The Algebraic Theory of Topological Quantum Information

by Milo Moses

California Institute of Technology

August 12, 2024

Abstract

This book aims to give a comprehensive account of the algebraic theory of topological quantum information. It is intended to be accessible both to mathematicians unfamiliar with quantum mechanics and theoretical physicists unfamiliar with category theory. Additionally, this text should make a good reference for working researchers in the field. A primary focus of this text is balancing powerful algebraic generalities with concrete examples, principles, and applications.

To my mentors

0 Preface

This book is a mathematical treatment of topological quantum information, with a focus on formal algebraic aspects and a special eye towards topological quantum computation. This manuscript began as an extended set of notes from a course on topological quantum field theory given by Zhenghan Wang in the winter of 2022 at UC Santa Barbara. Through his courses, his private tutoring, and his reccomendations, Zhenghan took me from a state of almost complete ignorance of mathematical physics to being a young researcher in the field. I am greatly emdebted to him for this, and it is certain that this book would not have existed without his guidance - he richly deserves of my apple.

This book would not have been possible without the tutelage of my esteemed mentors. Those who most direct contributed are the ones who used their time and energy to teach me topological quantum information - Dave Aasen, Mike Freedman, and Yuri Lensky. There are also those who took a chance on a young mathematician when they had every reason not to - Roald Dejean, Peter Bloomsburgh, Edward Frenkel, and Ken Ribet.

[WORK: There's some other people to thank. Andrew Sylvester for letting me try out my arguments on him.]

Great pains have been taken to make this book as pedagogical and accessable as possible. The hope is that it should be readable by both mathematicians unfamilar with quantum mechanics as well as theoretical physicists unfamiliar with category theory. A primary focus of this text is balancing powerful algebraic generalities with concrete examples, principles, and applications. The prerequisites for this book are a undergraduate-level understanding of topology, linear algebra, and group theory, as well as a popular-science level of familarity with quantum mechanics.

There are already many great references to learn aspects of the material covered in this book. An excellently written and relatively complete book on topological quantum information from the perspective of a physicist is Steven Simon's text [Sim23]. Simon's book is algebraic, but does *not* include any category theory. The main references for the relevant category theory are Bakalov-Kirillov [BK$^+$01] and Etingof-Gelaki-Nikshych-Ostrik [EGNO16]. While both excellent texts, they suffer notable shortcomings for learning topological quantum information. Bakalov-Kirillov was written in 2001, making it outdated. Etingof-Gelaki-Nikshych-Ostrik is modern, but makes no connections to physics and does not use the language of string diagrams. The manuscript most similar to this one is Kong-Zhang's preprint [KZ22]. We distinguish ourself from Kong-Zhang by our different choice of topics, our different choice of treatment, and our extended scope. Other relevant books and review articles include Wang's monograph [Wan10] and Kauffman-Lomonaco's quantum topology themed review [KL09].

[WORK: I will add a section detailing the structure of this book, and how it should be read. I have not written enough for this to be useful yet.]

Contents

1 Overview

1.1 Conceptual introduction

1.1.1 Motivation and applications

I will take as a definition *topological quantum information* to be the study of information in topological quantum systems. A topological quantum system is some mathematical or physical system which is in a fundamental sense described by the mathematics of both quantum mechanics and topology. The term *quantum system* here is used in contrast to *classical system*. The flow of current through a conducting copper wire is described perfectly well by classical electromagnetism, whereas the flow of current through a superconducting niobium-titanium wire necessarily requires quantum mechanics for its description.

The term *topological system* is used in contrast to *geometric systems*, though the term "geometric system" is a nonstandard one. In a geometric system measurable quantities and phenomena depend on quantitative local aspects of the system - the distance between wires, the exact shape of some sample, or the curvature of some component. In a topological system measurable quantities and phenomena depend only on qualitative global aspects of the system - whether two wires cross or not, whether a sample is connected or not, whether a component curves into a ball or has a boundary.

I say that this book is about "topological quantum information" and not "topological quantum systems" for two reasons. The first is to highlight the fact that there is more to a topological quantum systems than its global topological properties. Topological quantum systems also have local geometric descriptions which are important for understanding many phenomina. However, we will mostly be ignoring these local effects in favor of focusing on global topological properties. The beauty of topological quantum systems lies exactly in the fact that this global perspective retains all the essential information in the system. The second reason is to highlight this book's eye towards topological quantum computing, the idea of making computers using topological quantum systems.

Since Peter Shor's 1994 discovery of an efficient factoring algorithm on quantum computers [Sho94], the primary goal of quantum information theorists has been to harness quantum information sufficiently well so that it can be used to make an efficient scalable quantum computer. One of the major hurdles in achieving this goal is that quantum information is *fragile*. Small amounts of noise coming from nearby electromagnetic fields or imperfections in experimental devices are often enough to affect the information being stored, resulting in *errors* in the computation. In the early days of quantum computing it was not clear whether there was any way around this problem. Perhaps the inherent fragility of quantum information would make quantum computation impossible. This turned out to be false.

The beautiful observation is that errors are not nearly as catastrophic in *topological* quantum systems. Errors are typically local. By definition the information topological systems does not depend on local properties, and hence is not affected by local changes. Hence, under suitable conditions, topological systems are naturally error resistant! In the same way that invariants of topological spaces are supposed to be invariant under deformations in pure mathematics, information in topological systems is invariant under errors in mathematical physics. Hence, to solve the problem of noise all one has to do is make a *topological* quantum computer! This observation was made in 1997 and is due independently to Alexei Kitaev and Michael Freedman [Kit03, Fre98]. Since then topological quantum computing

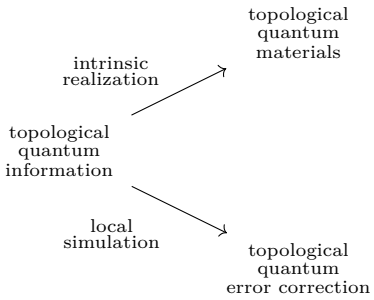


Figure 1.1: The two major branches of topological quantum information.

has grown and evolved, finding its way into almost every modern proposal for fault-tolerant quantum computing.

The first approach to topological quantum computing is to use a physical material, some literal condensed collection of atoms, which naturally behaves as a topological quantum system. These exist and have been studied for a long time. For instance, a two dimensional sheet of graphene behaves topologically when it is subjected to low temperatures ($\approx$5 degrees Kelvin) and large magnetic fields ($\approx$15 Teslas) [BGS$^+$09]. Topological quantum materials which can be used to make scalable quantum computers require intricate experiments to operate, which has been the most prominent roadblock in this approach.

The second approach to topological quantum computing is to artificially construct a topological system within a geometric one. The function of a quantum computer, almost by definition, is to simulate quantum systems. In particular, it can simulate *topological* quantum systems. Since topological systems are resistant to local errors, this means that the original computer which is simulating the topological system will itself become resistant to local noise! This works exactly as described as long as the simulation itself is local, that is, local effects in the original system correspond to local effects in the simulated system. This technique of simulating topological systems to inherit their error-resistant properties is known as *topological quantum error correction*. The advantage of this approach is that it works on any hardware available. The disadvantage is that to perform useful computations one must pass through simulation involved the topological quantum error correction. This additional layer adds a hefty amount of overhead, which can eat up the majority of runtime and resources. It is for this reason that *efficient* topological quantum error correction is an important and active area of research.

Of course, the above discussion presents only one motivation for topological quantum information and only one example of an application. Topological quantum materials open a whole world of potential applications, and it seems they may play an important role in the techonologies of the future [RS20]. Some proposed applications include processing classical information using topological defects in magnetic devices (with the end goal of making high-speed low-energy transmissions) [MZ21, ŠMYM18], creating highly sensitive photodetectors (with the end goal of making night-vision goggles or sensors) [CLRL17], creating technolgies with high thermoelectric effect (with the end goal of making efficient fridges or electric generators) [SF18], creating highly-efficient transistors [FEC$^+$21], and engineering tiny electrical components [VD14, PBD17].

This breadth of potential applications is due in part to the number of different types of topological materials which have been discovered or theorized. This includes quantized

Hall states [vKCK+20], topological insulators [HK10], fractional Chern insulators [RB11], Weyl/Dirac semimetals [AMV18], and topological superconductors [SA17]. The contents of this book certainly do not provide the entire picture for any of these materials. However, the hope is that it gives a picture of the algebraic structures within them, hence helping readers think both concretely and conceptually about these materials and their applications.

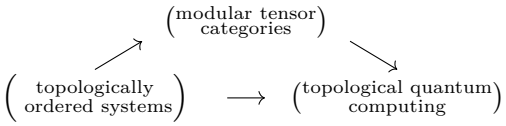
1.1.2 Mathematical picture

[WORK: use the guiding picture "MTC = topological quantum particle theory".]

The term *topological quantum system* is broad. To get a rigorous mathematical subject, we will focus on a specific type of topological quantum system known as a *topologically ordered* quantum system. Topological order is much more precise, though there are still conflicting definitions in the literature. Specifically, I will be focusing on *(2+1)-dimensional* topological order. Here, I am using the physicist convention of using (2+1)D to refer to two space dimensions and one time dimension. That is, I will be discussing a locally flat topologically ordered system. For example, a single sheet of graphene at low temperatures and large magnetic fields can exhibit a form of (2+1)D topological order, and any quantum computer running topological quantum error correction can also exhibits a form of (2+1)D topological order.

All systems in this book are two-dimensional unless stated otherwise.

