of categories (that is, admits a map $F^{-1} : \mathscr{D} \to \mathscr{C}$ making (F, F^{-1}) an equivalence of categories) if and only if it is fully faithful, and for every element $A \in \mathscr{D}$, there exists $B \in \mathscr{C}$ such that $F(B)$ is isomorphic to A. This condition is known as being *essentially surjective*. Show that this result still holds in the setting of (braided) monoidal categories. That is, a fully faithful essentially surjective (braided) monoidal functor will induce a (braided) equivalence of categories.(HINT: Construct F^{-1} by lifting objects, and show it is a functor)

5.5. The original list of axioms for a monoidal category was longer. It was later found by Max Kelly [Kel64] that the smaller set we gave implies the rest. This exercise asks to rederive his results.

(a) Show that for all monoidal categories $\mathscr{C}$ the diagram

$$
\begin{array}{c}
(1 \otimes A) \otimes B \\
{\scriptstyle \alpha_{1,A,B}} \downarrow \qquad \searrow {\scriptstyle \lambda_A \otimes \mathrm{id}_B} \\
1 \otimes (A \otimes B) \xrightarrow[\lambda_{A \otimes B}]{} A \otimes B
\end{array}
$$

commutes. (HINT: Suppressing identity maps and tensor products for clarity, show that the diagrams

and

commute)

(b) Using the result in part (a), show that for all monoidal categories $\mathscr{C}$ the maps $\rho_1, \lambda_1 : 1 \otimes 1 \to 1$ are equal.

5.6. Let $\mathscr{C}$ be a category. Define a tensor product on $\mathbf{Hom}(\mathscr{C}, \mathscr{C})$ by letting $F \otimes G = F \circ G$, for functors $F, G : \mathscr{C} \to \mathscr{C}$. Along with canonical associativity, unit, and unitors, show that this gives $\mathbf{Hom}(\mathscr{C}, \mathscr{C})$ the structure of a (not necessarily braided) monoidal category. In this way, we see that 2-categories (categories whose hom-spaces are morphisms) naturally give monoidal categories. Monoidal categories can be equivalently defined as "one object 2-categories", making them a stepping stone into higher category theory.

6 Modular Tensor Categories

6.1 Fusion Systems

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 3. 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 is assigned to every surface, and what morphisms are assigned to every bordism. As was seen in subsection 4.2, 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, 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 requires one to carry around even more data.

To summarize, what we want is a mathematical description of topological quantum phases of matter that puts anyons and their motions/behaviors front and center. This is what modular tensor categories give us. Abstractly, a modular tensor category (MTC) can be thought of as

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

For this subsection, however, no knowledge of categories will be needed. This is because 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 finite sets of numbers. At the end of the day, measuring physical phenomena always gives a number - wavelength, spin, energy etc... Thus, any practical physical theory should be boilable down to a collection of numbers.

The most fundamental operation on anyons is *fusion*: the process in which quasiparticles fuse into one. The topological quantum computing (TQC) process in section 3 was based on creation, and the subsequent fusion, of particle anti/particle pairs. Both the X-type and Z-type quasiparticles in the toric code are their own antiparticle, meaning they fuse with themselves to give the "do-nothing" quasiparticle. The X and Z type quasiparticles are named that way because they move by tensoring with σ_X and σ_Z. The do-nothing quasiparticle moves by tensoring with the identity I, and hence call it the I-type quasiparticle.

The subtle issue is what happens when we fuse X and Z type quasiparticles. 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
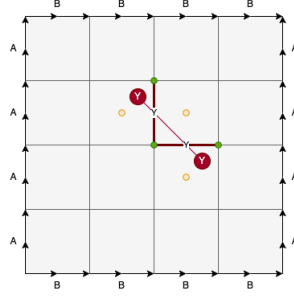
Figure 6.1: Movement of Y-type particles in toric code

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 Y-*type* particles.

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

In generalizing this theory, we find ourselves finding a key difference: fusion is no longer a deterministic process. There can be two quasiparticles which, upon fusion, can create different possible quasiparticles. Quasiparticles which fuse in deterministic ways are exactly, in fact, the *abelian* anyons [WORK: cite reference for this fact... Maybe make exercise?]. Thus, non-deterministic fusing is a key aspect of TQC.

To model this algebraically we are thus interested in spaces that look a lot like finite groups, but where the group operation on two elements (i.e. fusion) returns probability distribution on the other particles. This group operation should still have an analogue identity element, inverses, and associativity.

One key physical observation [WORK: cite reference. Maybe none exists?] is that when two quasiparticles are fused, the probability of observing any other quasiparticle will always be *rational*. Clearing denominators, we can thus represent the fusion operation as assining an integer "multiplicity" to every anyon type, which gives the relative probability of that particle being observed. For notation, we will say that if a and b are quasiparticle types which fuse to each anyon type c with relative probability $N_c^{a,b}$, then

$$a \otimes b = \sum_c N_c^{a,b} c.$$

We use the tensor product $\otimes$ for fusion because in category theoretic language it will extend to a monoidal structure, and we use the notation of summation on the right hand side because in category theoretic language it will extend

to a direct sum. The probability of observing c after fusing a and b is

$$\frac{N_c^{a,b}}{\sum_d N_d^{a,b}}.$$

This generalization of a group is called a fusion system. Those fusion systems which satisfy a generalization of commutivity are called *braided fusion systems*. MTCs are braided fusion categories which have a "twist" and satisfy a certain non-degeneracy condition. In this way, one can think of MTCs as being vast "non-degenerate" generalizations of finite abelian groups.

As we add all of this structure to our fusion systems to better approximate the physical world, we will find that higher multiplicity terms (i.e. $N_c^{a,b} \geq 2$) generate a great deal of complexity. For this reason we restrict ourselves to *multiplicity free* fusion systems, where all $N_c^{a,b}$ are 0 or 1. Physically, this means that when any two particles are fused, all of the possible results will occur equally likely. Many important MTCs are not multiplicity free. This is thus one of the advantages of the category theoretic viewpoint - we can consider the more general case with no extra effort. 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

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

$\square$

The next piece of the puzzle is based on one of the key ideas of monoidal categories: strict versus skeletal. Given quasiparticles a, b, c the quantities $(a \otimes b) \otimes c$ and $a \otimes (b \otimes c)$ may be equal (i.e. the category is skeletal), but that does *not* mean that the associativity map $(a \otimes b) \otimes c \to a \otimes (b \otimes c)$ is the identity (i.e the category is strict). This is in the same way that $X \otimes Y$ and $Y \otimes X$ are equal in the toric code, but the braiding map between them is non-trival: it is -1 times the identity. We roughly define a $6j$ fusion system to be a fusion system in which we have chosen isomorphisms between $(a \otimes b) \otimes c$ and $a \otimes (b \otimes c)$ for all $a, b, c \in \mathscr{L}$.

This is best visualized in a graphical language. The idea is to make rigorous the sorts of diagrams one will naturally draw when explaining the subject. 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 are found in Figure 6.2. Special functions are encoded 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 - 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 distinguished function $a \otimes b \to c$ as

$$
\begin{array}{c}
A \qquad B \\
\diagdown \diagup \\
| \\
C
\end{array}
$$
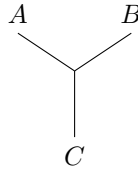
By our intuition of fusion there should be a morphism $a \otimes b \to c$ if and only if $N_c^{a,b} = 1$, i.e., if and only if the probability of a and b fusing into c is non-zero. We call a triple (a, b, c) with $N_c^{a,b} = 1$ *admissible*. It is here that our
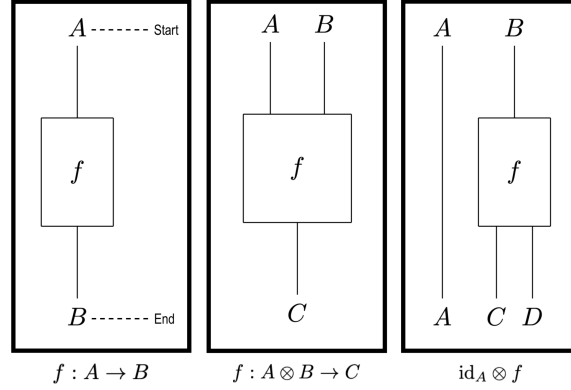
Figure 6.2: Examples of the quantum-algebraic graphical language

assumption of multiplicity-freedom is so vital. When higher multiplicity terms are present, the space of morphisms $a \otimes b \to c$ will be higher dimensional. We would have to choose a *basis* of distinguished morphisms. Keeping track of these basis functions is a hastle, but it is a fundamentally similar process.

Consider a function $(a \otimes b) \otimes c \to d$. This can be decomposed as first taking a function $a \otimes b \to n$, and then taking a function $n \otimes c \to d$, 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 give bases for the hom-space $a \otimes b \otimes c \to d$. In graphical language, we can express the change of basis as

These values $F^{a,b,c}_{d;n,m} \in \mathbb{C}$ are known as $6j$ symbols. Understanding $6j$ symbols without any handwaiving will have to wait until next section. However, for our purposes, this is not strictly necessary: they can be treated simply as complex numbers, with as much or as little intuition behind them as one desires. All one needs is that they satisfy some axioms:

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

1. A fusion system $(\mathscr{L}, N^{-,-}_{-})$

68

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 $N^{a,b}_c \neq 0$. 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 $F^{a,b,c}_d$ to be the matrix whose coefficients are $F^{a,b,c}_{d;n,m}$, where n, m run over pairs making (a, b, c, d, n, m) admissible. We have that

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

   for all $(a, b, c, d, n, m) \in \mathscr{L}^6$.

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

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

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

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.

$\square$

The pentagon is exactly the sort of identity for which graphical language is useful. As stated, it is quite non-obvious to decipher meaning from the expression. 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 terms in the pentagon are maps $a \otimes b \otimes c \otimes d \to e$. Each arrow corresponds to applying the appropriate F-matrix.

Time reversal symmetry can be explained as follows. Taking an inverse corresponds to doing a process in reverse. That is, instead of fusing particles the matrix F^{-1} will correspond to the creation of particles. The time reversal symmetry says associativity on creating particles will be the same associativity on fusing particles. Diagrammatically, this means
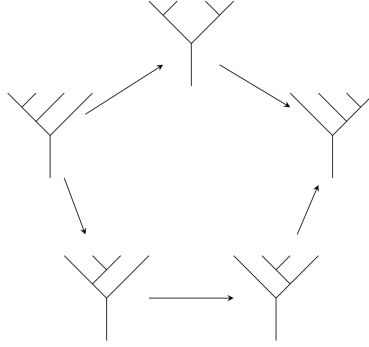
69

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

A natural question about $6j$ symbols could be as follows: the goal was to define an isomorphism $a \otimes (b \otimes c)$ to $(a \otimes b) \otimes c$. Instead, we 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. This sort of switch between studying objects to studying functions, however, is exactly what Yoneda's lemma gives us! The $6j$ symbols give a natural transformation between $\mathrm{Hom}(a \otimes (b \otimes c), -)$ and $\mathrm{Hom}((a \otimes b) \otimes c, -)$, which induces a unique isomorphism $(a \otimes b) \otimes c \to a \otimes (b \otimes c)$. Ravi Vakil explains Yoneda's lemma as follows:

> "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[16].

---

[16]This quote is relayed by an answer to the MathOverflow post "'Philosophical' meaning of the Yoneda Lemma" by Theo Johnson-Freyd

In this context, Vakil's quote is very literal - we are studying particles by looking at their fusion rules. Fusion, as a process, often happens when things hit each other very fast in a particle accelerator. Fusion, properly, is not the tensor product but functions out of the tensor product. By learning the relationship betwen the behaviors of $a \otimes (b \otimes c)$ and $(a \otimes b) \otimes c$ under every fusion process, we learn about the relationship between $a \otimes (b \otimes c)$ and $(a \otimes b) \otimes c$. The Yoneda perspective will persist through this manuscript.

We now define braided $6j$ fusion systems. Braiding gives an isomorphism between $a \otimes b$ and $b \otimes a$. For example, since X and Z anticommute in the toric code, the braiding isomorphism $X \otimes Z \to Z \otimes X$ is -1 times the identity. Keeping with our Yoneda perspective, instead of explicitly giving an isomorphism $a \otimes b$ and $b \otimes a$ we give isomorphism between the hom-paces $a \otimes b \to c$ and $b \otimes a \to c$ for every c. Graphically, this can be seen as the formula

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 $(\mathcal{L}, N_-^{-,-}, F_{-;-,-}^{-;-,-})$.

2. Complex numbers $R_c^{a,b}$ for all $a, b, c \in \mathcal{L}$.

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

1. (Admissibility) $R_c^{a,b} \neq 0$ if $(a, b, c) \in \mathcal{L}^3$ is admissible

2. (Hexagon) For all $a, b, c, d, e, m \in \mathcal{L}$,

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

$\square$

Again, the hexagon is a mess of symbols when written explicitly. In graphical language, however, it becomes the condition that going either way around the 6-term diagram in Figure 6.4 gives the same answer. The fact that there is a hexagon identity for R^+ and R^- corresponds to the fact that one can fix the notation
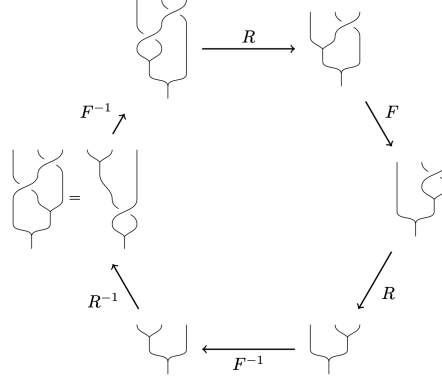
Figure 6.4: The hexagon identity in graphical language, with R and F denoting the respective applications of R and F matricies [WORK: this can be made way better]

and so the second hexagon identity is the fact that Figure 6.4 commutes with over crossings replaced by under crossings.

With all this, we can finally define MTCs:

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

1. (Spherical) $F^{a,b,c}_{1;a^*,c} F^{b,c^*,a}_{1;a^*a,a} F^{c^*,a,b}_{1;b^*,b} = 1$ for all $a, b, c \in \mathscr{L}$. [WORK: should there be a condition on admissibility?]

2. (Non-degenerate) For $a \in \mathscr{L}$, if $B^{a,b}_c = B^{b,a}_c$ for all $b, c \in \mathscr{L}$, then $a = 1$.

[WORK: A big confused about the structure vs. property thing here. Shouldn't we have twists as part of the data?]

$\square$

In graphical language, the spherical condition says [WORK: BRAID make diagram, explain why its necessary.]

The non-degeneracy condition says that every non-trivial particle should braid non-trivially with at least one other particle. Graphically, this is shown as

72

$$\text{[braid diagram]} \quad = \quad \forall b \implies a = 1.$$

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 systems and braided $6j$ fusion systems, we simply require that f should respect $6j$ symbols and R symbols as well. We can thus properly speak of the *category* of fusion systems. Naïve isomorphism of fusion systems (invertible morphisms) are the wrong notation of equivalence: it is too restrictive. The correction notion is *gauge equivalence*, which corresponds to performing a local change of basis on $6j$ symbols.

