

# Topological Quantum Computing via The Toric Code

by Milo Moses

*University of California, Santa Barbara*

April 5, 2023

## **Abstract**

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

# Contents

<b>0</b>	<b>Preface</b>	<b>3</b>
<b>1</b>	<b>Introduction</b>	<b>5</b>
<b>2</b>	<b>Quantum foundations</b>	<b>10</b>
<b>3</b>	<b>The Toric Code</b>	<b>20</b>
<b>4</b>	<b>Topological Quantum Field Theories</b>	<b>33</b>
4.1	The general picture . . . . .	33
4.2	The $\mathbb{Z}_2$ Dijkgraaf-Witten TQFT . . . . .	39
<b>5</b>	<b>Category Theory</b>	<b>46</b>
5.1	Objects, morphisms, and composition . . . . .	46
5.2	Braided monoidal categories . . . . .	57
<b>6</b>	<b>Modular Tensor Categories</b>	<b>64</b>
6.1	Fusion systems . . . . .	64
6.2	The category-theoretic viewpoint . . . . .	75
6.3	The MTC $\mathcal{Z}(\mathbf{Rep}_{\mathbb{Z}_2})$ . . . . .	90
<b>7</b>	<b>Topological Quantum Computing</b>	<b>105</b>
7.1	The TQC framework . . . . .	105
7.2	Revisiting toric code TQC . . . . .	106
7.3	Universal TQC with the Fibonacci anyon . . . . .	106
<b>A</b>	<b><math>\mathbb{Z}_2</math> Homology Theory</b>	<b>106</b>
<b>B</b>	<b>Unitarity</b>	<b>108</b>
B.1	Unitary TQFTs . . . . .	108
B.2	Unitary MTCs . . . . .	109
<b>C</b>	<b>Fusion System/MTC correspondance</b>	<b>114</b>
<b>D</b>	<b>Anyon data</b>	<b>114</b>

## 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 this microscopic world has proved quite challenging in large part due to thermal fluctuations of the outside world which cause quantum states to degenerate and scramble. Thus, the current state of quantum computing has been dubbed the “NISQ” era: The noisy intermediate-scale quantum era.

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

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

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

“Throughout my career I have been successful inventing toy models, some simple models that capture important features of a more complex problem.” - Alexei Kitaev<sup>1</sup>

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

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

---

<sup>1</sup>From Kitaev’s Simons Foundation interview, “*Alexei Kitaev and the Value of Toy Models*”

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

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

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

The structure of the manuscript is as follows:

- Section 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 would be extremely useful.
- Section 2 gives a treatment of the basics of quantum mechanics and quantum computation. The axioms of quantum mechanics are stated from a mathematical perspective, and are given ample motivation.
- Section 3 gives a mathematical description of the toric code in terms of undergraduate-level linear algebra. While not strictly necessary, having taken a first course in Algebraic Topology would be preferable. For those unfamiliar with the subject, an introduction is given in Appendix A.
- 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.
- Section 6 gives an introduction to Modular Tensor Categories (MTCs), the compressed mathematical abstraction of topological quantum phases of matter. Subsection 6.1 gives an overview of the subject, and the equivalence between MTCs and TQFTs. Subsection 6.2 gives the more elegant interpretation of MTCs in the language of categories. For those unfamiliar with the subject of Category Theory, a brief introduction is contained

in Appendix 5. Subsection 6.3 defines the  $\mathcal{Z}(\mathbf{Rep}_{\mathbb{Z}_2})$  MTC, which is the MTC associated with the toric code.

- Section 7 gives an introduction to the general TQC methodology, using all of the tools 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 this manuscript, we describe the simplest non-trivial example of TQC: The toric code. While not particularly useful in itself, a thorough understanding of the toric code undoubtedly elucidates the general TQC methodology.

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

1. How quantum information is stored (i.e. what physical model of qubits<sup>2</sup> one is using)
2. How quantum information is acted on (i.e. what physical actions one can perform on the qubits)
3. How quantum information is measured (i.e. what observables can be physically measured in the system)

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

While there are many proposed methods of quantum computation (superconducting quantum computers [Wen17], trapped ion quantum computers [DLF<sup>+</sup>16], semiconductor based quantum computers [Kan98], etc...), it is expected that every reasonable model will be essentially equivalent, in the sense that they can all *effectively* simulate each other: This is the content of the Freedman-Church-Turing thesis [FKLW03].

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

---

<sup>2</sup>Qubit (or, “quantum bit”) is the abstract unit of quantum information



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

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<sup>+</sup>19].

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

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

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



Figure 1.2: An Incan Quipu

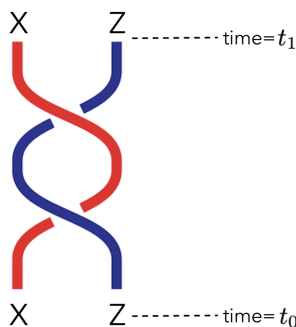


Figure 1.3: Braiding of quasiparticles in spacetime [WORK: BRAID do this in tikz]

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 strings being knotted are no longer physical pieces of twine, but *trajectories of quasiparticles through spacetime*. For instance, suppose  $X$  and  $Z$  are two quasiparticles (we will elaborate more on this in later). Moving through space from time  $t_0$  to  $t_1$ , the trajectories can look something like Figure 1.3. Quantum interactions cause the knotting to yield real differences in physical states, and hence these knots can be used to store quantum information.

Notice that to make 3 dimensional spacetime, we modeled space as being 2 dimensional. While one might initially think this is a quirk of our human incapacity of visualizing 4 dimensional space, there is a deeper mathematical truth

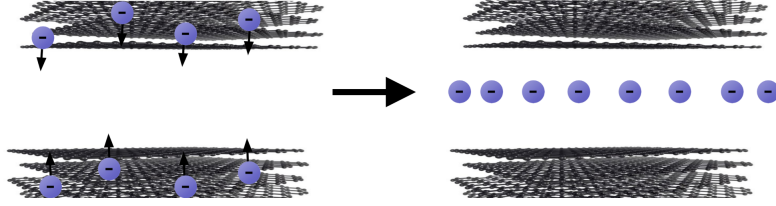


Figure 1.4: The formation of an electron gas from graphene.

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<sup>3</sup>. 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, all of the electrons move to the exact center of the setup. This resulting thin layer of electrons is a two dimensional electron gas. In such extreme conditions, all of the electrons will become highly entangled with each other, forming a quantum phase of matter [YZB<sup>+</sup>21]. A diagram showing this process is found in Figure 1.4

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

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

If your sheet of electrons was on a donut, however, the situation is much different. There are several ways to coherently assign unit tangent vectors to each point; thus there are several ways for all of the electrons to quantize their spins together, as seen in Figure 1.5. This is aptly known as a *spin liquid*.

<sup>3</sup>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.



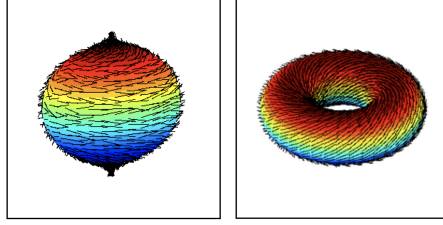


Figure 1.5: Assigning vector fields (spins) to a sphere, verses to a torus

In mathematical language a “donut” is called a torus, hence the name *toric code*. The spin liquid associated with this procedure on a torus is called the “ $\mathbb{Z}_2$  spin liquid”, and it is the physical realization of the toric code. We will spend the body of this manuscript describing the mathematics of the toric code in more detail. Note that generally when making such  $\mathbb{Z}_2$  spin liquids in labs one does not make an actual torus; instead, one artificially simulates the boundary conditions of a torus in nanowires, for technical reasons [AHM<sup>+</sup>16, MZF<sup>+</sup>12].

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

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

1. Information is stored in the ground states of topological quantum materials.
2. Ground states are acted on by braiding of quasiparticles, that is, by generating pairs of quasiparticles and knotting them in spacetime.
3. Measurements are performed by observing the topological properties of the resulting ground state.

Here, *ground state* refers to a state in the system with lowest possible energy. Note that in the previous description of spin liquids, all electrons having the same spin is a result of them being in the lowest energy state. An “excited” electron with deviant spin will raise the energy of the system. These excited electrons are quasiparticles. In this way, quasiparticles can be interpreted as

excitations of a topological quantum material. This motivates the fact that (topological) quantum computers must be exceptionally cold to function: Any extra energy will correspond to extra excitations, causing the computer to malfunction, since information is only stored in ground states.

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

## 2 Quantum foundations

In this appendix we introduce quantum mechanics and quantum computation, from a mathematical perspective. Namely, we state the axioms of quantum mechanics, the relevant definitions and theorems from linear algebra, and a short discussion of information theory. The goal of quantum mechanics is to describe the microscopic world, where physical 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 counter-intuitive phenomena, like *no-cloning theorems* and *quantum teleportation*.

Throughout this appendix, we will strongly use analogy with the classical theory of probability, which we recall in a mathematically rigorous way now. Let  $S$  be a finite set of states. For example, when modelling the flipping of a coin, we might let  $S = \{\text{heads}, \text{tails}\}$ . 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 the total probability  $\sum_{x \in S} p_x$  is 1. For example, if we have two states  $S = \{\text{accept}, \text{deny}\}$  and there is a 90% chance we will accept, then  $p_{\text{accept}} = .9$  and  $p_{\text{deny}} = .1$ .

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

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

We make a comment about our notation. We use the bars/angle-brackets  $|\cdot\rangle$  to formally separate elements of our set  $S$  from the numbers used when taking linear combinations. This is necessary, for if  $S$  the elements of  $S$  were numbers there would be immediate confusion otherwise. For instance, if  $S = \{0, 1\}$ , then the distribution with probability  $\frac{2}{3}$  given to 0 and probability  $\frac{1}{3}$  given to 1 would be notated  $\frac{2}{3}0 + \frac{1}{3}1$ . Upon separating with bars/angle-brackets, we arrive at the

much more sensible  $\frac{2}{3}|0\rangle + \frac{1}{3}|1\rangle$ . The symbol  $|\cdot\rangle$  is known as a *ket*. This notation is ubiquitous across quantum mechanics for representing states.

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

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

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

General probabilistic processes can be described very simply now. A process that goes from probability distribution on a finite set  $S$  to a probability distribution on a finite set  $S'$  can be described as a linear map  $\mathbb{R}[S] \rightarrow \mathbb{R}[S']$ , 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

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

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 in a complete way:

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

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

2. (Processes) A probabilistic process going from a system  $S$  to a system  $S'$  is a linear map  $\mathbb{R}[S] \rightarrow \mathbb{R}[S']$ , which sends normalized vectors to normalized vectors.
3. (Joining systems) If  $S$  and  $S'$  are two probabilistic systems, the system obtained by joining  $S$  and  $S'$  is equal to the system  $S \times S'$ .
4. (Measuring systems) Given a normalized vector  $\sum_{x \in S} p_x |x\rangle \in \mathbb{R}[S]$ , measurement corresponds to collapsing into a pure state, where we observe each  $x \in S$  with probability  $p_x$ .

□

We can state quantum mechanics in exactly the same way:

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

1. (Systems) A quantum system is a complex vector space of the form  $\mathbb{C}[S]$ , where  $S$  is a finite set. The normalized vectors in  $\mathbb{C}[S]$  correspond to complex states on  $S$ . A *normalized* vector  $v = \sum_{x \in S} c_x |x\rangle$  is one for which  $\sum_{x \in S} |c_x|^2 = 1$ , where  $|c_x|^2$  denotes the norm square.
2. (Processes) A quantum process going from a system  $S$  to a system  $S'$  is a linear map  $\mathbb{C}[S] \rightarrow \mathbb{C}[S']$ , which sends normalized vectors to normalized vectors.
3. (Joining systems) If  $S$  and  $S'$  are two quantum systems, the system obtained by joining  $S$  and  $S'$  is equal to the system  $S \times S'$ .
4. (Measuring systems) Given a normalized vector  $\sum_{x \in S} c_x |x\rangle \in \mathbb{C}[S]$ , measurement corresponds to collapsing into a pure state, where we observe each  $x \in S$  with probability  $|c_x|^2$ .

□

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

“What happens if you try to come up with a theory that’s *like* probability theory, but based on the 2-norm instead of the 1-norm?... Quantum mechanics is what inevitably results.” - Scott Aaronson<sup>4</sup>

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

- Particle = Single position; definite = pure state =  $|x\rangle$ ,  $x \in S$

---

<sup>4</sup>Page 112 of Aaronson’s “Quantum Computing since Democritus” [Aar13]

- Wave = Multiple positions; spread-out = mixed state =  $|\psi\rangle \in \mathbb{C}[S]$ .

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

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

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

We can summarize this as saying that there was *constructive interference* in the  $|0\rangle$ s, and *destructive interference* in the  $|1\rangle$ s. The amplitudes had the same signs in the  $|0\rangle$ s causing the 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 and give 0. This linear map  $M$  defined is called the Hadamard gate, and it is a very important process in quantum information theory. It is not immediately clear that  $H$  sends all normalized vectors to normalized vectors. For instance, if we had defined  $M(|1\rangle) = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$  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  $U : \mathbb{C}[S] \rightarrow \mathbb{C}[S]$  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 the two equivalent conditions are met, we call  $U$  a unitary matrix.*

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

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

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

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

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

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

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

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

and

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

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

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

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

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

which gives us the desired conclusion.  $\square$

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. Typically, states  $|\psi\rangle$  will be in superpositions of possible energies. Measuring energy results in collapsing the wavefunction onto a given energy level. The observed quantity is a number - the energy of the level that was collapsed to. Thus, a realistic model of measurement should correspond to not only collapsing onto a pure state, but also choosing a real number to be observed.

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

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

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 normalized vectors are a unitary basis-independent notion as well. This almost allows us to state the axioms of quantum mechanics in a basis independent way. The trouble is that the notations of unitary, Hermitian, and normalized are not invariant under 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 normalization, 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

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

Formally, we have the following:

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

1. A vector space  $V$
2. (Inner product) A map  $\langle \cdot | \cdot \rangle : V \times V \rightarrow \mathbb{C}$

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

□

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

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

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



**Proposition 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  $|x_k\rangle$ ,  $k \in \{0 \dots n-1\}$  such that*

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

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

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

*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 orthogonal change of basis with Hilbert spaces.*

*Proof.*

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

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

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

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

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

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

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

2. Verifying these axioms is immediate, and is left as an exercise to the reader (Exercise 2.3)
3. Suppose two bases are related by a unitary transformation. Since the unitary transformation preserves the inner product, the inner product induced by the two bases are the same. Conversely, suppose that two bases induce the same inner product. This means that the change of basis matrix preserves the inner product, hence is unitary, and hence the two bases are related by a unitary change of basis.

□

We can now state everything in a basis independent fashion. A normalized vector is one in which the norm square  $\langle \psi | \psi \rangle$  equals one. A unitary matrix is a matrix which preserves the norm. That is,  $\langle U\psi | U\phi \rangle = \langle \psi | \phi \rangle$  for all  $|\phi\rangle, |\psi\rangle$ . A Hermitian matrix is one which is a diagonal matrix with real entries in some orthonormal basis. In terms of the inner product, this can be characterized as saying that  $\langle \psi, H\phi \rangle = \langle H\psi, \phi \rangle$  (see Exercise 2.1).

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

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

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

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

where  $x_0, x_1 \in V$ ,  $y_0, y_1 \in W$ . We verify in Exercise 2.2 that this is indeed an inner product. Thus, we can state the axioms of quantum mechanics as follows:

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

1. (Systems) A quantum system is a complex Hilbert space  $V$
2. (Processes) A quantum process going from a system  $V$  to a system  $W$  is an orthogonal transformation from  $V$  to  $W$
3. (Joining systems) If  $V$  and  $W$  are two quantum systems, the system obtained by joining  $V$  and  $W$  is equal to the system  $V \otimes W$ .

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

□

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

1. In simple situations we will often be extremely explicit with choosing bases, and hence we will not need the basis independent language of Hilbert spaces
2. In complex situations the language of Hilbert spaces adds extra confusion and subtlety, so we work instead with vector spaces. Dealing with this subtlety by imposing the structure of Hilbert spaces of Topological Quantum Field Theories/Modular Tensor Categories and forcing all maps to be unitary is done in Appendix B.

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

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

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

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

A quantum computation is a quantum process

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

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  $\otimes n$  denotes 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

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

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

1. How quantum information is stored. That is, what physically object will have associated quantum state-space which we identify with  $(\mathbb{C}^2)^{\otimes n}$ .
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, how one can observables one can measure to reliably read information about quantum states from  $(\mathbb{C}^2)^{\otimes m}$ .

This concludes our introduction of quantum mechanics.

### Exercises:

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

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

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

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

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

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

- 2.3. Verify Proposition 2.3 part (2).



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

### 3 The Toric Code

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

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

Working with a continuous torus and the corresponding infinite dimensional vector spaces is cumbersome and unnecessary. Instead, we celluate the torus into an  $n$  by  $n$  square lattice with opposing sides identified, as in Figure 3.1. We will work with the understanding that the real physical system is the limit as  $n \rightarrow \infty$ . We define the quantum system associated with the  $n$  by  $n$  celluated torus to be the vector space

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

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

<sup>5</sup>A qubit is the quantum-computing term for “two dimensional quantum system”, i.e.,  $\mathbb{C}^2$ .

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

The Hamiltonian is defined by

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

where

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

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

Letting  $I$  denote the identity matrix, the key facts about the  $A_v$ s and  $B_p$ s 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  $A_v$ s and  $B_p$ s have half eigenvalues  $+1$  and half eigenvalues  $-1$
- (iii) All  $A_v$ s and  $B_p$ s commute
- (iv)  $\prod_{\text{vertices } v} A_v = I$  and  $\prod_{\text{faces } p} B_p = I$

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

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

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

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

between the desired eigenspaces. Applying  $\sigma_Z$  instead of  $\sigma_X$ , we can define a similar isomorphism for  $B_p$ .