Topological quantum systems can be described in many different ways. In this book we will take an *algebraic* approach. [WORK: what does it mean to take an algebraic approach to something?]. The algebraic structure which houses the algebraic data of a (2+1)D topologically ordered system is known as a *modular tensor category*. These algebraic structures are the main mathematical object of this text. Once one has a modular tensor category it is easy to manipulate the stored information to perform computations. This gives us the overall schema of our mathematical discussion, illustrated visually below:



In Chapter [ref] we describe topological order. In Chapter [ref] we describe topological order algebraically in terms of modular tensor categories. In Chapter [ref] we describe further algebraic structures which lie beyond plain modular tensor categories, which allow us to describe more complex behaviors in topological order. Finally, in Chapter [ref] we will use the tools we have established to detail several algorithms and procedures for topological quantum computaiton. Two introductory chapters are also included: Chapter [ref] which establishes the theory of finite dimensional quantum systems and Chapter [ref] which establishes category theory.

1.1.3 History of the subject

Like with any sufficiently rich subject, the history of topological quantum information can be traced back as far as one wants. So let us do exactly that. The first use of topology in information science was roughly 2600 BCE, with the South American *Quipu* [AA81]. Quipu are intricate knotted strings typically made out of cotton fibers. The knots in the string are

used to store various types of information, typically numbers. Mathematically we say that Quipu store their information in knot invariants, and hence hold *topological* information.

Quipu were so successful that they remained the primary method of information processing in much of South America for thousands of years. They reached their peak of usage in the 15th century via the Inca empire. The Inca empire was the largest pre-Columbian empire in the western hemisphere, with over ten million subjects and spanning over two million square kilometers. Despite their intricate government, the Incas had *no written language*. This distinguished them from their contemporary empires, such as the Mali, Mongolian, or Chinese empires, which all relied on the written word. The success of the Inca empire can be seen as a testament to the versatility and power of knot invariants. The difference between the Inca and modern proposals for topological quantum computers is that instead of the strings being made out of cotton fibers they are made out of the spacetime trajectories of quasiparticles in topological systems.

Just like the history of topology in information science can be traced back to the origin of information science, the history of topology in quantum mechanics can be traced back to the origins of quantum mechanics. There is a 1931 paper of Paul Dirac [Dir31] which introduces many of the ideas which would become foundational to topological quantum mechanics. In the 1950s, explicitly topological ideas such as the Aharanov-Bohm effect [AB59] and the theory of point defects by Tony Skyrme [Sky62] were beginning to emerge. By the 1970s nontrivial abstract topological considerations were leading to novel contributions to contemporary physics, such as the theoretical description of the A-phase of superfluid Helium-3 [AT77] and the theory of phase transitions in the xy model proposed by Kosterlitz-Thouless [KT73]. These results were associated with the 1996 and 2016 Nobel prize respectively.

It was in the 1980s, however, that topology established itself as one of the leading themes in condensed matter physics. The discovery of the quantum Hall effect in 1980 [KDP80] and the subsequent discovery of the fractional quantum Hall effect in 1982 [TSG82] gave the first examples of topologically ordered systems in our modern sense of the word, and resulted in the 1985 and 1998 Nobel prizes respectively. These systems gave theorists the license to dream big about what possibilities could lie ahead. This led to major work by theorists such as Frank Wilczek [Wil82b, ASWZ85], Duncan Haldane [Hal83, Hal88], and others on the theory of topological quantum systems.

The most notable of these theorists for our present story is Edward Witten, with his introduction of *topological quantum field theory* in 1988 [Wit88]. This work not only put the modern experiments within a larger context, but it also connected these developments to a parallel story which had been developing within pure mathematics. Namely, knot theory. In 1984 Vaughn Jones discovered his landmark knot invariant, which was powerful in its ability to distinguish between non-equivalent knots [Jon97]. This marked the first major progress in the field since Alexander's invariant in 1928 [Ale28]. However, Jones' construction was steeped in opaque subfactor theory, so much so that the fact that it resulted in knot invariant felt almost like a happy accident. Hence, a widespread topic on the mind of contemporary mathematicians was how to properly interpret the Jones invariant, and how to construct other invariants like it. Witten seemed to answer both. After defining topological quantum field theory, he showed how the Jones invariant could be obtained as an observable quantity within a certain field theory [Wit89]! This shocking result gave a new interpretation of the Jones invariant in terms of mathematical physics which was appealing to experts. Seeing as the Jones invariant was constructed from a topological quantum field theory, it was natural to expect that other field theories might give new invariants which could distinguish between even more knots. This vision of invariants in low-dimensional topology constructed using

topological quantum field theory became known as *quantum topology*, and evolved into its own discipline in the following years.

This brings us to 1997. Quantum topology is an active area in pure mathematics, and topological themes in condensed matter physics are at the forefront of the field. The open problem is how to construct a fault tolerant quantum computer. Peter Shor had recently discovered his factoring algorithm [Sho94], and there was debate about whether scalable quantum error correction was possible [Lan95]. This led to two independent proposals for topological quantum computation in the same year. One was by the mathematician Michael Freedman [Fre98]. His vision was clear. A recent paper had shown that computing the Jones invariant of knots was in general an NP-hard problem [JVW90]. However, by the work of Witten, the Jones invariants of knots were observables in certain topological quantum field theories. Hence, if one could construct physically a topologically ordered system which was described by Witten's topological quantum field theory then the Jones polynomial of knots could be computed efficiently by making measurements on the system. Hence, one would obtain a very powerful computer! This was Freedman's proposal.

The other proposal was made by theoretical physicist Alexei Kitaev [Kit03]. His proposal was much more precise. He gave a toy model for a certain family of topologically ordered systems. He then outlined a technique for storing and manipulating information within these systems. The deep observation was that these systems were intricate enough that they could be used to make a powerful quantum computer [Moc03].

In the subsequent years Freedman and Kitaev teamed up with collaborators Zhenghan Wang, Michael Larsen, and others to study the new field of topological quantum information and the possibility of constructing a topological quantum computer. One of the first major results was that no topological quantum computer could be more powerful than a standard quantum computer [FKW02]. This went against Freedman's original hope to solve NP-hard problems using topological quantum computers. Freedman's mistake was in asserting that topological quantum computers could compute the Jones polynomial. The measurements which give the Jones invariant in topological quantum field theory will always be *approximate*. Approximating the Jones invariant in this way is computationally easier than evaluating the Jones invariant exactly. In fact, this way of approximating the Jones invariant is *not* NP-hard - it can only be used to solve problems which could efficiently be solved using standard quantum computers.

The second major result of Freedman, Kitaev, Wang, and Larsen was the converse of their first result [FLW02]. Namely, they showed that every quantum algorithm can be efficiently run on a topological quantum computer. They do this by showing that every quantum algorithm can be efficiently reinterpreted in terms of computing the Jones invariant of some knot. In this way computing the Jones invariant is not NP-hard, but it is a *universal problem* for quantum computation. They then formalize Freedman's ideas about topological quantum field theory, and show directly that realistic operations on a topologically ordered quantum system described by Witten's quantum field theory can be used to compute the Jones invariants of knots.

Together, these two results show in a real sense that topological quantum computing is equally powerful as standard quantum computing with quantum circuits. This laid the groundwork for fruitful studies of fault-tolerant topological quantum computing, both using error correcting codes and physical materials. This has resulted in a great number of important results, which we will discuss at length throughout the rest of this manuscript.

1.2 Technical introduction

1.2.1 Principles of topological quantum information

In this section we will lay out the general principles of topological quantum information. As an organizational tool, these principles are introduced one by one as we construct a sample topological system. This example is meant to be representative of the systems we will encounter throughout this text, and within the broader field of topological quantum information. As a further organization tool, this example is constructed with the stated goal of obtaining a topological quantum computer.

Our system will be flat, containing only two spatial dimensions. Our system will be mostly homogenous, essentially identical everywhere, at the exception of finitely many localized regions. These regions will differ substantially from the top-dimensional homogeneous bulk. These localized regions are called *quasiparticles*. The beauty of systems like these is that they behave as though the homogeneous bulk were empty, and the quasiparticles were fundamental particles within the bulk. In fact, in its algebraic description, these topological systems are *identical* to ones in which the homogenous bulk is empty and the quasiparticles are fundamental particles. This is where the term quasiparticle arises. It is important however to remember that in most relevant applications the bulk is *not* empty and the quasiparticles are *not* fundamental particles. The bulk is typically some highly entangled quantum wavefunction, and the quasiparticles are emergent phenomena made up of smaller microscopic degrees of freedom.

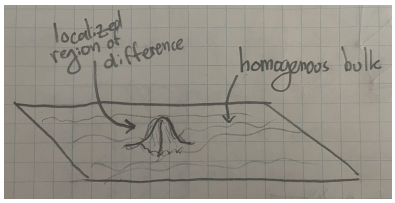


Figure 1.2: A quasiparticle in a two dimensional system

Our aim is to build a computer. In general this requires three components:

1. A method of storing information;
2. A method of manipulating information;
3. A method of reading out information.

Information is stored in the state of the system - the bulk is described by some parameters, and the details of those parameters encodes information. Our method for manipulating information is *braiding*. Braiding is the process whereby quasiparticles are moved along continuous paths around one another. There are two important points about braiding to keep in mind. The first is that braiding changes the state of the system. Even though the quasiparticles might be in identical places before and after the braid, the details of the system will change - there is more to the state of the system than just the positions of the quasiparticles. The second point is that the way that the state of the system changes depends *only depends on the topology of the braid*, and not the geometry. Small deformations in the path taken by

the quasiparticles do not affect the result - only global changes, like whether a path is taken clockwise or counterclockwise, makes a difference. This invariance is due to the fact that our system is topological. In geometric systems we expect the exact path taken by quasiparticles matters a great deal. The independence of the details of the paths is extremely specific to topological systems, and in the present setting is the *defining topological feature*.

[WORK: add braid diagrams to demonstrate what braiding is like. Doesn't have to be string-diagram like - probably best to keep it in-plane 2D.]