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

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

Additionally, a gauge equivalence 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 $a, b, c, d, n, m \in \mathscr{L}$,

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

$\square$

More generally, a gauge equivalence between $6j$ fusion systems $(\mathscr{L}, N, F)$ and $(\mathscr{L}', N', F')$ is a gauge equivalence between $(\mathscr{L}, N, F)$ and some system $(\mathscr{L}, N, \tilde{F})$, followed by an isomorphism of fusion systems $(\mathscr{L}, N, \tilde{F}) \to (\mathscr{L}', N', F')$
.[WORK: BRAID Give explanation of rectangle axiom, preferably with graphical language]

Definition (Braided gauge equivilance of R-matricies)**.** A braided gauge equivilance of R-matricies $R^{-,-}_-$ and $\tilde{R}^{-,-}_-$ on a $6j$ fusion system $(\mathscr{L}, N^{-,-}_-, F^{-;-;-}_{-;-,-})$ is the following data:

1. .[WORK: idk]

Additionally, a braided gauge equivilance of R-matricies is required to satisfy the following properties:

1. .[WORK: idk]

$\square$

In the case of the toric code we summarize the relevant data. The label set is $\mathscr{L} = \{I, X, Y, Z\}$. For every pair $(a, b)^2 \in \mathscr{L}$, there is a unique c such that $N_c^{a,b} = 1$ - all other values are zero. A table of $(a, b) \in \mathscr{L}^2$ along with that unique value of c is 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

All F-matrices 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		$R_Y^{Z,X} = -1$	$R_X^{Z,Y} = -1$	

.[WORK: Give twistings!]

This gives a full definition of the toric code as modular tensor fusion system. All that is left is to show is that 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 start with the category-theory analogues of monoids[17], groups, finite groups, finite abelian groups, and then end with non-degeneracy. 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

---

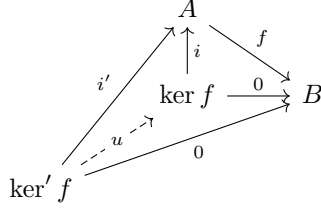[17]A monoid is a set equipped with an associative binary operation and an identity element

Seeing as we have already treated monoidal categories, we move on to fusion categories. Fusion categories are characterized by the fact that they have good tensor product and direct sum structures, such that every element is the direct sum of "simple" objects. Translating into the language of fusion systems, the the set of isomorphism classes of simple objects will correspond to the finite label set $\mathscr{L}$.

There are a few difficulties in trying to formalize this idea. For one, you might be in the strange case that there are objects which cannot be decomposed as direct sums, but still have proper non-trivial subobjects. For example, consider the category of abelian groups. The group $\mathbb{Z}_4$ has the subject $\mathbb{Z}_2$. However, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \neq \mathbb{Z}_4$. Objects with no proper-nontrivial subobjects are called *simple*. What we want is that every object is the direct sum of simple objects.

The discussion above strongly uses the notion of *subobject*. However, it is not clear in general what subobject should mean. The classic intuition is that A is a subobject of B if there is an injective map $f : A \hookrightarrow B$. Injectivity is the statement that the kernel of f is 0, but in arbitrary 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, notably the existence of kernels. In abelian categories we require that all hom-sets be given the structure of abelian groups. Seeing as our eyes are towards quantum physics, all hom-sets will moreover be $\mathbb{C}$ vector spaces. Linear combinations of morphisms corresponds to superposition. Formally, a $\mathbb{C}$-linear category is a category whose hom-spaces are given the structure of $\mathbb{C}$ vector spaces, and whose composition maps are bilinear.
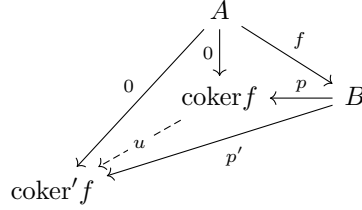
Definition ($\mathbb{C}$-linear abelian category). A $\mathbb{C}$-linear abelian category is a $\mathbb{C}$-linear category. Additionally, a $\mathbb{C}$-linaer abelian category is required to satisfy the following properties:

1. (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 $0 \to A$.

2. (Has direct sums) For all $A, B \in \mathscr{C}$ the direct sum of A and B, denoted $A \oplus B$, exists. The direct sum is an object $A \oplus B$, paired with morphisms $\pi_A, \pi_B : A \oplus B \to A, B$, and $i_A, i_B : A, B \to A \oplus B$, such that

   - $\pi_X \circ i_Y$ is id_X when $X = Y$ and 0 otherwise,
   - $i_A \circ \pi_A + i_B \circ \pi_B = \mathrm{id}_{A \oplus B}$.

3. (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 $i : \ker f \to A$, $p : B \to \mathrm{coker} f$ such 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

$$
\begin{array}{c}
A \\
\nearrow \ \uparrow i \ \searrow f \\
i' \quad \mathrm{ker}\, f \xrightarrow{\ 0\ } B \\
\nwarrow \ \ \dashrightarrow u \quad \nearrow 0 \\
\mathrm{ker}'\, f
\end{array}
$$

commutes.

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

$$
\begin{array}{c}
A \\
\swarrow \ 0\downarrow \ \searrow f \\
0 \quad \mathrm{coker}f \xleftarrow{\ p\ } B \\
\swarrow \ \ \dashleftarrow u \quad \swarrow p' \\
\mathrm{coker}'\, f
\end{array}
$$

commutes

4. (All monomorphisms and epimorphisms are normal) 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, i.e., it satisfies the universal property of $\mathrm{ker}\, f$ for some f. 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.

$\square$

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 $F : \mathrm{Hom}(A, B) \to \mathrm{Hom}(F(A), F(B))$ is a linear map of vector spaces for all $A, B \in \mathscr{C}$.

$\square$

Given a morphism $f : A \to B$, we have a cokernel $B \to \mathrm{coker}f$. We define $\mathrm{im}f$ to be the kernel of the cokernel. Alternatively, the image of f could be defined as the cokernel of the kernel. The fact that these two definitions of image coincide is *equivalent* to the fact that all monomorphisms and epimorphisms are normal (see Exercise 6.5). An exact sequence of morphisms is one in which the image of the incoming map at each term is equal to the kernel of the outgoing map. With these definitions out of the way, we can 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. (Evaluation/co-evaluation) Choices of morphisms $\operatorname{ev}_A : A \otimes A^* \to 1$ and $\operatorname{coev}_A : 1 \to A^* \otimes A$ 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

$$
\begin{array}{ccc}
A \otimes (A^* \otimes A) & \xrightarrow{\alpha_{A,A^*,A}} & (A \otimes A^*) \otimes A \\
{\scriptstyle \operatorname{id}_A \otimes \operatorname{coev}_A} \uparrow & & \downarrow {\scriptstyle \operatorname{ev}_A \otimes \operatorname{id}_A} \\
A \otimes 1 & \xrightarrow[\lambda_A \circ \rho_A^{-1}]{} & 1 \otimes A
\end{array}
$$

and

$$
\begin{array}{ccc}
(A^* \otimes A) \otimes A^* & \xrightarrow{\alpha_{A^*,A,A^*}^{-1}} & A^* \otimes (A \otimes A^*) \\
{\scriptstyle \operatorname{coev}_A \otimes \operatorname{id}_{A^*}} \uparrow & & \downarrow {\scriptstyle \operatorname{id}_{A^*} \otimes \operatorname{ev}_A} \\
1 \otimes A^* & \xrightarrow[\rho_A \circ \lambda_{A^*}^{-1}]{} & A^* \otimes 1
\end{array}
$$

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

3. (Semisimplicity) 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.

$\square$

Duals are best understood in graphical language. Namely, using, the conventions established in the previous section, rigidity can be stated as the condition that

Here and throughout, we suppress unitors and associativity from our diagrams. The axioms of monoidal categories imply that this will not cause any issues. Additionally, the only maps $A \otimes A^* \to 1$ and $1 \to A^* \otimes A$ regularly being used are the evaluation/co-evaluation maps. Hence, when it does not cause confusion, we fix the notation

$$\mathrm{ev}_A = \begin{array}{c} A \ A^* \\ \cup \end{array} \quad , \quad \mathrm{coev}_A = \begin{array}{c} \cap \\ A^* \ A \end{array}$$

This turns the rigidity graphical diagrams into the following much easier to parse form:

We now use this graphical language to prove some basic results about duals which would have been much more cumbersome in the language of commutative diagrams. Seeing as we will not be using any structures of fusion categories other than duals, we broaden our attention to the more general case of *rigid categories*. That is, monoidal categories with duals and evaluation/co-evaluation maps satisfying the axiom of rigidity.

Proposition 6.1. *The following claims about duals in a rigid category $\mathscr{C}$ are true.*

1. *Duals are unique up to unique isomorphism. That is, let $A \in \mathscr{C}$ be an object and let $(\tilde{A}^*, \tilde{ev}_A, \tilde{coev}_A)$ be another triple satisfying the axioms of rigidity. There is a unique isomorphism $A^* \xrightarrow{\sim} \tilde{A}^*$ making the diagrams*

commute.

2. *Duality is functorial. That is, the assignment* $(-)^* : \mathscr{C}^{\mathrm{op}} \to \mathscr{C}$ *sending an object* $A^{\mathrm{op}} \in \mathscr{C}^{\mathrm{op}}$ *to* $A^* \in \mathscr{C}$ *and sending a morphism* $f^{\mathrm{op}} \in \mathrm{Hom}(A^{\mathrm{op}}, B^{\mathrm{op}})$ *to the morphism*

$$f^* : A^* \xrightarrow{\mathrm{coev}_B \otimes \mathrm{id}_{A^*}} B^* \otimes B \otimes A^* \xrightarrow{\mathrm{id}_{B^*} \otimes f \otimes \mathrm{id}_{A^*}} B^* \otimes A \otimes A^* \xrightarrow{\mathrm{id}_{B^*} \otimes \mathrm{ev}_A} B^*$$

in $\mathrm{Hom}(A^*, B^*)$ *is a fully faithful functor. If* $\mathscr{C}$ *is a fusion category, then this functor induces an equivalence of between* $\mathscr{C}^{\mathrm{op}}$ *and* $\mathscr{C}$.

3. *Duals preserve tensor products. That is,* $B^* \otimes A^*$ *is a dual for* $A \otimes B$, *for all* $A, B \in \mathscr{C}$.

Proof. We begin by proving part (1). We claim that the map

$$(\mathrm{id}_{\tilde{A}^*} \otimes \mathrm{ev}_A) \circ (\mathrm{co\tilde{e}v}_A \otimes \mathrm{id}_{A^*}) : A^* \to \tilde{A}^*$$

is an isomorphism, whose inverse is given by $(\mathrm{id}_{A^*} \otimes \mathrm{\tilde{e}v}_A) \circ (\mathrm{coev}_A \otimes \mathrm{id}_{\tilde{A}^*})$. In graphical language, we compute

79

Hence,

$$(\mathrm{id}_{A^*} \otimes \tilde{\mathrm{ev}}_A) \circ (\mathrm{coev}_A \otimes \mathrm{id}_{\tilde{A}^*}) \circ (\mathrm{id}_{\tilde{A}^*} \otimes \mathrm{ev}_A) \circ (\tilde{\mathrm{coev}}_A \otimes \mathrm{id}_{A^*}) = \mathrm{id}_{A^*}$$

They key point is that one can re-arrange the order of terms that affect disjoint strands, by the funtoriality of the tensor product. This allows us to put the $\tilde{\mathrm{ev}}_A$ and $\tilde{\mathrm{coev}}_A$ together, apply rigidity of $\tilde{A}^*$, and then apply rigidity of A^*. The proof that the other composition equals the identity is exactly the same. Showing this isomorphism uniquely makes the desired diagrams commute is straightforward.

We now move on to point (2). We need to prove that if $f^{\mathrm{op}} : A^{\mathrm{op}} \to B^{\mathrm{op}}$ and $g^{\mathrm{op}} : B^{\mathrm{op}} \to C^{\mathrm{op}}$ are morphisms in $\mathscr{C}^{\mathrm{op}}$, then $(f \circ g)^* = g^* \circ f^*$. Graphically, we have the diagram

Thus, changing the orders morphisms which affect disjoint sets of tensor factors when necessary and applying rigidity, we find that

as desired. The fact that $(\mathrm{id}_A)^* = \mathrm{id}_{A^*}$ follows immediately from rigidity. We now show that $(-)^*$ full, faithful, and essentially surjective, which by Exercise 6.6 is enough to conclude that $(-)^*$ induces an equivalence of categories. For fully faithfulness, we define a linear mpa $\mathrm{Hom}(A^*, B^*) \to \mathrm{Hom}(B, A)$ taking the morphism $f : A^* \to B^*$ to the composition

80

It is straightforward to see that this serves an inverse to the duality map $\mathrm{Hom}(B, A) \to \mathrm{Hom}(A^*, B^*)$, and hence that $(-)^*$ induces isomorphisms on hom-spaces. Now, assume that $\mathscr{C}$ is a fusion category. It is clear from uniqueness of duals that if two simple objects have the isomorphic dual, then they must be isomorphic. By a counting argument on the finite set of isomorphism classes of simple objects, we find that every object is is isomorphic to the dual of some other object. Taking direct sums, we thus find that $(-)^*$ is essentially surjective. The result thus follows from Exercise 5.4.

We now move on to point (3). We define maps $\tilde{\mathrm{ev}}_{A\otimes B} : A\otimes B\otimes B^*\otimes A^* \to 1$ and $\tilde{\mathrm{coev}}_{A\otimes B} : B^*\otimes A^*\otimes A\otimes B$ by first applying ev/coev on the center terms, and then applying ev/coev on the remaining outside terms. These satisfy the axioms of rigidity, since

In light of this proposition, we will often assume that $(A\otimes B)^* = B^*\otimes A^*$. While technically incorrect, these two objects are always canonically isomorphic and we do not lose any generality by imposing this condition. We now contrast fusion categories and fusion systems. The first claim is as follows:

Proposition 6.2. *Let $\mathscr{C}$ be a fusion category, in the. 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*

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

We call $\mathscr{C}$ multiplicity free if $N_c^{a,b} \in \{0, 1\}$ for all triples. The pair $(\mathscr{L}, N_-^{-,-})$ is a fusion system whenever $\mathscr{C}$ is multiplicity free.

Proof. We verify the axioms one by one.

1. (Identity/Do-nothing) In a fusion category we assume that the tensor unit is simple, hence it gives a unit in $\mathscr{L}$. Uniqueness comes from the fact that the unit in a monoidal category is well defined up to isomorphism. That is, if 1 and $1'$ are two monoidal units then $1 \cong 1 \otimes 1' \cong 1'$.

2. (Inverse/anti-particle) This property comes from the fact that duals of simple objects are simple and unique, and shown in Proposition 6.1.

3. (Associativity) This follows immediately from the existence of an associativity isomorphism on the monoidal structure of $\mathscr{C}$.

$\square$

The interesting fact is that one can *not* uniquely go the other direction. That is, there there are non-equivalent fusion categories which give the same fusion system. However, the failure is in some sense bounded:

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

The correct correspondence, in fact, is between fusion categories and $6j$ fusion systems. Before stating this correspondence, we need an important alternate characterization of simple objects.

Theorem 6.2 (Schur's Lemma)**.** *Let $\mathscr{C}$ be a $\mathbb{C}$-linear abelian category. If $A \in \mathscr{C}$ is simple, then $\mathrm{End}(A)$ is one dimensional. If A and B are non-isomorphic simple objects, $\mathrm{Hom}(A, B) = 0$. If $\mathscr{C}$ is semisimple, then $\mathrm{End}(A)$ is one-dimensional if and only if A is simple.*

Proof. Recall that A, B are defined to be simple if it has no proper nontrivial subobjects. Suppose A and B are simple. Let $f : A \to B$ be a morphism. We have an exact sequence

$$0 \to \ker f \to A \xrightarrow{f} B \to \mathrm{coker} f \to 0.$$

Seeing as $\ker f$ is a subobject of A, we have either that $\ker f = 0$ or $\ker f = A$. If $\ker f = A$, then f must be the zero map, so we are done. If $\ker f = 0$, then we have an exact sequence

$$0 \to A \to B \to \mathrm{coker} f \to 0.$$

Hence, A is a subobject of B, and so $A \cong B$. Thus, we have recovered that $\mathrm{Hom}(A, B) = 0$ when $A \not\cong B$.