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

(iii). All the  $A_v$ s commute with each other since  $\sigma_Z$  commutes with itself, and all the  $B_p$ s commute with each other since  $\sigma_X$  commutes with itself. What's left to check is that  $A_v B_p = B_p A_v$ . Notice that if  $v$  is not touching the face  $p$ , none of the  $\sigma_Z$ s in the tensor product of  $A_v$  will be in the same spots as any of the  $\sigma_X$ s 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  $\sigma_Z$ s in the tensor product of  $A_v$  will be in the same spots as  $\sigma_X$ s in the tensor product of  $B_p$ . Hence, pulling  $B_p$  through  $A_v$  corresponds to switching  $\sigma_X$  and  $\sigma_Z$ . 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  $\sigma_Z$  to each vertex 2 times, since each edge touches exactly 2 vertices. Hence,

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

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

Using the above facts about the  $A_v$ s and  $B_p$ s, 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  $-2n^2 + 4q$  can be described as the space of states  $|\psi\rangle$  such that*

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

*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  $\lambda$ , then

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

Hence,  $M$  respect the eigenspaces of  $N$ , and vice versa. This implies that the eigenspaces for  $H$  will be simultaneous eigenspaces for all of the  $A_v$ s and  $B_p$ s, since all of the  $A_v$ s and  $B_p$ s 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

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

Thus, to complete the initial description of the eigenstates, we must show that the number of  $v$  such that  $A_v |\psi\rangle = -1$  and the number of  $p$  such that  $B_p |\psi\rangle = -1$  is even. This follows from the computation that if this number were odd, then we would have by Proposition 3.1 (iv) that

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

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

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

is  $D$  dimensional. We proceed by induction on  $|\mathbf{v} + \mathbf{p}|$ . If  $|\mathbf{v} + \mathbf{p}| = 0$ , then this is the definition of  $D$ . Without loss of generality, suppose  $|\mathbf{v}| \geq 2$ . If  $|\mathbf{p}| \geq 2$ , we apply the same argument with vertices replaced by faces. Choose two vertices  $v_0, v_1 \in \mathbf{v}$ . Choose a path  $\gamma$  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  $\sigma_X^2 = \text{id}$ , 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  $B_p$ s, and commutes with all of the  $A_v$ s at vertices that  $\gamma$  passes through an even number of times. The only vertices that  $\gamma$  passes through an odd number of times are its endpoints (by definition), and hence  $A_v$  has exactly the effect of flipping the



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

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

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

The total dimension of eigenspaces of  $H$  can be computed as

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

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

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, bringing 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  $\gamma$ , we write  $|\gamma\rangle$  for the associated pure state. Given any  $\gamma, \gamma'$ , we write  $\gamma \sim \gamma'$  to mean that  $\gamma$  and  $\gamma'$  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. Then, letting  $\gamma$  run over all  $\mathbb{Z}_2$ -cycles, we have that*

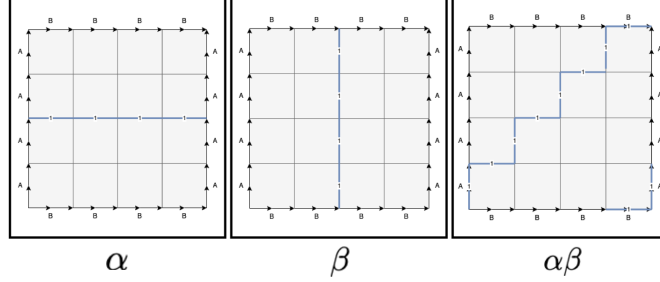


Figure 3.2: The three non-trivial homology classes of a torus

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

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

*Proof.* Choose  $\omega \in H_1(T; \mathbb{Z}_2)$ . To show that  $|\omega\rangle$  is in the codespace, we observe that it is in the +1 eigenspace of every  $A_v$  and  $B_p$ . Since  $\sigma_Z$  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  $\gamma$  has an odd or even count of edges touching the vertex  $v$ . In particular, because  $\gamma$  is running over cycles, we have that each  $|\gamma\rangle$  is in the +1 eigenspace of all the  $A_v$ , and hence the same applies to  $|\omega\rangle$ .

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

To show that  $|\omega\rangle$  is normalized, we observe that there are exactly that there are exactly  $2^{n^2-1}$  cycles homologous to  $\omega$ . This is proved as follows. Starting with a fixed representative  $\omega_0$  of  $\omega$ , cycles homologous to  $\omega$  correspond to flipping qubits around the edges, i.e., applying  $B_p$ s at faces. Since there are  $n^2$  faces, this gives  $2^{n^2}$  cycles. This overcounts the space of cycles homologous to  $\omega$  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  $B_p$ s. Hence, there are  $2^{n^2-1}$  cycles.

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

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

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

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

$$\begin{aligned} A_{v_0} |\psi'\rangle &= A_{v_0} \left( \bigotimes_{\text{edge } e} \sigma_X \right) |\psi\rangle = -A_{v_0} |\psi\rangle = |\psi\rangle, \\ A_{v_1} |\psi'\rangle &= A_{v_1} \left( \bigotimes_{\text{edge } e} \sigma_X \right) |\psi\rangle = -A_{v_1} |\psi\rangle = -|\psi\rangle, \end{aligned}$$

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

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

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



Figure 3.3: Topological quantum process implementing the  $\text{NOT}_\alpha$  gate

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

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

1. Quantum information is stored in the ground state of the toric code, i.e., the lowest eigenvalue eigenspace of the Hamiltonian.
2. Ground states are acted on by generating and manipulating quasiparticles, moving them around the torus, and annihilating them. Mathematically, this is realized by repeatedly tensoring with  $\sigma_X$  and  $\sigma_Z$  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 “ $\text{NOT}_\alpha$ ” gate, which flips the input state depending on whether it has an  $\alpha$  component, namely

$$\begin{aligned} |\mathbf{0}\rangle &\mapsto |\alpha\rangle, \quad |\beta\rangle \mapsto |\alpha\beta\rangle \\ |\alpha\rangle &\mapsto |\mathbf{0}\rangle, \quad |\alpha\beta\rangle \mapsto |\beta\rangle. \end{aligned}$$

A diagram visualizing the process described in the following proposition is shown in Figure 3.3.

**Proposition 3.4.** *The following computation has the effect of performing the  $\text{NOT}_\alpha$  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  $\alpha$ . Finally, fuse your two adjacent  $X$ -type particles together.*

*Proof.* Let  $v_0$  and  $v_1$  be adjacent vertices. Let  $\alpha_0$  be a cycle homologous to  $\alpha$  going from  $v_1$  to itself. The process described in the statement of the proposition can be reworded as saying the following. First, we create a particle pair at  $v_0$  and  $v_1$ , i.e., we tensor with  $\sigma_X$  at the edge connecting  $v_0$  and  $v_1$ . Then we move  $v_1$  along  $\alpha_0$ , i.e., we tensor with  $\sigma_X$  along the edges in  $\alpha_0$ . Then, we fuse the  $X$ -type quasiparticles at  $v_0$  and  $v_1$  back together, i.e., we tensor along the edge connecting  $v_0$  and  $v_1$  again. Since  $\sigma_X^2 = 1$ , this whole process can be described mathematically as

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

Seeing as  $\sigma_X$ s 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  $\alpha_0$ . 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  $\alpha$  to a cycle homologous to  $\omega$  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  $\text{NOT}_\alpha$  gate.  $\square$

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

$$\begin{aligned} |0\rangle &\mapsto |0\rangle, \quad |\beta\rangle \mapsto |\beta\rangle \\ |\alpha\rangle &\mapsto -|\alpha\rangle, \quad |\alpha\beta\rangle \mapsto -|\alpha\beta\rangle. \end{aligned}$$

**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  $\beta$ . Finally, fuse your two adjacent  $Z$ -type particles together.*

*Proof.* Let  $p_0$  and  $p_1$  be adjacent faces. Let  $\beta_0$  be a cycle homologous to  $\beta$  going from  $p_1$  to itself. Note that since  $Z$ -type particles live on faces,  $\beta_0$  does not consist of a series of edges. Instead, it is a path going through the centers of faces. We take  $\hat{\beta}_0$  to be the set of edges that  $\beta_0$  passes through. Tensoring with  $\sigma_Z$  along  $\hat{\beta}_0$  corresponds to motion of a particle from  $p_1$  along  $\beta_0$  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 cellulation, 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 cellulation satisfy the dual condition ‘every face touches an even number of 1s’.

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

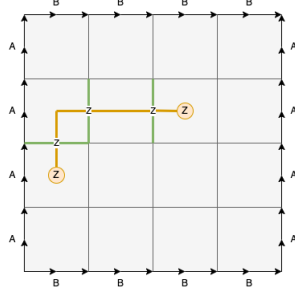


Figure 3.4: Sample trajectory along dual cellulation of torus

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

The matrix  $\sigma_Z$  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  $\hat{\beta}_0$ . Thus, when acting on a pure state  $\gamma$ , the definition of  $\hat{\beta}_0$  shows that this process has the effect of introduce a phase shift of  $-1$  to the power of the number of intersection between  $\gamma$  and  $\hat{\beta}_0$ .

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  $\beta$ ,  $\beta$  doesn’t intersect  $\beta$  (representatives can be chosen to be parallel),  $\alpha$  intersects  $\beta$  (horizontal loops and vertical loops meet at exactly one point), and  $\alpha\beta$  intersects  $\beta$ . Thus, this process has the effect of adding a  $-1$  phase shift to those states which include an ‘ $\alpha$ ’, as desired.  $\square$

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

**Proposition 3.6.** *There are exactly 8 possible computations in the toric codes. The group of gates is (non canonically) isomorphic to the Pauli group, i.e., the group whose objects are*

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

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

*Proof.* To begin, we define  $NOT_\beta, NOT_{\alpha\beta}, (-1)_\beta$ , and  $(-1)_{\alpha\beta}$  in complete analogy to how we define  $NOT_\alpha$  and  $(-1)_\alpha$ . Namely,  $NOT_\beta$  flips whether or not a state has a ‘ $\beta$ ’ in it, and  $NOT_{\alpha\beta}$  flips whether or not a state has an ‘ $\alpha\beta$ ’ in it, i.e.,

$$\begin{aligned} |\mathbf{0}\rangle &\mapsto |\alpha\beta\rangle, \quad |\beta\rangle \mapsto |\alpha\rangle \\ |\alpha\rangle &\mapsto |\beta\rangle, \quad |\alpha\beta\rangle \mapsto |\mathbf{0}\rangle. \end{aligned}$$

The relation  $\sigma_X\sigma_Z = -\sigma_Z\sigma_X$  implies that we can switch the order of operations between first applying all our  $\sigma_X$ s and then applying all our  $\sigma_Z$ s, up to an operator-wise phase shift  $-1$ . Any process of creating and annihilating  $X$ -type quasiparticles can be modeled in sequence as repeatedly creating particles, moving them around a loop, then annihilating them. Following the proof of Proposition 3.5, this is the same as repeatedly applying  $NOT_\omega$  gates, for homology classes  $\omega$ . 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:  $\{\pm I, NOT_\omega, (-1)_\omega\}$ , where  $\omega$  runs over homology classes. The relations  $NOT_\alpha NOT_\beta = NOT_{\alpha\beta}$  and  $(-1)_\alpha (-1)_\beta = (-1)_{\alpha\beta}$  allow one to reduce the generating set further. The relations

$$NOT_\alpha (-1)_\alpha NOT_\alpha = (-1)_\beta$$

and

$$(-1)_\alpha NOT_\alpha (-1)_\alpha = -I$$

reduce the generating set to  $\{NOT_\alpha, NOT_\beta, (-1)_\alpha\}$ . Verifying simple relations gates, it is simple to see that the gate group is isomorphic to the Pauli group, as desired.  $\square$

Before moving on to the next section, we make a few final remarks about the behavior of quasiparticles on the toric codes. Namely, we observe the following. Consider the full vector space  $\mathcal{N}$ , and adjacent two adjacent  $X$ -type and  $Z$ -type quasiparticles. Consider the simple braiding of these particles around each other, as in Figure 1.3. A line going under another corresponds to the particle having passed through that space first, before the other particle. This braiding can be obtained by first performing a twist halfway around the circle by  $X$ , then a twist all the way around the circle by  $Z$ , then finally moving the second half of the circle by  $X$ . This process corresponds to a transformation  $\mathcal{N} \rightarrow \mathcal{N}$

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

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

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

## Exercises:

3.1. For edges  $v$  and faces  $p$ , define

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

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

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

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

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



- 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*, which is a more general phenomenon in TQC. (HINT: Prove this for ground states first, then lift to general eigenstates using an induction argument along the lines of the proof of Proposition 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?]. Show that this map is linear and injective, and hence that  $\mathcal{N}_n$  can be realized as a sub vector space of  $\mathcal{N}_m$ . Show that  $\tilde{H}_m$  restricted to  $\mathcal{N}_n$  is equal to  $\tilde{H}_n$ . Show that the map  $\mathcal{N}_n \hookrightarrow \mathcal{N}_m$  is norm-preserving, in the sense that if  $|\chi\rangle, |\psi\rangle$  are states on  $\mathcal{N}_n$ , the inner product  $\langle\chi|\psi\rangle$  is independent of whether or not it was computed in  $\mathcal{N}_n$  or  $\mathcal{N}_m$ . Define

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

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

## 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 are the mathematical formalism of topological quantum phases of matter. Namely, every topological quantum phase of matter (physical object) has an associated Topological Quantum Field Theory (mathematical object) to describe it. To make

---

<sup>6</sup>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 cellulation.



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

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

$$\left( \begin{array}{c} \text{Collections of} \\ \text{particles} \end{array} \right) \rightsquigarrow \left( \begin{array}{c} \text{Physical} \\ \text{systems} \end{array} \right),$$

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

$$\left( \begin{array}{c} \text{Collections of} \\ \text{particles} \end{array} \right) \rightsquigarrow \left( \begin{array}{c} \text{Quantum} \\ \text{systems} \end{array} \right).$$

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

$$\left( \begin{array}{c} \text{Topological} \\ \text{spaces} \end{array} \right) \rightsquigarrow \left( \begin{array}{c} \text{Quantum} \\ \text{systems} \end{array} \right).$$

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

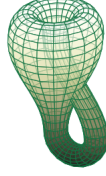


Figure 4.2: A Klein bottle, attempting to be embedded in 3d space

into three dimensional space, i.e., those surfaces which can be realized physically in our three dimensional world. Note that there are some weird surfaces which can not be embedded into three dimensional space, such as the Klein bottle (shown in Figure 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.

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 surface that*

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

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

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

$$\left( \begin{array}{c} \text{Surfaces} \\ \text{in space} \end{array} \right) \rightsquigarrow \left( \begin{array}{c} \text{Quantum} \\ \text{systems} \end{array} \right).$$

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

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

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

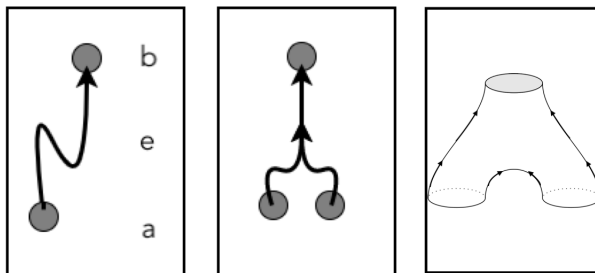


Figure 4.3: First box - A path in spacetime from  $a$  to  $b$  by  $e$ , i.e., a path  $e$  with  $\partial e = a \sqcup b$ . Second box - The fusion of two particles in spacetime. Third box - the fusion of two circles in spacetime, known informally as a “Pair of Pants”.

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

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

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

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

Additionally, by the axioms of quantum mechanics, transformations of a surface through spacetime should correspond to linear maps on quantum systems. We think mathematically about what a trajectory through spacetime looks like. In the one dimensional case, suppose we have two particles  $a$  and  $b$ . A trajectory through spacetime from  $a$  to  $b$  is a path  $e$  connecting  $a$  and  $b$ . Thinking deeply, one observes that the condition of “connecting”  $a$  and  $b$  can be mathematically stated as  $\partial e = a \sqcup b$ , where  $\partial e$  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 circles of particles - loops - through spacetime. The merging of two circles will look exactly like it did before, except that now instead of tracing a path through spacetime it will trace a surface with boundary. The boundary components correspond exactly to the particles at the start and end of the process, as seen in the third box of Figure 4.3.

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

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

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

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

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

---

<sup>7</sup>Sometimes called a cobordism; the difference is immaterial.

$S$ .

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

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

1. (Union = tensor product).  $V(S_0 \sqcup S_1) = V(S_0) \otimes V(S_1)$ . Here,  $S_0$  and  $S_1$  are any two surfaces.
2. (Do nothing = identity)  $Z(S \times [0, 1]) = \text{id}_{V(S)}$ . Here,  $S \times [0, 1]$  is the Cartesian product of  $S$  with the interval, treated as a bordism from  $S$  to itself. Concretely  $\partial(S \times [0, 1]) = S \times \{0\} \sqcup S \times \{1\}$ , and we identify  $S \times \{0\}$  and  $S \times \{1\}$  both with  $S$ .
3. (Composing bordisms = composing maps).  $Z(X_1 \cup X_0) = Z(X_1) \circ Z(X_0)$ . Here,  $X_0$  is a bordism from two surfaces  $S_0$  and  $S_1$  and  $X_1$  is a bordism from surfaces  $S_1$  to  $S_2$ . One easily verifies that their union  $X_1 \cup X_0$  is a bordism between  $S_0$  and  $S_2$ , whose induced map we can compare with the composition of the induced maps of  $X_0$  and  $X_1$ .
4. (Swap spaces = swap tensor factors)  $Z(X)(v_0 \otimes v_1) = v_1 \otimes v_0$  for all  $v_0 \in V(S_0)$ ,  $v_1 \in V(S_1)$ . Here,  $X$  is the bordism from  $S_0 \sqcup S_1$  to  $S_1 \sqcup S_0$  defined by taking  $S_0, S_1$  and moving them around each other.

□

We offer a few remarks. The term “ $(2 + 1)$ ” refers to the fact that there are two space dimensions, plus one time dimension. More generally, an  $(n + 1)$ -TQFT is an assignment of  $n$ -manifolds to vector spaces, and of  $(n + 1)$ -manifolds to linear transformations. We also remark on the structure of the definition. We first defined a few assignments of objects of one type to objects of another type, and then we defined a laundry list of properties that those assignments should satisfy. This is extremely standard practice in higher mathematics. The abstraction of this practice is known as Category Theory. The assignments of one type of object to another type of object are known as functors, and the properties to satisfy are known as axioms. The category theory definition of a TQFT is “a symmetric monoidal functor from the category of bordisms to the category of vector spaces”<sup>8</sup>. 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 cellulations. A cellulation is a way of splitting up a space into vertices, edges, and faces. The utility of cellulations 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

---

<sup>8</sup>symmetric=axiom 4, monoidal=axiom 1, functor=axiom 3, bordism category=axiom 2



Figure 4.4: The Pachner moves.