At this point we can already see we have succeeded in our goal of making our computations fault-tolerant. Noise in the system will correspond to uncontrolled perturbations in the trajectories of the quasiparticles. This uncontrolled movement won't change global properties of paths taken, and hence will not change the action of the braids on the system. That is, small errors won't affect computation! Of course, large enough errors could unintentionally make one quasiparticle wind around another. This would change the topology of the braid and hence ruin the computation. These errors are controllable, however, by moving the quasiparticles far apart and limiting the magnitude of the noise.

The final step in making our computer is to introduce a method for reading out information. This is done using *fusion*. Fusion is the process whereby two quasiparticles are brought together, resulting in a single quasiparticle. In sufficiently complicated topological systems the result of fusion depends on the details of the state of the overall system. That is, the result of fusion can be used as a way of reading out information about the state! In its most basic form, when two quasiparticles fuse they can either result in a localized region which is identical to the homogenous bulk or is different from the homogenous bulk. If they result in a localized region identical to the bulk we say that the two quasiparticles have *annihilated* each other. This can be seen as the difference between constructive and destructive interference. Two waves can either have destructive interference and annihilate each other when they meet, or they can have constructive inteference and result in a new wave. Measuring whether or not two quasiparticles annihilate upon fusion gives a method for reading out information.

In some situations, the result of fusion can even be nondeterministic. In this case the fusion can be repeated multiple times, which allows one to measure the *probability* that two quasiparticles will annihilate each other. These probabilities are a rich source of data, and will serve as our way of reading out information in the current setting. The fact that our system is topological implies that the result of fusion does not depend on the specifics of the path taken, and hence this method of readout preserves the invariance of our computation to noise. This gives us a full picture of topological quantum computation, as seen in figure 1.3.

To make the above discussion more concrete, we will give a worked example. In this example we use a specific topological order known as the *Fibonacci particle theory* to run Shor's efficient quantum factorization algorithm [Sho94]. The input of Shor's algorithm is a positive integer. The output of Shor's algorithm is the factorization of that integer. Shor's algorithm is *efficient* in the sense that it uses polynomially many quantum logic gates to arrive at its answer relative to the size of the input. Throughout this passage we will use *efficient* and *polynomially sized* interchangeably. The Fibonacci particle theory is a specific topological order, which describes in an algebraic fashion how the overall state changes when quasiparticles are braided and fused.

The first step in running Shor's algorithm on a Fibonacci quantum computer is to translate the positive integer input into a certain braid. This is done using an efficient classical algorithm. The second step is to run this braid on a Fibonacci quantum computer. This is

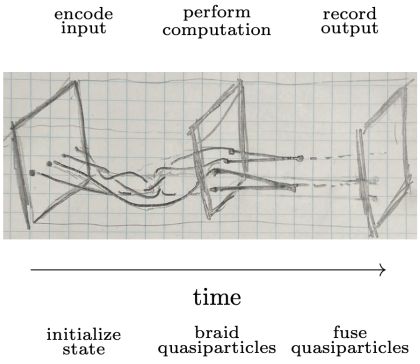
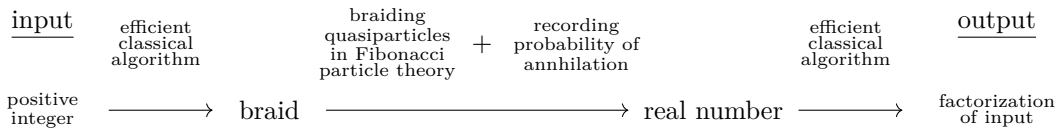


Figure 1.3: A schematic of topological quantum computing

done by initializing some prescribed state and then braiding its quasiparticles. This initialization and braiding is performed repeatedly, and after every time two of the quasiparticles are fused. This lets us record a real number between 0 and 1, which is the probability that the two quasiparticles annihilate after the braiding. An efficient classical algorithm is then used to take this real number and obtain from it the factorization of the original input. Since all of these steps are efficient, it gives a topological quantum algorithm for factoring integers. The schematic for this process is shown below:



The magic in the above procedure is the existence of these two efficient classical algorithms: a first one for encoding integers into braids and a second one for decoding real numbers into factorizations. These algorithms are nontrivial. They are due to Freedman-Larsen-Kitaev-Wang [FLW02]. In fact, Freedman-Larsen-Kitaev-Wang showed that any problem which can be efficiently solved using a quantum circuit can also be solved using the Fibonacci particle theory, via a similar method of efficient classical preprocessing and postprocessing. It is in this sense that the Fibonacci theory is *universal* for quantum computation.

The final step of this process would be to create a physical topological system which is described by the Fibonacci theory, which would serve as our quantum computer. In the realm of materials, the most promising approach seems to be to use specially tuned versions of the fractional quantum Hall system [ZGHS15]. While these materials are theorized to host quasiparticles described by the Fibonacci theory, the difficulty of the experiment makes them inaccessible to current technology. There has been progress made on topological quantum error correcting codes which work by simulating the Fibonacci theory [SZBV22, SBZ22, XSW$^+$24]. However these codes at the current moment have structural issues and require an unbearable amount of overhead to run, making them unfeasible to use on modern computers.

Progress on topological quantum computing has thus been focused on realizing topologi-

cal particle theories other than the Fibonacci theory. These other theories can be constructed in more workable materials, and can be simulated as topological quantum error correcting codes with less overhead. The drawback of these other theories is that they are typically less computationally powerful, meaning that they require more tricks and techniques to achieve universal quantum computing. There are a great number of different proposals for how to achieve universal topological quantum computing, based on different particle theories, different methods of encoding information, different methods of manipulating information, and different methods of reading out information. It is an exciting time to be a theorist in the field of topological quantum information!

1.2.2 Defects in ordered media

We will now work through a complete mathematical example of a family of topological systems. Seeing as we don't assume that the reader is familiar with quantum mechanics, our examples will be *classical* topological systems. Many of the important subtlties of topological quantum information are already present in the classical case. However, topological classical information is a smaller domain than topological quantum information - the reader should have a relatively complete grasp of the subject by the end of the chapter. Much of the discussion in this chapter is taken from an excellent review article by Mermin [Mer79].

The family of systems we will describe goes by many names. In communities of experimentally focused physicists it goes by the name *ordered media*. In mathematical physics communities it goes by the name *classical field theory*. In pure mathematics it would be described as *homotopy theory*. We will construct a system based on every topological space M. We will call M the order space of our theory. We will assume throughout this chapter that M is path connected.

To describe a system in physics, the first step is to define the space of possible states of the system. In this case, states will correspond to *continuous maps* $\phi : \mathbb{R}^2 \to M$. We now give physical intuition for this choice of state space. The choice of $\mathbb{R}^2$ as a source represents the underlying material. We are working on an infinite flat plane. Describing a function $\phi : \mathbb{R}^2 \to M$ amounts to choosing a value $\phi(x)$ for every point $x \in \mathbb{R}^2$. In this way we imagine our system as being made up of infinitely many objects, one placed at each point in $\mathbb{R}^2$, each of which has an internal state space M. Choosing the state of the overall system amounts to choosing the state of each individual object, that is, a value in M for every point in the plane. The fact that ϕ must be continuous is a compatibility condition between the states of the objects at nearby points. It says that nearby objects must have similar states. We now list some examples which are described by this model:

- **Classical xy model of a 2D electron gas**. This model describes a possible behavior electrons in a flat 2D plane. An electron can be modeled as a point particle with a magnetic dipole pointing in some direction. This magnetic dipole is known as the *spin* of the election, and can point in any direction in the plane. The topological space of all possible directions in the plane is a circle. Hence, in this system, the order space M is the circle. The fact that nearby electrons must have similar spins is known as Hund's rule, and is the most fundamental incarnation of ferromagnetism. It is physically derived as a consequence of the Pauli exclusion principle.

- **Superfluid Helium-3** One famous example of ordered media is superfluid helium-3. Helium is an element. It has two stable isotopes: helium-3 and helium-4. The vast majority of helium on earth is helium-4, but there still is naturally occuring helium-3.

At extremely cold temperatures helium-3 undergoes a phase transition, and becomes a superfluid. There are several different superfluid phases helium-3 can go into: B-phase, dipole-locked A-phase, dipole-free A-phase. For our purposes we will work with the dipole-locked A-phase. Its order space is $M = \mathrm{SO}(3)$, the group of rotations in three dimensional space.

- **Biaxial nematics**. The objects at every point in the biaxial nematic should be thought of as small rectangles with unequal side lengths. These rectangles can be oriented in any direction in three dimensional space. In practice these objects will often be molecular compounds. They will not be exactly rectangular, but have the same symmetry group as a rectangle which is enough for the model to be accurate. To compute the space of possible orientations of a small rectangle, we work by the method of symmetries. Choosing some reference orientation to start with, every rotation in three dimensional space brings the rectangles to new orientations. The space of orientations of the rectangle is hence equal to SO(3) modulo the rotations which fix the rectangle. That is, M is equal to SO(3) modulo the symmetry group of a rectangle.

[WORK: add diagrams for all three models]

We will now analyze these systems. In doing this analysis we will want to use the ideas of *deformation* and *topological equivalence*. Of course, these ideas are vague and require rigorous notions to make precise. We define these notions now. [WORK: this need to be reworded, with a proper caveat about rigor. Maybe bring up Jordan curve theorem for a laugh. Need to figure out what the policy on statements is.]

We now add a picture of *dynamics* into our model - how it will be changing through time. In particular, we image that as time passes the system changes continuously. Let $\phi_t : \mathbb{R}^2 \to M$ be the state of the system at time t. We image that if t_0, t_1 are similar times then $\phi_{t_0}(x)$ and $\phi_{t_1}(x)$ will be close. Formally, this means that the maps $\mathbb{R}_{\geq 0} to M$ assigning t to $\phi_t(x)$ is continuous for all $x \in \mathbb{R}^2$. This captures our intuitive notion of *deformation*. We will image that the state of the system is constantly changing by deformations.