The above argument also shows that every map in $\mathrm{End}(A)$ must be an isomorphism. Choosing any nonzero $f \in \mathrm{End}(A)$, there is a map $\mathrm{End}(A) \to \mathrm{End}(A)$ induced by precomposition with f. This is clearly a $\mathbb{C}$-linear map, and seeing as f is an isomorphism on A it must be an isomorphism on $\mathrm{End}(A)$. Linear algebra tells us that this map $\mathrm{End}(A) \to \mathrm{End}(A)$ must have an eigenvector, since $\mathbb{C}$ is algebraically closed. Thus, there exists a nonzero $g \in \mathrm{End}(A)$ such that $g \circ f = \lambda \cdot g$ for some scalar $\lambda \in \mathbb{C}$. Postcomposing with g^{-1}, we find that $f = \lambda \cdot \mathrm{id}_A$. Thus, every map in $\mathrm{End}(A)$ is a scalar multiple of the identity, hence $\mathrm{End}(A)$ is one dimensional.

Finally, let $A \in \mathscr{C}$ be an object in a semisimple category. By assumption, there is a finite set S of simple objects such that $A \cong \bigoplus_{B \in S} B$. We compute as follows:

$$
\begin{aligned}
\dim \operatorname{End}(A) &= \dim \operatorname{Hom}\left(\bigoplus_{B \in S} B, \bigoplus_{B \in S} B \right) \\
&= \dim \bigoplus_{B_0 \in S} \bigoplus_{B_1 \in S} \operatorname{Hom}(B_0, B_1) \\
&= \bigoplus_{\substack{B_0, B_1 \in S \\ B_0 \cong B_1}} 1.
\end{aligned}
$$

The first step follows from Exercise 6.12, which implies that the direct sum can be pulled out of Hom in both the first and second argument. The second step follows from the fact that $\operatorname{Hom}(B_0, B_1)$ is one dimensional when $B_0 \cong B_1$, and 0 dimensional otherwise. If $|S| \geq 2$, we thus get that $\dim \operatorname{End}(A) \geq 2$. Hence, $\operatorname{End}(A)$ is one dimensional if and only if A is simple as desired. $\qquad \square$

Proposition 6.3. *Let $\mathscr{C}$ be a multiplicity free fusion category, with associated fusion system $(\mathscr{L}, N_-^{-,-})$. For all triples $a, b, c \in \mathscr{L}$, choose representatives $A, B, C \in \mathscr{C}$. Seeing as each hom-space $\operatorname{Hom}(A \otimes B, C)$ is at most one dimensional, we can choose distinguished generators*
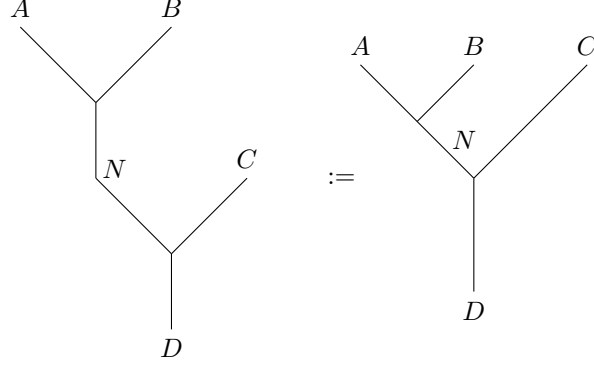

$$\in \operatorname{Hom}(A \otimes B, C) \cong \mathbb{C}.$$

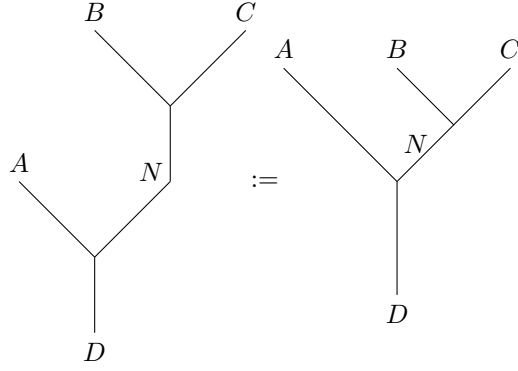*[WORK: Add discussion of admissability] These generators are chosen arbitrarily, except for the exceptional cases outlined below:*

$$= \rho_A, \qquad = \lambda_A.$$

We find that $\operatorname{Hom}((A \otimes B) \otimes C, D)$ 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, and D is a representative of an isomorphism class $d \in \mathscr{L}$. 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, where we set $F^{a,b,c}_{d;n,m} = 0$ if any of the relevant generators are zero (i.e. (a, b, c, d, n, m) is not admissible).

   The triple $(\mathscr{L}, N, F)$ specifies a $6j$ fusion system.

Proof. We postpone the proof to Appendix C   □

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

Proof. The proof of this result is constructive. Namely, given a $6j$ fusion system one defines objects to be direct sums of elements of $\mathscr{L}$, the tensor product in terms of the fusion rules, and associativity in terms of $6j$ symbols. It is a natural consequence of the axioms of a $6j$ fusion system that the resulting category is a fusion category. Full details are found in Appendix C.   □

We now give some commentary on Proposition 6.3, through the Yoneda perspective. Namely, we elaborate on why we encode associativity 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-set are vector spaces, not our objects. Another answer is that this keeps in line with the Yoneda perspective - it is better to look at the relationship of an object with those around it (i.e., hom-spaces) than the object itself. In this case, we systematically defined F-matrices to associate $\mathrm{Hom}((A \otimes B) \otimes C, D)$ with $\mathrm{Hom}(A \otimes (B \otimes C), D)$. Since our F-matrices were chosen coherently, this gives a natural transformation $\mathrm{Hom}((A \otimes B) \otimes C, -) \to \mathrm{Hom}(A \otimes (B \otimes C), -)$. 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 $\alpha_{A,B,C}$.

A *braided fusion category* is a fusion category whose underlying monoidal category is a braided monoidal category. There are no extra compatibility conditions. Seeing as we will be very often using the braiding isomorphism β, we fix the notation

It is a signficant advantage of our graphical language that the hexagon iden- tiites, like with the triangles and pentagon, becomes invisible. That is, the hexagon identities are the statement that braiding between $A \otimes B$ and C is unambigious for objects A, B, C in a braided category $\mathscr{C}$:

[WORK: graphical-hexagon]

From braided fusion categories, we can construct braided $6j$ fusion systems:

Proposition 6.4. *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 representatives $A, B, C \in \mathscr{C}$, and distinguished generators of $\mathrm{Hom}(A \otimes B, C)$. Define a $6j$ fusion system just as in Proposition 6.3. Define $R_c^{a,b}$ to be the unique value such that*

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

Proof. See Appendix C. □

As usual, a braided monoidal equivalence of two categories means a pair of braided monoidal functors, such that both compositions are monoidally equivalent to the identity. We now establish a useful graphical lemma about braided monoidal categories which will be useful:

Lemma 6.1. *Let $A, B, C, D \in \mathscr{C}$ be objects in a braided monoidal category, and let $f : C \to B \otimes D$ and $g : A \otimes C \to 1$ be morphisms. We have that*

Proof. We compute as follows:

$$(\beta_{B,D}^{-1} \circ \beta_{B,D} = \mathrm{id}_{B \otimes D})$$

$$(\text{Naturality of braiding})$$

and hence we conclude the result. □

We now move on to MTCs. A *non-degenerate* braided fusion category is one in which for all simple objects $A \in \mathscr{C}$,

$$\beta_{B,A} \circ \beta_{A,B} = \mathrm{id}_{A \otimes B} \ \forall \ B \text{ simple} \implies A \cong 1.$$

The physical motivation for this non-degeneracy condition is given in section 7. It is a key subtlety of the theory that MTCs are *not* simply non-degenerate braided fusion categories. Every MTC will additionally have a "twisting" operation. The reason for this is as follows. Not only should our theory have distinguihsed moprhisms $A \otimes A^* \to 1$ and $1 \to A^* \otimes A$, but it should also have

distinguished morphisms $A^* \otimes A \to 1$ and $1 \to A \otimes A^*$. Doing this naively using braiding works to a limited degree, but it ends up being incompatible with tensor products. Hence, we must introduce a twist to remedy the situation:

Definition (Ribbon category). A ribbon category is the following data:

1. A braided monoidal category $\mathscr{C}$.

2. (Twist) A natural isomorphism $\theta : \mathrm{id}_{\mathscr{C}} \to \mathrm{id}_{\mathscr{C}}$.

Additionally, an ribbon 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 $A \in \mathscr{C}$.

$\square$

This allows us to define the distinguished morphisms

The key point which would be invalid if we did not add the twist is as follows[18]: [WORK: use term "topological spin" to motivate why we are using a twist-centric definition]

Proposition 6.5. *.[WORK: move this to the end of us building up the ribbon?] Let $\mathscr{C}$ be a ribbon category. For all $A, B \in \mathscr{C}$,*

and

Proof. We prove only the first identity, since the proof of the second is identical. We compute as follows:

---

[18]It is for this reason that we call ribbon categories *ribbon*. We can replace single strands properly with their two-strand counterparts, forming bands which look like ribbons

$\square$

We now have our main definition:

Definition (Modular tensor category)**.** A modular tensor category (MTC) is a non-degenerate ribbon fusion category.

$\square$

Morphisms between ribbon categories should respect the twisting operation. A *ribbon functor*[19] between two MTCs $(\mathscr{C}, \theta_{\mathscr{C}}), (\mathscr{D}, \theta_{\mathscr{D}})$ is a braided monoidal functor $F : \mathscr{C} \to \mathscr{D}$ such that $F(\theta_{\mathscr{C};A}) = \theta_{\mathscr{D};A}$ for all $A \in \mathscr{C}$. A ribbon equivalence is thus a pair of ribbon functors whose compositions in either direction are monoidally naturall equivalent to the identity. This allows us to state our final equivalence:

Proposition 6.6. *The process in Proposition 6.4 gives a one-to-one correspondence between MTCs up to ribbon equivalence and modular tensor fusion systems up to gauge equivalence.*

Proof. See Appendix C. $\square$

We spend the remainder of this section discussing the properties of MTCs. Seeing as we will be often refering to the twist, we demonstrate that it can be expressed in a purely graphical formula:

Proposition 6.7. *Let $A \in \mathscr{C}$ be an object in an MTC. We have that*

---

[19]This is more popularly refered to as a *braided tensor functor*. [WORK: Do I need to define this at all?]

Proof. We compute using Lemma 6.1 and rigidity that

as desired. The second equality follows similarly. □

The distinguished morphisms of a ribbon category give good "two-sided" duals, in the sense that if A is a dual of A^* then A^* is also a dual of A. That is, we can identify A with A^{**}. We will later find ourselves interested more generally in the categories wit such two-sieded duals, known as pivotal categories [Sel11]. Formally, a pivotal category is a monoidal category $\mathscr{C}$ paired with a monoidal natural isomorphism $(-) \to (-)^{**}$. Pivotal categories can be described explicitely in graphical language:

Proposition 6.8. *. [WORK: write out what the axioms of a pivotal category imply. Remove the associated exercise.]*

[WORK: Re-do this introduction sentence]The following shows that all MTCs are pivotal, but also that braided monoidal categoires without twist are pivotal:

Proposition 6.9. *Let $\mathscr{C}$ be a braided monoidal category, and let $\theta : \mathrm{id}_{\mathscr{C}} \to \mathrm{id}_{\mathscr{C}}$ be a natural transformation such that $(\theta_A)^* = \theta_{A^*}$ for all $A \in \mathscr{C}$. The distinguished morphisms. [WORK: Re-do this. Go through Deligne's lemma that giving a pivotal structure is the same as giving a twist, for braided categories. Original reference]*

give $\mathscr{C}$ the structure of a pivotal category.

89

Proof. . [WORK: Do proof] □

The power of pivotal categories is that one can define the *trace* of a morphism $f : A \to A$. The trace is a powerful operation, since it allows you to qualify morphisms in terms of dnumbers, which can be used both for linearization and defining invariants. Naturally, one wants to define trace by "closing the loop" on f. That is,

$$\text{tr}(f) = A^* \left(\boxed{f}\right) \begin{matrix} A \\ \\ A \end{matrix}$$

The space $\text{End}(1)$ is one dimensional by Schur's Lemma (Theorem 6.2), with generator id_1. Hence, we can canonically identify $\text{tr}(f)$ with a complex number. Written out explicitly, $\text{tr}(f) \in \text{End}(1) = \mathbb{C}$ is the composition

$$\text{tr}(f) : 1 \xrightarrow{\text{coev}_A} A^* \otimes A \xrightarrow{\text{id}_{A^*} \otimes (\theta_X \circ f)} A^* \otimes A \xrightarrow{\beta_{A^*, A}} A \otimes A^* \xrightarrow{\text{ev}_A} 1.$$

However, there is an ambiguity: one could also close the loop the other direction. For trace to be well behaved, these should give the same answer. Thus, we define a *spherical category*[20] to be a pivotal category in which

$$A^* \left(\boxed{f}\right) \begin{matrix} A \\ \\ A \end{matrix} = \begin{matrix} A \\ \\ A \end{matrix} \left(\boxed{f}\right) A^*$$

When working with pivotal categories, one only has the weaker notions of "left trace" and "right trace". MTCs are automatically spherical:

Proposition 6.10. *Let $(\mathscr{C}, \theta)$ be as in Proposition 6.9. $\mathscr{C}$ is a spherical category. [WORK: There is an extra condition needed which is equivalent to being spherical - cite it exactly. Lemma 4.27 in reference.]*

Proof. . [WORK: Do proof] □

We now demonstrate some basic facts traces:

[WORK: I want to know what's true. I DON'T think you can move f to f^* on the other. I can't figure out how to prove that trace commutes with composition.]

---

[20]Spherical categories were originally defined by Barrett and Westbury in [BW99], with immediate applications towards $(2+1)$-TQFTs [BW96]. The name comes from the fact that the loop can be moved around f as though the diagram were on a 2-sphere

Proposition 6.11. *Let $\mathscr{C}$ be a spherical category. For all $A, B \in \mathscr{C}$, $f \in$* $\mathrm{End}(A)$ *the following claims are all true:*

1. $\mathrm{tr}(f \oplus g) = \mathrm{tr}(f) + \mathrm{tr}(g)$ *for all $g \in \mathrm{End}(B)$*

2. $\mathrm{tr}(f \circ g) = \mathrm{tr}(g \circ f)$ *for all $g \in \mathrm{End}(A)$*

3. $\mathrm{tr}(f^*) = \mathrm{tr}(f)$

4. *Trace is independent of choice of duals. That is, let $(\tilde{A}^*, \widetilde{\mathrm{coev}}_A, \widetilde{\mathrm{ev}}_A)$ be a different choice of dual for A. Defining $\widetilde{\mathrm{tr}}(f)$ exactly like $\mathrm{tr}(f)$ except with this new unit, we find that $\widetilde{\mathrm{tr}}(f) = \mathrm{tr}(f)$.*

5. *Trace is preserved by functors. That is, let $\mathscr{C}, \mathscr{D}$ be spherical categories with traces $\mathrm{tr}_{\mathscr{C}}, \mathrm{tr}_{\mathscr{D}}$ respectively. Let $F : \mathscr{C} \to \mathscr{D}$ be a braided tensor functor. We have that $\mathrm{tr}_{\mathscr{C}}(f) = \mathrm{tr}_{\mathscr{D}}(F(f))$.*

Proof. .[WORK: BRAID do proof] □

For compatibility with the tensor product, one needs the ribbon axiom:

Proposition 6.12. *Let $\mathscr{C}$ be a ribbon category. For all $A \in \mathscr{C}$, $f \in \mathrm{End}(A)$,* $\mathrm{tr}(f \otimes g) = \mathrm{tr}(f) \cdot \mathrm{tr}(g)$.