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  $(X, \Delta_X)$  and  $(X, \Delta'_X)$  be two manifolds with triangulations (i.e. celluations in which every face has three edges). There exists a finite sequence of so-called Pachner moves relating  $\Delta_X$  to  $\Delta'_X$ . 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 “a-b” move is the move that takes a cells to b cells.*

This massively facilitates the verification of whether or not a definition is independent of celluation. Namely, first you show that the definition is invariant under adding/removing edges (allowing you to turn the celluation into a triangulation), and then you check that the definition is invariant under applying the Pachner moves. Typically, this verification is entirely elementary and does not require any great show of cleverness. As such, our standard practice for Subsection 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  $\Delta_S$  is a celluation of  $S$ . That is,  $\Delta_S$  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  $\Delta$  could be the  $n$  by  $n$  lattice with opposite edges identified. For every surface  $S$  and celluation  $\Delta_S$ , we define

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

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

Notice that a  $\mathbb{Z}_2$  cocycle is the same thing as a  $\mathbb{Z}_2$  cycle in the dual celluation, as discussed in the proof of Proposition 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  $\Delta_S$  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  $\Delta_S$ , 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,  $\alpha$  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  $(S_0, \Delta_{S_0})$  and  $(S_1, \Delta_{S_1})$  be two surfaces with celluations. Let  $X$  be a bordism from  $S_0$  to  $S_1$ . Let  $\Delta_X$  be a celluation on  $X$  compatible with the celluations on  $S_0$  and  $S_1$ . By compatible we mean that if we restrict  $\Delta_X$  to  $\partial X$  then we will recover the celluations  $\Delta_{S_0}$  and  $\Delta_{S_1}$ . This restriction process can be described visually as dropping all vertices, edges, and faces, from  $\Delta_X$  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  $\omega_{S_0}$  when restricted to  $S_0$  and  $\omega_{S_1}$  when restricted to  $S_1$ . Let  $N_X$  be the number of cocycles in  $C^1(S_1; \mathbb{Z}_2)$  with which the 0 cocycle on  $S_0$  can be extended. We define

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

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

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

Our goal is to show that  $\tilde{Z}(X, \Delta_X)$  restricts to a map  $V(S_0) \rightarrow V(S_1)$ , and that this restriction is independent of our choice of  $\Delta_{S_0}, \Delta_{S_1}$  and  $\Delta_X$ . 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  $(S_0, \Delta_{S_0})$  and  $(S_1, \Delta_{S_1})$  be surfaces with celluations,  $X$  a bordism from  $S_0$  to  $S_1$ , and  $\Delta_X$  a celluation of  $X$  compatible with the celluations on  $S_0$  and  $S_1$ . Then, the map  $\tilde{Z}(X, \Delta_X) : \tilde{V}(S_0, \Delta_{S_0}) \rightarrow \tilde{V}(S_1, \Delta_{S_1})$  is independent of the choice of celluation  $\Delta_X$ . Hence, we can properly omit  $\Delta_X$  from our notation, and speak of a well defined map  $\tilde{Z}(X)$ .*

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

That is,  $(\omega_{S_0}, \omega_{S_1})$  are extendable in  $\Delta_X$  if and if they are extendable in  $\Delta'_X$ . 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 cellulation 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 of the proof as an exercise to the reader (Exercise 4.1).  $\square$

**Lemma 4.1.** *Let  $(S_0, \Delta_{S_0})$ ,  $(S_1, \Delta_{S_1})$ ,  $(S_1, \Delta_{S_2})$  be surfaces with cellulations, let  $X_0$  be a bordism from  $S_0$  to  $S_1$ , and let  $X_1$  be a bordism from  $S_1$  to  $S_2$ .*

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

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

*Proof.* We prove (i), and leave (ii) as an exercise (Exercise 4.2) since the proof is identical. Let  $\omega_{S_1}$  and  $\omega'_{S_1}$  be such that  $(\omega_{S_0}, \omega_{S_1})$  and  $(\omega_{S_0}, \omega'_{S_1})$  are extendable. Then, adding extensions of these pairs together edgewise we get that  $(\omega_{S_0} + \omega_{S_0}, \omega_{S_1} + \omega'_{S_1})$  is extendable. Since  $\omega_{S_0} + \omega_{S_0} = 0$ , we find that there is a 1-to-1 bijection between  $\omega_{S_1}$  such that  $(0, \omega_{S_1})$  is extendable and  $\omega_{S_1}$  such that  $(\omega_{S_0}, \omega_{S_1})$  is extendable, sending  $\omega_{S_1}$  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

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

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

number of ways of choosing  $\omega_{S_2}$  (i.e.  $N_{X_0 \cup X_1}$ ), and then by counting the number of ways of filling in  $\omega_{S_1}$ . The right hand side computes this value by first counting the number of ways of choosing  $\omega_{S_1}$  (i.e.  $N_{X_0}$ ) and then counting the number of ways of choosing  $\omega_{S_2}$  (i.e.  $N_{X_1}$ ). Note the implicit use of Lemma 4.1, saying that all of these 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  $(S, \Delta_S)$  be a surface with cellulation and let  $S \times [0, 1]$  be the product of  $S$  with the real interval of numbers between 0 and 1. That is, elements of  $S \times [0, 1]$  are pairs  $(s, t)$  where  $s \in S$  and  $t \in [0, 1]$ . This is a 3-manifold, and gives a bordism from  $S$  to itself. Namely,  $\partial(S \times [0, 1])$  is built of the two components  $S \times \{0\}$  and  $S \times \{1\}$ . The orientation on  $S \times [0, 1]$  is induced by the orientation on  $[0, 1]$ . This can be viewed as the identity bordism:  $S$  is doing nothing as time increases from 0 to 1. The boundary components correspond to the placement of  $S$  at time 0 and  $S$  at time 1. When time passes on a system, we expect it to ambiently decrease in energy. Thus, physically  $Z(S \times [0, 1])$  should act by the identity on ground states, and send higher energy states down to the ground state. This is exactly the statement that  $Z(S \times [0, 1])$  should be a projection from the full state space to the ground state space. The following proposition in this lens thus says that  $V(S)$  are exactly the ground space:

**Proposition 4.3.** *Let  $(S, \Delta_S)$  be a surface with cellulation. Viewing  $S \times [0, 1]$  as a bordism from  $S$  to itself, we have that  $\tilde{Z}(S \times [0, 1])$  is a projection from  $\tilde{V}(S, \Delta_S)$  to  $V(S)$ . Namely, the image of  $\tilde{Z}(S \times [0, 1])$  is  $V(S)$ , and  $\tilde{Z}(S \times [0, 1])$  acts by the identity on  $V(S)$ . Explicitly,  $\tilde{Z}(S \times [0, 1])$  is given by the map*

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

*Proof.* Let  $\omega_S, \omega'_S$  be two cocycles on  $\Delta_S$ . We show that  $(\omega_S, \omega'_S)$  is extendable if and only if  $\omega_S$  and  $\omega'_S$  are cohomologous. Consider the cellulation  $\Delta_{S \times [0, 1]}$  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  $\omega_X$  of  $(\omega_S, \omega'_S)$ . 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  $\omega_X$ . Let  $\omega'_X$  be the cocycle obtained by flipping  $e$  to 0, as well as flipping all of the edges touching  $e$  in  $S \times \{1\}$ .  $\omega'_X$  satisfies the cocycle condition since faces in the center touching  $e$  will also touch exactly 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  $\omega'_S$  and  $\omega_S$  are cohomologous. This process is demonstrated in Figure 4.5.

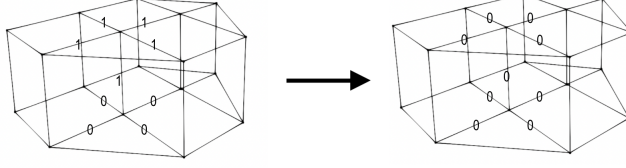


Figure 4.5: Removing the 1s from the central edges in  $S \times [0, 1]$

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

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

**Proposition 4.4.** *Let  $(S_0, \Delta_{S_0})$  and  $(S_1, \Delta_{S_1})$  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  $V(S_0) \rightarrow V(S_1)$ . This map is independent of our choice of  $\Delta_{S_0}$  and  $\Delta_{S_1}$ . We define  $Z(X) : V(S_0) \rightarrow V(S_1)$  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  $\omega'_{S_0}$  homologous to  $\omega_{S_0}$ . 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 homologous to  $\omega_{S_0}$  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  $\Delta_S$  and  $S \times \{1\}$  given a celluation  $\Delta'_S$ . We show that a cocycle in  $C^1(\Delta_S; \mathbb{Z}_2)$  can be lifted to a class in  $C^1(\Delta'_S; \mathbb{Z}_2)$  if and only if they are homologous. Applying this with  $S = S_0$  and precomposing with  $S_0 \times [0, 1]$  gives the desired independence of choice of celluation on  $S_0$ , and applying this with  $S = S_1$  and postcomposing with  $S_1 \times [0, 1]$  gives the desired independence of choice of celluation on  $S_1$ .

The above claim again follows from applying induction with respect to the moves in Theorem 4.2, and thus is left as an exercise (Exercise 4.3).  $\square$

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 Topological Quantum Field Theory, called the  $\mathbb{Z}_2$  Dijkgraaf-Witten TQFT.*

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

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

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

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

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

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.

□

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 cellulation, and so this discrepancy is really 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  $\tilde{Z}(X)$ . 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 would take a long time to simulate the process on a classical computer. This gives a sort of quantum computer, known as an Adiabatic quantum computation. It is interesting to note that the original definition of the toric code did not include a Hamiltonian, and this was only introduced later to facilitate the study [Kit97]. A more general study of TQFTs with Hamiltonians was conducted by Levin-Wen [LW05], but is still not the norm.

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

### 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 the mathematical abstraction of things, and relationships between things. It is a language that almost all other mathematical fields can be expressed in, with often very fruitful consequences. Formally, a category is defined as follows:

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

1. (Objects) A set  $\mathcal{C}$ .
2. (Morphisms) A set  $\text{Hom}(A, B)$  for all  $A, B \in \mathcal{C}$

### 3. (Composition) Functions

$$\circ : \text{Hom}(B, C) \times \text{Hom}(A, B) \rightarrow \text{Hom}(A, C)$$

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

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

1. For all objects  $A, B, C, D \in \mathcal{C}$  and morphisms  $f \in \text{Hom}(A, B)$ ,  $g \in \text{Hom}(B, C)$ , and  $h \in \text{Hom}(C, D)$ ,

$$(h \circ g) \circ f = h \circ (g \circ f).$$

2. (Identity) For all objects  $A \in \mathcal{C}$  there exists a morphism  $\text{id}_A : A \rightarrow A$  such that for all  $B \in \mathcal{C}$ ,  $f \in \text{Hom}(A, B)$  we have

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

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

$$\text{id}_A \circ f = f.$$

□

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

The composition operation  $\circ$  is the fundamental operation of category theory. It is the deep idea that given two transformations, doing one after the other gives another transformation. The axiom that  $(h \circ g) \circ f = h \circ (g \circ f)$  simply makes sure that composition works like we think it should. Every category that one naturally considers has identity elements. That is, the “do-nothing” function from an object to itself should always be an allowed morphism. The do nothing 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 the generality of its language. 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 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 work this example out in detail to give a general idea of category theory.

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

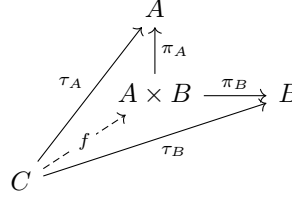
1. An object  $A \times B \in \mathcal{C}$ .
2. A morphism  $\pi_A \in \text{Hom}(A \times B, A)$ .
3. A morphism  $\pi_B \in \text{Hom}(A \times B, B)$ .

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

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

- 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  $\pi_A, \pi_B$  turn out to be the key parts of the definition. For instance, in the case of set we have maps  $\pi_A : A \times B \rightarrow A$  sending  $(a, b)$  to  $a$ , and  $\pi_B : A \times B \rightarrow B$  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**.
- The definitions are very abstract, and get to the core of the relevant theory. In this case, 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. Applying the case  $\mathcal{C} = \mathbf{Set}, \mathbf{Top}, \mathbf{Grp}, \mathbf{Vec}$ , one recovers the standard definitions of product.
- Definitions can often be hard to read. It is for this reason we use diagrammatic notation that elucidates ideas. Instead of writing  $f \in \text{Hom}(A, B)$ , we will often write  $f : A \rightarrow B$ . This will make our intuition of  $f$  as a function from  $A$  to  $B$  clear. We will 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.

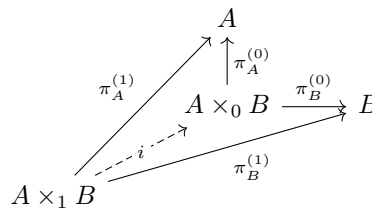




The fact that  $f \circ \pi_A = \tau_A$  and  $f \circ \pi_B = \tau_B$  is exactly the statement that picking any two paths between any two objects will give you the same function, when you compose all of the functions along each path. We call a diagram with this property a commutative diagram. The product condition is thus the statement is that there exists a function  $f : C \rightarrow A \times B$  such that the above diagram commutes. The diagrammatic language is often easier to read, and leaves room for more ease-of-use features. For instance, we make the line under  $f$  dotted to reinforce that it is different than the others - we are required to show that  $f$  exists, whereas  $\pi_A, \tau_A, \pi_B, \tau_B$  are given.

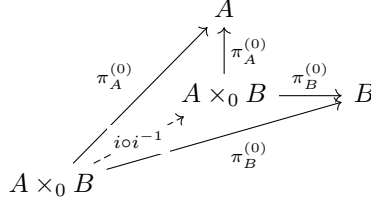
A fundamental question in category theory is what it should mean for two things to be equivalent. For instance, one might want to show that the product  $A \times B$  of two elements is unique. If we take the strictest definition of equivalent - equal - then this is not the case. There can be multiple products. However, all of these will be *isomorphic*. An isomorphism between an object  $A$  and an object  $B$  is a function  $f : A \rightarrow B$  such that there exists  $f^{-1} : B \rightarrow A$ , such that  $f^{-1} \circ f = \text{id}_A$  and  $f \circ f^{-1} = \text{id}_B$ . This recovers bijections 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  $\mathcal{C}$  be a category, and let  $A, B \in \mathcal{C}$  be objects. Let  $(A \times_0 B, \pi_A^{(0)}, \pi_B^{(0)})$  and  $(A \times_1 B, \pi_B^{(1)}, \pi_A^{(1)})$  be products of  $A$  and  $B$ . There is a unique isomorphism  $i : A \times_0 B \rightarrow A \times_1 B$  such that*



*commutes.*

*Proof.* By the universal property of  $A \times_0 B$ , there is a unique map  $i : A \times_1 B \rightarrow A \times_0 B$  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  $i^{-1} : A \times_0 B \rightarrow A \times_1 B$  making the same map commute. Now, we observe the commutative diagram



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

Observe that not only do we recover an isomorphism between  $A \times_0 B$  and  $A \times_1 B$ , but we recover an isomorphism which respects the relevant structure. Namely, the projection maps onto  $A$  and  $B$ . With this isomorphism in hand, we can reasonably say that the product of  $A$  and  $B$  is unique. There are many choices, but they all have unique isomorphisms between each other which respect structure. We say in this situation that  $A \times_0 B$  and  $A \times_1 B$  can be *canonically* identified. A structure is canonical if there is a unique natural choice of construction. In this case, the isomorphism is canonical since there is a unique choice, the one which makes the diagram commute. 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 studying category theory to develop the most canonical possible constructions:

“I can assure you, at any rate, that [...] my results are invariant, probably canonical, perhaps even functorial.” - Rudolf Lipschitz<sup>9</sup>

The term *functorial* in the above quote makes reference to one of the most systematic measures of canonicity in category theory. Suppose one has two categories  $\mathcal{C}$  and  $\mathcal{D}$ , and has an assignment of objects from  $\mathcal{C}$  to  $\mathcal{D}$ . For instance  $\mathcal{C} = \mathbf{Top}$ ,  $\mathcal{D} = \mathbf{Grp}$ , 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  $\mathcal{C} = \mathbf{Set}$ ,  $\mathcal{D} = \mathbf{Vec}$ , and the assignment sends a set<sup>10</sup>  $S$  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 can say these maps are *functorial*. This means that these assignments can be extended to functors, which we define below:

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

<sup>9</sup>This quote appears in a correspondence between Lipschitz and André Weil, which was documented in the collection [Wei09], on page 558.

<sup>10</sup>To get a finite dimensional vector space,  $S$  has to be finite. Thus, this is really a functor  $\mathbf{finSet} \rightarrow \mathbf{Vec}$  whose source is the category of finite sets.

1. An object  $F(A) \in \mathcal{D}$  for every object  $A \in \mathcal{C}$ .
2. A morphism  $F(f) : F(A) \rightarrow F(B)$  for every morphism  $f : A \rightarrow B$ ,  $A, B \in \mathcal{C}$ .

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

1. (Preserves composition)  $F(g \circ f) = F(g) \circ F(f)$ , for all  $f : A \rightarrow B$ ,  $g : B \rightarrow C$ ,  $A, B, C \in \mathcal{C}$ .
2. (Preserves identity)  $F(\text{id}_A) = \text{id}_{F(A)}$  for all  $A \in \mathcal{C}$ .

□

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) *Given  $F \in \text{Hom}(\mathcal{C}, \mathcal{D})$ ,  $G \in \text{Hom}(\mathcal{D}, \mathcal{E})$ , we define the composition  $G \circ F : \mathcal{C} \rightarrow \mathcal{E}$  to be the functor sending an object  $A \in \mathcal{C}$  to  $G(F(A)) \in \mathcal{E}$ , and sending  $f \in \text{Hom}(A, B)$  to the map*

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

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

*Proof.* Verifying that rule given satisfies the composition axiom is trivial. The identity element of  $\mathcal{C}$  is the functor  $\text{id}_{\mathcal{C}} : \mathcal{C} \rightarrow \mathcal{C}$ , 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. □

This gives a natural notion of isomorphism between two categories. Namely, two categories  $\mathcal{C}$  and  $\mathcal{D}$  are isomorphic if there is an invertible functor between them. This is where the subtlety of the “find out what it should mean for two things to be equivalent” question of category theory shows its head. Requiring two categories to be isomorphic is often too restrictive. For instance, in Topological Quantum Computing, we find that models of quasiparticles correspond to certain categories up to a weaker notion of equivalence. Namely, letting  $F : \mathcal{C} \rightarrow \mathcal{D}$  and  $F^{-1} : \mathcal{D} \rightarrow \mathcal{C}$  be functors, requiring  $F^{-1} \circ F = \text{id}_{\mathcal{C}}$  and  $F \circ F^{-1} = \text{id}_{\mathcal{D}}$  is too restrictive. That is, we shouldn’t force the functors to be equal to the identity, only *isomorphic* to the identity. That is, there should be a natural transformation between  $F^{-1} \circ F$  and the identity, where natural transformations are defined as follows:

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

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

commutes.

□

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

$$\mathbf{Hom}(\mathcal{C}, \mathcal{D}) = \left( \begin{array}{l} \text{objects : Functors } \mathcal{C} \rightarrow \mathcal{D} \\ \text{morphisms : Natural transformations} \end{array} \right)$$

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

*Proof.* Let  $\eta^{(0)} : F_0 \rightarrow F_1$ ,  $\eta^{(1)} : F_1 \rightarrow F_2$ ,  $\eta^{(2)} : F_2 \rightarrow F_3$  be natural transformations, with  $F_1, F_1, F_2, F_3 : \mathcal{C} \rightarrow \mathcal{D}$  functors. We define the composition  $\eta^{(1)} \circ \eta^{(0)} : F_0 \rightarrow F_2$  by  $(\eta^{(1)} \circ \eta^{(0)})_A = \eta_A^{(1)} \circ \eta_A^{(0)}$ . This satisfies the composition law, since

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

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

With this, we can succinctly state the notion of equivalence we will use throughout this text. Two categories  $\mathcal{C}$  and  $\mathcal{D}$  are equivalent if there are functors  $F : \mathcal{C} \rightarrow \mathcal{D}$  and  $F^{-1} : \mathcal{D} \rightarrow \mathcal{C}$  such that  $F \circ F^{-1}$  and  $F^{-1} \circ F$  are both isomorphic (in the category  $\mathbf{Hom}(\mathcal{C}, \mathcal{D})$ ) to the identity. Whenever the category being assumed is unclear, we use the more precise notation  $\text{Hom}_{\mathcal{C}}(A, B)$  for morphisms in  $\mathcal{C}$ .

We make a comment about the above situation. We used as a key fact that the hom-spaces in the category  $\mathbf{Cat}$  can themselves be realized as categories. This is not a property unique to  $\mathbf{Cat}$ . There are many sets which not only

have morphisms (category structure), but 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 language of higher category theory in this manuscript, delving deeper into the mathematics of Topological Quantum Computing strongly uses  $n$ -categories. For instance, this is the founding philosophy of the  $n$ Lab, 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” -  $n$ Lab<sup>11</sup>

We now give such a story where category theory helps unify our understanding of concepts involved. Let  $V$  be a vector space, and let  $V^*$  denote the dual vector space, consisting of morphisms  $V \rightarrow \mathbb{C}$ . Both  $V$  and  $V^*$  have the same dimension, hence choosing bases when 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

$$\begin{aligned} V &\rightarrow V^{**}. \\ v &\mapsto (\varphi \mapsto \varphi(v)) \end{aligned}$$

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 keely on the fact that  $V$  is finite dimensional - it could fail in general, where we only have an embedding  $V \hookrightarrow V^{**}$ . We state this formally below as a proposition, leaving out details in the statement, which we fill in during the proof. This is standard practice in category theory. Definitions are all very similar, and the exact details are left implicit. Stating everything explicitly becomes quickly untenable, so this is a necessary measure.