The first thing to notice about our system is that it is not storing any topologically-invariant information. In particular, every state can be continuously deformed to every other state. This is a general fact from topology: every pair of maps $\phi_0, \phi_1 : \mathbb{R}^2 \to M$ can be continuously deformed from one to the other.

Clearly, this means that our system is not complicated enough to build a computer yet because it cannot store information. We rectify the situation by introducing quasiparticles. These quasiparticles go by many names. In the theory of ordered media they are known as defects. In field theory they are known as particles. In homotopy theory they are known as point singularities. For the sake of brevity, we will use the term defect.

A defect is a point at which we will drop our condition that the state $\phi : \mathbb{R}^2 \to M$ be continuous. This is done by making ϕ *undefined* at certain points. Our new system is called *ordered media with finitely many defects*. The state space consists of pairs (S, ϕ), where $S \subset \mathbb{R}^2$ is a finite set and $\phi : \mathbb{R}^2$
$S \to M$ is a continuous map.

[WORK: add picture of defects in ordered media]

Dynamics in our new system still correspond to continuous deformations. The subtelty now is that the defects can move as the state is deformed. We call these *defect-mobile deformations*.

The vision for building our computer is that the experimenter should have control of the trajectories of the defects. This means that the system will trasform under defect-mobile

deformations with definite paths chosen by the epxerimenter, but the details of the rest of the deformation is arbitarily and uncontrollable.

We can now outline the big idea of how the computer will work. We will arrange n defects on a line in the plane. We keep these defects still, so that the system is changing only by deformations which keep the defects in place. We call these *defect-fixed deformations*. We store our information in the possible configurations of this system:

[WORK: information storage space = (states with n defects arranged in a line)/ (defect-fixed deformation)]

The way we act on this information is by moving the defects around each other. This movement of defects induces some defect-mobile deformation. The space we are storing our information in is invariant under defect-fixed deformation, but not defect-mobile deformations. Hence, moving the defects around non-trivial paths will have non-trivial action on the stored information. This action on stored information is exaclty how we perform our computations.

Finally, we must introduce a method for reading out information. This is done via fusion. Two defects can be brought together and fused. The result of this fusion is a topologically invariant quantity, and we will assume that it can be measured by an experimenter. In its most simple form, this amounts to detecting whether two defects annhilated or not. This gives us some information about the state, which is the output of our computation.

[WORK: add schematic for this process]

In the rest of this chapter we will describe exactly what the space we are storing our information in looks like, how braids act on that information, and how this can be used to make a functioning computer. This will give a detailed picture of how topological computation works.

1.2.3 The fundamental group

To understand topological computation in ordered media we will need to put in some real work in analysing the system, and make some non-trivial observations. The structure of this analysis will be largely the same as the analysis which will be taking place throughout the rest of this book. We recall the overall outline of this text, which goes as follows:

[WORK: add outline.]

In this section we will do a very similar thing. We will take our physical model, ordered media, and take its algebraic description. That algebraic description can then be used for making a computer. Luckily for us, the algebraic theory underlying ordered media is much simpler than the algebraic theory underlying topological order: it's group theory. In particular, we will even assume that all relevant groups are *finite*. In this way, modular tensor categories can be seen as vast quantum generalizations of finite groups. The schematic in our case is shown below:

[WORK: add outline w/ group theory instead of MTC.]

The way we go from defects in ordered media to group theory is by using a construction known as the *fundamental group* from homotopy theory.

The fundamental group is derived from a careful analysis of loops in topological spaces. We first clairfy what we mean by *loop*. Loops, for our purposes, are always *oriented* and are allowed arbitrary self intersections. Examples of loops around a point are shown below:

[WORK: add pictures of loops.]

Formally, we define a loop in a topological space M to be a continuous map $\alpha : [0, 1] \to M$ such that $\phi(0) = \phi(1)$. Our main goal us to understand topological information. Topological

information is stored in properties which are invariant under deformations. Hence, we are naturally interested in the space of loops up to deformation.

In the plane $\mathbb{R}^2$ with a point removed, points up to deformation are classified by their *winding number*. This winding number is an integer which says how many times the loop went around the point. This windingn number is an integer in $\mathbb{Z}$, with positive numbers corresponding to counterclockwise rotations and negative numbers corresponding to clockwise rotations. The loops in figure [ref] have their winding numbers given as an illustration of the concept.

The key ingredient we are missing is the *group structure*. We want to get groups out of topological spaces, but so far all we have is a set. The group structure comes from composition. Given two loops we can compose them by first following one loop and then following the othe. In this language, we see the topologists' winding-number version of $1 + 1 = 2$ below:

[WORK: add 1+1=2 with winding numbers.]

This definition has a big problem though. To compose, we need to choice a point to start and stop two two loops being composed at. This special starting/stopping point is known as a *basepoint*. This deal of choosing basepoints is very important for the theory. Formally, a loop in M based at $m \in M$ is a map $\alpha : [0, 1] \to M$ such that $\phi(0) = \phi(1) = m$. We define the composition of two loops α_0, α_1 in M based at $m \in M$ to be

$$(\alpha_1 \circ \alpha_0)(t) = \begin{cases} \alpha_0(2t) & 0 \leq t \leq 1/2 \\ \alpha_1(2(t - 1/2)) & 1/2 < t \leq 1. \end{cases}$$

The reason we need to add the factors of 2 is to ensure that the domain of the loop is still the unit interval $[0, 1]$. Intuitively, to fit two loops in the same amount of time we had to speed-up both loops by a factor of 2.

We are now almost ready to define the fundamental group: we have defined based loops, and we have defined a rule for their composition. The last subtelty is in discussing what it means to deform based loops. In particular, should deformations be allowed to move the basepoint? The issue that we want to be able to compose our loops. To compose loops they need to have the same basepoint. If the basepoint moves then we will lose out composition structure. Hence, for the time being, we should only work with deformations which preserve the basepoint. With this subtelty out of the way, we can finally define the fundamental group. Given any connected topological space M and any point $m \in M$, we define the *fundamental group of M based at m* to be the group

$$\pi_1(M, m) \coloneqq (\text{loops in } M \text{ based at } m) \,/\, (\text{basepoint preserving deformations})$$

whose group structure is given by the composition of based loops. As an example, our earlier comments about loops around points can be summarized as the statement that $\pi_1(\mathbb{R}^2 \backslash \{p\}, b) \cong \mathbb{Z}$ for any distinct points $b, p \in \mathbb{R}^2$. The identity element in the fundamental group is the trivial loop which stays at its basepoint and doesn't move (formally, the constant map $\alpha : [0, 1] \to M$), and inverses are given by reversing orientation (formally, the inverse of $\alpha : [0, 1] \to M$ is $\alpha^{-1}(t) = \alpha(1 - t)$.)

We can now start to use the fundamental group to analyse defects in ordered media. The first major insight is that loops in physical space yield loops in order space. Let S be a finite set of defects and let $\phi : \mathbb{R}^2 \backslash S \to M$ be a state. Given any loop α in $\mathbb{R}^2 \backslash S$ based at $b \notin S$, postcomposing with ϕ gives a loop in M:

$$(\phi \circ \alpha) : [0,1] \xrightarrow{\alpha} \mathbb{R}^2 \backslash S \xrightarrow{\phi} M.$$

This loop has basepoint $(\phi \circ \alpha)(0) = (\phi \circ \alpha)(1) = \phi(b)$. This gives an element of $\pi_1(M, \phi(b))$. Given any state ϕ and given any loop α based at b, we call the corresponding element of $\pi_1(M, \phi(b))$ the *winding number of ϕ along α*. This sort of winding number generalizes the standard notion of a winding number of a loop around a point discussed before.

Now, consider the system with n defects arranged in a line. We can choose a basepoint b above all of the defects. We add loops α_i based at b for each $1 \leq i \leq n$, each of which go directly around defect i counterclockwise exactly once. This is depicted visually below:

[WORK: add picture.]

Given any ordered state ϕ on this system, we can take the winding numbers of each loop $\{\alpha_i\}_{i=1}^n$. These winding numbers all live in $\pi_1(M, \phi(b))$. Hence, to each state we can assign an element in the n-fold Cartesian product $\pi_1(M, \phi(b))^n$.

Fantastically, the values in $\pi_1(M, \phi(b))^n$ change in a well-behaved way under braids. We use a 2-defect system to illustrate the principle.

[WORK: add good pictures to show why making g_1 go under g_2 maps (g_1, g_2) to (g_2, g_1). Talk a bit about it in words too]

This gives us a picture for how our computer works: information is stored in the winding numbers of the defects, and braiding acts by conjugating the winding numbers by each other.

There are a still a few lingering points that need to be sorted out before we can start building our computer. The first is the issue of whether our information being stored is actually invariant under defect-fixed deformations. Unfortunately, it is *not*. The problem is that deformations in general have no reason to preserve the value of $\phi(b)$. The deformations will hence change the basepoints. However, elements of the fundamental group are only defined up to basepoint-preserving deformations! Hence, deformations of the state will change its winding numbers. In general we have the following key relation:

$$(\text{loops in } M \text{ based at } m) \,/\, (\text{basepoint preserving deformations}) = \pi_1(M, m)$$

$$(\text{loops in } M \text{ based at } m) \,/\, (\text{arbitrary deformations}) = (\text{conjugacy classes in } \pi_1(M, m)) \,.$$

The intution for this above fact is as follows. Let α be a loop based at b. Let α' be the same loop but with a different choice of basepoint b'. Let ϵ be the portion of the loop between b and b'. Going along α is the same as first going along ϵ to get to b', then going along α', and then going along ϵ^{-1} to get back to b. Hence, we have $\alpha = \epsilon^{-1} \circ \alpha' \circ \epsilon$. Hence, choosing different basepoints amounts to conjugation. This is illustrated below:

[WORK: add diagram]

All this is to say that the winding numebrs in an n-defect ordered media state ϕ are not preserved up to defect-fixed deformations. Properly dealing deformations requires properly keeping track of conjugacy classes versus group elements. This sort of effort, however, is unnececary because it does not change any of the key takeways or any of the important concepts. Hence, *we will assume that all of our deformations do not change the value of $\phi(b)$*. We will choose some element $m \in M$ and assume $\phi(b) = m$ is fixed. For physical motivation, one can imagine moving the basepoint far away towards infinity. Since all of our physics is local we can imagine that the magnitute of the deformations go to zero away from the origin and hence the point at infinity is preserved by all local nosie.