Proof. Using the ribbon property of Proposition 6.5, we compute

Traces allow us to naturally define many very powerful, physically observable, and mathematically interesting invariants. For example, let $A \in \mathscr{C}$ be an object in a spherical category. In vector spaces, the trace of the identity gives the dimension of the vector space. Thus, we define more generally $d_A = \mathrm{tr}(\mathrm{id}_A)$ to be the *quantum dimension* of A. The following properties give a taste of the depth present in this theory:

Theorem 6.4. *Let $A \in \mathscr{C}$ be a simple object in an MTC. The following claims about the quantum dimension are all true:*

1. $d_A = 1$ *if and only if A is an abelian anyon. That is, $\beta_{B,A} \circ \beta_{A,B}$ is a scalar multiple of the identity for every other simple object $B \in \mathscr{C}$.*

2. *([WORK: get reference]) If $1 \leq d_A \leq 2$, then $d_A = 2\cos(\pi/m)$ for some integer $m \geq 3$. Otherwise, $d_A \geq 4$.*

3. *([WORK: get reference]) The fusion matrix N_A has a unique eigenvalue of largest absolute value. This eigenvalue is real, and is equal to d_A.*

Proof. . [WORK: prove first part] $\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

This theorem is quite useful experimentally. For example, suppose we wish to observe non-abelian anyons. The state of current laboratories are such that creating the appropriate conditions, braiding anyons, and recording non-abelian statistics is out of reach with proposed methods [BSS06]. Thus, one observes non-abelian anyons indirectly by measuring physical quantities which are associated with non-abelian statistics. For example, the quantum dimension can be related to the *entropy* of a physical system [KP06]. Abelian MTCs have $d_A = 1$, whereas non-abelian MTCs will have measurably larger quantum dimensions - the second part of the theorem implies $d_A \geq 2\cos(\pi/4) = \sqrt{2}$. This distinctly different entropy can be physically measured. Namely, the thermodynamic Maxwell's equation relates entropy to chemical potential, which in turn can be measured by changes in voltage [CS09]. [WORK: Brian says TEE comes from the fact that non-trivial knots exist, which store information. This is a mathematical statement explaining why TQC could work. Cool! Say this.]

If d_A measures the size of each individual anyon-type, then their sum should give a measure of the total size of the MTC. Thus, we define for a general spherical category

$$\dim \mathscr{C} = \sum_{a \in \mathscr{L}} d_a^2,$$

where as usual $\mathscr{L}$ is the set of isomorphism of classes of simple objects. The dimension can be split into two Gauss sums, $p_{\mathscr{C}}^{\pm}$

Theorem 6.5 (Vafa, [Vaf88]). *Let $\mathscr{C}$ be a spherical fusion category, and let $\mathscr{L}$ be the set of isomorphism classes of simple objects. For each simple object $A \in \mathscr{C}$, $\theta_A \in \mathrm{End}(A)$ lives in a one dimensional space with generator id_A. Hence, we can canonically identify θ_A with a complex number. Define*

$$p_{\mathscr{C}}^{\pm} = \sum_{a \in \mathscr{L}} \theta_a^{\pm 1} d_a^2.$$

The quantities θ_a and $p_{\mathscr{C}}^+/p_{\mathscr{C}}^-$ are roots of unity, for all $a \in \mathscr{L}$. Additionally,

$$p_{\mathscr{C}}^+ p_{\mathscr{C}}^- = \dim \mathscr{C}.$$

We are now ready to define the most important invariants of MTCs: representations of the group $\mathrm{SL}_2(\mathbb{Z})$ of 2 by 2 matrices with unit determinant. $\mathrm{SL}_2(\mathbb{Z})$ is known as the modular group, due to its connections with moduli spaces of elliptic curves. It is because of these representations that modular tensor categories are called modular. We define the modular representations:

Theorem 6.6 ([BK01])**.** *Let $\mathscr{C}$ be an MTC, with set $\mathscr{L}$ of isomorphism classes of simple. We define the S-matrix of an MTC to be the matrix whose $[a,b]$th coefficient is*

$$S_{a,b} = \mathrm{tr}\,(\beta_{A,B} \cdot \beta_{B,A}) = \; A^* \left(B \bigcirc A \right) B^*$$

where A, B are representatives of $a, b \in \mathscr{L}$. Similarly, we define the T-matrix of an MTC to be the diagonal matrix whose $[a,a]$th coefficient is θ_A. The map

$$\rho_{\mathscr{C}} : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Aut}(\mathbb{C}[\mathscr{L}])$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \mapsto \frac{1}{\sqrt{\dim \mathscr{C}}} \cdot S,$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto \frac{\sqrt[3]{p_{\mathscr{C}}^+}}{\sqrt[6]{\dim \mathscr{C}}} \cdot T.$$

is a representation of the modular group. That is, extending $\rho_{\mathscr{C}}$ by matrix multiplication gives a well-defined group homomorphism.

These S-matrices and T-matrices are very important invariants of MTCs, and are refered to as the *modular data*. They do not, however, uniquely determine the MTC [MS21]. We summarize some relevant facts:

Theorem 6.7. *The following claims about MTCs are all true:*

- *(Bruguieres, [Bru00]) Ribbon fusion categories are non-degenerate (and hence are MTCs) if and only if their S-matrix is invertible.*

- *(Bruillard-Ng-Rowell-Wang, [BNRW16]) There are finitely many MTCs, up to braided monoidal equivalence, of a given rank.*

- *(Schauenburg-Ng, [NS10]) The modular representations of MTCs have finite image. More precisely the kernels of modular representations are congruence subgroups, meaning that they all contain the subgroup*

$$\{\, M \in \mathrm{SL}_2(\mathbb{Z}) \,|\, M \equiv I \mod n \,\}$$

for some $n \geq 1$.

Finally, we end with a comment. It is a fascinating feature of this theory that not all fusion categories are a-priori pivotal. What we have is the weaker structure of a natural isomorphism between the identity and the *quadruple* dual, known as the Radford isomorphism. Explicitly:

Theorem 6.8 ([ENO05]). *In every fusion category, there is a natural monoidal isomorphism between the identity functor and the quadruple dual functor* $(-)^{****}$.

It is a deep conjecture that two duals should always suffice:

Conjecture 6.1 (Etingof, Nikshych, and Ostrik). *In every fusion category, there is a natural monoidal isomorphism between the identity functor and the double dual functor* $(-)^{**}$. *That is, every fusion category admits a pivotal structure.*

While these questions are of much interest to the general community, they are not extremely relevant to topological quantum computing. This is because all of our fusion categories will have hom-spaces coming from quantum systems and hence will not just be vector spaces, but Hilbert spaces. This condition is called *unitarity*. All unitary fusion categories admit pivotal structures, which will even be spherical. This is discussed in Appendix B.

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

This section introduces the MTC corresponding to the toric code: $\mathcal{Z}(\mathbf{Vec}_{\mathbb{Z}_2})$. Intuitively, we describe the situation as follows. If fusion categories are generalized groups, then groups should certainly give fusion categories. This is done by assigning a finite group G the *category of G-graded vector spaces* $\mathbf{Vec}_G$. We now recall what the modular tensor fusion system for the toric code looked like. It consisted of four elements $1, \alpha, \beta, \alpha\beta$, with a fusion rule much like $\mathbb{Z}_2 \times \mathbb{Z}_2$, where the first copy of $\mathbb{Z}_2$ is generated by α and the second copy of $\mathbb{Z}_2$ is generated by β. The only non-group like behavior was the braiding, which was non-trivial between the two copies of $\mathbb{Z}_2$. In this way, the modular tensor fusion system of the toric code looks like "gluing two copies of $\mathbb{Z}_2$ with a twist". The category-theoretic construction which realizes this "glue two copies of $\mathscr{C}$ with a twist" procedure is the Drinfeld center, $\mathcal{Z}(\mathscr{C})$. Hence, the MTC attached to the toric code is $\mathcal{Z}(\mathbf{Vec}_{\mathbb{Z}_2})$.

The category $\mathbf{Vec}_G$ of G-graded vector spaces can be defined when G is any set. Endowing G with more algebraic structure corresponds to endowing $\mathbf{Vec}_G$ with more categorical structure. In particular, the guiding analogy of subsection 6.2 now becomes very explicit. Making G a monoid/finite group/finite abelian group corresponds to making $\mathbf{Vec}_G$ a monoidal/fusion/braided fusion category. The category $\mathbf{Vec}_G$ will never be an MTC - one needs the Drinfeld center construction to make it non-degenerate. Formally, we define the following category:

$$\mathbf{Vec}_G = \begin{pmatrix} \textbf{objects} : \text{collections of } \mathbb{C} \text{ vector spaces } \{V_g\}_{g \in G} \\ \textbf{morphisms} : \text{collections of } \mathbb{C}\text{-linear maps} \end{pmatrix}.$$

That is, a morphism between $\{V_g\}_{g \in G}$ and $\{W_g\}_{g \in G}$ is a collection of linear maps $\{f_g : V_g \to W_g\}_{g \in G}$. Often, we will use the notation V for an element in

$\mathbf{Vec}_G$, and implicitly let V_g denote the g-component of V. This is compactly written as

$$V = \bigoplus_{g \in G} V_g.$$

Objects in $\mathbf{Vec}_G$ are in this way seen as vector spaces paired with canonical decompositions as direct sums of g-components for each $g \in G$. Morphisms are linear maps which "respect the grading", by sending g-component to g-component. We now add algebraic structure to G, and recover categorical structure on $\mathbf{Vec}_G$:

[WORK: Add explanation of subscripts in the morphisms between categories.]

Lemma 6.2. *Let G be a set. Given $V, W \in \mathbf{Vec}_G$, $\mathrm{Hom}_{\mathbf{Vec}_G}(V, W)$ is a sub vector space of $\mathrm{Hom}_{\mathbf{Vec}}(V, W)$. Hence, we can naturally endow $\mathrm{Hom}_{\mathbf{Vec}_G}(V, W)$ with the structure of a vector space. This turns $\mathbf{Vec}_G$ into a $\mathbb{C}$-linear abelian category.*

Proof. We check that the axioms are satisfied one-by-one.

1. (Has a zero object) Define the object 0 to be the G-graded vector space whose g-component is 0-dimensional for all $g \in G$. Choose $V \in \mathbf{Vec}_G$. Since linear maps must send 0 to 0, there is a unique map $0_g \to V_g$ for all $g \in G$, and hence there is a unique map $0 \to V$. Thus, 0 is a zero object.

2. (Has binary biproducts) Given $V, W \in \mathbf{Vec}_G$, we define $V \oplus W$ to be the object with $(V \oplus W) = V_g \oplus W_g$, where $\oplus$ is the direct sum of vector spaces. The projection maps π_V (resp. π_W) are defined on g-components by sending $(v, w) \in V_g \oplus W_g$ to v (resp. w). The injection maps i_A (resp. i_B) are defined on g-components by sending v (resp. w) in V_g (resp. W_g) to $(v, 0)$ (resp. $(0, w)$). It is trivial to verify that these maps satisfy the required axioms.

3. (Has kernels and cokernels) For all $V, W \in \mathbf{Vec}_G$ and $f : V \to W$, we define $\ker f$ and $\operatorname{coker} f$ on g-components by $(\ker f)_g = \ker f_g$ and $(\operatorname{coker} f)_g = \operatorname{coker} f_g$. On the right hand side of these formulas, $\ker$ and coker are being used as the standard notions of kernel and cokernel from linear algebra. The map $i : \ker f \to V$ is the natural inclusion map, and the map $\pi : B \to \operatorname{coker} f$ is the natural projection map. We show that the kernel satisfies the desired universal property, and leave the cokernel as an exercise since the proof is identical.

   The fact that $f \circ i = 0$ follows from the definition of kernel. Suppose now that $i' : \ker' f \to A$ is such that $f \circ i' = 0$. On the level of g-components, this means that for any $v \in (\ker' f)_g$ we have that $f(i'(v)) = 0$. Hence, $i'(v) \in \ker f$. Letting u by i' with codomain restricted to $\ker f$, it is tautological that the desired diagram commutes. This completes the proof.

4. (All monomorphisms and epimorphisms are normal) Let $f : A \to B$ be a linear map. We show that if f is a monomorphism then it is injective, and that if f is injective it is a kernel, from which we derive the result. Similarly one can show that if f is a epimorphism it is surjective, and if f is surjective it is a cokernel Seeing as the proof for cokernels is identical to the proof for kernels, we leave it as an exercise.

- (monomorphism $\implies$ injective) Suppose $f : V \to W$ is a monomorphism. Consider two maps $\ker f \to V$, one defined to be the zero map and the other defined to be the natural inclusion. Both maps are equal (i.e zero) after being postcomposed with f. Hence, they must be equal, hence $\ker f = 0$ so f is injective.

- (injective $\implies$ kernel) Suppose $f : V \to W$ is injective. Define $\tilde{f} : W \to W/V$ to be the map defined on g-components by being the natural projection of W_g onto W_g/V_g for all $g \in G$, where V_g is canonically identified with a subspace of W_g by injectivity. We show that f satisfies the universal property of $\ker \tilde{f}$. Suppose that $i' : \ker' \tilde{f} \to W$ is a map for which $\tilde{f} \circ i' = 0$. By the definition of $\tilde{f}$ this implies that the image of i' lives in V. Hence, we can let $u : \ker' f \to V$ to be the map equal to i' but with restricted codomain. It is clear that the desired diagram commutes, and hence we are done.

Note that the converses to all of these statements are true - injection, kernel, and monomorphism are all synonyms in $\mathbf{Vec}_G$ (see Exercise 6.8).

$\square$

Proposition 6.13. *Let G be a monoid. Define the structures for a monoidal category as follows:*

1. *(Underlying category)* $\mathbf{Vec}_G$.

2. *(Tensor product)* $\otimes : \mathbf{Vec}_G \times \mathbf{Vec}_G \to \mathbf{Vec}_G$ *sending* (V, W) *to the object whose g-component is*

$$(V \otimes W)_g = \bigoplus_{hk=g} V_h \otimes W_k,$$

for all $g \in G$, where h, k run over elements of G.

3. *(Identity)* $1 = \mathbb{C}_e$, *where $e \in G$ is the identity element of G.*

4. *(Associativity) Given V_0, V_1, V_3 we define α on the g-component by the natural map*

$$((V_0 \otimes V_1) \otimes V_2)_g \quad = \quad \bigoplus_{(hk)l=g} (V_{0;h} \otimes V_{1;k}) \otimes V_{2;l}$$

$$\downarrow$$

$$\bigoplus_{h(kl)=g} V_{0;h} \otimes (V_{0;k} \otimes V_{1;l}) \quad = \quad (V_0 \otimes (V_1 \otimes V_2))_g,$$

where $g \in G$, and h, k, l run over elements of G.

5. *(Unitors) Given V, we define λ on the g-component by the obvious map*

$$(\mathbb{C}_e \otimes V)_g = \mathbb{C}_e \otimes V_g \to V_g,$$

where $g \in G$. *The definition of ρ is completely analogous.*

These structures give a well-defined monoidal category.

Proof. Verifying the triangle and pentagon identities comes down to a simple unravelling of definitions, so we leave the proof as an exercise. $\square$

Proposition 6.14. *Let G be a finite group. Define the structures for a fusion category as follows:*

1. *(Underlying $\mathbb{C}$-linear abelian monoidal category)* $\mathbf{Vec}_G$.