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

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

---

<sup>11</sup>This is the first line of the  $n$ Lab’s “ $n$ POV” page.

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

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  $f^{**}(\varphi \mapsto \varphi(v)) \in W^{**}$ . Unwaveling 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  $V \rightarrow V^{**}$  are isomorphisms, so we can define a natural transformation  $(-)^{**} \rightarrow \text{id}_{\mathcal{C}}$  whose component  $(-)_V^*$  is the inverse of the double dual  $V \rightarrow V^{**}$ . 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, or more accurately, the functorial embedding  $V \hookrightarrow V^{**}$ . Switching perspectives from points to functions can be illuminating. While not a direct generalization, the version of duality most similar to this in category theory is known as Yoneda's lemma, where we can switch perspectives from objects to functors. We state it below, after a lemma.

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

*Proof.* Given  $f : A^{\text{op}} \rightarrow B^{\text{op}}$ ,  $g : B^{\text{op}} \rightarrow C^{\text{op}}$ ,  $h : C^{\text{op}} \rightarrow D^{\text{op}}$  with  $A, B, C, D \in \mathcal{C}$ , we define  $g^{\text{op}} \circ f^{\text{op}} = (f \circ g)^{\text{op}}$ . The composition law is verified by the composition

$$\begin{aligned}
h^{\text{op}} \circ (g^{\text{op}} \circ f^{\text{op}}) &= h^{\text{op}} \circ (f \circ g)^{\text{op}} \\
&= ((f \circ g) \circ h)^{\text{op}} \\
&= (f \circ (g \circ h))^{\text{op}} \\
&= ((g \circ h)^{\text{op}} \circ f^{\text{op}}) \\
&= (h^{\text{op}} \circ g^{\text{op}}) \circ f^{\text{op}}.
\end{aligned}$$

It is trivial to check that  $(\text{id}_A)^{\text{op}}$  serves as an identity element for  $A^{\text{op}}$ , so we are done.  $\square$

**Theorem 5.1** (Yoneda's Lemma). *Let  $\mathcal{C}$  be a category. We define a mapping*

$$\begin{aligned}\mathcal{C} &\rightarrow \mathbf{Hom}(\mathcal{C}^{\text{op}}, \mathbf{Set}). \\ A &\mapsto (B^{\text{op}} \mapsto \text{Hom}_{\mathcal{C}}(B, A))\end{aligned}$$

*This assignment is functorial. 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 that the assignment above is a fully faithful embedding of categories.*

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

$$\begin{aligned}\text{Hom}_{\mathcal{C}}(B, A) &\xrightarrow{\text{Hom}_{\mathcal{C}}(f, A)} \text{Hom}_{\mathcal{C}}(C, A). \\ \varphi &\mapsto \varphi \circ f\end{aligned}$$

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

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

$$\begin{aligned}\text{Hom}_{\mathcal{C}}(C, A) &\xrightarrow{\eta_C^{(f)}} \text{Hom}_{\mathcal{C}}(C, B). \\ \varphi &\mapsto f \circ \varphi\end{aligned}$$

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  $(C^{\text{op}} \mapsto \text{Hom}_{\mathcal{C}}(C, A))$  and  $(C^{\text{op}} \mapsto \text{Hom}_{\mathcal{C}}(C, B))$  will be literally different assignments. For instance, when  $C = A$ , then  $\text{Hom}(A, A)$  contains  $\text{id}_A$  but  $\text{Hom}(A, B)$  does not.

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

$$f = \eta_A^{(f)}(\text{id}_A) = \eta_A^{(g)}(\text{id}_A) = g.$$

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

for all  $C \in \mathcal{C}$  and  $\varphi \in \text{Hom}(C, A)$ . Since  $\eta$  is a natural transformation, the square corresponding to  $\varphi$  commutes:

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

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

The Yoneda lemma is considered one of the most fundamental results in category theory, while seemingly abstract it can quickly become very useful. It can be loosely read as saying that if two source objects has the “same” (i.e. naturally isomorphic) hom-sets into every other target object, then the source objects must be the same.

The Yoneda lemma can be stated in an alternative way, in the language of pairings. There is a natural map  $V \times V^* = V \times \text{Hom}(V, \mathbb{C}) \rightarrow \mathbb{C}$ , sending  $(v, \varphi)$  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  $\varphi$  then  $v = 0$ . There is a pairing on the level of categories,  $\mathcal{C} \times \mathcal{C}^{\text{op}} \rightarrow \mathbf{Set}$ , and the Yoneda lemma is exactly the statement that it is non-degenerate. 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 the product in the category of categories! Proving this alternative form of Yoneda’s Lemma, along with yet another, is found in Exercises 5.1 - 5.2. Explicitly, we can also describe the product as follows:

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

1. (Objects) Pairs  $(A, B)$ ,  $A \times B \in \mathcal{C} \times \mathcal{D}$
2. (Morphisms) We set

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

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

3. (Composition) Given  $(f_0, g_0) \in \text{Hom}((A_0, B_0), (A_1, B_1))$  and  $(f_1, g_1) \in \text{Hom}((A_1, B_1), (A_2, B_2))$ , we define

$$(f_1, g_1) \circ (f_0, g_0) = (f_1 \circ f_0, g_1 \circ g_0),$$

for all  $(A_0, B_0), (A_1, B_1), (A_2, B_2) \in \mathcal{C} \times \mathcal{D}$ .



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

*Proof.* Verifying that  $\mathcal{C} \times \mathcal{D}$  forms a category is trivial, so we omit the details. On the level of objects, we define

$$\begin{aligned}\pi_{\mathcal{C}} : \mathcal{C} \times \mathcal{D} &\rightarrow \mathcal{C} \\ (A, B) &\mapsto A\end{aligned}$$

and

$$\begin{aligned}\pi_{\mathcal{D}} : \mathcal{C} \times \mathcal{D} &\rightarrow \mathcal{D}. \\ (A, B) &\mapsto B\end{aligned}$$

It is trivial to show that these assignments are functorial. We now show that the triple  $(\mathcal{C} \times \mathcal{D}, \pi_{\mathcal{C}}, \pi_{\mathcal{D}})$  is a product. Suppose we are given a category  $\mathcal{E}$  and functors  $\tau_{\mathcal{C}} : \mathcal{E} \rightarrow \mathcal{C}$ ,  $\tau_{\mathcal{D}} : \mathcal{E} \rightarrow \mathcal{D}$ . We define the assignment

$$\begin{aligned}F : \mathcal{E} &\rightarrow \mathcal{C} \times \mathcal{D}. \\ E &\mapsto (\tau_{\mathcal{C}}(E), \tau_{\mathcal{D}}(E))\end{aligned}$$

The assignment of morphisms  $F(f) = (\tau_{\mathcal{C}}(f), \tau_{\mathcal{D}}(f))$  turns  $F$  into a functor. It is clear that the diagram

commutes. Seeing as  $F$  and  $\mathcal{E}$  were chosen arbitrarily, this completes the proof.  $\square$

This concludes our introduction to category theory. The canonical reference for category theory 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

[WORK: Add a “this will be our policy on including structures in statements” clause.]

The tensor product is an extremely important operation in linear algebra, especially in its applications to TQC. Braided monoidal categories are categories in which there is a generalization of the tensor product. Physically, this will represent “fusion”. Namely, a monoidal category  $\mathcal{C}$  will be a category along with a functor  $\otimes : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$  which satisfies axioms reminiscent of the tensor product. Namely, there will be a tensor unit  $1$  such that for all  $A, B, C \in \mathcal{C}$

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

The key subtlety in the theory is that these isomorphisms are *not* equalities. That is,  $1 \otimes A$  and  $A$  need not be equal - they only need be isomorphic. The above thus aren't just axioms - they're structures. One must make a *choice* of isomorphism. These choices should 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 original included more conditions than the treatment below - we give commentary about this in 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  $\mathcal{C}$ .
2. A functor  $\otimes : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$ .
3. (Identity) A distinguished element  $1 \in \mathcal{C}$ .
4. (Associativity) A natural equivalence  $\alpha : - \otimes (- \otimes -) \rightarrow (- \otimes -) \otimes -$ , where  $- \otimes (- \otimes -)$  denotes the functor  $\mathcal{C} \times \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$  sending  $(A, B, C)$  to  $A \otimes (B \otimes C)$ , and similarly for  $(- \otimes -) \otimes -$ .
5. (Left unitor) A natural equivalence  $\lambda : 1 \otimes - \rightarrow -$ , where  $1 \otimes -$  denotes the functor  $\mathcal{C} \rightarrow \mathcal{C}$  sending  $A$  to  $1 \otimes A$ , and  $-$  denotes the identity.
6. (Right unitor) A natural equivalence  $\rho : - \otimes 1 \rightarrow -$ , where  $- \otimes 1$  is the functor  $\mathcal{C} \rightarrow \mathcal{C}$  sending  $A$  to  $A \otimes 1$ .

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

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

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

commutes.

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

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

commutes.

□

The following theorem answers in what sense we really do get mileage out of considering categories in which we make strange choices of  $\alpha, \lambda, \rho$ , and in what sense we really do get mileage out of considering categories with multiple objects in the same equivalence class. The notion of monoidal equivalence is used in the theorem; we postpone the definition until after the statement:

**Theorem 5.2** ([HH09]). *Let  $(\mathcal{C}, \otimes_{\mathcal{C}}, \alpha_{\mathcal{C}}, \lambda_{\mathcal{C}}, \rho_{\mathcal{C}})$  be a monoidal category. Then*

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

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

This theorem really says that you cannot have your cake and eat it too. You can forget about non-trivial maps or you can forget about non-equal isomorphic objects, but you can't do both at once. Authors will often assume either one condition or the other (known as *strict* and *skeletal* respectively), and this

will sometimes lead to confusion across the literature. A monoidal equivalence between two categories is a pair of monoidal functors between them, such that both compositions are monoidally naturally equivalent to the identity.

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

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

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

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

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

commutes.

2. (Unitality) The diagrams

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

and

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

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

□

**Definition** (Monoidal natural transformation). A monoidal natural transformation between two functors  $(F_0, \mu_0, \epsilon_0)$  and  $(F_1, \mu_1, \epsilon_1)$  between monoidal categories  $(\mathcal{C}, \otimes_{\mathcal{C}}, 1_{\mathcal{C}})$  and  $(\mathcal{D}, \otimes_{\mathcal{D}}, 1_{\mathcal{D}})$  is a natural transformation  $\eta$  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  $A, B \in \mathcal{C}$ , the diagram

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

commutes.

2. (Compatibility with unit) The diagram

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

commutes.

□

We are now ready to define braiding on our monoidal categories:

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

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

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

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

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

and

$$\begin{array}{ccccc}
(A \otimes B) \otimes C & \xrightarrow{\alpha_{A,B,C}^{-1}} & A \otimes (B \otimes C) & \xrightarrow{\beta_{A,B \otimes C}} & (B \otimes C) \otimes A \\
\beta_{A,B} \otimes \text{id}_C \downarrow & & & & \downarrow \alpha_{B,C,A}^{-1} \\
(B \otimes A) \otimes C & \xrightarrow{\alpha_{B,A,C}^{-1}} & B \otimes (A \otimes C) & \xrightarrow{\text{id}_B \otimes \beta_{A,C}} & B \otimes (C \otimes A)
\end{array}$$

commute.

□

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

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

$$\begin{array}{ccc}
F(A) \otimes_{\mathcal{D}} F(B) & \xrightarrow{\beta_{\mathcal{D}; F(A), F(B)}} & F(B) \otimes_{\mathcal{D}} F(A) \\
\mu_{A,B} \downarrow & & \downarrow \mu_{B,A} \\
F(A \otimes_{\mathcal{C}} B) & \xrightarrow{F(\beta_{\mathcal{C}; A, B})} & F(B \otimes_{\mathcal{C}} A)
\end{array}$$

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

□

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 [WORK: find reference. Even just the coherence theorems would do.]

We now give our last relevant definition for monoidal categories - the opposite of a monoidal category. We note first given a functor  $F : \mathcal{C} \rightarrow \mathcal{D}$  there is a canonical functor  $F^{\text{op}} : \mathcal{C}^{\text{op}} \rightarrow \mathcal{D}^{\text{op}}$  defined by  $F^{\text{op}}(A^{\text{op}}) = F(A)$  for all  $A \in \mathcal{C}$ , and similarly for every natural transformation  $\eta$  between two functors there is canonical natural transformation  $\eta^{\text{op}}$  between the opposite of those two functors.

**Proposition 5.6.** . [WORK: define opposite category for monoidal/braided monoidal categories; state that it is a category of the correct form.]

*Proof.* . [WORK: Do the proof]

□

### Exercises:

- 5.1. Given a category  $\mathcal{C}$ , show that the mapping

$$\begin{aligned}\mathcal{C} \times \mathbf{Hom}(\mathcal{C}, \mathbf{Set}) &\rightarrow \mathbf{Set} \\ (A, F) &\mapsto F(A)\end{aligned}$$

is functorial. Use the Yoneda lemma to show that this pairing is non-degenerate, in the sense that if  $F(A) = G(A)$  for all  $A$  then  $F = G$ , and if  $F(A) = F(B)$  for all  $F$  then  $A = B$ .

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

$$\begin{aligned}\mathrm{Hom}(A, B) &\rightarrow \mathrm{Hom}_{\mathbf{Hom}(\mathcal{C}^{\mathrm{op}}, \mathbf{Set})}(\mathrm{Hom}_{\mathcal{C}}(B, -), \mathrm{Hom}_{\mathcal{C}}(A, -)) \\ \varphi &\mapsto (f \mapsto f \circ \varphi)\end{aligned}$$

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

- 5.3. Show that the following are functors.

- (a) The assignment  $\mathbb{C}[-] : \mathbf{finSet} \rightarrow \mathbf{Vecc}$  going from the category of finite sets to the category of (finite dimensional) vector spaces, when assigns to each set  $A$  the vector space  $\mathbb{C}[A]$ , and assigns to each function  $f : A \rightarrow B$  the linear map

$$\begin{aligned}\mathbb{C}[A] &\rightarrow \mathbb{C}[B] \\ \sum_{a \in A} c_a[a] &\mapsto \sum_{a \in A} c_a[f(a)]\end{aligned}$$

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

- 5.4. Let  $\mathcal{C}, \mathcal{D}$  be categories. Show that a functor  $F : \mathcal{C} \rightarrow \mathcal{D}$  induces an equivalence of categories (that is, admits a map  $F^{-1} : \mathcal{D} \rightarrow \mathcal{C}$  making  $(F, F^{-1})$  an equivalence of categories) if and only if it is full (surjective on hom sets), faithful (injective on hom sets), and essentially surjective (for every element  $A \in \mathcal{D}$ , there exists  $B \in \mathcal{C}$  such that  $F(B)$  is isomorphic to  $A$ ). Show that this result still holds in the setting of monoidal and braided monoidal categories. That is, a fully faithful essentially surjective (braided) monoidal functor will induce a (braided) equivalence of categories. (HINT: Construct  $F^{-1}$  arbitrarily 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 derive his results.

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

$$\begin{array}{ccc} (1 \otimes A) \otimes B & & \\ \alpha_{1,A,B} \downarrow & \searrow \lambda_A \otimes \text{id}_B & \\ 1 \otimes (A \otimes B) & \xrightarrow{\lambda_{A \otimes B}} & A \otimes B \end{array}$$

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

$$\begin{array}{ccccc} & & (1(1A)B) & \xrightarrow{\alpha_{1,1A,B}} & 1((1A)B) \\ & \nearrow \alpha_{1,1,A} & & & \searrow \alpha_{1,A,B} \\ ((11)A)B & \xrightarrow{\alpha_{11,A,B}} & (11)(AB) & \xrightarrow{\alpha_{1,1,AB}} & 1(1(AB)) \\ & \searrow \rho_1 & & & \nearrow \lambda_{AB} \\ & & (1A)B & \xrightarrow{\alpha_{1,A,B}} & 1(AB) \end{array}$$

and

$$\begin{array}{ccccc} ((11)A)B & \xrightarrow{\alpha_{1,1,A}} & (1(1A))B & \xrightarrow{\alpha_{1,1A,B}} & 1((1A)B) & \xrightarrow{\alpha_{1,A,B}} & 1(1(AB)) \\ & \searrow \rho_1 & \downarrow \lambda_A & & \downarrow \lambda_A & & \nearrow \lambda_{AB} \\ & & (1A)B & \xrightarrow{\alpha_{1,A,B}} & 1(AB) & & \end{array}$$

commute)

- (b) Let  $\mathcal{C}$  be a category. Define a tensor product on  $\text{Hom}(\mathcal{C}, \mathcal{C})$  by letting  $F \otimes G = F \circ G$ , for functors  $F, G : \mathcal{C} \rightarrow \mathcal{C}$ . Along with canonical associativity, unit, and unitors, show that this gives  $\text{Hom}(\mathcal{C}, \mathcal{C})$  the structure of a (not necessarily braided) monoidal category.



## 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:

- (a) There is a large amount of data that needs to be specified to define a TQFT. Namely, one needs to keep track of what vector spaces are assigned to every surface, and what morphisms are assigned to every bordism. As was seen in subsection 4.2, this can make defining TQFTs very difficult, and can lead to the verification of even basic axioms being difficult.
- (b) It is hard to deal directly with anyons (quasiparticles), which can make describing TQC (the braiding of anyons) very difficult. This is resolved in part by the consideration of *extended* TQFTs, where we allow punctures in surfaces to represent anyons, but this results in even more data to carry around.

To 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

$$\left( \begin{array}{l} \textbf{objects} : \text{finite collections of anyons} \\ \textbf{morphisms} : \text{motions/behaviors of anyons} \end{array} \right).$$

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 a finite set of numbers. At the end of the day, when measuring physical phenomena all one will get is a number - wavelength, spin, energy etc... Thus, any practical physical theory should be able to be boiled down to a collection of numbers.

The most fundamental operation on anyons is *fusion*, which we have up to now seldom discussed. The reason for this is that the elementary description of the toric code given in Section 3 works perfectly well without introducing fusion, so the notion was omitted for clarity. We now revisit the picture of Section 3, with our eyes towards fusion. Fusion is the process in which two elementary particles collide, and output other types of particles.

In the context of the toric code, we have discussed two types of quasiparticles: *X*-type and *Z*-type. When they fuse together, we get a third *Y*-type

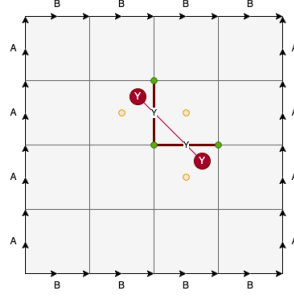


Figure 6.1: Movement of  $Y$ -type particles in toric code

particle. Seeing as  $X$ -type particles move along edges and  $Z$ -type particles move along faces, we observe that the intersection of the trajectory of an  $X$ -type particle and a  $Z$ -type particle must occur at the center of an edge. Moving the  $X$ -type particle along that edge corresponds to tensoring that edge with  $\sigma_X$ , and moving the  $Z$ -type particle corresponds to tensoring with  $\sigma_Z$ . Hence, creating two pairs of  $X$  and  $Z$  type particles and fusing them together corresponds to tensoring with  $\sigma_X \sigma_Z$ . Seeing as  $\sigma_X \sigma_Z = i\sigma_Y$ , we call these new particles  $Y$ -type particles.