Our last subtelty to discuss is reading out information. As we have just discussed, the values of the winding numbers in $\pi_1(M, m)$ are very dependent on the choice of basepoint. This means that the information encoded in this winding number is spread out over the whole region between the defect and the basepoint. This nonlocal nature makes it hard to measure, especially when the basepoint is taken away towards infinity. The readily measurable local information is the non basepoint-preserving winding number of the loop around defects. That is, the conjugacy classes in $\pi_1(M, m)$ associated to the defects. These conjugacy classes should be measurable in a reasonable experimental setup.

However, as we braid, these conjugacy classes do not change, and hence the outcomes of our measurments won't be affected. In a way, this is the point - braiding can change the spread-out global topological information, but will not change local quantities, like the conjugacy class in $\pi_1(M, m)$. In this way we can think of the conjugacy class as a well-defined *type* of the defect, whereas the exact value in $\pi_1(M, m)$ is a global quantity which depends on the choice of basepoint

The way to get around this issue is to fuse the defects before braiding. Fusing defects together amounts to bringing them close together until they act like a single defect. If the defects have winding number g_1, g_2, then their fused defect will have winding number $g_1 g_2$ as illustrated by the below diagram:

[WORK: add diagram.]

Hence, given a state $(g_1, g_2 ... g_n)$, the measurable quantities are the conjugacy classes of products of adjacent defects. For instance, fusing all of the defects one-by-one to the left would allow one to measure the conjugacy classes of g_1, $g_1 g_2$, $g_1 g_2 g_3$, all the way up to $g_1 g_2 g_3 ... g_n$.

This completes our analysis of defects in ordered media based on the fundamental group.

1.2.4 Topological classical computation

We are now ready to describe the theory of topological classical computation. In the previous section, we showed how all of the topological information of defects in ordered media is controlled by the fundamental group $G = \pi_1(M, m)$ of the order space M relative to some basepoint $m \in M$. This is the heart of the algebraic theory of topological computing. Even though our physical model is complicated, the algebraic data can be succicntly summarized as a single group $G = \pi_1(M, m)$. In this way, we will formulate our discussion of topological classical computation in a way which does not make reference to the order space at all. We will choose an abstract group G and make a computer using it.

On a purely mathematical level we don't need to make any restrictions on the group G. It is a theorem from homotopy theory that every group is the fundamental group of some topological space. However, we will make restrictions on our choice of group coming from physical concerns. We will ask that our group be *finite*. A first reason for this is error protection. Suppose that G were some continuous group, like $G = \mathbb{R}$. If the stored information was $\pi = 3.1415...$, it would be difficult for this information to not drift to 3.1416.... Even though there aren't any continuous deformations which would change a winding number, small non-continuous deformations could still make this sort of jump. For this reason it is preferable to work with *discrete* groups - groups whose natural topology is discrete. Discreteness implies a degree of seperation, which means that winding numbers will not spontaneously jump from one element to the next. This gives the system error resistance.

The choice to make the group finite is more subtle. For instance, $G = \mathbb{Z}$ appears in many

physically reasonable contexts. Our choice mainly steps from the practical consideration that finite groups are simpler to work with than infinite ones, and the general physical principle that symmetry groups should be compact. Any compact discrete group must be finite. This compactness argument will become especially relevant once we pass to quantum mechanics.

In summary, the algebraic theory of topological classical information we present is really just a special case of finite group theory, which is a well understood subject.

Our systems will consist of n defects on a straight line. These defects will be labeled with group elements $g_i \in G$, for $1 \leq i \leq n$. We recall that these labels correspond to winding numbers around loops:

[WORK: add diagram.]

Braiding g_i under g_{i+1} amounts to replacing g_i with g_{i+1}, and replacing g_{i+1} with $g_{i+1}^{-1} g_i g_{i+1}$. Fusing the defects g_i and g_{i+1} amounts to replacing them with a single defect labeled $g_i g_{i+1}$. The *type* of a defect is the conjugacy class of its label in G. These types are local observables which can be measured by the experimenter.

[WORK: add little pictures summarizing these rules]

This leads to the very natural question: *for which groups G can I make a full classical computer?* This is a design problem in finite group theory.

Our first step towards answering it is making a closer analysis of how braiding works. We define the braid group as our main tool:

[WORK: Bn = ways of braiding n points around each other/endpoint-preserving deformations. Define Pn too. Also give examples. Maybe this is where to introduce the graphical language, things going thru time?]

Every braid can be made up piece-by-piece using indivudal swaps. Let σ_i denote the swap which sends the point at positoin i under the point at position $i+1$. The group B_n is generated by the σ_i, for $1 \leq i \leq n-1$. We observe that the following two braids can be deformed from one to the other:

[WORK: add Yang-Baxter braid]

Algebraically, this is the identity $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$. Additionally, if i and j are not adjacent, that is $|i-j| \geq 2$, then $\sigma_i \sigma j = \sigma_j \sigma_i$ as seen in the below picture:

[WORK: far-commutivity picture.]

This yields the algebraic fact that

$$B_n = \left\langle \sigma_1, \sigma_2, ...\sigma_{n-1} \middle| \begin{smallmatrix} \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, \\ \sigma_i \sigma_j = \sigma_j \sigma_i \end{smallmatrix} \ \forall 1 \leq i, j \leq n-1, \ |i-j| \geq 2 \right\rangle .$$

It is at this point that we can move past our non-rigorous topological considerations for braiding. The lack of rigor in our treatment of braid groups and our lack of rigor in our treatment of defect trajectories cancel, giving us our first well-formed mathematical proposition. It encodes the fact that moving defects by braids acts on the stored information:

Proposition 1.1. *Let G be a finite group, and let $n \geq 1$ be an integer. The map*

$$\begin{aligned} \rho_n : B_n &\to \mathrm{Sym}\left(G^n\right) \\ \sigma_i &\mapsto \left((g_1 ... g_i, g_{i+1} ... g_n) \mapsto (g_1 ... g_{i+1}, g_{i+1}^{-1} g_i g_{i+1} ... g_n) \right) \end{aligned}$$

defines a homomorphism of groups between the braid group B_n and the group of set-wise permutations of the Cartesian product G^n, $\mathrm{Sym}(G^n)$.

Proof. .[WORK: do proof] □

The dream would be that braids alone would be enough for universal classical computation. For instance, suppose that G is a finite group with a conjugacy class C that has order 2. Identifying $C \cong \{0,1\}$ as a set, we can identity $C^n \cong \{0,1\}^n$ with n-bit strings. Suppose the homomorphism $\rho_n : B_n \to \mathrm{Sym}\,(C^n) \cong \mathrm{Sym}(\{0,1\}^n)$ were surjective. This would mean that every element of $\mathrm{Sym}(\{0,1\}^n)$ could be written in terms of braids on G. In the language of computer science, maps $\{0,1\}^n \to \{0,1\}^n$ are called *boolean functions*. The surjectivity of the braid group homomorphism would say that every bijective boolean function could be implemented by braiding defects, and hence every bijective computation could be done using braiding. Bijective boolean functions in the world of computation are known as *reversible*. Most problems we care about are not inversible. For instance, adding integers is not reversible because multiple summands could give the same sum as demonstrated in $1 + 3 = 2 + 2 = 4$.

This leads to two problems to deal with:

1. Braids can only ever give reversible computations. This is not a major issue because it's known that there is an efficient clever way of turning every non-reversible computation problem into a reversible one [Ben73]. However, reversibility is still cumbersome and annoying.

2. There aren't any groups G which have conjugacy classes C for which the map $\rho_n : B_n \to \mathrm{Sym}\,(C^n)$ is surjective.This is because, for instance, choosing some $x \in C^n$ we could have the whole input be a string of all x: $(x)_{i=1}^n \in C^n$. Since x commutes by itself and the braid group acts by conjugation, every braid will act trivially on this input. Hence, $\rho_n(\beta)\left((x)_{i=1}^n\right) = (x)_{i=1}^n$ for every braid $\beta \in B_n$. There is no way to make a nontrivial computation from braiding if all inputs commute.

The way around the problem of commuting inputs is to use pair-creation. Just like how at any time two defects (g_1, g_2) to make the defect $g_1 g_2$, at any time this process could reverse and out of nothing the pair of defects (g, g^{-1}) could be created. The important part of this process is that g can be chosen so that it does not commute with the inputs.

[WORK: add a bit of explanation about this, introducing all the ingredients we need]

We now have all of our ingredients, we can finally state our main results about making computers. Clearly, if G is abelian then it won't be useful for making a computer. Our computer is based on acting by conjugation, and conjugaction is trivial in abelian groups. However, just being nonabelian is not enough. The group needs to be *sufficiently non-abelian* so that conjugation is powerful enough to implement any computation possible.