2. *(Duals) Given $V \in \mathscr{C}$, we define the dual by*

$$(V^*)_g = \left(V_{g^{-1}}\right)^*.$$

3. *(Evaluation) Given $V \in \mathscr{C}$, we define* ev *on the e-component as*

$$(V \otimes V^*)_e = \bigoplus_{g \in G} V_g \otimes (V_g)^* \to \mathbb{C}_e,$$

$$\bigoplus_{g \in G} v \otimes \varphi \mapsto \varphi(v)$$

and zero otherwise.

4. *(Co-evaluation) Given $V \in \mathscr{C}$, we define* coev *on the e-component as*

$$\mathbb{C}_e \to \bigoplus_{g \in G} (V_g)^* \otimes V_g = (V^* \otimes V)_e,$$

$$x \to \bigoplus_{g \in G} \mathrm{coev}_{V_g}(x)$$

97

and zero otherwise. The map coev_{V_g} *is defined as follows. First, choose a basis* $\{v_i\}_{i\in I}$ *for* V_g. *This gives a dual basis* $\{\varphi_i\}_{i\in I}$ *for* $(V_g)^*$, *defined by*

$$\varphi_i(v_j) = \begin{cases} 1 & i = j \\ 0 & otherwise. \end{cases}$$

We let $\mathrm{coev}_{V_g}(x) = x \cdot \sum_{i\in I} \varphi_i \otimes v_i$. *This map is well defined and independent of choice of basis.*

These structures give a well-defiend fusion category.

Proof. We check the axioms one by one.

1. Verifying that the tensor product, associativity, left unitor, and right unitors are $\mathbb{C}$-linear functors is straightforward, and is left as an exercise to the reader.

2. (Rigidity) To begin, we verify that coev_{V_g} is independent of choice of basis $(v_i)_{i\in I}$. Suppose $(\tilde{v}_i)_{i\in I}$ is another choice of basis. There is a chance of basis matrix $(c_{i,j})_{(i,j)\in I\times I}$ between them. It is straightforward to see that the dual bases are related by the inverse change of basis matrix c^{-1}. Expanding, we find that

$$\sum_i \tilde{v}_i \otimes \tilde{\varphi}_i = \sum_i \left(\sum_j c_{i,j} \cdot v_i \right) \otimes \left(\sum_k (c^{-1})_{k,i} \cdot \varphi_i \right)$$

$$= \sum_{j,k} \left(\sum_i c_{i,j}(c^{-1})_{k,i} \right) \cdot v_i \otimes \varphi_i.$$

The definition of the inverse matrix says that $\sum_i c_{i,j}(c^{-1})_{k,i} = \begin{cases} 1 & j = k \\ 0 & \text{otherwise} \end{cases}$.

Hence, we conclude that

$$\sum_i \tilde{v}_i \otimes \tilde{\varphi}_i = \sum_i v_i \otimes \varphi_i,$$

so coev_{V_g} is well defined as desired. We now show that the rigidity diagrams commute. Going around the square, we find that this is equivalent to the condition that $1 \otimes w = \sum_i \varphi_i(w) \otimes v_i$ for all $w \in V_g$. This follows from choosing a basis such that $v_i = w$ for some i. Then, $\varphi_i(w) \otimes v_i = w$ and all the other terms are zero, making the equality obvious.

3. (Semisimplicity) Let $V \in \mathbf{Vec}_G$ be an object. It is clear that V is the direct sum of its g-components V_g, as g ranges over elements of G. Now, each component V_g is the direct sum of $\dim V_g$ copies of the vector space $\mathbb{C}_g$, which has 1-dimensional component in component g and 0-dimensions in every other component. It is clear that $\mathbb{C}_g$ is simple for all $g \in G$. Thus, V is the direct sum of simple objects.

4. Since **Vec** only consists of finite dimensional vector spaces, its hom-spaces are clearly finite dimensional. Since G is finite, the hom-spaces will be finite direct sums of finite dimensional spaces, and hence will still be finite dimensional.

5. All simple obect are of the form $\mathbb{C}_g$ for some $g \in G$. Since G is finite, we get the desired result.

6. $\mathbb{C}_e$ is clearly simple.

$\square$

Proposition 6.15. *Let G be a finite abelian group. Define the structures for a braided fusion category as follows:*

1. *(Underlying fusion category)* $\mathbf{Vec}_G$.

2. *(Braiding) Given $V, W \in \mathbf{Vec}_G$, we define β on the g-component by*

$$(V \otimes W)_g = \bigoplus_{hk=g} V_h \otimes W_k \to \bigoplus_{kh=g} W_k \otimes V_h = (W \otimes V)_g$$

where $g \in G$, and h, k run over elements of G.

These structures give a well-defined braided monoidal category.

Proof. The hexagon identities follow from unraveling definitions, so are left as exercises. $\square$

To motivate the Drinfeld center, we recall the usual center of a monoid. Namely, given a monoid G its center $\mathcal{Z}(G)$ is defined as

$$\mathcal{Z}(G) = \{g \in G \text{ s.t. } gh = hg \ \forall \ h \in G\},$$

the submonoid of elements that commute with all other elements. When defining the center of an MTC, we find ourself having a subtle issue. Commutivity in the context of monoids is replaced by braiding in the context of categories. While commutivity of monoids is a property, braiding of categories is a structure. One needs to choose a braiding, of which there can be many. The center $\mathcal{Z}(\mathscr{C})$ of an MTC $\mathscr{C}$ thus consists of elements $A \in \mathscr{C}$, along with choices of natural isomorphism between the functors $A \otimes -$ and $- \otimes A$. That is, elements of $\mathscr{C}$ that commute under $\otimes$ with every other element of $\mathscr{C}$, and a functorial choice of how that commuting should be done. These choices of commutivity are called *half-braidings*.

Proposition 6.16. *The Drinfeld center of a monoidal category $\mathscr{C}$ is a braided monoidal category defined as follows:*

- *(Objects) Pairs $(A, \beta_{A,-})$, where $A \in \mathscr{C}$, and $\beta_{A,-}$ 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*

$$\beta_{A,B\otimes C} = (\mathrm{id}_B \otimes \beta_{A,C}) \circ (\beta_{A,B} \otimes \mathrm{id}_C).$$

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

$$(\mathrm{id}_C \otimes f) \circ \beta_{A,C} = \beta_{B,C} \circ (f \otimes \mathrm{id}_C).$$

- *(Tensor product) Given $(A, \beta_{A,-}), (B, \beta_{B,-}) \in \mathcal{Z}(\mathscr{C})$, we define*

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

- *(Unit) The element $(1, \rho \circ \lambda^{-1})$*

- *(Braiding) We define the braiding between two elements $(A, \beta_{A,-}), (B, \beta_{B,-}) \in \mathcal{Z}(\mathscr{C})$ to be $\beta_{A,B} = \beta_{A,B}$.*

Inheriting associativity, unitors, and composition from $\mathscr{C}$, this gives $\mathcal{Z}(\mathscr{C})$ the structure of a braided monoidal category.

Proof. Since morphisms in $\mathcal{Z}(\mathscr{C})$ are a subspace of morphisms in $\mathscr{C}$, commutative diagrams don't change when going from $\mathscr{C}$ to $\mathcal{Z}(\mathscr{C})$. Hence, the triangle and pentagon axioms for $\mathcal{Z}(\mathscr{C})$ follow immediately from the triangle and pentagon axioms on $\mathscr{C}$. One thing to be checked is that evaluation/co-evaluaiton satisfy the compatibility condition required to a morphism in $\mathcal{Z}(\mathscr{C})$, but this is straightforward. We remark on the hexagon identities. The condition imposed on $\beta_{A,B\otimes C}$ given is technically incorrect. To make the parentheses work in the braiding one has to add associators, and impose the longer condition

$$\beta_{A,B\otimes C} = \alpha^{-1}_{C,A,B} \circ (\mathrm{id}_B \otimes \beta_{A,C}) \circ \alpha_{A,C,B} \circ (\beta_{A,B} \otimes \mathrm{id}_C) \circ \alpha^{-1}_{A,B,C}.$$

This condition makes the second hexagon identity tautological. Similarly, the definition of tensor product given is not strictly correct - one must add the correct associator terms, making the first hexagon identity tautological.

Lastly one must verify the half-braidings defined on the tensor unit/tensor product are actually half braidings, i.e., that they satisfy the hexagon condition. The fact that the condition is satisfied for the tensor unit follows in a straightforward fashion from the triangle identity. The fact that the condition is satisfied for the tensor product follows from the following computation, where $A, B \in \mathcal{Z}(\mathscr{C})$, $C, D \in \mathscr{C}$:

$$\beta_{A \otimes B, C \otimes D} = (\beta_{A, C \otimes D} \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \beta_{B, C \otimes D})$$
$$= (\mathrm{id}_C \otimes \beta_{A,D} \otimes \mathrm{id}_B) \circ (\beta_{A,C} \otimes \mathrm{id}_D \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \mathrm{id}_C \otimes \beta_{B,D}) \circ (\mathrm{id}_A \otimes \beta_{B,C} \otimes \mathrm{id}_D)$$
$$= (\mathrm{id}_C \otimes \beta_{A,D} \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \mathrm{id}_C \otimes \beta_{B,D}) \circ (\beta_{A,C} \otimes \mathrm{id}_D \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \beta_{B,C} \otimes \mathrm{id}_D)$$
$$= (\mathrm{id}_C \otimes \beta_{A \otimes B, D}) \circ (\beta_{A \otimes B} \otimes \mathrm{id}_D).$$

Note the key use of the fact that the central terms in the composition could be freely exchanged, since they act by non-identity on a disjoint set of tensor factors. This completes the proof.

$\square$

Proposition 6.17. *Let $\mathscr{C}$ be a fusion category. Define the following data for a fusion category:*

1. *(Underlying $\mathbb{C}$-linear abelian monoidal category) $\mathcal{Z}(\mathscr{C})$, with vector space structure on hom-spaces inherited from $\mathscr{C}$.*

2. *(Duals) Given $(A, \beta_{A,-}) \in \mathcal{Z}(\mathscr{C})$, we define the dual to be $(A^*, \beta_{A^*,-})$, where $\beta_{A^*,-}$ is the composition*

$$A^* \otimes - \xrightarrow{\mathrm{coev}_A} A^* \otimes - \otimes A^* \otimes A \xrightarrow{\beta_{A,-}} A^* \otimes A \otimes - \otimes A^* \xrightarrow{\mathrm{ev}_A} - \otimes A^*.$$

Along with canonical evaluation and co-evaluation maps inherited from $\mathscr{C}$, this gives $\mathcal{Z}(\mathscr{C})$ the structure of a braided fusion category.

Proof. To begin, we need to show that $\mathcal{Z}(\mathscr{C})$ with this vector space structure on hom-spaces is is indeed $\mathbb{C}$-linear abelian. We demonstrate the axioms one at a time.

1. (Has a zero object) Let $0 \in \mathscr{C}$ be the zero object. It is clear that $0 \otimes A \cong 0$ for all $A \in \mathscr{C}$, and hence the defining property of the zero object says that there is a unique map $0 \times A \to A \times 0$. Thus, there is a unique half-braiding $\beta_{0,-}$. It is straightforward to verify that $(0, \beta_{0,-}) \in \mathscr{C}$ is a zero object.

2. (Has binary biproducts) Choose $A, B \in \mathcal{Z}(\mathscr{C})$. We define a canonical half braiding $\beta_{A \oplus B,-}$ on $A \oplus B$ by the following formula, for all $C \in \mathscr{C}$:

$$(A \oplus B) \otimes C \xrightarrow{\sim} (A \otimes C) \oplus (B \otimes C)$$
$$\xrightarrow{\beta_{A,C} \oplus \beta_{B,C}} (C \otimes A) \oplus (C \otimes B)$$
$$\xrightarrow{\sim} C \otimes (A \oplus B).$$

Here, the top and bottom maps are the isomorphisms of Exercise 6.8 (a). It is straightforward to verify that $(A \oplus B, \beta_{A \oplus B})$ satisfies the axioms of a biproduct, completing our proof.

3. (Has kernels and cokernels) We demonstrate that $\mathcal{Z}(\mathscr{C})$ has kernels, and leave the construction of cokernels as an exercise. Let $f : A \to B$ be a morphism, with $A, B \in \mathcal{Z}(\mathscr{C})$, whose kernel we wish to show exists. By Exercise 6.8 (b), there is a canonical isomorphism $\ker(f \otimes \mathrm{id}_C) \cong \ker f \otimes C$. The universal property of the kernel allows us to obtain a unique map $\beta_{\ker f, C} : \ker f \otimes C \to C \otimes \ker f$ making the following diagram commute:

$$
\begin{array}{ccc}
B \otimes C & \xrightarrow{\ \beta_{B,C}\ } & C \otimes B \\
\Big\uparrow{\scriptstyle f \otimes \mathrm{id}_C} & & \Big\uparrow{\scriptstyle \mathrm{id}_C \otimes f} \\
0 \Big(\ A \otimes C & \xrightarrow{\ \beta_{A,C}\ } & C \otimes A \ \Big) 0 \\
\Big\uparrow & & \Big\uparrow \\
\ker A \otimes C & \xdashrightarrow{\ \beta_{\ker A, C}\ } & C \otimes \ker A
\end{array}
$$

It is straightforward to show to show that $(\ker f, \beta_{\ker,-})$ is a valid element of $\mathcal{Z}(\mathscr{C})$, and is the kernel of f. This completes the proof.

4. (All monomorphisms and epimorphisms are normal) Endowing kernels/cokernels with their canonical half-braidings, this is immediate.

We now move on to showing that $\mathcal{Z}(\mathscr{C})$ is really a braided fusion category, one axiom at a time.

1. Linearity of $\mathcal{Z}(\mathscr{C})$ follows from the linearity of $\mathscr{C}$.

2. (Rigidity) Diagrams commuting in $\mathscr{C}$ implies they commute in $\mathcal{Z}(\mathscr{C})$, hence rigidity is immediate. However, one does need to make sure that $\beta_{A^*,-}$ is a valid half-braiding. Graphically, $\beta_{A^*,B}$ is given the compostion

Hence, we can compute as follows:

Additionally we must check that ev and coev satisfy the compatibility condition required to be morphisms in $\mathcal{Z}(\mathscr{C})$. This is straightforward, and we ommit the proof.

3. (Semisimplicity) Suppose $A \in \mathcal{Z}(\mathscr{C})$ has a decomposition $A \cong A_0 \oplus A_1$ in $\mathscr{C}$. We can canonically define the half braiding $\beta_{A_0,-}$ by being the composition

$$A_0 \otimes B \xrightarrow{i_0 \otimes B} A \otimes B \xrightarrow{\beta_{A,B}} B \otimes A \xrightarrow{\mathrm{id}_B \otimes \pi_0} B \otimes A_0,$$

and similarly for $\beta_{A_1,-}$. It is straightforward to verify that these are half-braidings, giving A_0 and A_1 the structure of elements in $\mathcal{Z}(\mathscr{C})$. Moreover, one can verify that the isomorphism $A \cong A_0 \oplus A_1$ is in $\mathcal{Z}(\mathscr{C})$. Hence, every decomposition in $\mathscr{C}$ gives a decomposition in $\mathcal{Z}(\mathscr{C})$. If the underlying $\mathscr{C}$-object of a $\mathcal{Z}(\mathscr{C})$-object is simple, then that $\mathcal{Z}(\mathscr{C})$-object must be simple. Hence, since every element is the $\mathscr{C}$-direct sum of simple $\mathscr{C}$ objects we conclude that every object is the $\mathcal{Z}(\mathscr{C})$-direct sum of simple $\mathcal{Z}(\mathscr{C})$ objects.