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

To write out the full set of fusion rules for the toric code, we need one last particle type. Namely, the “do-nothing” particle that one gets when fusing a particle with its own antiparticle. While physically trivial, this particle is necceary to make our mathematical descriptions. Seeing as the do-nothing particle moves by doing nothing, we call it the  $I$ -type particle since it moves by tensoring with  $I$ . We denote  $a \otimes b$  for the fusion of two particles  $a$  and  $b$ . It will become clear in the category theoretic notation why the tensor product symbol is used. The fusion rules are given as a table below:

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

We make a few observations. The fact that  $X$  fused with  $Z$  is  $Y$  is by

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

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

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

This formula intuitively says that when  $a$  and  $b$  are fused this will result in a collection of particles, consisting of  $N_c^{a,b}$  copies of  $c$  for each  $c \in \mathcal{L}$ . This can be thought of as the generalization of a finite group, where now the group law is allowed to output formal linear combinations of elements in the group. These generalizations of groups are called *fusion systems*. Those fusion systems which satisfy a generalization of commutivity are called *braided fusion systems*, and correspond to braided fusion categories. Modular Tensor Categories are braided fusion categories which satisfy a certain non-degeneracy and symmetry condition. In this way, one can think of MTCs as being vast “non-degenerate” generalizations of finite abelian groups. We now formally state the definition of fusion system:

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

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

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

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

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

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

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

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

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

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

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

(c) (Associativity) We have

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

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

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

□

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

The next piece of the puzzle is based on one of the key ideas from category theory: Equal versus isomorphic. Given quasiparticles  $a, b, c$  fusing via  $(a \otimes b) \otimes c$  or  $a \otimes (b \otimes c)$  will result in the same particles. However, just because the particles present are the same does not mean that the quantum systems are the same. A huge theme in Section 3 is that changing order in processes like braiding might result in the same particles, but different states. Namely, different states in the same eigenspace. The processes  $(a \otimes b) \otimes c$  and  $a \otimes (b \otimes c)$  need only be equal up to an invertible linear transformation, i.e., isomorphism. We will define a  $6j$  fusion system to be a fusion system in which we have chosen isomorphisms between all  $(a \otimes b) \otimes c$  and  $a \otimes (b \otimes c)$ .

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

- (a) The diagrams are to be read from top to bottom.
- (b) Strands correspond to anyons.
- (c) Operations on strands correspond to operations on anyons.

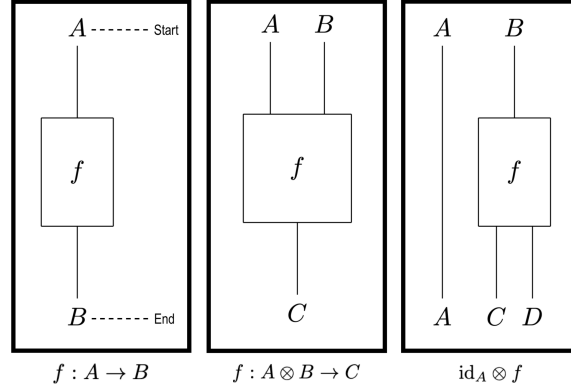
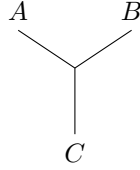


Figure 6.2: Examples of the quantum-algebraic graphical language

Some examples can be found in Figure 6.2. Some special functions are encoded via special graphical diagrams. For example, suppose we choose a distinguished function  $a \otimes b \rightarrow c$  to represent  $a \otimes b$  fusing into  $c$ . In general the choice is mostly arbitrary, and changing our choices of such functions is *gauge symmetry*, as will be formally defined later. Our informal notion of function will be put in firmer footing in Subsection 6.2 when we use category theory. We graphically write our distinguished function  $a \otimes b \rightarrow c$  as



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

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

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

$$= \sum_{m \in \mathcal{L}} F_{d;n,m}^{a,b,c}.$$

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

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

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

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

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

- ☐

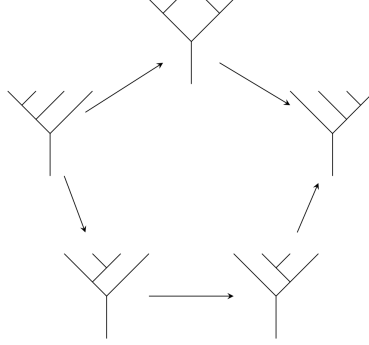


Figure 6.3: The pentagon axiom for  $6j$  symbols

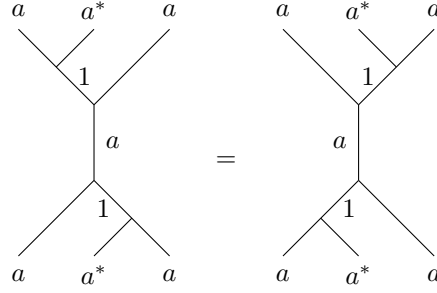
Seeing as these axioms are more complicated, we explain them all in detail. Admissibility of the triple  $(a, b, c)$  says that when  $N_c^{a,b} \neq 0$ , which is equivalent to saying that when  $a$  and  $b$  fuse, a  $c$  particle is created. In the language of functions, this is saying that there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

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

The pentagon identity is exactly the sort of identity for which graphical language is useful. As stated, it is quite non-obvious to decipher meaning from the expression. It becomes the statement that applying associativity in two different ways is identical. In graphical language, it becomes the fact that going either way around the 5-term diagram in Figure 6.3 gives the same answer (hence the name pentagon). All of terms in the pentagon are maps  $a \otimes b \otimes c \otimes d \rightarrow e$ . Each of the arrows 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 associivity on creating particles will be the same associativity on fusing particles. Diagrammatically, this means



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

“You work at a particle accelerator. You want to understand some particle. All you can do are throw other particles at it and see what happens. If you understand how your mystery particle responds to all possible test particles at all possible test energies, then you know everything there is to know about your mystery particle” - Ravi Vakil<sup>12</sup>.

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

We now define braided  $6j$  fusion systems. A braiding should give the relationship between  $a \otimes b$  and  $b \otimes a$ . These objects will be isomorphic, but not equal. For example, the fact that  $X$  and  $Z$  anticommute in the toric code is exactly the statement that isomorphism  $X \otimes Z \rightarrow Z \otimes X$  should

<sup>12</sup>This quote is folklore, relayed by a MathOverflow post of Theo Johnson-Freyd



be  $-1$  times the identity. Keeping with our Yoneda perspective, instead of giving an isomorphism  $a \otimes b$  and  $b \otimes a$  we give isomorphism between the spaces  $a \otimes b \rightarrow c$  and  $b \otimes a \rightarrow c$  for every  $c$ . Graphically, this can be seen in Figure [WORK: BRAID make figure]. The formal definition is as follows:

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

- (a) A  $6j$  fusion system  $(\mathcal{L}, N_{-,-}^-, F_{-,-,-}^-)$ .
- (b) 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:

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

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

□

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

[WORK: BRAID Make hexagon]

With all this, we can finally define an MTC:

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

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

□

In graphical language, the spherical condition looks like [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 in [WORK: BRAID make diagram].

It is important to remember that even though the definition is long, at the end of the day these are still just finite collections of numbers satisfying

a finite number of polynomial equations. This makes many things simple. For instance, we can define a morphism between fusion systems  $(\mathcal{L}, N)$  and  $(\mathcal{L}', N')$  to be a function  $f : \mathcal{L} \rightarrow \mathcal{L}'$  such that  $N_c^{a,b} = N_{f(c)}^{f(a),f(b)}$ . For  $6j$  fusion systems and braided  $6j$  fusion systems, we simply require that  $f$  should respect  $F$  symbols and  $R$  symbols as well. We can thus properly speak of fusion systems up to equivalence. We will see in the next section, however, that the correct notion of equivalence is a weaker *gauge equivalence*. This corresponds to keeping the same label set, but performing a local change of basis on  $F$  matrices.

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

- (a) Complex numbers  $f_c^{a,b}$  for all  $a, b, c \in \mathcal{L}$ .

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

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

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

□

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

[WORK: BRAID Give explanation of rectangle axiom, preferably with graphical language]

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

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

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

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

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

## 6.2 The category-theoretic viewpoint

In this subsection, we give the category theoretic perspective on Modular Tensor Categories (MTCs). As with subsection 6.1, we will build up to the definition of a MTC slowly. Thinking of MTCs as corresponding to “non-degenerate” finite abelian groups, we will start with the category-theory analogues of monoids<sup>13</sup>, groups, finite groups, finite abelian groups, and then end with non-degenerate finite abelian group. The category theory analogues are as below:

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

[WORK: Here lies the corpse of the definition of monoidal category]

We now define fusion categories. One key difficulty is deciding what category-theoretical object should correspond to the label set  $\mathcal{L}$  of a fusion system. The answer is as follows. We want general elements of  $\mathcal{C}$  to be uniquely representable as direct sums of the elements in the label set. The elements of  $\mathcal{C}$  which cannot be broken down further as direct sums of smaller objects are known as indecomposable objects. Direct sums are also known as biproducts because they can be alternatively defined as objects which simultaneously satisfy the axioms of a product, as well as the duals axioms of a “co”-product. This is explored in Exercise 6.7.

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

<sup>13</sup>A monoid is a set equipped with an associative binary operation and an identity element

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

does not split. An introduction to exact sequences is found in Appendix 5. What we really want is that every object should be the direct sum of objects which themselves have no subobjects. Objects with no subobjects are called irriducible objects. This discrepancy between irriducible and indecomposable forms one of the key themes of representation theory, and leads to a great deal of subtlety. Irrididucible objects are also called simple objects. Categories in which there is no discrepancy between irrididuble and indecomposable are called semisimple, i.e., semisimple categories are those categories in which every object is the direct sum of simple objects.

This discussion above strongly uses the notion of *subobject*. However, it is not clear in general what subobject should mean. The classic intuition is that  $A$  is a subobject of  $B$  if there is an injective map  $f : A \hookrightarrow B$ . Being injective is the statement that the kernel of  $f$  is 0, but in 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, and most categories people consider are abelian. In abelian categories, we require that all hom sets are 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 will correspond to superpositions. To preserve space, we combine “abelian” and “ $\mathbb{C}$ -linear” into one definition:

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

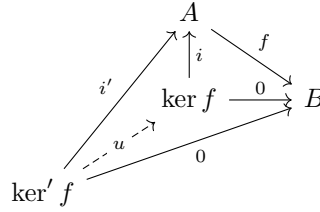
- (a) A category  $\mathcal{C}$ .
- (b) The structure of a  $\mathbb{C}$  vector space on  $\text{Hom}(A, B)$  for all  $A, B \in \mathcal{C}$ .

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

- (a) (Linearity) The composition map  $\text{Hom}(A, B) \times \text{Hom}(B, C) \rightarrow \text{Hom}(A, C)$  is bilinear for all  $A, B, C \in \mathcal{C}$ .
- (b) (Has a zero object) There is an object  $0 \in \mathcal{C}$  such that for every  $A \in \mathcal{C}$  there is a unique morphism  $0 \rightarrow A$ .
- (c) (Has binary biproducts) For all  $A, B \in \mathcal{C}$  the biproduct of  $A$  and  $B$  exists. This biproduct is denoted  $A \oplus B$ , and refered to as the direct sum. Here, we define the biproduct of  $A$  and  $B$  to be an object  $A \oplus B$ , paired with morphisms  $p_A, p_B : A \oplus B \rightarrow A, B$ , and  $i_A, i_B : A, B \rightarrow A \oplus B$ , such that
  - $p_X \circ i_Y$  is  $\text{id}_X$  when  $X = Y$ , and 0 otherwise,
  - $i_A \circ p_A + i_B \circ p_B = \text{id}_{A \oplus B}$ .

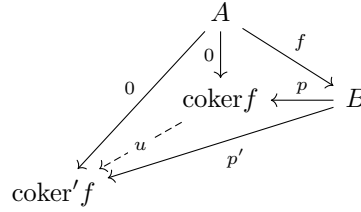
- (d) (Has kernels and cokernels) For all  $A, B \in \mathcal{C}$  and  $f : A \rightarrow B$ , we have objects  $\ker f, \operatorname{coker} f$ , and morphisms  $i : \ker f \rightarrow A$ ,  $p : B \rightarrow \operatorname{coker} f$ . We require that

- $f \circ i = 0$ .
- For any  $i' : \ker' f \rightarrow A$  with  $f \circ i' = 0$ , there is a morphism  $u : \ker' f \rightarrow \ker f$  such that



commutes.

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



commutes

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

□

We now can define exact sequence, as desired. Namely, given a morphism  $f : A \rightarrow B$ , we have a cokernel  $B \rightarrow \operatorname{coker} f$ . We define the image  $\operatorname{im} f$  of  $f$  to be the kernel of the cokernel. An exact sequence is defined to be a sequence of morphisms, in which the image of the incoming map at each object is equal to the kernel of the outgoing map. Alternatively, the image of  $f$  could be defined as the cokernel of the kernel. The fact that these two definitions of image coincide is *equivilant* to the fact that all monomorphisms and epimorphisms are normal. This is Exercise 6.5.

A non-abelian  $\mathbb{C}$ -linear category is a category whose hom spaces are  $\mathbb{C}$  vector spaces, and whose composition maps are linear, with no other restrictions. As always, when defining an object one must define the appropriate morphisms:

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

We will often assume implicitly that functors between  $\mathbb{C}$ -linear categories are abelian. With these definitions out of the way, we can now define fusion categories.

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

- (a) A  $\mathbb{C}$ -linear abelian monoidal category  $\mathcal{C}$ .
- (b) (Duals) Choices of objects  $A^*$  for every object  $A \in \mathcal{C}$ .
- (c) (Evaluation/co-evaluation) Choices of morphisms  $\text{ev}_A : A \otimes A^* \rightarrow 1$  and  $\text{coev}_A : 1 \rightarrow A^* \otimes A$  for all  $A \in \mathcal{C}$

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

- (a) The tensor product, associativity, left unitor, and right unitor of  $\mathcal{C}$  are all  $\mathbb{C}$ -linear functors.
- (b) (Rigidity) The diagrams

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

and

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

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

- (c) (Semisimplicity) Every object is the direct sum of finitely many simple objects. We call an object simple if it has no proper nontrivial subobjects.
- (d) All hom spaces are finite dimensional.

- (e) There are only finitely many isomorphism classes of simple objects
- (f) The tensor unit  $1$  is simple.

□

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

$$\begin{array}{c} A & 1 & A \\ | & | & | \\ \text{coev}_A & & \\ | & & \\ A^* & & \\ | & & \\ \text{ev}_A & & \\ | & & \\ 1 & A & A \end{array} = \begin{array}{c} A \\ | \\ A \\ | \\ A \end{array} \quad \text{and} \quad \begin{array}{c} 1 & A^* & A^* \\ | & | & | \\ \text{coev}_A & & \\ | & & \\ A & & \\ | & & \\ \text{ev}_A & & \\ | & & \\ A^* & 1 & A^* \end{array} = \begin{array}{c} A^* \\ | \\ A^* \\ | \\ A^* \end{array}$$

As is always implicit in graphical language, all associativity maps are suppressed by notation. Additionally, when we use the equality symbol we really mean “equal after applying the appropriate unitors”. Seeing as this is always what we will mean by equality, including floating tensor units is unnecessary and cumbersome, and will be omitted. Additionally, overwhelmingly the only maps  $A \otimes A^* \rightarrow 1$  and  $1 \rightarrow A^* \otimes A$  regularly being used are the evaluation/co-evaluation maps. Hence, when it does not cause confusion, we fix the notation

$$\text{ev}_A = \begin{array}{c} A^* & A \\ \searrow & \nearrow \\ & \end{array}, \quad \text{coev}_A = \begin{array}{c} & \\ \nearrow & \searrow \\ A^* & A \end{array}$$

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

$$\begin{array}{c} A & A \\ | & | \\ \text{ev}_A & \\ | & \\ A & A \end{array} = \begin{array}{c} A \\ | \\ A \end{array} \quad \text{and} \quad \begin{array}{c} A^* & A^* \\ | & | \\ \text{coev}_A & \\ | & \\ A^* & A^* \end{array} = \begin{array}{c} A^* \\ | \\ A^* \end{array}$$

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 broadened 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  $\mathcal{C}$  are true.*

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

$$\begin{array}{ccc} & A^* \otimes A & \\ \text{coev}_A \nearrow & \downarrow \sim & \nwarrow \text{ev}_A \\ 1 & & 1 \\ \text{co}\tilde{\text{ev}}_A \searrow & A \otimes \tilde{A}^* & \nearrow \tilde{\text{ev}}_A \end{array}, \quad \begin{array}{ccc} & A \otimes A^* & \\ \tilde{\text{coev}}_A \nearrow & \downarrow \sim & \nwarrow \text{ev}_A \\ A \otimes \tilde{A}^* & & 1 \end{array}$$

*commute.*

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

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

*in  $\text{Hom}(A^*, B^*)$  is a monoidal functor. Moreover, this functor induces a monoidal equivalence of between  $\mathcal{C}^{\text{op}}$  and  $\mathcal{C}$ .*

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

$$(\text{id}_{\tilde{A}^*} \otimes \text{ev}_A) \circ (\text{co}\tilde{\text{ev}}_A \otimes \text{id}_{A^*}) : A^* \rightarrow \tilde{A}^*$$

is an isomorphism, whose inverse is given by  $(\text{id}_{A^*} \otimes \tilde{\text{ev}}_A) \circ (\text{coev}_A \otimes \text{id}_{\tilde{A}^*})$ . Once this has been done, showing that the isomorphism satisfies the desired diagrams and that it is unique is straightforward and left as an exercise to the reader. We now compute

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

in graphical language as follows:



$$\begin{array}{c}
\text{Diagram 1: } A^* \text{ (bottom) } \xrightarrow{\text{coev}_A} A \xrightarrow{\text{ev}_A} \tilde{A}^* \xrightarrow{\text{ev}_A} A \xrightarrow{\text{coev}_A} A^* \text{ (top)} \\
= \\
\text{Diagram 2: } A^* \text{ (bottom) } \xrightarrow{\text{coev}_A} A \xrightarrow{\text{ev}_A} \tilde{A}^* \xrightarrow{\text{ev}_A} A \xrightarrow{\text{coev}_A} A^* \text{ (top)} \\
= \\
\text{Diagram 3: } A^* \text{ (bottom) } \xrightarrow{\text{coev}_A} A \xrightarrow{\text{ev}_A} A^* \text{ (top)} \\
= \\
\text{Diagram 4: } A^* \text{ (bottom) } \xrightarrow{\text{coev}_A} A \xrightarrow{\text{ev}_A} A^* \text{ (top)} \\
= \\
\text{Diagram 5: } A^* \text{ (bottom) } \xrightarrow{\text{coev}_A} A \xrightarrow{\text{ev}_A} A^* \text{ (top)}
\end{array}$$

The key point is that one can re-arrange the order of terms that affect disjoint strands, by the functoriality of the tensor product. This allows us to put the  $\tilde{\text{ev}}_A$  and  $\text{coev}_A$  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.