We define the subgroup

$$[G,G] = \{\text{subgroup of } G \text{ generated by elements of the form } g_0 g_1 g_0^{-1} g_1^{-1} \text{ for } g_0, g_1 \in G\}.$$

The subgroup $[G,G]$ is called the *commutator subgroup* of G, and the elements $g_0 g_1 g_0^{-1} g_1^{-1}$ are called commutators. Clearly, if G is abelian then all of its commutators are trivial and hence $[G,G] = 0$. To make a good computer, we need sufficiently many commutators. In fact, we need the following condition: $[G,G] = G$. For technical reasons it also easiest to assume that G is *simple*. That is, it has no proper nontrivial normal subgroups.

We observe that every non-abelian simple group is automatically perfect. This follows from the fact that the commutator subgroup $[G,G]$ is a normal subgroup of G. Since G is nonabelian the commutator subgroup $[G,G]$ is nontrivial, and since the only nontrivial subgroup of G is itself we get that $[G,G] = G$.

In this case we have the following important result:

Theorem 1.1 (Mochon)**.** . *[WORK: I want a good statement of Mochon's theorem, need to think more about it and read Mochon's paper again. State it as "for every non-abelian simple group G".]*

Proof. . [WORK: do proof.] □

We can now give a full example of how this works. [WORK: give a full example, using $G = A_5$. Of course, full is a tricky word here. Enough to make what's going on clear to people.]

Now that we know how to make a universal computer, we can analyse how the power of computation changes as G is chosen to be more or less abelian. The general theme is that if a group is more non-abelian then it will have more computaional power. Of course, being "more" or "less" abelian is not a well-defined term. We introduce here some formal notions from group theory which measure abelianness.

If a group is very nonabelian it should have a big commutator subgroup. That is, $[G, G]$ should be large in a certain sense. One way for this to be true is for the group to be perfect, that is, $[G, G] = G$. A weaker condition is that G should have a perfect subgroup - a subgroup $H \leq G$ such that $[H, H] = H$. Intuitively, it makes sense that any group with a perfect subgroup should be useable for universal topological computatoin. You can just focus on the perfect subgroup and use Mochon's theorem, and forget about the rest of the group. A group with a perfect subgroup is called *non-solvable*.

There is another useful step to consider between non-solvable and abelian. Some groups G have subgroups H such that $[H, H]$ might be small, but $[H, G]$ is bigger. When H is allowed to take commutators with elements of G you get potentially more elements, so $[H, H] \leq [H, G]$. When H is a normal subgroup, we find that $[H, G] \leq H$ since for all $h \in H$, $g \in G$, the commutator

$$ghg^{-1}h^{-1} = (ghg^{-1})h \in H$$

since $(ghg^{-1}) \in H$ by the normality of H and $h \in H$ by assumption. If G has a normal subgroup H such that $[H, G] = H$, we call G *non-nilpotent*. Clearly we have the following inclusioins:

$$\binom{\text{non-solvable}}{\text{groups}} \subset \binom{\text{non-nilpotent}}{\text{groups}} \subset \binom{\text{non-abelian}}{\text{groups}}.$$

This induces a hierarchy of adjectives, from most abelian to least abelian:

$$\underset{\text{more abelian}}{\longleftarrow} \quad \text{(abelian)} \quad \binom{\text{nilpotent}}{\text{non-abelian}} \quad \binom{\text{solvable}}{\text{non-nilpotent}} \quad \text{(non-solvable)} \quad \underset{\text{less abelian}}{\longrightarrow}$$

The following phenominon presents itself. We find that less abelian a group is the more computational power it has. Additionally, the more computational power it has the harder it is to create topological systems in the lab which are algebraically described that group. It is harder to make systems which make good computers.

This phenominon is especially well developped in the quantum case. Given a finite group G, we can describe a classical system of ordered media based on G. This system can be *quantized*. This turns it into a topological quantum system whose behavior is still goverened by the group G. This quantized system is known as the *quantum double* of G, and is denote $\mathfrak{D}(G)$. These systems behave very similarly to the ones discussed in this chapter, just made quantum. These quantum doubles and the algebraic theory describing them and their generalizations will be the topic of much of this book.

In the case of quantum doubles we can make a table detailing exactly the relationship between level of abelianness, computational power, and experimental status:

[WORK: need to introduce universality as a concept]

Abelianness	Smallest Example	Computational power of $\mathfrak{D}(G)$	Experimental Status
non-solvable	$G = A_5$, alternating group with $\lvert A_5 \rvert = 60$	Straightforwardly universal. (Chapter [ref], [Moc03])	Fundamental limitations coming from intensive circuit-depth requirements, and the size of the. smallest example. ([BKKK22]).
solvable non-nilpotent	$G = S_3$, symmetric group with $\lvert S_3 \rvert = 6$	Universal with tricks. (Chapter [ref], [Moc04])	Has yet to be done. There are some inherent difficulties involved. ([TVV23])
nilpotent non-abelian	$G = D_4$, dihedral group with $\lvert D_4 \rvert = 8$	?	Preliminary experiments have been successful. ([ITV+24])
abelian	$G = \mathbb{Z}_2$, cyclic group with $\lvert \mathbb{Z}_2 \rvert = 2$	Universal schemes seem to be impossible. Non-topological methods seem to be required. (Chapter [ref], [BK13, EK09])	Widely used in most applications. ([BCG+24, HDSHL24] [BKK+24, goo23])

We make a few comments about this table.

1. We notice that difficulty inherent to experimentally realizing topological phases is *not* completely controlled by the size of that group. The quantum double $\mathfrak{D}(D_4)$ is simpler to realize than $\mathfrak{D}(S_3)$ because it is nilpotent and S_3 is not, despite the fact that $\lvert D_4 \rvert = 8$ is larger than $\lvert S_3 \rvert = 6$.

2. All of the experimental results cited come from the side of topological quantum error correction and not topological quantum materials. This is because most topological quantum materials are described by algebraic theories which are not doubles of finite groups. Doubles of finite groups are primarily used in topological quantum error correction theory.

3. This table details a general programme. Given an algebraic theory of topological information, there is the question of how to make a universal quantum computer. The culmination of this book is Chapter [ref], where we show describe six different families

of algebraic theories and show how to make a universal quantum computer out of all of them.

This concludes our overview of the subject!

Exercises:

1.1. .[WORK: show that simulability $\implies$ *efficient* simulability. Do the work in the case $G = A_5$]

1.2. .[WORK: show that nilpotent $\implies$ polynomial growth? Can reference the more general picture of size of braid group images.]

2 Quantum mechanics

2.1 Overview

2.1.1 Introduction

In this chapter we will give an introduction to quantum mechanics. The goal of this book is to give an exposition of topological quantum information. So far we have described topological *classical* information - all that's missing now is quantum mechanics!

One of the difficulties of quantum mechanics is that it is physically unintuitive to most unitiated learners. Conversely, one of the advantages of quantum mechanics is that it is mathematically basic. Quantum mechanics is mathematically linear algebra. The mathematical intricacies of quantum mechanics often arrise from complications from working in infintie dimensional spaces. In topological quanum information, however, all of the spaces of interest are finite dimensional and hence the mathematics involved is quite straightforward: finite dimensional linear algebra is largely a solved subject. In this chapter we will give a dictionary between the physical language of quantum mechanics and the mathematical language of linear algebra.

The first physical principle about quantum mechanics to know is that it is typically used to describe small objects. A natural question is *why*. If quantum mechanics is correct, then it should equally well apply to small and large objects. The answer to this question is subtle, and brings us to back to the thesis of this book.

Large scale macroscopic phenomina are emergent from coherent small scale microscopic phenomina. The word *coherent* is used intentionally. It is used to mean "held together", "integrated", or "organized". Sometimes collections of microscopic degrees of freedom fail to form observable macroscopic degrees of freedom. This failiture is known as *decoherence*. It is an empirically observed fact that microscopic quantum degrees of freedom typically decohere. It is the ubiquity of decoherence which makes are macroscopic world seem classical.

It is exactly for this reason that topological quantum systems are so special. They are essentially unique in the fact that they can cohrently hold quantum information at macroscopic length and time scales. This is because decoherence is caused by repeated noise from the environment, which corrupts fragile quantum information. Topological quantum systems are defined by the property that their stored information is not affected by local changes. Hence, if noise is sufficiently local and sufficiently controlled, the information in topological quantum systems will remain coherent.

This makes topological quantum matter a fantastic place to first learn quantum theory. The mathematics is simple because all spaces involved are finite dimensional, and the quantum effects are more dominant than in almost any other macroscopic phenomina! It is an exciting and rich subject.

2.1.2 Experimental motivation

Before diving into a formal treatment of quantum mechanics, let us first motivate why quantum mechanics has to be like it is. The most famous aspect of quantum mechanics is its probabilistic nature. As Einstein famously said, *"God does not play dice"*. If quantum mechanics was just probabilistic, however, it wouldn't bother physicists nearly as much at it does. Quantum mechanics is a sort of twisted probability theory:

> "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[1]

Throughout this introduction to quantum mechanics we will take the lens of comparing quantum mechanics with classical probability theory. Some properties of quantum mechanics, like *superposition* and *entanglement*, are already clearly present in the world of probability. Other properties, like *interference*, are not. To make this clear, we will present a few experiements which demonstrate the proabilistic nature of quantum mechanics, and the ways in which quantum mechanics goes beyond probability theory.

[WORK: which experiments should I chose? Double slit? Polarized light? Pairs of entangled photos? It would be cool to get experiments which are relevant to topological matter if possible. It would also be cool to get experiments which almost immediately motivate the exact form of quantum mechanics. I'm not a physicist though - need to get someone else more knowledgable to give me a lecture.]

2.2 Axiomatic development

2.2.1 Probability theory

Seeing as quantum mechanics is a modified probability theory, before axiomatizing quantum mechanics we will first axiomatize probability theory in terms of linear algebra. The goal is to highlight what an axiomatization of a physical theory should look like, so that the jump to quantum mechanics is as predictable as possible.