4. All hom-spaces in $\mathcal{Z}(\mathscr{C})$ are subspaces of hom-spaces in $\mathscr{C}$, hence they must be finite dimensional.

5. From the discussion of semisimplicity, we find that simple objects in $\mathcal{Z}(\mathscr{C})$ are exactly those objects whose underlying $\mathscr{C}$-object is simple. We first prove a lemma: on a given simple object $A \in \mathscr{C}$, the half-braidings on A are linearly independent as elements of the vector space $\bigoplus_{B \in \mathscr{C}} \mathrm{Hom}(A \otimes B, B \otimes A)$.

Suppose we had a non-trivial linear relationship of half-braidings $\beta_{A,-} = \sum_{i \in I} \lambda_i \cdot \beta_{A,-}^{(i)}$, for some finite indexing set I. The hexagon identity tells us that for any $B, C \in \mathscr{C}$

$$\left(\sum_{i\in I}\lambda_i \cdot \beta_{A,C}^{(i)}\right) \circ \left(\sum_{i\in I}\lambda_i \cdot \beta_{A,B}^{(i)}\right) = \sum_{i\in I}\lambda_i \cdot \beta_{A,C}^{(i)} \circ \beta_{A,B}^{(i)}.$$

Without loss of generality, we can assume that the $\left\{\beta_{A,-}^{(i)}\right\}$ are linearly independent; otherwise we could have chosen a smaller linear relationship. Expanding both sides of the formula and using the bilinearity of composition, we find that there must be exactly one non-zero value of λ_i, and that that value satisfies $\lambda_i^2 = \lambda_i$, hence must be 1. Thus, $\beta_{A,-} = \beta_{A,-}^{(i)}$ for some $i \in I$. This contradicts the fact that the linear relationship was non-trivial, concluding the proof of the lemma.

If two half-braidings are equal on simple elements, then semisimplicity implies they are equal everywhere. Hence, the lemma tells us that the isomorphism classes of simple objects of $\mathcal{Z}(\mathscr{C})$ are a linearly independent subset of

$$\bigoplus_{a,b\in\mathscr{L}} \mathrm{Hom}(A \otimes B, B \otimes A),$$

where $\mathscr{L}$ is the set of isomorphism classes of simple objects of $\mathscr{C}$, and A (resp. B) is a representative of a (resp. b). Thus, we find that the number of isomorphism classes of simple objects in $\mathcal{Z}(\mathscr{C})$ is bounded above by the finite quantity

$$\sum_{a,b\in\mathscr{L}} \dim \mathrm{Hom}(a \otimes b, b \otimes a),$$

finishing the proof. Note that this equality can be tight (such as in the case of the toric code).

6. The unit 1 is simple by the above discussion.

$\square$

In general, not every fusion category's center will be an MTC. The categories whose centers are MTCs are, in fact, spherical fusion categories.

Proposition 6.18. *Let $\mathscr{C}$ be a spherical fusion category. Define the following data for a ribbon fusion category:*

1. *(Underlying braided fusion category) $\mathcal{Z}(\mathscr{C})$.*

2. *(Twist) Given $(A, \beta_{A,-}) \in \mathscr{C}$, we define the twist $\theta_{(A,\beta_{A,-})}$ by the composition*

$$\beta_{A,A^*}\ \begin{array}{c} A \\ \text{(diagram)} \\ A \end{array}$$
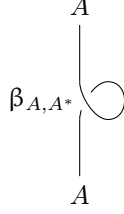
This gives $\mathcal{Z}(\mathscr{C})$ the structure of an MTC.

Proof. .[WORK: It might be useful to look at Etingof's fusion categories book. For instance, Example 8.5.4 and Proposition 8.6.3, Corollary 8.20.13]We verify the axioms one at a time.

1. .[WORK: BRAID Do the proof.]

2. .[WORK: BRAID This seems really annoying as well.]

3. (Non-degeneracy) .[WORK: BRAID How do I define the right half-braiding? Hopefully there's an explicit construction...]

$\square$

We can apply to construct MTCs from G-graded vector spaces:

Proposition 6.19. *Let G be a finite group. The double dual maps on vector spaces*

$$V \xrightarrow{\sim} V^{**}$$
$$v \mapsto (\varphi \mapsto \varphi(v))$$

induces a natural isomorphim between the identity functor and the double dual functor on $\mathbf{Vec}_G$. This gives $\mathbf{Vec}_G$ the structure of a spherical fusion category.

Proof. .[WORK: Do proof] $\square$

Thus, we have arrived at the MTC associated with the toric code: $\mathcal{Z}(\mathbf{Vec}_{\mathbb{Z}_2})$, the Drinfeld center of of the category of $\mathbb{Z}_2$ graded vector spaces. This is in some sense the simplest MTC. Namely, the simplest MTCs are those which come from spherical fusion categories, $\mathcal{Z}(\mathscr{C})$ for some $\mathscr{C}$. The simplest fusion categories are those which come from groups, $\mathbf{Rep}_G$ for some G. The simplest non-trivial group is $\mathbb{Z}_2$.

Another intuition for $\mathcal{Z}(\mathscr{C})$, alluded to in the introduction of this section, is that it is a sort of "quantum double" [dF17]. The intuition for why $\mathcal{Z}$ can be viewed as gluing two copies of $\mathscr{C}$ with a twist is seen as follows. Suppose $(\mathscr{C}, \beta)$

is a braided monoidal category. Then, there is a canonical braided monoidal functor

$$\mathscr{C} \to \mathcal{Z}(\mathscr{C}).$$
$$A \mapsto (A, \beta_{A,-})$$

Let $\mathscr{C}^{\mathrm{rev}}$ denote the braided monoidal category whose underlying monoidal category is $\mathscr{C}$, but the braiding between A, B is given by $\beta_{B,A}^{-1}$ instead of $\beta_{A,B}$.[21] That is, the same category but with braiding reversed. There is a canonical braided monoidal functor

$$\mathscr{C}^{\mathrm{rev}} \to \mathcal{Z}(\mathscr{C}).$$
$$A \mapsto (A, \beta_{-,A}^{-1})$$

These two functors in some sense generate $\mathcal{Z}(\mathscr{C})$, and thus $\mathcal{Z}(\mathscr{C})$ can be seen as $\mathscr{C}$ and $\mathscr{C}^{\mathrm{rev}}$ glued together in a non-degenerate fashion. This doubling is numerically seen in the following proposition:

Proposition 6.20. *Let $\mathscr{C}$ be a spherical category. We have that $\dim \mathcal{Z}(\mathscr{C}) = (\dim \mathscr{C})^2$. Moreover, both Gauss sums for $\mathcal{Z}(\mathscr{C})$ are equal, $p_{\mathcal{Z}(\mathscr{C})}^{\pm} = \dim \mathscr{C}$.*

Proof. . [WORK: Do proof] □

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

Proposition 6.21. *Applying the process in Proposition 6.4 to $\mathcal{Z}(\mathbf{Vec}_{\mathbb{Z}_2})$ recovers the MTC data for the toric code, as detailed at the end of subsection 6.1*

Proof. .[WORK: do proof. This should come down to explicitly giving a set of representatives of isomorphism classes of simple objects for $\mathcal{Z}(\mathbf{Vec}_{\mathbb{Z}_2})$. Then, showing that they satisfy the correct conditions shouldn't be too hard.] □

Exercises:

6.1. The standard definition of topological quantum field theory (TQFT) is in terms of functors, which we present here.

   (a) Define the following structures for a braided monoidal category:

      i. (Objects) Closed oriented n-manifolds.

---

[21] $\mathscr{C}^{\mathrm{rev}}$ is *not* equal to $\mathscr{C}^{\mathrm{op}}$.

    ii. (Morphisms) A morphism between closed oriented n-manifolds Y_0, Y_1 is an oriented $(n+1)$-manifolds X such that

$$\partial X = Y_0 \sqcup Y_1,$$

    where Y_1 has the correct induced orientation from X and Y_0 has opposite induced orientation.

    iii. (Composition) Union.

    iv. (Tensor product) $Y_0 \otimes Y_1 = Y_0 \sqcup Y_1$.

    v. (Unit) $\emptyset$

    Letting the associativity, left/right unitors, and braiding, be the identity, show that this forms a braided monoidal category, $\mathbf{Bord}(n+1)$.

(b) Define an $(n+1)$-TQFT to be a braided monoidal functor $\mathbf{Bord}(n+1) \to \mathbf{Vec}$. Show that this definition is canonically equivalent to the definition given in section 4 when $n = 2$.

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

6.3. Let $\mathscr{C}$ be an MTC, and let $\mathscr{L}$ be the set of isomorphism classes of simple objects. Then, [WORK: doing what? Apparently one just takes the trace of the "twisting relation"...] the coefficients of the S-matrix of $\mathscr{C}$ can be expressed in terms of the twist, fusion coefficients, and quantum dimensions as follows:

$$s_{a,b} = \frac{1}{\theta_a \theta_b} \sum_{c \in \mathscr{L}} N_c^{a^*,b} d_c \theta_c.$$

By [WORK: doing what?], one arrives the the *Verlinde formula* for MTCs:

$$N_c^{a,b} = \sum_{d \in \mathscr{L}} \frac{s_{a,d} s_{b,d} s_{c^*,d}}{\dim \mathscr{C} \cdot d_d}$$

6.4. Let $\mathscr{C}$ be a category satisfying all of the axioms of a $\mathbb{C}$-linear abelian category, except that monomorphisms and epimorphism are not necessarily normal. Let $f : A \to B$ be a morphism. Recall that f is called a kernel if it satisfies the universal property of $\ker \overline{f}$ for some morphism $\overline{f}$, and f is called a cokernel if it satisfies the universal property of $\operatorname{coker} \overline{f}$ for some morphism $\overline{f}$.

(a) If f is a kernel it must be a monomorphism.

(b) If f is a kernel, it must be an epimorphism.

(c) f is a kernel if and only if f satisfies the universal property of $\ker(\operatorname{coker} f)$.

(d) f is a cokernel if and only if f satisfies the universal property of $\operatorname{coker}(\ker f)$

(e) There is a natural map $\operatorname{coker}(\ker f) \xrightarrow{\overline{f}} \ker(\operatorname{coker} f)$ uniquely to make the below diagram commute:

$$
\begin{array}{ccccccc}
\ker f & \longrightarrow & A & \xrightarrow{\ f\ } & B & \longrightarrow & \operatorname{coker} f \\
& & \downarrow & & \uparrow & & \\
& & \operatorname{coker}(\ker f) & \dashrightarrow[\overline{f}] & \ker(\operatorname{coker} f) & &
\end{array}
$$

where the map $\operatorname{coker}(\ker f) \to B$ is first obtained by the universal property of the cokernel, and the map $\overline{f}$ is then obtained by the universal property of the kernel. Show that $\overline{f}$ is an isomorphism for all choices of f if and only if all monomorphisms and epimorphisms are normal.

6.5. There is a canonical braided monoidal functor

$$
\begin{aligned}
\mathbf{Vec} &\to \mathcal{Z}(\mathbf{Vec}), \\
V &\mapsto (V, \beta_{V,-})
\end{aligned}
$$

where $\beta_{-,-}$ is the natural braiding on the fusion category of vector spaces. Show that this is an equivalence of categories. (HINT: Since $\mathcal{Z}(\mathbf{Vec})$ is semisimple, it's enough to show that there are no non-trivial half braidings on $\mathbb{C} \in \mathbf{Vec}$. Show that this is equivalent to there being no non-trivial monoidal natural isomorphisms from the identity functor on $\mathbf{Vec}$ to itself. Finally, use the fact that the transformation is monoidal to conclude it acts by the identity on $\mathbb{C}$, and then lift to show it must act by the identity everywhere else as well)

6.6. Let A, B be objects in a $\mathbb{C}$-linear abelian category $\mathscr{C}$.

(a) Show that the direct sum $A \oplus B$ simultaneously satisfies the category-theoretic conditions of a product, as well as the dual conditions of a co-product. That is, the triple $(A \oplus B, p_A, p_B)$ is a product in $\mathscr{C}$, and the triple $((A \oplus B)^{\mathrm{op}}, (i_A)^{\mathrm{op}}, (i_B)^{\mathrm{op}})$ is a product in $\mathscr{C}^{\mathrm{op}}$. For this reason, the direct sum is often refered to as a *biproduct*.

(b) Given a morphism $f : A \to B$, show there are canonical isomorphisms $A \cong \operatorname{im} f \oplus \ker f$ and $B \cong \operatorname{im} f \oplus \operatorname{coker} f$.

6.7. Let A, B, C be objects a fusion category $\mathscr{C}$.

(a) For any $A, B, C \in \mathscr{C}$, show that the natural maps

$$
\begin{aligned}
\operatorname{Hom}(A \oplus B, C) &\to \operatorname{Hom}(A, C) \oplus \operatorname{Hom}(B, C) \\
f &\mapsto (f \circ i_A) \oplus (f \circ i_B)
\end{aligned}
$$

and

$$\operatorname{Hom}(C, A \oplus B) \to \operatorname{Hom}(A, C) \oplus \operatorname{Hom}(B, C)$$
$$f \mapsto (p_A \circ f) \oplus (p_B \circ f)$$

are isomorphisms for all $C \in \mathscr{C}$.

(b) Given a morphism $f : A \to B$ that there are canonical isomorphisms $\ker(f \otimes \operatorname{id}_C) \cong \ker f \otimes C$ and $\operatorname{coker}(f \otimes \operatorname{id}_C) \cong \operatorname{coker} f$ for all $C \in \mathscr{C}$.

6.8. Given a rigid category $\mathscr{C}$, show that pivotal structures on $\mathscr{C}$ are in canonical bijection with natural isomorphisms between the functors $(-)^{**}$ and $\operatorname{id}_{\mathscr{C}}$.

6.9. Let $\mathscr{C}$ be a rigid monoidal category. Fix the following statements:

(i) $\mathscr{C}$ admits a twisting natural transformation $\theta : \operatorname{id}_{\mathscr{C}} \to \operatorname{id}_{\mathscr{C}}$, satisfying the compatibility axioms $(\theta_A)^* = \theta_{A^*}$ and $\theta_{A \otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$, just as in the definition of MTC.

(ii) $\mathscr{C}$ admits a pivotal structure such that [WORK: what is the correct condition? Seems like I will have to do something fancy.]

Just as with MTCs, twists θ induce pivotal structures. Conversely, any pivotal structure satisfying the condition of (ii) gives a twisting by [WORK: what process? Seems fancy again.]. Show that these two processes are well defined and are inverses of one another, hence given an equivalence between statements (i) and (ii). A rigid monoidal category satisfying either of these conditions is called a *ribbon* monoidal category. Thus, MTCs can be defined as "non-degenerate ribbon fusion categories".

6.10. . [WORK: Define the Deligne tensor product. Show that there is a map $\mathscr{C} \boxtimes \mathscr{C}^{rev} \to \mathcal{Z}(\mathscr{C})$. Can I walk people through the proof that this is an isomorphism if and only if $\mathscr{C}$ is modular?]. [WORK: This whose "property vs. structure" buisness is messing me up. Given a braided fusion category, is being modular a property or a structure?]

6.11. .[WORK: Frobenius-Schur indicator exercise? I think it might be a bit unnecarily actually.]

7 Topological Quantum Computing

7.1 The TQC framework

[WORK: Change particle types from A, B, C to X, Y, Z.]

[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: Find full correct reference to TQFT/MTC correspondence (I think the best is here: [BDSPV15]) Can I find one for the unitary case?]

[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!