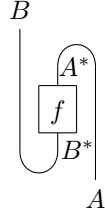
We now move on to point (2). We need to prove that if  $f^{\text{op}} : A^{\text{op}} \rightarrow B^{\text{op}}$  and  $g^{\text{op}} : B^{\text{op}} \rightarrow C^{\text{op}}$  are morphisms in  $\mathcal{C}^{\text{op}}$ , then  $(f \circ g)^* = g^* \circ f^*$ . Graphically, we have the diagram

$$f^* = \begin{array}{c} A^* \\ | \\ \boxed{f} \\ | \\ B^* \end{array}$$

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

$$g^* \circ f^* = \begin{array}{c} A^* \\ | \\ \boxed{g} \\ | \\ \boxed{f} \\ | \\ C^* \end{array} = \begin{array}{c} A^* \\ | \\ \boxed{g} \\ | \\ \boxed{f} \\ | \\ C^* \end{array} = (f \circ g)^*$$

as desired. The fact that  $(\text{id}_A)^* = \text{id}_{A^*}$  follows immediately from rigidity. [WORK: there are other axioms (probably trivial) to make this a monoidal functor]. 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 map  $\text{Hom}(A^*, B^*) \rightarrow \text{Hom}(B, A)$  taking the morphism  $f : A^* \rightarrow B^*$  to the composition



It is straightforward to see that this serves as an inverse to the duality map  $\text{Hom}(B, A) \rightarrow \text{Hom}(A^*, B^*)$ , and hence  $(-)^*$  induces isomorphisms on hom sets. To see that the functor is essentially surjective, [WORK: I don't see how to do this. It follows from a straightforward counting argument on fusion categories shows this is the case there, but I don't see how to go in full generality.]

□

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

**Proposition 6.2.** *Let  $\mathcal{C}$  be a fusion category. Let  $\mathcal{L}$  be the set of isomorphism classes of simple objects in  $\mathcal{C}$ . For any  $a, b, c \in \mathcal{L}$  with representatives  $A, B, C \in \mathcal{C}$ , define*

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

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

*Proof.* We verify the axioms one by one.

- (a) (Identity/Do-nothing) In a fusion category we assume that the tensor unit is simple, hence it gives an element in  $\mathcal{L}$ . 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  $1 \cong 1 \otimes 1' \cong 1'$ .
- (b) (Inverse/anti-particle) This property comes from the fact that duals of simple objects are simple and unique, and shown in Proposition 6.1.
- (c) (Associativity) This follows immediately from the existence of an associativity isomorphism on the monoidal structure of  $\mathcal{C}$ .

□

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

**Theorem 6.1** (Ocneanu rigidity, [GHS23]). *Let  $\mathcal{L}$  be a fusion system. There are finitely many (possibly 0) fusion categories, up to monoidal equivalence, which give systems equivalent to  $\mathcal{L}$  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  $\mathcal{C}$  be a  $\mathbb{C}$ -linear abelian category. An object  $A \in \mathcal{C}$  is simple, then  $\text{End}(A)$  is one dimensional. If  $A$  and  $B$  are non-isomorphic simple objects,  $\text{Hom}(A, B) = 0$ . If  $\mathcal{C}$  is semisimple, then  $\text{End}(A)$  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 non-trivial subobjects. Suppose  $A$  and  $B$  are simple. Let  $f : A \rightarrow B$  be a morphism. We have an exact sequence

$$0 \rightarrow \ker f \rightarrow A \xrightarrow{f} B \rightarrow \text{coker } f \rightarrow 0,$$

where by exact we mean that the image of each map in the sequence is equal to the kernel of the following map. 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

$$0 \rightarrow A \rightarrow B \rightarrow \text{coker } f \rightarrow 0.$$

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


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

Finally, suppose  $\mathcal{C}$  is semisimple. Let  $A$  be an object such that  $\text{End}(A)$  is one dimensional. By assumption, there is a finite set  $S$  of simple objects such that  $A = \bigoplus_{B \in S} B$ . 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 the properties of the biproduct, which implies that the direct sum can be pulled out of  $\text{Hom}$  in both the first and second argument (see Exercise 6.7). The second step follows from the fact that  $\text{Hom}(B_0, B_1)$  is one dimensional when  $B_0 \cong B_1$ , and 0 dimensional otherwise. If  $|S| \geq 2$ , then we thus get that  $\dim \text{End}(A) \geq 2$ , which is a contradiction. Hence,  $A$  is a simple object as desired.  $\square$

**Proposition 6.3.** *Let  $\mathcal{C}$  be a fusion category, with associated fusion system  $(\mathcal{L}, N_{-}^{-})$ . Assume further that  $\mathcal{C}$  is multiplicity free, in the sense that all  $N_{-}^{-} \in \{0, 1\}$ . For all triples  $a, b, c \in \mathcal{L}$ , choose representatives  $A, B, C \in \mathcal{C}$ . Additionally, seeing as each hom space  $\text{Hom}(A \otimes B, C)$  is at most one dimensional, we can choose distinguished generators*

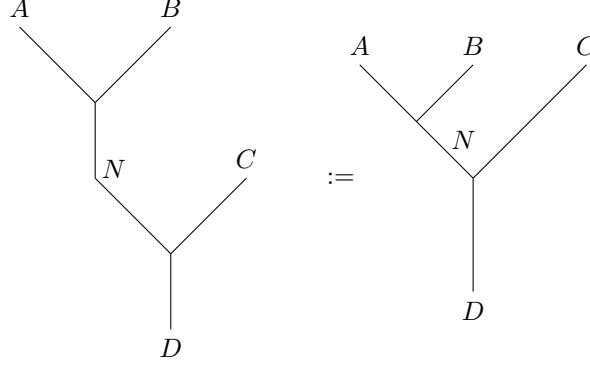


$\in \text{Hom}(A \otimes B, C) \cong \mathbb{C}.$

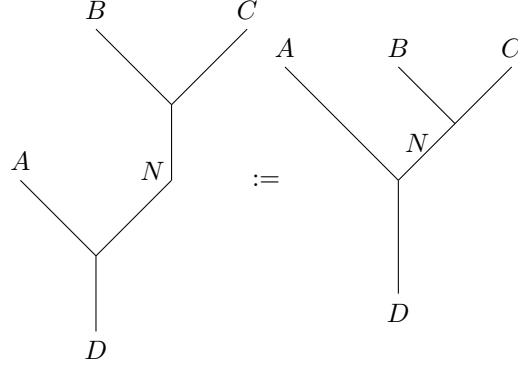
*These generators are chosen arbitrarily, except for the exceptional cases outlined below:*

$$\begin{array}{ccc}
\begin{array}{c} A \quad 1 \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \\ A \end{array} & = \rho_A, & \begin{array}{c} 1 \quad A \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \\ A \end{array} = \lambda_A, & \begin{array}{c} A^* \quad A \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \\ 1 \end{array} = \text{coev}_A.
\end{array}$$

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



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



In both bases,  $N$  ranges over representatives of isomorphism classes of simple objects. Define  $F_{d;n,m}^{a,b,c}$  to be  $[n, m]$  coefficient of the associativity morphism  $\alpha_{A,B,C} : \text{Hom}((A \otimes B) \otimes C, D) \rightarrow \text{Hom}(A \otimes (B \otimes C), D)$ , expressed as a matrix in the bases above, where we set  $F_{d;n,m}^{a,b,c} = 0$  if any of the relevant generators are zero (i.e.  $(a, b, c, d, n, m)$  is not admissible).

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

*Proof.* The proof of this equivalence is cumbersome. To streamline discussion, we leave the details of the verification of the correspondence between fusion categories and fusion systems in Appendix C  $\square$

**Theorem 6.3** ([Yam02]). *Let  $\mathcal{L}$  be a  $6j$  fusion system. There is a unique fusion category up to monoidal equivalence which gives  $\mathcal{L}$  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  $\mathcal{L}$ , the tensor product in terms of the fusion rules, and associativity in terms of the  $6j$  symbols. It is a natural consequence of the axioms of a  $6j$  fusion system

that the result category is a fusion category. Full details are found in Appendix C.  $\square$

We now give some commentary on Proposition 6.3, through the Yoneda perspective. Namely, we elaborate on why it is that we encode associative in terms of the induced map  $\text{Hom}((A \otimes B) \otimes C, D) \rightarrow \text{Hom}(A \otimes (B \otimes C), D)$  for all  $D$ , instead of as the original map  $(A \otimes B) \otimes C \rightarrow A \otimes (B \otimes C)$ . One pragmatic answer is that our hom spaces are vector spaces, not our objects, and so choosing bases of hom spaces is easier. Another 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  $\text{Hom}((A \otimes B) \otimes C, D)$  with  $\text{Hom}(A \otimes (B \otimes C), D)$ . Since ranging  $D$  over simple objects generates  $\mathcal{C}$  by semisimplicity, this means that we have associates  $\text{Hom}((A \otimes B) \otimes C, -)$  and  $\text{Hom}(A \otimes (B \otimes C), -)$  for all possible choices of target. Since our  $F$  matrices were chosen coherently, this assignment is a natural transformation. Thus, by the Yoneda lemma, this canonically specifies an isomorphism in  $\text{Hom}((A \otimes B) \otimes C, A \otimes (B \otimes C))$ , namely, the associator  $\alpha_{A,B,C}$ . While encoding  $\alpha_{A,B,C}$  as a collection of numbers proves difficult, encoding the associated natural transformation is simpler.

A braided fusion category is a fusion category whose underlying monoidal category is a braided monoidal category. There are no extra compatibility conditions.

**Proposition 6.4.** *Let  $\mathcal{C}$  be a multiplicity free braided fusion category, with associated 6j fusion system  $(\mathcal{L}, N_{-}^{-}, F_{-}^{-})$ . For all triples  $a, b, c \in \mathcal{L}$ , choose representatives  $A, B, C \in \mathcal{C}$ . We define*

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

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

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

*Proof.* The proof of this proposition is found in Appendix C.  $\square$

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 are now ready to give our final definition:

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

- (a) A braided fusion category  $\mathcal{C}$ .
- (b) (Twist) A natural isomorphism  $\theta : \text{id}_{\mathcal{C}} \rightarrow \text{id}_{\mathcal{C}}$ .

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

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

$$\beta_{A,B} \circ \beta_{B,A} = \text{id}_{A \otimes B},$$

then  $A \cong 1$ .

□

**Definition** (Braided tensor functor). A braided tensor functor between two MTCs  $(\mathcal{C}, \theta_{\mathcal{C}})$ ,  $(\mathcal{D}, \theta_{\mathcal{D}})$  is a braided monoidal functor  $F : \mathcal{C} \rightarrow \mathcal{D}$  such that  $F(\theta_{\mathcal{C};A}) = \theta_{\mathcal{D};A}$  for all  $A \in \mathcal{C}$ .

□

This allows us to state our final equivariance:

**Proposition 6.5.** *The process in Proposition 6.4 gives a one-to-one correspondence between Modular Tensor Categories up to modular equivariance and modular tensor fusion systems up to gauge equivariance.*

*Proof.* The proof of this fact is in Appendix C.

□

The intuition for the twist of a MTC is that it helps deal with the non-triviality of the braiding. In particular, it allows one to define the *trace* of a morphism  $f : A \rightarrow A$ . The trace is a powerful operation, since it allows you to describe maps in terms of numbers, can be used both for linearization and invariants. The formal definition and basic properties of trace are as follows:

**Proposition 6.6.** *Let  $(\mathcal{C}, \otimes, \beta, \theta, \text{ev}, \text{coev})$  be a modular tensor category. For any  $A \in \mathcal{C}$  and  $f \in \text{End}(A)$ , we define*

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

*The space  $\text{End}(1)$  is one dimensional by Schur's Lemma (Theorem 6.2), with generator  $\text{id}_1$ . Hence, we can canonically identify  $\text{tr}(f)$  with a complex number. Graphically, we represent trace as the closed loop [WORK: BRAID make diagram, fix notation for un-standard cup and cap using twist to make this rigorous].*

*For all  $A, B \in \mathcal{C}$ , the following claims are all true:*

- (a)  $\text{tr}(f \otimes g) = \text{tr}(f) \cdot \text{tr}(g)$  for all  $f \in \text{End}(A)$ ,  $g \in \text{End}(B)$
- (b)  $\text{tr}(f \oplus g) = \text{tr}(f) + \text{tr}(g)$  for all  $f \in \text{End}(A)$ ,  $g \in \text{End}(B)$
- (c)  $\text{tr}(f \circ g) = \text{tr}(g \circ f)$  for all  $f, g \in \text{End}(A)$
- (d) .[WORK:  $\text{tr}(f^*) = \text{tr}(f)$ ?]
- (e) .[WORK: BRAID 2nd formula for trace, putting  $\beta$  and  $\theta$  before  $f$ ]
- (f) Trace is independent of choice of duals. That is, let  $(\tilde{A}^*, \text{co}\tilde{\text{ev}}_A, \tilde{\text{ev}}_A)$  be a different choice of dual for  $A$ . Defining  $\tilde{\text{tr}}(f)$  exactly like  $\text{tr}(f)$  except with this new unit, we find that  $\tilde{\text{tr}}(f) = \text{tr}(f)$ .
- (g) Trace is preserved by functors. That is, let  $\mathcal{C}, \mathcal{D}$  be MTCs with traces  $\text{tr}_{\mathcal{C}}, \text{tr}_{\mathcal{D}}$  respectively. Let  $F : \mathcal{C} \rightarrow \mathcal{D}$  be a braided tensor functor. We have that  $\text{tr}_{\mathcal{D}}(F(f)) = \text{tr}_{\mathcal{C}}(f)$ .

*Proof.* .[WORK: BRAID do proof] □

The trace allows us to naturally define many very powerful, physically observable, and mathematically interesting invariants. For example, let  $A \in \mathcal{C}$  be an object in an MTC. Then,  $\text{tr}(\text{id}_A)$  measures in some sense the size of  $A$ . For a vector space, the trace of the identity gives the dimension of the vector space. Thus, we define  $d_A = \text{tr}(\text{id}_A)$  to be the *quantum dimension* of  $A$ . The following properties give a taste of the deep mathematics present in this situation:

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

- (a)  $d_A = 1$  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  $B \in \mathcal{C}$ .
- (b) ([WORK: get reference]) If  $1 \leq d_A \leq 2$ , then  $d_A = 2 \cos(\pi/m)$  for some integer  $m \geq 3$ . Otherwise,  $d_A \geq 4$ .
- (c) ([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] □

This theorem is quite useful experimentally. It is the goal of many physicists to discover 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 the proposed methods [BSS06]. Thus, one observes non-abelian anyons indirectly by measuring physical quantities which are associated with non-abelian properties. 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 measurely 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 readily physically measured. Namely, the thermodynamic Maxwell's equation relates entropy to chemical potential, which in turn can be measured by simple changes in voltage [CS09].

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

$$\dim \mathcal{C} = \sum_{A \in \mathcal{L}} d_A^2,$$

where as usual  $\mathcal{L}$  is the set of isomorphism of classes of simple objects. The trace is well defined on isomorphism classes, and hence this quantity is well defined. The twisting of  $\mathcal{C}$  allows for a twisting of the definition of  $\dim \mathcal{C}$ . This results in the following very interesting Gauss sums:

**Theorem 6.5** ([Vaf88]). *Let  $\mathcal{C}$  be an MTC, and let  $\mathcal{L}$  be the set of isomorphism classes of simple objects. For each simple object  $A \in \mathcal{C}$ ,  $\theta_A \in \text{End}(A)$  lives in a one dimensional space with generator  $\text{id}_A$ . Hence, we can canonically identify  $\theta_A$  with a complex number, and this complex number is independent of isomorphism class. Define*

$$p_{\mathcal{C}}^{\pm} = \sum_{A \in \mathcal{L}} \theta_A^{\pm 1} d_A^2.$$

*The quantities  $\theta_A$  for all  $A$ , as well as  $p_{\mathcal{C}}^+/p_{\mathcal{C}}^-$ , are all roots of unity. Additionally,*

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

We are now ready to define the most important invariants of MTCs, representations of the group of 2 by 2 matrices with unit determinant,  $\text{SL}_2(\mathbb{Z})$ . The group  $\text{SL}_2(\mathbb{Z})$  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 representation as follows:

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

$$S_{a,b} = \text{tr}(\beta_{A,B} \cdot \beta_{B,A}) = [\text{WORK} : \text{BRAIDmake graphical formula}]$$

*where  $a, b$  are isomorphism classes of simple objects with representatives  $A, B$ . Similarly, we define the  $T$ -matrix of an MTC to be the  $n$  by  $n$  diagonal matrix whose  $[a, a]$ th coefficient is  $\theta_A$ . The map*

$$\begin{aligned}\rho_{\mathcal{C}} : \mathrm{SL}_2(\mathbb{Z}) &\rightarrow \mathrm{Aut}(\mathbb{C}[\mathcal{L}]) \\ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} &\mapsto \frac{1}{\sqrt{\dim \mathcal{C}}} \cdot S, \\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} &\mapsto \frac{\sqrt[3]{p_{\mathcal{C}}^+}}{\sqrt[6]{\dim \mathcal{C}}} \cdot T.\end{aligned}$$

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

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

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

- ([Bru00]) Suppose  $\mathcal{C}$  is a category satisfying all of the conditions of a MTC, except for non-degeneracy (this is called a *pre-modular category*). Then,  $\mathcal{C}$  is modular if and only if the  $S$ -matrix is invertible.
- ([BNRW16]) There are finitely many MTCs, up to braided monoidal equivalence, of a given rank.
- ([NS10]) The modular representations of MTCs have finite image.

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

In this section we introduce the MTC which corresponds to the toric code,  $\mathcal{Z}(\mathrm{Vec}_{\mathbb{Z}_2})$ . 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*  $\mathrm{Vec}_G$ . 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  $\alpha$  and the second copy of  $\mathbb{Z}_2$  is generated by  $\beta$ . 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  $\mathcal{C}$  with a twist” procedure is the Drinfeld center,  $\mathcal{Z}(\mathcal{C})$ . Hence, the MTC attached to the toric code is  $\mathcal{Z}(\mathrm{Vec}_{\mathbb{Z}_2})$ .

The category  $\mathrm{Vec}_G$  of  $G$ -graded vector spaces can be defined when  $G$  is any set. Endowing  $G$  with more algebraic structure corresponds to endowing  $\mathrm{Vec}_G$  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 have the following:

$$\mathbf{Vec}_G = \left( \begin{array}{l} \text{objects : collections of } \mathbb{C} \text{ vector spaces } \{V_g\}_{g \in G} \\ \text{morphisms : collections of } \mathbb{C}\text{-linear maps} \end{array} \right).$$

That is, a morphism between  $\{V_g\}_{g \in G}$  and  $\{W_g\}_{g \in G}$  is a collection of linear maps  $\{f_g : V_g \rightarrow W_g\}_{g \in G}$ . 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 will often be 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  $\mathbf{Vec}_G$ :

**Lemma 6.1.** *Let  $G$  be a set. Given  $V, W \in \mathbf{Vec}_G$ ,  $\text{Hom}_{\mathbf{Vec}_G}(V, W)$  is a sub vector space of  $\text{Hom}_{\mathbf{Vec}}(V, W)$ . Hence, we can naturally endow  $\text{Hom}_{\mathbf{Vec}_G}(V, W)$  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.

- (a) (Linearity) This is trivial to verify.
- (b) (Has a zero object) Define the object  $0$  to be the (unique)  $G$ -graded vector space for which  $0_g$  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  $0_g \rightarrow V_g$  for all  $g \in G$ , and hence there is a unique map  $0 \rightarrow V$ . Thus,  $0$  is a zero object.
- (c) (Has binary biproducts) Given  $V, W \in \mathbf{Vec}_G$ , we define  $V \oplus W$  to be the object with  $(V \oplus W)_g = V_g \oplus W_g$ , where  $\oplus$  is the direct sum of vector spaces. The projection maps  $p_V$  (resp.  $p_W$ ) 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.
- (d) (Has kernels and cokernels) For all  $V, W \in \mathbf{Vec}_G$  and  $f : V \rightarrow W$ , we define  $\ker f$  and  $\text{coker} f$  on  $g$ -components by  $(\ker f)_g = \ker f_g$  and  $(\text{coker} f)_g = \text{coker} f_g$ . On the right hand side of these formulas,  $\ker$

and coker are being used as the standard notions of kernel (elements in  $V_g$  that get mapped to zero) and cokernel ( $W_g/\text{im} f_g$ ) from linear algebra. The map  $i : \ker f \rightarrow V$  is the natural inclusion map from a subspace, and the map  $p : B \rightarrow \text{coker} f$  is the natural projection map onto a kernel. We show that the kernel satisfies the desired universal property, and leave the kernel as an exercise to the reader since the proof is identical.