Intuitively, we all know what probability theory is. We start with some set S which represents the possible outcomes of our probability theory. States in the probabilistic system are probability distributions on S. That is, assignments of probabilities (positive real numbers) to each elements of S such that the total probability is 1. We will focus entirely on *finite* probability spaces. This greatly simplifies our analysis. Finite probability spaces require only basic linear algebra to describe, wheras infinite probability spaces requires measure theory.

For example, suppose we are flipping a coin. The space of possible outcomes is $S = \{\text{head}, \text{tails}\}$. A fair coin flip would have $50\% = 1/2$ probability of giving heads, and $50\% = 1/2$ probability of giving tails.

A convement notation for proability distribution is the language of weighted sums. The state $\sum_{x \in S} p_x \left|x\right\rangle$ denotes the state with probability $p_x \geq 0$ of having outcome $\left|x\right\rangle$, where $\sum_{x \in S} p_x = 1$. In the case of heads and tais, we would write

$$\left|\text{fair flip}\right\rangle \coloneqq \frac{1}{2}\left|\text{heads}\right\rangle + \frac{1}{2}\left|\text{tails}\right\rangle.$$

The notation $\left|\cdot\right\rangle$ for states is known as a *ket*. This is part of so-called *Dirac notation*, which is widespread in quantum theory. We use it here to help ease our transition from probability theory to quantum mechancis.

Mathematically a formal sum is an element of a vector space. That is, the weighted sums corresponding to probability distributions are elements of the vector space

$$\mathbb{R}[S] \coloneqq \operatorname{span}\left\{\left|x\right\rangle \middle| \, x \in S\right\}.$$

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

For convenience we will refer to elements of $\mathbb{R}[S]$ of the form $\sum_{x \in S} p_x |x\rangle$ with $p_x \geq 0$, $\sum_{x \in S} p_x = 1$ as *normalized vectors*. Our disucssion can be summarized as saying that probability distributions on S correspond to normalized vectors in $\mathbb{R}[S]$.

We now move on to discussing the way that probability spaces can evolve, or be related to one another. Certainly, a relation between a probability space with outcomes S and a probability space with outcomes S' will be some function

$$(\text{normalized vectors in } \mathbb{R}[S]) \to (\text{normalized vectors in } \mathbb{R}[S'])$$

which gives a rule for going from proability distrubutions on S to probability distributions on S'. However, not every function will give a valid assignment. For example, suppose we are studying the outcomes of lottery tickets. Ticket 1 has an 80% chance of being a winner, and Ticket 2 has a 40% of being a winner. You haven't scratched your ticket yet, so you know you have a 50% chance of having Ticket 1 and a 50% chance of having Ticket 2. What is the probability that you win the lottery? The standard way of computing it would be as follows:

$$\begin{aligned}
\text{result}(|\text{your ticket}\rangle) &= \text{result}\left(\frac{1}{2}|\text{Ticket 1}\rangle + \frac{1}{2}|\text{Ticket 2}\rangle)\right) \\
&= \frac{1}{2}\text{result}(|\text{Ticket 1}\rangle) + \frac{1}{2}\text{result}(|\text{Ticket 2}\rangle) \\
&= \frac{1}{2}\left(\frac{4}{5}|\text{win}\rangle + \frac{1}{5}|\text{lose}\rangle\right) + \frac{1}{2}\left(\frac{2}{5}|\text{win}\rangle + \frac{3}{5}|\text{lose}\rangle\right) \\
&= \frac{3}{5}|\text{win}\rangle + \frac{2}{5}|\text{lose}\rangle\,.
\end{aligned}$$

Hence, you have a $3/5 = 60\%$ chance of winning. The key insight in this computation was that probabilistic processes are *linear*. That is, "result" induces a linear map from $\mathbb{R}[\{\text{Ticket 1}, \text{Ticket 2}\}]$ to $\mathbb{R}[\text{win}, \text{lose}]$. More generally, given finite sets S, S' any linear map $\mathbb{R}[S] \to \mathbb{R}[S']$ which sends normalized vectors to normalized vectors could represent some valid probabilistic process.

The final topic to tackle before giving the full axiomatization is the question of *joining* probabilitstic systems. In this book we will mostly be constructing systems out of a lot of smaller consitutent parts, so the question of fitting together smaller systems to make one larger system is of utmost importance. Suppose we have two smaller systems with possible outcomes S, S'. To describe a state in the joined system, it is neccecary and sufficient to describe how that state restricts to each subsystem. In this way, possible outcomes of the joined system will correspond to pairs (x, x') where $x \in S$ is the portion of the overall state in S and $x' \in S'$ is the portion of the overall state in S'. This means the space out outcomes in the joined system is the Cartesian product $S \times S'$.

We are now ready to state the full axioms of probability theory:

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. Valid states are normalized vectors in $\mathbb{R}[S]$, which we call probability distributions on S.

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

3. (Joining systems) If S and S' are two finite sets, the system obtained by joining $\mathbb{R}[S]$ and $\mathbb{R}[S']$ is $\mathbb{R}[S \times S']$.

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

□

2.2.2 Basis-dependent quantum mechanics

The basis-dependent version of quantum mechanics can be estblished by copying the axioms of probability theory almost verbatim, replacing the 1-norm with the 2-norm.

Given a finite set S, a normalized vector in $\mathbb{R}[S]$ is one of the form $\sum_{x \in S} p_x |x\rangle$, where $p_x \geq 0$ and $\sum_{x \in S} p_x = 1$. This quantity $\sum_{x \in S} p_x$ is known as the *1-norm* of the vector $p = (p_x)_{x \in S}$.

In quantum mechanics we re-define the notation of normalized vector. A normalized vector in quantum mechanics is a state $\sum_{x \in S} c_x |x\rangle$, where $c_x \in \mathbb{C}$ are arbitary complex numbers and $\sum_{x \in S} |c_x|^2 = 1$. The root of the sum of norm-squares $\sqrt{\sum_{x \in S} |c_x|^2}$ is known as the *2-norm* of the vector $c = (c_x)_{x \in S}$. In this way, the norm-squares $|c_x|^2$ form a probility distrubution on S.

Thus, given some finite set S, states in the quantum system based on S correspond to normalized vectors in $\mathbb{C}[S]$. As a matter of convention, normalized vectors in $\mathbb{R}[S]$ will always refer to the 1-norm definition and normalized vectors in $\mathbb{C}[S]$ will always refer to the 2-norm definition. We are now ready to state the basic axioms of quantum theory, with the caveat that it does not give the full picture of measurement:

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

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

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

3. (Joining systems) If S and S' are two finite sets, the system obtained by joining $\mathbb{C}[S]$ and $\mathbb{C}[S']$ is $\mathbb{C}[S \times S']$.

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

□

We now relate these axioms to the previous dicussion and introduce terminology. The formal sums $\sum_{x \in S} c_x |x\rangle$ are not probability distributions. They are called *wavefunctions*. Every state in quantum mechanics is encoded in a wavefunction. Treating the possible outcomes in S as positions, we get the analogy

- Wave = multiple positions, spread-out $= \sum_{x \in S} c_x |x\rangle \in \mathbb{C}[S]$;

- Particle = single positions, definite = $|x\rangle$, $x \in S$.

By axiom (4), measuring of wavefunction collapses it into a single particle. This is the essence of wave-particle duality in quantum mechanics. The numbers c_x are not probilities. They are called *amplitudes*. If a state $|\psi\rangle = \sum_{x \in S} c_x |x\rangle$ has non-zero aplidue at $x, y \in S$, then we say that $|\psi\rangle$ is in a *superposition* of being in state $|x\rangle$ and $|y\rangle$.

Within this framework it is easy to demonstrate the phenominon of interference. Define the transformation $M : \mathbb{C}[S] \to \mathbb{C}[S]$ by

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

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

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

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

We can summarize this as saying that there was *constructive interference* in the $|0\rangle$, and *destructive interference* in the $|1\rangle$. The amplitudes had the same signs in the $|0\rangle$ causing the probability of measuring 0 to add, and the amplitudes had opposite signs in the $|1\rangle$, causing the probabilities of measuring 1 to cancel.

2.2.3 Measurement

The axioms in the previous section are all accurate, but they do not give a complete picture of measurement in quantum theory. In particular, the type of measurment which takes a state $\sum_{x \in S} c_x |x\rangle$ and collapses it to $|x\rangle$ with probability $|c_x|^2$ is only a special type of measurement. There are key subtleties that are ignored in our naive treatment:

1. It is possible to measure with respect to bases other than the standard basis;
2. Measurements can be incomplete, meaning that they do not collapse a wavefunction all the way down to a particle;
3. Measurements always have *observables* associated with them.

The easiest point to discuss is observables. Every time you measure something in a laboratory, there is always a real number output associated with the measurement:

- If you measure the velocity of a particle, the ouput is a speed in meters/second;
- If you measure the relative position of two objects, the output is a distance in meters;
- If you measure the intensity of a light source, the output is a luminescence in candelas/square meter;
- etc, etc...

Seeing as these real numbers are the only quantities which we actually get to record as experiments, we have to incorporate them into our theory. For example, consider some finite set S with associated quantum system $\mathbb{C}[S]$. Suppose we measure the energy of the system in joules (J). Since S is finite there are finitely many possibilities for the energy, say 1J, 5J, 10J. In a quantum system, measuring with respect to energy will produce some output (1J, 5J, or 10J) and collapse the system onto a state with a well-defined energy.

A crucial point is that these states with well-defined energy have *absolutely no reason* to be the same as the elements of S. Different observables can have different collections of states with well-defined values of those observables. A state with a well-defined value of some observable is called an *eigenstate* of that observable. This will connect back to our usual notation of eigenvector from linear algebra.