This sort of "TQC $\implies$ QC" has an analogy to the process of "QC $\implies$ classical", which can be seen as a big motivation for QC. Namely, quantum algorithms can be used to construct or prove things about classical algorithms in various areas, such as cryptography [Reg09] and machine learning [Tan19].]

[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 + necessary 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[22]

---

[22][WORK: make description][Aub19]

]

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

[WORK: Here's a good motivation for the non-degeneracy condition. We want MTCs to give TQFTs. In particular, we need a map from automorphisms of a surface (mapping class group!) to automorphisms of a vector space. Now, there is the celebrated result that MCG(torus)=$SL_2(\mathbb{Z})$. Letting $(V_{\mathscr{C}}, Z_{\mathscr{C}})$ denote the TQFT attached to $\mathscr{C}$, we can very explicitly in this case write out the commutative diagram

$$\mathrm{Aut}(\bigcirc) \xrightarrow{Z_{\mathscr{C}}} \mathrm{Aut}(V(\bigcirc))$$
$$\| \qquad\qquad \|$$
$$SL_2(\mathbb{Z}) \xrightarrow{\rho_{\mathscr{C}}} \mathrm{Aut}(\mathbb{C}[\mathscr{L}])$$

that is, the TQFT mapping class group representation on the torus is the MTC modular representation. For this to be an actual representation, we need the S matrix to be invertible. It is a miracle that this implies all other MCG reps are reps, as well as other axioms of a TQFT (not too surprising tho, since all other surfaces are more-holed torii). . "A certain invertible physical process should give an invertible quantum transformation, i.e., a matrix with nonzero determinant". Also, this $\implies$ that S matrix non-degeneracy is the "correct" way of thinking about non-degeneracy.]

[WORK: From the above, we can also give the intuation of a TQFT as (roughly) a collection of compatible mapping class group representations.]

7.2 Revisiting toric code TQC

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

7.3 Universal TQC with Fibonacci anyons

.[WORK: introduces Fibonacci anyon. Prove they are universal with braiding alone. Really what I want to do is show that any form of TQC is universal, but I just think Fibonacci will be simplest. If anyone has a definition it should be here: [TTWL08]. There's a cool physics paper which motivates the fact that the Fibonacci anyon can't be made in the lab [FGH+12].]

[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 with 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: 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 3.2. These non-trivial cycles correspond exactly to the continuous vector fields described in the introduction [Fra57].

Loosely, we will call two cycles homologous 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., homologous 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, and let $Z_1(X; \mathbb{Z}_2)$ be the subgroup generated by the cycles consisting of 1s along the boundaries of single 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 homologous if they are in the same coset of $H_1(X; \mathbb{Z}_2)$. Alternatively, two elements are homologous 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 in 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 $H_1(X)$. The groups are related by the fact that $H_1(X)$ is the abelianization of $\pi_1(X)$, i.e., the maximal abelian quotient of $\pi_1(X)$. 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   Unitarity

B.1   Unitary TQFTs

Topological quantum field theories (TQFTs) and modular tensor categories (MTCs) were both defined in terms of vector spaces. However, quantum mechanics is based on the stricter notion Hilbert spaces. This can be rectified by imposing the condition of *unitarity* on TQFTs and MTCs. Simply speaking, unitarity functorially imposes a † operation, mimicking the conjugate transpose, which is compatible with all structures at hand. The unitary condition for TQFTs can be stated as follows:

Definition (Unitary (2+1) Topological Quantum Field Theory). A unitary (2+1) topological quantum field theory is the following data:

1. A (2+1)-TQFT (V, Z).

2. (Conjugation) A linear map $\dagger : \text{Hom}(V(S_0), V(S_1)) \to \text{Hom}(V(S_1), V(S_0))$ for all surfaces S_0, S_1.

Additionally, a unitary topological quantum field theory is required to satisfy the following properties:

1. (Preserves conjugation) $Z\left(X^\dagger\right) = Z(X)^\dagger$. Here S_0, S_1 are surfaces, and X is a bordism from S_0 to S_1. We define $X^\dagger : S_1 \to S_0$ to be the bordism which is the same underlying manifold, but with its orientation reversed.

2. (Unitarity) The map $\langle\cdot|\cdot\rangle : \mathrm{Hom}(V(S_0), V(S_1)) \times \mathrm{Hom}(V(S_0), V(S_1)) \to \mathbb{C}$ defined by $\langle f|g\rangle = \mathrm{tr}(f \circ g^\dagger)$ is an inner product, endowing $\mathrm{Hom}(V(S_0), V(S_1))$ with the structure of a Hilbert space.

3. $(f^\dagger)^\dagger = f$ for all $f \in \mathrm{Hom}(V(S_0), V(S_1))$, S_0, S_1 surfaces.

4. $(f \circ g)^\dagger = g^\dagger \circ f^\dagger$ for all $f \in \mathrm{Hom}(V(S_1), V(S_2))$, $g \in \mathrm{Hom}(V(S_0), V(S_1))$, S_0, S_1, S_2 surfaces.

5. $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$ for all $f \in \mathrm{Hom}(V(S_2), V(S_3))$, $g \in \mathrm{Hom}(V(S_0), V(S_1))$, S_0, S_1, S_2, S_3 surfaces.

$\square$

In the case of the $\mathbb{Z}_2$ Dijkgraaf-Witten theory, this is obvious to do. Namely, the vector spaces $V(S) = \mathbb{C}[H_1(S; \mathbb{Z}_2)]$ comes equipped with a canonical basis, and hence inherits the structure of a Hilbert space. We define $\dagger$ by taking the conjugate transpose. That is, given $f : V(Y_0) \to V(Y_1)$ we define $f^\dagger$ to be the unique map such that

$$\langle f(v), w \rangle = \langle v, f^\dagger(w) \rangle$$

for all $v \in V(Y_0)$, $w \in V(Y_1)$ (see Exercise 2.2). All that is left to check is that the axioms are satisfied:

Proposition B.1. *The $\mathbb{Z}_2$ Dijkgraaf-Witten theory is a unitary (2+1)-TQFT.*

Proof. Working through the axioms is straightforward, and left as an exercise.
$\square$

This concludes our treatment of unitary TQFTs.

B.2 Unitary MTCs

The unitarity condition on MTCs can be stated very explicitly on the level of $6j$-symbols. Unitarity is best studied first as a property first defined on $6j$ fusion systems, and then extended to modular tensor fusion systems:

Definition (Unitary $6j$ fusion system)**.** A unitary $6j$ fusion system is a $6j$ fusion system $\mathscr{L}$ which is gauge equivalent to a $6j$ fusion system $\mathscr{L}'$ such that $F_d^{a,b,c}$ is a unitary matrix for all $a, b, c, d \in \mathscr{L}'$.

$\square$

Definition (Unitary modular tensor fusion system)**.** A unitary modular tensor fusion system is a modular tensor fusion system which is braided gauge equivalent to a modular tensor fusion system $\mathscr{L}'$ such that $F_d^{a,b,c}$ is a unitary matrix for all $a, b, c, d \in \mathscr{L}'$. [WORK: Are these conditions correct? Do I need to force the fusion matrices and braiding matrices to be unitary as well?]

$\square$

We now proceed in category-theoretic language.

Definition (Unitary fusion category). A unitary fusion category is the following data:

1. An fusion category $\mathscr{C}$.

2. (Conjugation) A linear map $\dagger : \mathrm{Hom}(A, B) \to \mathrm{Hom}(B, A)$ for all $A, B \in \mathscr{C}$.

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

1. (Unitarity) Given $f : A \to A$ an endomorphism of $A \in \mathscr{C}$, define

$$\mathrm{tr}(f) = \mathrm{ev}_A \circ (\mathrm{id}_{A^*} \otimes f) \circ (\mathrm{ev}_A)^\dagger.$$

The map $\langle \cdot | \cdot \rangle : \mathrm{Hom}(A, B) \times \mathrm{Hom}(A, B) \to \mathbb{C}$ defined by $\langle f | g \rangle = \mathrm{tr}(f \circ g^\dagger)$ is an inner product, endowing $\mathrm{Hom}(A, B)$ with the structure of a Hilbert space.

2. $\left(f^\dagger \right)^\dagger = f$ for all $f \in \mathrm{Hom}(A, B)$, $A, B \in \mathscr{C}$.

3. $(f \circ g)^\dagger = g^\dagger \circ f^\dagger$ for all $f \in \mathrm{Hom}(B, C)$, $g \in \mathrm{Hom}(A, B)$, $A, B, C \in \mathscr{C}$.

4. $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$ for all $f \in \mathrm{Hom}(A, B)$, $g \in \mathrm{Hom}(C, D)$, $A, B, C, D \in \mathscr{C}$.

5. $(\mathrm{coev}_A)^\dagger \circ (f \otimes \mathrm{id}_{A^*}) \circ \mathrm{coev}_A = \mathrm{tr}(f)$ for all $A \in \mathscr{C}$

$\square$

Unitary fusion categories make for a pleasant object of study because the distinguished maps $(\mathrm{ev}_A)^\dagger : 1 \to A^* \otimes A$ and $(\mathrm{coev}_A)^\dagger : A \otimes A^* \to 1$ induce a spherical structure:

Proposition B.2. *All unitary fusion categories are spherical.*

Proof. .[WORK: Should be literally trivial...] $\square$

We can now define unitary MTCs. The compatibility conditions for the twist are chosen so that the definition of trace as an MTC and the definition of trace as a unitary fusion category coincide.

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

1. An MTC $\mathscr{C}$.

2. (Conjugation) A linear map $\dagger : \mathrm{Hom}(A, B) \to \mathrm{Hom}(B, A)$ for all $A, B \in \mathscr{C}$.

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

1. Forgetting the twist and braiding, $(\mathscr{C}, \dagger)$ forms a unitary fusion category.

2. $(\beta_{A,B})^\dagger = \beta_{A,B}^{-1}$ for all $A, B \in \mathscr{C}$.

3. $(\theta_A)^\dagger = (\theta_A)^{-1}$ for all $A \in \mathscr{C}$.

4. $(\mathrm{ev}_A)^\dagger = \left(\mathrm{id}_{A^*} \otimes \theta_A^{-1}\right) \circ \beta_{A^*,A}^{-1} \circ \mathrm{coev}_A$ for all $A \in \mathscr{C}$

5. $(\mathrm{coev}_A)^\dagger = \mathrm{ev}_A \circ \beta_{A,A^*} \circ (\theta_A \otimes \mathrm{id}_{A^*})$ for all $A \in \mathscr{C}$

$\square$

An important point to note is that even without enforcing a unitarity condition, there will naturally be unitary properties afoot:

Theorem B.1 ([ENO05])**.** *Let $\mathscr{C}$ be an MTC, and $\mathscr{L}$ be the set of isomorphism classes of simple objects. The modular representation*

$$\rho_\mathscr{C} : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Aut}(\mathbb{C}[\mathscr{L}])$$

is unitary, in the sense that all matrices in the image are unitary. In particular, the S-matrix of every MTC is unitary.

Since unitary fusion categories are spherical, Proposition 6.18 implies their centers are MTCs. Further, they can canonically be made unitary:

Proposition B.3. *$\mathcal{Z}(\mathscr{C})$ inherits a canonical conjugation structure from $\mathscr{C}$, endowing it with the structure of a unitary MTC.*

Proof. . [WORK: BRAID do proof.] $\square$

Of course, as always there is an equivalence between the language of fusion systems and the language of categories:

Proposition B.4. *Let $\mathscr{C}$ be a multiplicity-free fusion category. The construction in Proposition 6.3 gives a unitary $6j$ fusion system if and only if there exists a unitary structure on $\mathscr{C}$.*

Similarly, let $\mathscr{C}$ be a multiplicity-free modular tensor category. The construction in Proposition 6.4 gives a unitary modular tensor fusion system if and only if there exists a unitary structure on $\mathscr{C}$.

Proof. We give proofs of these results in Appendix C. $\square$

We now define a unitary structure on the MTC associated with the toric code, $\mathcal{Z}(\mathbf{Vec}_{\mathbb{Z}_2})$. The main point is that the categories **Vec** of finite dimensional vector spaces and **Hilb** of finite dimensional Hilbert spaces are (non-canonically) equivalent. This allows one to endow $\mathbf{Vec}_G$ (again, non-canonically) with the structure of a unitary fusion category. Taking Drinfeld centers this endows $\mathcal{Z}(\mathbf{Vec}_{\mathbb{Z}_2})$ with the structure of a unitary MTC. Formally, we have the following:

Proposition B.5. *There is a braided monoidal equivalence of categories* **Vec** $\xrightarrow{\sim}$ **Hilb**.

Proof. Let $F :$ **Hilb** $\to$ **Vec** be the forgetful functor, assigning to each Hilbert space its underlying vector space. Morphisms of Hilbert spaces and exactly linear maps of vector spaces. Hence, this functor is fully faithful. Moreover, it is surjective on the level of objects since every vector space has a Hilbert space structure. The proposition follows from Exercise 6.6. $\qquad\square$

Proposition B.6. *Let G be a finite group. Fix an equivalence of categories* **Vec** $\to$ **Hilb**. *Define the data for a unitary fusion category as follows:*

1. *(Underlying fusion category)* $\mathbf{Vec}_G$.

2. *(Conjugation) Given $f : V \to W$, define $f^\dagger : W \to V$ as follows. First, endow V and W with the structure of Hilbert spaces via the equivalence* **Vec** $\to$ **Hilb**. *Then, make $f^\dagger$ act on W_g by the conjugate transpose of f.*

This gives $\mathbf{Vec}_G$ *the structure on a unitary fusion category.*

Proof. To begin we perform a useful computation on $\mathrm{tr}_{\mathbf{Vec}_G}(f)$, for morphisms $f : V \to V$, $V \in \mathbf{Vec}_G$. Namely we show that

$$\mathrm{tr}_{\mathbf{Vec}_G}(f) = \sum_{g \in G} \mathrm{tr}(f_g),$$

where $f_g : V_g \to V_g$ are the g-components of f, whose trace is defined in the standard linear algebra sense. In particular, we find when G is the trivial group that the categorical traces in **Vec** agree with the standard linear algebra traces. Moreover, from the base case of **Vec** the general case follows in a straightforward fashion from the fact that the identity component of $V^* \otimes V$ is $\bigoplus_{g \in G} V_g^* \otimes V_g$, hence we assume that G is trivial without loss of generality. Let $\{v_i\}_{i \in I}$ be a basis for V labeled by some indexing set I, and let $\{\varphi_i\}_{i \in I}$ be the dual basis of V^*. Seeing as the evaluation map assigns 1 to pairs $\varphi_i \otimes v_j$ when $i = j$ and zero otherwise, the conjugate transpose sends the vector $1 \in \mathbb{C}$ to $\sum_{i \in I} \varphi_i \otimes v_i$. That is, the co-evaluation map is the conjugate transpose of the evaluation map. The definition of trace now gives that

$$\mathrm{tr}_{\mathbf{Vec}_G}(f) = \sum_{i \in I} \varphi_i(f(v_i)).$$

The term $\varphi_i(f(v_i))$ is exactly the ith diagonal entry of the matrix representation of f in the basis v_i, and thus we recover tr as a sum of diagonal entries. Moreover, we observe that linear trace adds over direct sums. If we think of $f : V \to V$ as a linear map of the vector space $\bigoplus_{g \in G} V_g$ to itself, this lemma shows that the trace of f computed by linear algebra or category theory gives the same answer.