The fact that  $f \circ i = 0$  follows from the definition of kernel. Suppose that  $i' : \ker' f \rightarrow A$  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  $u$  be  $i'$  with codomain restricted to  $\ker f$ , it is tautological the desired diagram commutes. Thus, this completes the proof.

- (e) (All monomorphisms and epimorphisms are normal) Let  $f : A \rightarrow B$  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 an 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 for the reader. Note that the converses to all of these statements are true - injection, kernel, and monomorphism are all synonyms in this case.

- (monomorphism  $\implies$  injective) Suppose  $f : V \rightarrow W$  is a monomorphism. Consider two maps  $\ker f \rightarrow V$ , 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  $f : V \rightarrow W$  is injective. Define  $\tilde{f} : W \rightarrow W/V$  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  $\tilde{f}$  satisfies the universal property of  $\ker \tilde{f}$ . Suppose that  $i' : \ker' \tilde{f} \rightarrow W$  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  $u : \ker' \tilde{f} \rightarrow V$  to be the map equal to  $i'$  but with restricted codomain. It is clear that the desired diagram commutes, and hence we are done.

□

**Proposition 6.7.** *Let  $G$  be a monoid. Define the structures for a monoidal category as follows:*

- (a) (Underlying category)  $\mathbf{Vec}_G$ .

- (b) (Tensor product)  $\otimes : \mathbf{Vec}_G \times \mathbf{Vec}_G \rightarrow \mathbf{Vec}_G$  sending  $(V, W)$  to the object whose  $g$ -component is given by

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

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

- (c) (Identity)  $1 = \mathbb{C}_e$ , where  $e \in G$  is the identity element of  $G$ .  
(d) (Associativity) Given  $V, W, X$  we define  $\alpha$  on the  $g$ -component by the natural map

$$\begin{aligned} ((V \otimes W) \otimes X)_g &= \bigoplus_{(hk)l=g} (V_h \otimes W_k) \otimes X_l \\ &\quad \downarrow \\ \bigoplus_{h(kl)=g} V_h \otimes (W_k \otimes X_l) &= (V \otimes (W \otimes X))_g, \end{aligned}$$

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

- (e) (Unitors) Given  $V$ , we define  $\lambda$  on the  $g$ -component by the obvious map

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

where  $g \in G$ . The definition of  $\rho$  is completely analagous.

These structures give a well-defined monoidal category.

*Proof.* Verifying the triangle and pentagon identities comes down to a simple unwravelling of definitions; we leave the proof as an exercise to the reader.  $\square$

**Proposition 6.8.** *Let  $G$  be a finite group. Define the structures for a fusion category as follows:*

- (a) (Underlying  $\mathbb{C}$ -linear abelian monoidal category)  $\mathbf{Vec}_G$ .  
(b) (Duals) Given  $V \in \mathcal{C}$ , we define the dual by

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

- (c) (Evaluation) Given  $V \in \mathcal{C}$ , we define  $\text{ev}$  as the map on the  $e$ -component as

$$\begin{aligned} (V \otimes V^*)_e &= \bigoplus_{g \in G} V_g \otimes (V_g)^* \rightarrow \mathbb{C}_e, \\ &\quad \bigoplus_{g \in G} v \otimes \varphi \mapsto \varphi(v) \end{aligned}$$

and zero otherwise.

- (d) (Co-evaluation) Given  $V \in \mathcal{C}$ , we define  $\text{coev}$  as the map on the  $e$ -component as the map

$$\begin{aligned}\mathbb{C}_e &\rightarrow \bigoplus_{g \in G} (V_g)^* \otimes V_g = (V^* \otimes V)_e, \\ x &\rightarrow \bigoplus_{g \in G} \text{coev}_{V_g}(x)\end{aligned}$$

and zero otherwise. The map  $\text{coev}_{V_g}$  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

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

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

These structures give a well-defined fusion category.

*Proof.* We check the axioms one by one.

- (a) 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.
- (b) (Rigidity) To begin, we verify that  $\text{coev}_{V_g}$  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 change 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

$$\begin{aligned}\sum_i \tilde{v}_i \otimes \tilde{\varphi}_i &= \sum_i \left( \sum_j c_{i,j} \cdot v_j \right) \otimes \left( \sum_k (c^{-1})_{k,i} \cdot \varphi_k \right) \\ &= \sum_{j,k} \left( \sum_i c_{i,j} (c^{-1})_{k,i} \right) \cdot v_j \otimes \varphi_k.\end{aligned}$$

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

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

as desired, and hence  $\text{coev}_{V_g}$  is well defined. 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 is clear, however, since we can choose 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 hence the equality is obvious.

- (c) (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  $g \in G$ . Hence, going back through the argument, we find that  $V$  is the direct sum of simple object.
- (d) Since  $\mathbf{Vec}$  only consists of finite dimensional vector spaces, all of 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.
- (e) We claim that there is a natural bijection between the set  $G$  and the simple objects of  $\mathbf{Vec}_G$ , sending  $g \in G$  to  $\mathbb{C}_g \in \mathbf{Vec}_G$ . To prove this, we observe the following. If the total dimension of the object is more than 1, then there will be a subobject. Hence, the only simple objects will be one-dimensional vector spaces on one component. That is,  $G$ -graded vector spaces isomorphic to  $\mathbb{C}_g$  for some  $g \in G$ . Since  $G$  is finite, we get the desired result.
- (f)  $\mathbb{C}_e$  has total dimension 1, and is clearly simple.

□

**Proposition 6.9.** *Let  $G$  be a finite abelian group. Define the structures for a braided fusion category as follows:*

- (a) (Underlying fusion category)  $\mathbf{Vec}_G$ .
- (b) (Braiding) Given  $V, W \in \mathbf{Vec}_G$ , we define  $\beta$  on the  $g$ -component by

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

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

These structures give a well-defined braided monoidal category.

*Proof.* Demonstrating the hexagon identities follows from simply unwraveling definitions, and is left as an exercise to the reader. □

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

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

the monoid of elements that commute with all other elements. When defining the center of an MTC, we find ourself having a subtle issue. Commutativity in the context of monoids is replaced by braiding in the context of categories. While commutativity of monoids is a property - do the elements commute or not - braiding of categories is a structure. One needs to choose a choice of braiding, of which there can be many. The center  $\mathcal{Z}(\mathcal{C})$  of an MTC  $\mathcal{C}$  thus consists of elements  $A \in \mathcal{C}$ , along with choices of natural isomorphism between the functors  $A \otimes -$  and  $- \otimes A$ . That is, elements of  $\mathcal{C}$  that commute under  $\otimes$  with every other element of  $\mathcal{C}$ , and a functorial choice of how that commuting should be done.

**Proposition 6.10.** *The Drinfeld center of a monoidal category  $\mathcal{C}$  is a braided monoidal category defined as follows:*

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

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

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

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

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

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

- **unit:** The element  $(1, \rho \circ \lambda^{-1})$
- **braiding:** We define the braiding between two elements  $(A, \beta_{A,-}), (B, \beta_{B,-}) \in \mathcal{Z}(\mathcal{C})$  to be  $\beta_{A,B} = \beta_{A,B}$ .

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

*Proof.* Inheriting the definition of composition of morphisms from  $\mathcal{C}$ , it is straightforward to check that  $\mathcal{Z}(\mathcal{C})$  does indeed form a category. The extra  $\beta_{-,-}$  doesn't change the structure of diagrams, and so inheriting further the definition of unitors from  $\mathcal{C}$  we find that the triangle and pentagon axioms follow immediately from the triangle and pentagon axioms on  $\mathcal{C}$ . The one



thing to be checked is that all of the morphisms satisfy the compatibility condition required to a morphism in  $\mathcal{Z}(\mathcal{C})$ , but this is straightforward. Finally, we remark on the hexagon identities. The condition imposed of  $\beta_{A,B \otimes C}$  given is technically incorrect. To make the parentheses work in the braiding one has to add associators, and impose the longer condition

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

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. This makes the first hexagon identity tautological.

The last thing one must verify is that 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  $A, B \in \mathcal{Z}(\mathcal{C})$ ,  $C, D \in \mathcal{C}$ :

$$\begin{aligned} \beta_{A \otimes B, C \otimes D} &= (\beta_{A, C \otimes D} \otimes \text{id}_B) \circ (\text{id}_A \otimes \beta_{B, C \otimes D}) \\ &= (\text{id}_C \otimes \beta_{A,D} \otimes \text{id}_B) \circ (\beta_{A,C} \otimes \text{id}_D \otimes \text{id}_B) \circ (\text{id}_A \otimes \text{id}_C \otimes \beta_{B,D}) \circ (\text{id}_A \otimes \beta_{B,C} \otimes \text{id}_D) \\ &= (\text{id}_C \otimes \beta_{A,D} \otimes \text{id}_B) \circ (\text{id}_A \otimes \text{id}_C \otimes \beta_{B,D}) \circ (\beta_{A,C} \otimes \text{id}_D \otimes \text{id}_B) \circ (\text{id}_A \otimes \beta_{B,C} \otimes \text{id}_D) \\ &= (\text{id}_C \otimes \beta_{A \otimes B, D}) \circ (\beta_{A \otimes B} \otimes \text{id}_D). \end{aligned}$$

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 6.11.** *Let  $\mathcal{C}$  be a fusion category. Define the following data for a fusion category:*

- (a) *(Underlying  $\mathbb{C}$ -linear abelian monoidal category)  $\mathcal{Z}(\mathcal{C})$ , with vector space structure on hom-spaces inherited from  $\mathcal{C}$ .*
- (b) *(Duals) Given  $(A, \beta_{A,-}) \in \mathcal{Z}(\mathcal{C})$ , we define the dual to be  $(A^*, \beta_{A^*, -})$ , where  $\beta_{A^*, -}$  is the composition*

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

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

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

- (a) (Linearity) This is a straightforward computation, which we leave as an exercise.
- (b) (Has a zero object) Let  $0 \in \mathcal{C}$  be the zero object. It is clear that  $0 \otimes A \cong 0$  for all  $A \in \mathcal{C}$ , and hence the defining property of the zero object says that there is a unique map  $0 \times A \rightarrow A \times 0$ . Thus, there is a unique half-braiding  $\beta_{0,-}$ . It is straightforward to verify that  $(0, \beta_{0,-}) \in \mathcal{C}$  is a zero object.
- (c) (Has binary biproducts) Choose  $A, B \in \mathcal{Z}(\mathcal{C})$ . We define a canonical half braiding  $\beta_{A \oplus B, -}$  on  $A \oplus B$  by the following formula, for all  $C \in \mathcal{C}$ :

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

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.

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

$$\begin{array}{ccc} B \otimes C & \xrightarrow{\beta_{B,C}} & C \otimes B \\ \uparrow f \otimes \text{id}_C & & \uparrow \text{id}_C \otimes f \\ A \otimes C & \xrightarrow{\beta_{A,C}} & C \otimes A \\ \uparrow & & \uparrow \\ \ker A \otimes C & \xrightarrow{\beta_{\ker A, C}} & C \otimes \ker A \end{array}$$

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

- (e) (All monomorphisms and epimorphisms are normal) Endowing kernels/cokernels with their canonical half-braidings, it is immediate to show that every monomorphism and epimorphism is normal.

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

- (a) It is straightforward to verify that the tensor product, associativity, and unitors are  $\mathbb{C}$ -linear, so we leave this as an exercise to the reader.
- (b) (Rigidity) Diagrams commuting in  $\mathcal{C}$  implies they commute in  $\mathcal{Z}(\mathcal{C})$ , hence rigidity is immediate. However, one does need to make sure that  $\beta_{A^*, -}$  is a valid half-braiding, as well as that  $\text{ev}$  and  $\text{coev}$  satisfy the compatibility condition required to be morphisms in  $\mathcal{C}$ . Seeing as the only term in the definition of  $\beta_{A^*, B \otimes C}$  that deals with  $B \otimes C$  is  $\beta_{A, -}$ , the fact that  $\beta_{A, -}$  is a half-braiding immediately implies that  $\beta_{A^*, -}$ . The fact that  $\text{ev}_A$  and  $\text{coev}_A$  satisfy the compatibility conditions follows from a straightforward computation.
- (c) (Semisimplicity) Suppose  $A \in \mathcal{Z}(\mathcal{C})$ . Suppose that there is a decomposition  $A \cong A_0 \oplus A_1$  of  $A$  in  $\mathcal{C}$ . We can canonically define the half braiding  $\beta_{A_0, -}$  by being the composition

$$A_0 \otimes B \xrightarrow{i_0 \otimes B} A \otimes B \xrightarrow{\beta_{A, B}} B \otimes A \xrightarrow{\text{id}_B \otimes p_0} B \otimes A_0,$$

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  $\mathcal{Z}(\mathcal{C})$ . Moreover, one can verify that the isomorphism  $A \cong A_0 \oplus A_1$  now is a  $\mathcal{Z}(\mathcal{C})$ . Hence, whenever one can decompose in  $\mathcal{C}$  one can also decompose in  $\mathcal{Z}(\mathcal{C})$ . If the underlying  $\mathcal{C}$ -object of a  $\mathcal{Z}(\mathcal{C})$ -object is simple, then that  $\mathcal{Z}(\mathcal{C})$ -object must be simple. Hence, since every element is the  $\mathcal{C}$ -direct sum of simple  $\mathcal{C}$  objects we conclude that every object is the  $\mathcal{Z}(\mathcal{C})$ -direct sum of simple  $\mathcal{Z}(\mathcal{C})$  objects.

- (d) All hom spaces in  $\mathcal{Z}(\mathcal{C})$  are subspaces of hom spaces in  $\mathcal{C}$ , hence they must be finite dimensional.
- (e) From the discussion of semisimplicity, we find that the simple objects in  $\mathcal{Z}(\mathcal{C})$  are exactly those objects whose underlying  $\mathcal{C}$ -object is simple. We first prove a lemma: On a given simple object  $A \in \mathcal{C}$ , the half-braidings on  $A$  are linearly independent as elements of the vector space  $\bigoplus_{B \in \mathcal{C}} \text{Hom}(A \otimes B, B \otimes A)$ .

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  $B, C \in \mathcal{C}$

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

Without loss of generality, we can assume that the  $\{\beta_{A, -}^{(i)}\}$  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  $\lambda_i$ , 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  $\mathcal{Z}(\mathcal{C})$  are a linearly independent subset of

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

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

$$\sum_{a,b \in \mathcal{L}} \dim \text{Hom}(a \otimes b, b \otimes a),$$

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

- (f) The unit 1 being simple is immediate from the above discussion.

□

We now show that these Drinfeld centers are MTCs. In general, not every fusion category's center will be an MTC. The categories whose centers are naturally MTCs are known as *spherical categories*. The slogan for spherical categories is that they are the minimal situation in which the categorical trace (as in Proposition 6.6) is well defined and has desirable properties.

**Proposition 6.12.** *Let  $G$  be a finite group. Define the following data for an MTC:*

- (a) *(Underlying braided fusion category)  $\mathcal{Z}(\mathbf{Vec}_G)$ .*
- (b) *(Twist) Given  $(V, \beta_{V,-}) \in \mathcal{C}$ , we define the twist  $\theta_{(V, \beta_{V,-})}$  by the composition*

$$V \xrightarrow{\text{coev}_{V^*}} V \otimes V^* \otimes V^{**} \xrightarrow{\beta_{V, V^*}} V^* \otimes V \otimes V^{**} \xrightarrow{\text{ev}_V} V^{**} \rightarrow V.$$

*The last arrow  $V^{**} \rightarrow V$  is the double dual map of linear algebra,*

$$\begin{aligned} V &\xrightarrow{\sim} V^{**} \\ v &\mapsto (\varphi \mapsto \varphi(v)) \end{aligned}$$

This gives  $\mathcal{Z}(\mathbf{Vec}_G)$  the structure of an MTC.

*Proof.* We verify the axioms one at a time.

- (a) .[WORK: BRAID Do the proof.]
- (b) .[WORK: BRAID This seems really annoying as well.]
- (c) (Non-degeneracy) .[WORK: BRAID How do I define the right half-braiding? Hopefully there's an explicit construction...]

□

We observe the key use of the vector space double-dual map for our definition. This is no coincidence. Spherical categories - those categories whose Drinfeld centers are MTCs - are required to have natural isomorphisms between the double dual functor  $(-)^{**}$  and the identity. It is a fascinating feature of the theory that this is not always a-priori the case. What is the following:

**Theorem 6.8** ([ENO05]). *Let  $\mathcal{C}$  be a fusion category. There is a natural monoidal equivalence between the identity functor on  $\mathcal{C}$  and the quadruple dual functor  $(-)^{****}$ .*

It is a deep conjecture that two duals should always suffice. This would lead to a larger number of spherical categories, and hence a larger number of MTCs:

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

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 naturally have isomorphisms  $(-) \rightarrow (-)^{**}$ , and thus admit spherical structures. This is discussed in detail in Appendix B.

Thus, we have arrived at the MTC associated with the toric code:  $\mathcal{Z}(\mathbf{Vec}_{\mathbb{Z}_2})$ , The Drinfeld center 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, as  $\mathcal{Z}(\mathcal{C})$  for some  $\mathcal{C}$ . The simplest fusion categories are those which come from groups, as  $\mathbf{Rep}_G$  for some  $G$ . The simplest non-trivial group is  $\mathbb{Z}_2$ .

Another intuition for  $\mathcal{Z}(\mathcal{C})$ , 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  $\mathcal{C}$  with a twist is seen as follows.

Suppose  $(\mathcal{C}, \beta)$  is a braided monoidal category. Then, there is a canonical braided monoidal functor

$$\begin{aligned}\mathcal{C} &\rightarrow \mathcal{Z}(\mathcal{C}). \\ A &\mapsto (A, \beta_{A,-})\end{aligned}$$

Let  $\mathcal{C}^{\text{rev}}$  denote the braided monoidal category whose underlying monoidal category is  $\mathcal{C}$ , but the braiding between  $A, B$  is given by  $\beta_{B,A}^{-1}$  instead of  $\beta_{A,B}$ .<sup>14</sup> That is, the same category but with the braiding reversed. There is a canonical braided monoidal functor

$$\begin{aligned}\mathcal{C}^{\text{rev}} &\rightarrow \mathcal{Z}(\mathcal{C}). \\ A &\mapsto (A, \beta_{-,A}^{-1})\end{aligned}$$

These two functors in some sense generate  $\mathcal{Z}(\mathcal{C})$ , and thus  $\mathcal{Z}(\mathcal{C})$  can be seen as  $\mathcal{C}$  and  $\mathcal{C}^{\text{rev}}$  glued together in a non-degenerate fashion.

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

**Proposition 6.13.** *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*

*WORK: do proof. This should come down to explicitly giving a set of representatives of isomorphism classes.* □

## Exercises:

6.1. The standard definition of Topological Quantum Field Theory is in terms of functors, which we present here.

- (a) Define the following structures for a braided monoidal category:
  - A. (Objects) Closed oriented  $n$ -manifolds.
  - B. (Morphisms) A morphism between closed oriented  $n$ -manifolds  $Y_0, Y_1$  is an oriented  $(n+1)$ -manifold  $X$  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.

---

<sup>14</sup> $\mathcal{C}^{\text{rev}}$  is *not* equal to  $\mathcal{C}^{\text{op}}$ .

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

D. (Unit)  $\emptyset$

Along with natural choices of associativity, left/right unit, and braiding, show that this forms a braided monoidal category,  $\mathbf{Bord}(n+1)$ .

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

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

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

6.7. Let  $\mathcal{C}$  be an MTC, and let  $\mathcal{L}$  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  $\mathcal{C}$  can be expressed in terms of the twist, fusion coefficients, and quantum dimensions as follows:

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

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

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

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

- (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  $\operatorname{coker}(\ker f) \xrightarrow{\bar{f}} \ker(\operatorname{coker} f)$  uniquely to make the below diagram commute:

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

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

- 6.9. Let  $\mathcal{C}, \mathcal{D}$  be monoidal categories (resp. braided monoidal categories, MTCs). Let  $F : \mathcal{C} \rightarrow \mathcal{D}$  be monoidal functor (resp. braided monoidal functor, braided tensor functor). Show that  $F$  induces a monoidal equivalence of categories (resp. braided monoidal equivalence of categories, braided tensor equivalence of categories) if and only if  $F$  is fully faithful and essentially surjective (c.f. Exercise 5.4).

- 6.10. There is a canonical braided monoidal functor

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

where  $\beta_{-, -}$  is the natural braiding on the fusion category of vector spaces. Show that this is an equivalence of categories. [WORK: how do you do this?]

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

- Show that the direct sum (biproduct)  $A \oplus B$  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  $\mathcal{C}$ , and the triple  $((A \oplus B)^{\operatorname{op}}, (i_A)^{\operatorname{op}}, (i_B)^{\operatorname{op}})$  is a product in  $\mathcal{C}^{\operatorname{op}}$ .
- Given a morphism  $f : A \rightarrow B$ , show that there are canonical isomorphisms  $A \cong \operatorname{im} f \oplus \ker f$  and  $B \cong \operatorname{im} f \oplus \operatorname{coker} f$ .

- 6.12. Let  $A, B, C$  be objects a fusion category  $\mathcal{C}$ .

- For any  $A, B, C \in \mathcal{C}$ , show that the natural maps

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

and



$$\begin{aligned}\mathrm{Hom}(C, A \oplus B) &\rightarrow \mathrm{Hom}(A, C) \oplus \mathrm{Hom}(B, C) \\ f &\mapsto (p_A \circ f) \oplus (p_B \circ f)\end{aligned}$$

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

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

## 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: 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<sup>15</sup>

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

## 7.2 Revisiting toric code TQC

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

## 7.3 Universal TQC with the Fibonacci anyon

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

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

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

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

Why can I always lift cellulations? 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

---

<sup>15</sup>[WORK: make description][Aub19]

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

The goal of homology theory is to describe cycles on a geometric object, up to deformations. If one cycle can be continuously deformed into another, then they should be considered equivalent. On the sphere, for example, all loops can be contracted away into nothing. On the torus there are four distinct cycles, namely, the zero cycle, the cycle that goes around the torus horizontally, the cycle that goes around the torus vertically, and the cycle that twists around the torus, as in Figure 3.2. These non-trivial cycles correspond exactly to the continuous vector fields described in the introduction [Fra57].

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

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

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

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

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

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

1. Cycles being continuously deformed to each other

2. Cycles that can be obtained from one another by flipping edges along the boundary of faces.

The worry regarding the distinction between these two notions is justified. In general, the group obtained by imposing the equivalence relation of continuous deformations will not be equal to the homology group  $H_1(X)$ . The group resulting from imposing the continuous deformation restriction is called the *fundamental group* of  $X$ , and is denoted  $\pi_1(X)$ . In general  $\pi_1(X)$  can be quite a bit larger than  $H_1(X)$ , i.e., the equivalence relation can be weaker. The groups are always related by the fact that  $H_1(X)$  is canonically isomorphic to the abelianization of  $\pi_1(X)$ , i.e., the maximal abelian quotient of  $\pi_1(X)$ . 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 stronger notion Hilbert spaces. This can be rectified by imposing the condition of *unitarity* on TQFTs and MTCs. This condition can be described abstractly as adding a functorial inner product, and requiring that all relevant transformations are unitary. 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  $\dagger : \text{Hom}(V(S_0), V(S_1)) \rightarrow \text{Hom}(V(S_1), V(S_0))$  for all surfaces  $S_0, S_1$ .

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

1. (Preserves conjugation)  $Z(X^\dagger) = Z(X)^\dagger$ . Here  $S_0, S_1$  are surfaces, and  $X$  is a bordism from  $S_0$  to  $S_1$ . We define  $X^\dagger$  to be the bordism which is the same underlying manifold, but with its orientation reversed.  $X^\dagger$  is a bordism from  $S_1$  to  $S_0$ .
2. (Unitarity) The map  $\langle \cdot | \cdot \rangle : \text{Hom}(V(S_0), V(S_1)) \times \text{Hom}(V(S_0), V(S_1)) \rightarrow \mathbb{C}$  defined by  $\langle f | g \rangle = \text{tr}(f \circ g^\dagger)$  is an inner product, endowing  $\text{Hom}(V(S_0), V(S_1))$  with the structure of a Hilbert space.

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

□

Really, this condition is just saying that  $V(S)$  should be compatibly given the structure of Hilbert spaces. 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  $f : V(Y_0) \rightarrow V(Y_1)$  we define  $f^\dagger$  to be the unique map such that

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

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

**Proposition B.1.** *Equipped with its natural conjugation structure, the  $\mathbb{Z}_2$  Dijkgraaf-Witten theory is a unitary  $(2+1)$ -TQFT.*

*Proof.* . [WORK: do proof.]

□

This also has a functorial interpretation. We saw in Exercise 6.1 that a  $(2+1)$  TQFT can be viewed as a braided monoidal functor  $\mathbf{Bord}(2+1) \rightarrow \mathbf{Vec}$ . This functorial language very naturally captures our setting:

**Proposition B.2.** *Define a unitary  $(n+1)$ -TQFT to be a braided monoidal functor*

$$\mathbf{Bord}(n+1) \rightarrow \mathbf{Hilb}$$

*such that  $Z(X^\dagger) = Z(X)^\dagger$  for all bordisms  $X$ . This can canonically be identified with the above definition of unitary TQFT when  $n = 2$ .*

*Proof.* . [WORK: do proof]

□

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  $\mathcal{L}$  which is gauge equivalent to a  $6j$  fusion system  $\mathcal{L}'$  such that  $F_d^{a,b,c}$  is a unitary matrix for all  $a, b, c, d \in \mathcal{L}'$ .  $\square$

**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  $\mathcal{L}'$  such that  $F_d^{a,b,c}$  is a unitary matrix for all  $a, b, c, d \in \mathcal{L}'$ .  $\square$

We now proceed in category-theoretic language.

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

1. An fusion category  $\mathcal{C}$ .
2. (Conjugation) A linear map  $\dagger : \text{Hom}(A, B) \rightarrow \text{Hom}(B, A)$  for all  $A, B \in \mathcal{C}$ .

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

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

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

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

2.  $(f^\dagger)^\dagger = f$  for all  $f \in \text{Hom}(A, B)$ ,  $A, B \in \mathcal{C}$ .
3.  $(f \circ g)^\dagger = g^\dagger \circ f^\dagger$  for all  $f \in \text{Hom}(B, C), g \in \text{Hom}(A, B)$ ,  $A, B, C \in \mathcal{C}$ .
4.  $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$  for all  $f \in \text{Hom}(A, B), g \in \text{Hom}(C, D)$ ,  $A, B, C, D \in \mathcal{C}$ .
5.  $(\text{coev}_A)^\dagger \circ (f \otimes \text{id}_{A^*}) \circ \text{coev}_A = \text{tr}(f)$  for all  $A \in \mathcal{C}$

$\square$

The study of unitary fusion categories is much nicer than the study of fusion categories, as there is a trace. This allows for one to define quantum dimensions and all of the other invariants one would want from a trace. Normally, this requires the twist of an MTC.

**Proposition B.3.** *Let  $\mathcal{C}$  be a unitary fusion category. For all  $A, B \in \mathcal{C}$ , the following claims are true:*

1.  $\text{tr}(f \otimes g) = \text{tr}(f) \cdot \text{tr}(g)$  for all  $f \in \text{End}(A)$ ,  $g \in \text{End}(B)$

2.  $\text{tr}(f \oplus g) = \text{tr}(f) + \text{tr}(g)$  for all  $f \in \text{End}(A)$ ,  $g \in \text{End}(B)$
3.  $\text{tr}(f \circ g) = \text{tr}(g \circ f)$  for all  $f, g \in \text{End}(A)$

*Proof.* . [WORK: BRAID do proof] □

We can now define an MTC. The compatibility conditions for the twist defined such that the definition for 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  $\mathcal{C}$ .
2. (Conjugation) A linear map  $\dagger : \text{Hom}(A, B) \rightarrow \text{Hom}(B, A)$  for all  $A, B \in \mathcal{C}$ .

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

1. Forgetting the twist and braiding,  $(\mathcal{C}, \dagger)$  forms a unitary fusion category.
  2.  $(\beta_{A,B})^\dagger = \beta_{A,B}^{-1}$  for all  $A, B \in \mathcal{C}$ .
  3.  $(\theta_A)^\dagger = (\theta_A)^{-1}$  for all  $A \in \mathcal{C}$ .
  4.  $(\text{ev}_A)^\dagger = (\text{id}_{A^*} \otimes \theta_A^{-1}) \circ \beta_{A^*,A}^{-1} \circ \text{coev}_A$  for all  $A \in \mathcal{C}$
  5.  $(\text{coev}_A)^\dagger = \text{ev}_A \circ \beta_{A,A^*} \circ (\theta_A \otimes \text{id}_{A^*})$  for all  $A \in \mathcal{C}$
- 

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  $\mathcal{C}$  be an MTC, and  $\mathcal{L}$  be the set of isomorphism classes of simple objects. The modular representation*

$$\rho_{\mathcal{C}} : \text{SL}_2(\mathbb{Z}) \rightarrow \text{Aut}(\mathbb{C}[\mathcal{L}])$$

*is unitary, in the sense that all matrices in the image are unitary. In particular, the S-matrix of every MTC is unitary.*

We saw in Subsection 6.3 that the Drinfeld center of a fusion category is not necessarily an MTC, as defining the twist requires a natural isomorphism between the double dual functor  $(-)^{**}$  and the identity. Unitary fusion categories can use their conjugation to define a double dual map, and thus we have the following:

**Proposition B.4.** *Let  $\mathcal{C}$  be a unitary fusion category. Define the data for a unitary MTC as follows:*

1. (Underlying braided fusion category)  $\mathcal{Z}(\mathcal{C})$ .
2. (Twist) Given  $(A, \beta_{A,-}) \in \mathcal{C}$ , we define the twist  $\theta_{(A, \beta_{A,-})}$  by the composition

$$A \xrightarrow{\text{coev}_{A^*}} A \otimes A^* \otimes A^{**} \xrightarrow{\beta_{A, A^*}} A^* \otimes A \otimes A^{**} \xrightarrow{\text{ev}_A} A^{**} \rightarrow A.$$

The last arrow  $A^{**} \rightarrow A$  is defined to be the inverse of

$$A \xrightarrow{\text{coev}_{A^*}} A \otimes A^* \otimes A^{**} \xrightarrow{(\text{coev}_A)^\dagger} A^{**}.$$

Along with the natural conjugation inherited from  $\mathcal{C}$ , this endows  $\mathcal{Z}(\mathcal{C})$  with the structure of a unitary MTC.

*Proof.* . [WORK: BRAID do proof.] □

This allows us to state a formula which makes somewhat explicit our intuition of  $\mathcal{Z}(\mathcal{C})$  as a “quantum double” of  $\mathcal{C}$ :

**Proposition B.5.** *Let  $\mathcal{C}$  be a unitary fusion category, and let  $\mathcal{L}$  be the set of isomorphism classes of simple objects of  $\mathcal{C}$ . Given  $a \in \mathcal{L}$  with representative  $A \in \mathcal{C}$ , we define*

$$d_a = \text{tr}(\text{id}_A).$$

*Additionally, define  $\dim \mathcal{C} = \sum_{a \in \mathcal{L}} d_a^2$ . We have that*

$$\dim \mathcal{Z}(\mathcal{C}) = (\dim \mathcal{C})^2.$$

*. [WORK: Add the fact that the gauss sums are both equal to  $\dim \mathcal{C}$ ]*

*Proof.* . [WORK: It would be AMAZING if I could prove this.] □

Of course, as always there is an equivalence between the language of fusion systems and the language of categories:

**Proposition B.6.** *Let  $\mathcal{C}$  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  $\mathcal{C}$ .*

*Similarly, let  $\mathcal{C}$  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  $\mathcal{C}$ .*

*Proof.* We give proofs of these results in Appendix C. □

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 as fusion categories, the category  $\mathbf{Vec}$  of finite dimensional vector spaces and  $\mathbf{Hilb}$  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.7.** *There is a braided monoidal equivalence of categories  $\mathbf{Vec} \xrightarrow{\sim} \mathbf{Hilb}$ .*

*Proof.* Let  $F : \mathbf{Hilb} \rightarrow \mathbf{Vec}$  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. Hence, the proposition follows from Exercise 6.6.  $\square$

**Proposition B.8.** *Let  $G$  be a finite group. Fix an equivalence of categories  $\mathbf{Hilb} \xrightarrow{\sim} \mathbf{Vec}$ . Define the data for a unitary fusion category as follows:*

1. (Underlying fusion category)  $\mathbf{Vec}_G$ .
2. (Conjugation) Given  $f : V \rightarrow W$ , define  $f^\dagger : W \rightarrow V$  as follows. First, endow  $V$  and  $W$  with the structure of Hilbert spaces via the equivalence  $\mathbf{Hilb} \xrightarrow{\sim} \mathbf{Vec}$ . Then, make  $f^\dagger$  act on  $W_g$  by the conjugate transpose of  $f$ . This is well defined, since the conjugate transpose can be specified in a Hilbert space as the unique map  $f^\dagger$  such that for all  $v \in V_g, w \in W_g$

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

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  $f : V \rightarrow V$ ,  $V \in \mathbf{Vec}_G$ . Namely we show that

$$\mathrm{tr}_{\mathbf{Vec}_G}(f) = \sum_{g \in G} \mathrm{tr}(f_g),$$

where  $f_g : V_g \rightarrow V_g$  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  $\mathbf{Vec}$  agree with the standard linear algebra traces. Moreover, from the base case of  $\mathbf{Vec}$  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 1s 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 coevaluation map is the conjugate transpose of the evaluation map. We thus see from the definition of trace that

$$\mathrm{tr}(f) = \sum_{i \in I} \varphi_i(f(v_i)).$$

The term  $\varphi_i(f(v_i))$  is exactly the  $i$ th diagonal entry of the matrix representation of  $f$  in the basis  $v_i$ , and thus we recover  $\mathrm{tr}$  as a sum of diagonal entries. Moreover, we observe that linear trace adds over direct sums. If we think of  $f : V \rightarrow V$  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 categorically or by linear algebra methods is the same.

From this we observe that the categorical inner product  $\langle \cdot | \cdot \rangle$  defined by  $\langle f | g \rangle = \text{tr}(f \cdot g^\dagger)$  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.4, 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. Thus, it is philosophically more correct to say that the unitary MTC associated with the toric code is not  $\mathcal{Z}(\mathbf{Vec}_{\mathbb{Z}_2})$ , but  $\mathcal{Z}(\mathbf{Hilb}_{\mathbb{Z}_2})$ .

As in the non-unitary case, there is an equivalence between unitary MTCs and (1-extended) unitary TQFTs [WORK: find source]. Under this equivalence,  $\mathcal{Z}(\mathbf{Hilb}_{\mathbb{Z}_2})$  as a unitary MTC is identified with the  $\mathbb{Z}_2$  Dijkgraaf-Witten theory as a unitary TQFT. Seeing as all physically realizable systems will be unitary, practically speaking it is this correspondence which is the most important.

## C Fusion System/MTC correspondance

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.

[WORK: Give full proofs for the correspondance between fusion systems and MTCs.]

## D Anyon data

[WORK: Add a section detailing the data for popular anyon models/MTCs. A discussion of the fillings of the Hall states and their corresponding (conjectural) models is found in [BGH<sup>+</sup>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<sup>+</sup>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<sup>+</sup>16] Sven Marian Albrecht, Andrew P Higginbotham, Morten Madsen, Ferdinand Kuemmeth, Thomas Sand Jespersen, Jesper Nygård, Peter Krogstrup, and CM Marcus. Exponential protection of zero modes in majorana islands. *Nature*, 531(7593):206–209, 2016.
- [Aub19] Clément Aubert. Categories for me, and you? *arXiv preprint arXiv:1910.05172*, 2019.
- [BGH<sup>+</sup>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 Bruguières. 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.
- [CS09] NR Cooper and Ady Stern. Observable bulk signatures of non-abelian quantum hall states. *Physical review letters*, 102(17):176807, 2009.
- [Day21] Cyrus Lawrence Day. *Quipus and Witches’ Knots: The Role of the Knot in Primitive and Ancient Culture, with a Translation and Analysis of” Oribasius de Laqueis”*. University Press of Kansas, 2021.
- [dF17] Giovanni de Felice. Hopf algebras in quantum computation. *Unpublished doctoral dissertation*, 2017.
- [DLF<sup>+</sup>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.
- [ENO05] Pavel Etingof, Dmitri Nikshych, and Viktor Ostrik. On fusion categories. *Annals of Mathematics*, pages 581–642, 2005.
- [FKLW03] Michael Freedman, Alexei Kitaev, Michael Larsen, and Zhenghan Wang. Topological quantum computation. *Bulletin of the American Mathematical Society*, 40(1):31–38, 2003.
- [FKW02] Michael H Freedman, Alexei Kitaev, and Zhenghan Wang. Simulation of topological field theories by quantum computers. *Communications in Mathematical Physics*, 227:587–603, 2002.
- [FLW02] Michael H Freedman, Michael Larsen, and Zhenghan Wang. A modular functor which is universal for quantum computation. *Communications in Mathematical Physics*, 227:605–622, 2002.
- [Fra57] Theodore Frankel. Homology and flows on manifolds. *Annals of Mathematics*, pages 331–339, 1957.
- [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. *Advances in Mathematics*, 414:108853, 2023.
- [Got98] Daniel Gottesman. Theory of fault-tolerant quantum computation. *Physical Review A*, 57(1):127, 1998.
- [Hal13] Brian C Hall. *Quantum theory for mathematicians*. Springer, 2013.
- [Hat05] Allen Hatcher. *Algebraic topology*. Tsinghua University Press, 2005.
- [HH09] Tobias J Hagge and Seung-Moon Hong. Some non-braided fusion categories of rank three. *Communications in Contemporary Mathematics*, 11(04):615–637, 2009.
- [Kan98] Bruce E Kane. A silicon-based nuclear spin quantum computer. *nature*, 393(6681):133–137, 1998.
- [Kel64] Gregory Maxwell Kelly. On mac\_lane’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<sup>+</sup>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<sup>+</sup>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.
- [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.
- [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*. Number 112. 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.
- [Yam02] Shigeru Yamagami. Polygonal presentations of semisimple tensor categories. *Journal of the Mathematical Society of Japan*, 54(1):61–88, 2002.
- [YZB<sup>+</sup>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.