From this we observe that the categorical inner product $\langle \cdot | \cdot \rangle$ defined by $\langle f | g \rangle = \mathrm{tr}(f \cdot g^\dagger)$ is exactly one of the standard inner products from linear algebra, as in Proposition 2.3. Hence, unitarity follows immediately. The remaining axioms are standard facts about conjugate transposes from linear algebra. $\square$

Thus, $\mathbf{Vec}_{\mathbb{Z}_2}$ can be given the structure of a unitary fusion category. Applying Proposition B.3, this means that $\mathcal{Z}(\mathbf{Vec}_{\mathbb{Z}_2})$ has the structure of a unitary MTC, as desired. If one wishes to have a canonical unitary structure, then one can use instead the category of G-graded Hilbert spaces, $\mathbf{Hilb}_G$. It is equivalent to $\mathbf{Vec}_G$, but its unitary structure is canonical. Philosophically it is thus more correct to say that the unitary MTC associated with the toric code is $\mathcal{Z}(\mathbf{Hilb}_{\mathbb{Z}_2})$, $\mathcal{Z}(\mathbf{Vec}_{\mathbb{Z}_2})$.

As in the non-unitary case, there is an equivalence between unitary MTCs and (1-extended) unitary TQFTs. Under this equivalence, $\mathcal{Z}(\mathbf{Hilb}_{\mathbb{Z}_2})$ is identified with the unitary $\mathbb{Z}_2$ Dijkgraaf-Witten theory. [WORK: cite something]

Exercises:

B.1. We saw in Exercise 6.1 that a (2+1) TQFT can be viewed as a braided monoidal functor $\mathbf{Bord}(2+1) \to \mathbf{Vec}$. Define a unitary $(n+1)$-TQFT to be a braided monoidal functor

$$\mathbf{Bord}(n+1) \to \mathbf{Hilb}$$

such that $Z\left(X^\dagger\right) = Z(X)^\dagger$ for all bordisms X. Show that this can canonically be identified with the explicit definition of unitary TQFT when $n = 2$.

C Fusion System/MTC Correspondence

[WORK: I found the "correct" reference - [DHW13]. I should state the fact that everything lives in algebraic extensions, and that the number theoretic properties are cool and mysterious.]

While the connection between fusion categories and fusion systems is relatively straightforward, giving full proofs and constructions can be somewhat cumbersome. In this appendix we offer these proofs and constructions in full detail. To begin we work through the proof of Proposition 6.3, which says we can construct a $6j$ fusion system from a fusion category.

Proof of Proposition 6.3. . [WORK: Do the proof] $\square$

We now move on to Proposition 6.3, which says that the above construction gives a bijection between $6j$ fusion systems and (multiplicity free) fusion categories. We go in stages. First, we show that monoidally equivalent fusion categories induce gauge equivalent $6j$ fusion systems. Secondly, we canonically

construct a fusion category from a $6j$ fusion system. After showing that gauge equivalent $6j$ fusion systems give monoidally equivalent fusion categories, the last step is showing that these two constructions are inverses of one another.

Proposition C.1. *Monoidally equivalent multiplicity free fusion categories induce gauge equivalent $6j$ fusion systems.*

Proof. . [WORK: prove this] □

We now give our converse construction:

Lemma C.1. *Let $(\mathscr{L}, N_{-,-}^{-}, F_{-;-,-}^{-;-;-})$ be a $6j$ fusion system. Define the data for a fusion category $\mathscr{C}$ as follows:*

- *(Objects) Collections of objects $\{a_i\}_{i \in I}$, where I is some indexing set and $a_i \in \mathscr{L}$.*

- *(Morphisms) Given objects $\{a_i\}_{i \in I}, \{b_j\}_{j \in J} \in \mathscr{C}$, we define*

$$\mathrm{Hom}(\{a_i\}_{i \in I}, \{b_j\}_{j \in J}) = \bigoplus_{(i,j) \in I \times J} \left(\begin{cases} \mathbb{C} & a_i = b_j \\ 0 & otherwise \end{cases} \right).$$

- *(Composition) Given objects $\{a_i\}_{i \in I}, \{b_j\}_{j \in J}, \{c_k\}_{k \in K} \in \mathscr{C}$, and morphisms*

$$\{\varphi_{i,j}\}_{(i,j) \in I \times J} \in \mathrm{Hom}(\{a_i\}_{i \in I}, \{b_j\}_{j \in J})$$
$$\{\phi_{j,k}\}_{(j,k) \in J \times K} \in \mathrm{Hom}(\{b_j\}_{j \in J}, \{c_k\}_{k \in K}),$$

we define

$$\{\phi_{j,k}\}_{(j,k) \in J \times K} \circ \{\varphi_{i,j}\}_{(i,j) \in I \times J} = \left\{ \sum_{j \in J} \phi_{j,k} \varphi_{i,j} \right\}_{(i,k) \in I \times K}$$

Along with the natural structure of $\mathbb{C}$-vector spaces on hom-sets inherited from the definitions, this gives $\mathscr{C}$ the structure of a $\mathbb{C}$-linear abelian category.

Proof. . [WORK: make sure construction works] □

We will refer to elements of $\mathscr{L}$, by abuse of notation, as elements in $\mathscr{C}$. That is, given $a \in \mathscr{L}$ we associate the object $\{a\}_{i \in \{a\}}$. This means in $\mathscr{C}$ that a is simultaneously the underlying $\mathscr{L}$-element and the label.

Proposition C.2. *Let $(\mathscr{L}, N_{-,-}^{-}, F_{-;-,-}^{-;-;-})$ be a $6j$ fusion system, with associated $\mathbb{C}$-linear abelian category $\mathscr{C}$. Define the data for a fusion category as follows:*

- *(Underlying $\mathbb{C}$-linear abelian category) $\mathscr{C}$.*

- *(Tensor product) Given objects $\{a_i\}_{i \in I}, \{b_j\}_{j \in J} \in \mathscr{C}$, we define*

$$\{a_i\}_{i \in I} \otimes \{b_j\}_{j \in J} = \{c\}_{\substack{(i,j,c) \in I \times J \times \mathscr{L} \\ N^c_{a_i, b_j} = 1}}.$$

- *(Associativity) Given an admissible triple $a, b, c, d \in \mathscr{L}$, interpreted as objects in $\mathscr{C}$, we define the symbol*

$$\in \mathrm{Hom}(a \otimes b, c)$$

to mean the morphism $1_{(a,b,c)}, c$. Composing these to give bases of $\mathrm{Hom}((a \otimes b) \otimes c, d)$ and $\mathrm{Hom}(a \otimes (b \otimes c), d)$, we define a morphism $\mathrm{Hom}((a \otimes b) \otimes c, d) \to \mathrm{Hom}(a \otimes (b \otimes c), d)$ by the formula

$$= \sum_{m \in \mathscr{L}} F^{a,b,c}_{d;n,m} \cdot$$

Extending through direct sums, this canonically gives a natural transformation between the functors $\mathrm{Hom}((a \otimes b) \otimes c, -)$ and $\mathrm{Hom}(a \otimes (b \otimes c), -)$. Define $\alpha_{a,b,c} : a \otimes (b \otimes c) \to (a \otimes b) \otimes c$ to be the morphism implied by Yoneda's lemma. Varying a, b, c, this defines a natural transformation $\alpha_{-,-,-}$ between the functors $- \otimes (- \otimes -)$ and $(- \otimes -) \otimes -$, which is our associativity.

- *(Unit) $1 \in \mathscr{L}$, as an object of $\mathscr{C}$.*

- *(Duals) Given $\{a_i\}_{i \in I} \in \mathscr{C}$, we define $\{a_i\}^*_{i \in I} = \{a_i^*\}_{i \in I}$*

- *(Evaluation/co-evaluation) Given $A = \{a_i\}_{i \in I} \in \mathscr{C}$, we define $\mathrm{ev}_A : A \otimes A^* \to 1$ as the map $\{\varphi_{i,j,c}\}_{\substack{(i,j,c) \in I \times I \times \mathscr{L} \\ N^c_{a_i, a_j^*} = 1}}$ with*

$$\varphi_{i,j,c} = \begin{cases} 1 & i = j, \ c = 1 \\ 0 & otherwise \end{cases}$$

The hom-space $\mathrm{Hom}(1, A^* \otimes A)$ *has the same underlying vector space as* $\mathrm{Hom}(A \otimes A^*, 1)$, *so we define* coev_A *as the map whose underlying vector exactly in the same as* ev_A.

Along with canonical choices of unitors, this gives $\mathscr{C}$ *the structure of a fusion category.*

Proof. . [WORK: make sure construction works] □

Proposition C.3. *Gauge equivalent* $6j$ *fusion systems induce monoidally equivalent fusion categories.*

Proof. . [WORK: prove this] □

Now, we can prove the desired result:

Proof of Proposition 6.3. . [WORK: do the proof] □

This correspondence generalizes to braided monoidal fusion categories, MTCs, and unitary MTCs. We now construct the categories corresponding to braided $6j$ fusion systems:

Proposition C.4. *Let* $(\mathscr{L}, N_-^{-,-}, F_{-;-,-}^{-,-,-}, R_-^{-,-})$ *be a braided* $6j$ *fusion system, with associated fusion category* $\mathscr{C}$. *Define the data for a braided fusion category as follows:*

- *(Underlying fusion category)* $\mathscr{C}$

- *(Braiding) [WORK: Do some Yoneda lemma trick]*

Proof. . [WORK: prove this] □

Proof of Proposition 6.4. .[WORK: do proof] □

We can now move on to the case of MTCs.

Proposition C.5. *Let* $(\mathscr{L}, N_-^{-,-}, F_{-;-,-}^{-,-,-}, R_-^{-,-})$ *be a modular tensor fusion system, with associated braided fusion category* $\mathscr{C}$. *Define the data for an MTC:*

- *(Underlying braided fusion category)* $\mathscr{C}$

- *(Twist) [WORK: How is this even defined?]*

Proof. . [WORK: prove this] □

Proof of Proposition 6.6. .[WORK: do proof] □

We can now move on to the case of unitary MTCs.

Proposition C.6. *Let* $(\mathscr{L}, N_-^{-,-}, F_{-;-,-}^{-,-,-}, R_-^{-,-})$ *be a unitary modular tensor fusion system, with associated modular tensor category* $\mathscr{C}$. *Define the data for a unitary MTC:*

- *(Underlying MTC) $\mathscr{C}$*
- *(Inner product) [WORK: How is this even defined?]*

Proof. . [WORK: prove this] □

Proof of Proposition B.4. .[WORK: do proof] □

D   Anyon Data

.[WORK: Add an detailing the data for popular anyon models/MTCs. A discussion of the fillings of the Hall states and their corresponding (conjectural) models in found in [BGH+17]. Zhenghan's monograph also has a lot. In general, if there are relevant tables/numbers then they should be included here.]

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.

[AL18] Tameem Albash and Daniel A Lidar. Adiabatic quantum computation. *Reviews of Modern Physics*, 90(1):015002, 2018.

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

[BDSPV15] Bruce Bartlett, Christopher L Douglas, Christopher J Schommer-Pries, and Jamie Vicary. Modular categories as representations of the 3-dimensional bordism 2-category. *arXiv preprint arXiv:1509.06811*, 2015.

[BGH+17] Paul Bruillard, César Galindo, Tobias Hagge, Siu-Hung Ng, Julia Yael Plavnik, Eric C Rowell, and Zhenghan Wang. Fermionic modular categories and the 16-fold way. *Journal of Mathematical Physics*, 58(4):041704, 2017.

[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.

[Bru00] Alain Bruguieres. Catégories prémodulaires, modularisations et invariants des variétés de dimension 3. *Mathematische Annalen*, 316(2):215–236, 2000.

[BSS06] Parsa Bonderson, Kirill Shtengel, and Joost K Slingerland. Probing non-abelian statistics with quasiparticle interferometry. *Physical review letters*, 97(1):016401, 2006.

[BW96] John Barrett and Bruce Westbury. Invariants of piecewise-linear 3-manifolds. *Transactions of the American Mathematical Society*, 348(10):3997–4022, 1996.

[BW99] John W Barrett and Bruce W Westbury. Spherical categories. *Advances in Mathematics*, 143(2):357–375, 1999.

[CM22] Alexander Cowtan and Shahn Majid. Quantum double aspects of surface code models. *Journal of Mathematical Physics*, 63(4):042202, 2022.

[CS09] NR Cooper and Ady Stern. Observable bulk signatures of non-abelian quantum hall states. *Physical review letters*, 102(17):176807, 2009.

[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.

[DHW13] Orit Davidovich, Tobias Hagge, and Zhenghan Wang. On arithmetic modular categories. *arXiv preprint arXiv:1305.2229*, 2013.

[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.

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

[EG79]   Murray Eisenberg and Robert Guy. A proof of the hairy ball the-
           orem. *The American Mathematical Monthly*, 86(7):571–574, 1979.

[ENO05]   Pavel Etingof, Dmitri Nikshych, and Viktor Ostrik. On fusion cat-
           egories. *Annals of Mathematics*, pages 581–642, 2005.

[FGH+12]   Michael H Freedman, Jan Gukelberger, Matthew B Hastings, Si-
           mon Trebst, Matthias Troyer, and Zhenghan Wang. Galois conju-
           gates of topological phases. *Physical Review B*, 85(4):045414, 2012.

[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. Simula-
           tion of topological field theories by quantum computers. *Commu-
           nications 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. *Com-
           munications in Mathematical Physics*, 227:605–622, 2002.

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

[FS19]   Brendan Fong and David I Spivak. *An invitation to applied category
           theory: seven sketches in compositionality*. Cambridge University
           Press, 2019.

[GHS23]   Azat M Gainutdinov, Jonas Haferkamp, and Christoph Schweigert.
           Davydov-yetter cohomology, comonads and ocneanu rigidity. *Ad-
           vances 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 Math-
           ematics*, 11(04):615–637, 2009.

[JS86]   André Joyal and Ross Street. Braided monoidal categories. *Math-
           ematics Reports*, 86008, 1986.

[JS06]   André Joyal and Ross Street. An introduction to tannaka dual-
           ity and quantum groups. In *Category Theory: Proceedings of the
           International Conference held in Como, Italy, July 22–28, 1990*,
           pages 413–492. Springer, 2006.

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

[Kel64] Gregory Maxwell Kelly. On maclane's conditions for coherence of natural associativities, commutativities, etc. *Journal of Algebra*, 1(4):397–402, 1964.

[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.

[KP06] Alexei Kitaev and John Preskill. Topological entanglement entropy. *Physical review letters*, 96(11):110404, 2006.

[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.

[ML13] Saunders Mac Lane. *Categories for the working mathematician*, volume 5. Springer Science & Business Media, 2013.

[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.

[NS10] Siu-Hung Ng and Peter Schauenburg. Congruence subgroups and generalized frobenius-schur indicators. *Communications in Mathematical Physics*, 300(1):1–46, 2010.

[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.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

[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.

[Sch09] Urs Schreiber. Aqft from n-functorial qft. *Communications in Mathematical Physics*, 291:357–401, 2009.

[Seg88] Graeme B Segal. The definition of conformal field theory. *Differential geometrical methods in theoretical physics*, pages 165–171, 1988.

[Sel11] Peter Selinger. A survey of graphical languages for monoidal categories. *New structures for physics*, pages 289–355, 2011.

[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.

[Sto14] Stephan Stolz. *Topology and Field Theories*, volume 613. American Mathematical Society, 2014.

[Tan19] Ewin Tang. A quantum-inspired classical algorithm for recommendation systems. In *Proceedings of the 51st annual ACM SIGACT symposium on theory of computing*, pages 217–228, 2019.

[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.

[Vaf88] Cumrun Vafa. Toward classification of conformal theories. *Physics Letters B*, 206(3):421–426, 1988.

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

[Wei09] André Weil. *Oeuvres Scientifiques/Collected Papers: Volume 2 (1951-1964)*, volume 2. Springer Science & Business Media, 2009.

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

[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.