As an example, suppose $S = \{0, 1\}$. We define an observable called energy. We say that the state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ has energy $2J$ and the state $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ has energy 3J. The state $|0\rangle$ can be decomposed as

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

We see here that $|0\rangle$ is in an equal superposition of the state with energy 2J and the state with energy 3J. When we measure this state, it will collapse onto some energy eigenstate. It will collapse onto $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}$ with probability $1/2$ and it will collapse onto $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ with probability $1/2$, depending on the value of energy that was measured.

It is important that one needs to take care when defining observables to make sure that no contradictions appear. For instance, once the values of the observable are specified on a basis then the rest of the values of the observable follow by linearity. A more subtle restricition is seen in the following example. Supose that $|0\rangle$ is given energy 2J and $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}$ is given energy 3J. Then, we can write

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

In this way, $|1\rangle$ has energy 2J with amplitude $-\sqrt{2}$ and energy 3J with amplitude $+\sqrt{2}$. Clearly, the norm squares of these amplitdues does not give a valid probability distribution. They key algebraic requirement is *orthogonality*. Namely, we have an *inner product* on $\mathbb{C}[S]$ defined by

$$\left\langle \sum_{x\in S} c_x |x\rangle \middle| \sum_{x\in S} c'_x |x\rangle \right\rangle = \sum_{x\in S} c_x \overline{c'_x}.$$

Two states in $\mathbb{C}[S]$ are called *orthogonal* if their inner product is 0. If the values of an observable are specififed with respect to a basis in which every basis vector is normalized and every pair of basis vectors is orthogonal, then this observable can be extended to all normalized vectors in $\mathbb{C}[S]$ without issues. Before stating this axiom formally, we introduce some notation. If a basis of $\mathbb{C}[S]$ consists of normalized pairwise orthogonal vectors, we call it *orthonormal*. An *obervable* on $\mathbb{C}[S]$ is a pair (B, v) where $B \subset \mathbb{C}[S]$ is an orthonormal basis and $v : B \to \mathbb{R}$ is a set function.

This gives us our next version of the axioms of quantum mechanics. There are issues that arise when v is not injective, so we state our axioms with a restriction on v for now:

3'. (Measuring systems) Let (B, v) be an observable for which v is injective. The system $\mathbb{C}[S]$ can be measured with respect to (B, v). When $|\psi\rangle = \sum_{b\in B} c_b |b\rangle \in \mathbb{C}[S]$ is measured with respect to (B, v), the state collapses to each $|b\rangle$, $b \in B$, with probability $|c_b|^2$. In the case that $|\psi\rangle$ collapses onto $|b\rangle$, we say that the outcome of the measurement is $v(b) \in \mathbb{R}$.

We will verify that the values $|c_b|^2$ indeed form a probability distribuution later in the section.

2.2.4 Incomplete measurement

The above discussion is still missing some generality. Namely, it ignores the fact that that measurements can be *incomplete*. Incomplete measurements arrise when two linearly indendent vectors have the same value of an observable. When the observable is measured, it doesn't know which of those two linearly independent vectors to collapse to! In this situation, we say that the observable is *degenerate*. The term degeneracy here comes from its general mathematical usage, whereby it used to describe edge cases where not-neccecarily-equal values happen to be equal.

Instead of collapsing all the way down to an eigenstate, the measurement of degenerate observables will project a state onto the subspace spanned by the eigenstates with the measured value of the observable. For example, let $S = \{0, 1, 2\}$. Suppose that the state $|0\rangle$ has energy 5J, and that the states $|1\rangle$ and $|2\rangle$ have energy 10J. Suppose further that we measure the state

$$\frac{1}{\sqrt{3}} |0\rangle + \frac{1}{\sqrt{3}} |1\rangle - \frac{i}{\sqrt{3}} |2\rangle$$

with respect to energy, and the observed valu is 10J. This will collapse the state onto $\frac{1}{\sqrt{2}} |1\rangle - \frac{i}{\sqrt{2}} |2\rangle$. The projection respects phases, but scales the absolute value of the state so that it becomes normalized. Formally, this is an orthogonal projection. To state this axiom it is good to introduce some notation. Let S be a finite set and let $|\psi\rangle$, $|\varphi\rangle$ be states in $\mathbb{C}[S]$. We use the notation

$$\langle |\psi\rangle | |\varphi\rangle \rangle \coloneqq \langle \psi | \varphi \rangle .$$

This gives us a complete description of measurement in quantum mechanics:

3". (Measuring systems) Let (B, v) be an observable. The system $\mathbb{C}[S]$ can be measured with respect to (B, v). Let $|\psi\rangle = \sum_{b\in B} c_b |b\rangle \in \mathbb{C}[S]$ be a state, and let $\lambda \in \mathbb{R}$ be a real number. The probability that the outcome of the measurement is equal to λ is $\sum_{v(b)=\lambda} |c_b|^2$. In this case, the state $|\psi\rangle$ will collapse onto

$$\left(\sum_{v(b)=\lambda} c_b |b\rangle \right) \Bigg/ \left(\sum_{v(b)=\lambda} |c_b|^2 \right) .$$

2.2.5 Basis-independent quantum mechanics

From our discussion of measurement it is clear that, unlike probibilistic systems, quantum systems do not have a favored choice of basis. However, our definition of quantum system is still woefully basis-dependent. Namely, it starts by choosing a distinguished basis S of

$\mathbb{C}[S]$. What would be better if we could remove this choice, and make a quantum system simply a vector space.

This poses some immediate problems however. The first is that vector spaces have no notion of norm. Hence, we cannot speak of normalized vectors, and hence we cannot speak of sates. What's more, measurements are required to use an orthonormal basis. To define orthogonality we used the canonical inner product on $\mathbb{C}[S]$. Without a basis there is no distinguished choice of inner product. However, in a real sense that is the *only* piece of information we need about our basis - its inner product. This means that we can state the axioms of quantum mechanics for any vector space with a distinguished choice of inner product. We define what it means for a space to have an inner product below:

[WORK: define Hilbert space]

In any Hilbert space V, we can define the 2-norm of a vector $|\psi\rangle \in V$ to be

$$|\,|\psi\rangle\,| = \sqrt{\langle\psi\,|\,\psi\rangle}$$

.

A normalized vector in a Hilbert space is any state for which $|\,|\psi\rangle\,| = 1$. Observe that this agrees with our previous definition of normalized vector. If B is any orthonormal basis of V and $|\psi\rangle = \sum_{b\in B} c_b\,|b\rangle$, then

$$\begin{aligned}\langle\psi\,|\,\psi\rangle &= \left\langle \sum_{b\in B} c_b\,|b\rangle \,\middle|\, \sum_{b\in B} c_b\,|b\rangle \right\rangle \\ &= \sum_{b_0,b_1\in B} c_{b_0}\overline{c}_{b_1}\,\langle b_0\,|\,b_1\rangle \\ &= \sum_{b\in B} |c_b|^2.\end{aligned}$$

Thus, $|\,|\psi\rangle\,| = 1$ if and only if $\sum_{b\in B}|c_b|^2 = 1$ relative to any (equivalently, all) orthonormal bases.

The quantum process and quantum measurement axioms are obvious to state in any Hilbert space. The difficulty is in the joining axiom. It's here that we observe that for any finite sets S, S', there is a canonical isomorphism

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

where $\otimes$ is the tensor product. For those unfamilar with the tensor product, this could be taken as the *definition* of it. We note that the tensor product of two Hilbert spaces $(V, \langle\cdot|\cdot\rangle_V)$, $(V', \langle\cdot|\cdot\rangle_{V'})$ is a Hilbert space. The inner product on $V\otimes V'$ is given by

$$\langle(v\otimes v')|(w\otimes w')\rangle_{V\otimes V'} = \langle v|w\rangle_V \cdot \langle v'|w'\rangle_{V'}\,.$$

This leads us to the following basis independent formulation of the axioms of quantum mechanics:

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

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

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

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

4. (Measuring systems) Let (B, v) be an observable. The system V can be measured with respect to (B, v). Let $|\psi\rangle = \sum_{b \in B} c_b |b\rangle \in V$ be a state, and let $\lambda \in \mathbb{R}$ be a real number. The probability that the outcome of the measurement is equal to λ is $\sum_{v(b)=\lambda} |c_b|^2$. In this case, the state $|\psi\rangle$ will collapse onto

$$\left(\sum_{v(b)=\lambda} c_b |b\rangle \right) \Big/ \left(\sum_{v(b)=\lambda} |c_b|^2 \right).$$

□

Now that we have stated our final version of the axioms of quantum mechanics, we make some technical comments which aid in our future endevors. The first is that operators which send normalized states to normalized states have a very concise charactarization in terms of the *conjugate tranpose*. Of course, without a basis we have no way of identifying linear operators with matrces, and hence no way of defining the transpose. Given a Hilbert space V and a linear map $M : V \to V$ there may be no way to define the transpose but there *is* a way of defining the component-wise conjugate transpose of V. This conjugate tranpose is denoted $M^\dagger$, and is defined by the inner-product formula

$$\langle U\psi \,|\, \varphi \rangle = \left\langle \psi \,\middle|\, U^\dagger \varphi \right\rangle.$$

It is verified in Exercise [ref] that this formula always specifies a unique well-defined operator, and that this operator is equal to the conjugate tranpose of V relative to any orthonormal basis. Here is our charactarization of maps which send normalized vectors to normalized vectors:

Proposition 2.1. *Let V be a Hilbert space, and let $U : V \to V$ be a linear transformation. The following are equivalent:*

1. *U sends normalized vectors to normalized vectors;*
2. *$U^\dagger = U^{-1}$.*

If either of these two equivalent conditions are met, we call U a unitary transformation.

Proof. We observe that if $U^\dagger = U^{-1}$, then for any normalized vector $|\psi\rangle$

$$|U|\psi\rangle| = \langle U\psi \,|\, U\psi \rangle = \left\langle \psi \,\middle|\, U^\dagger U\psi \right\rangle = \langle \psi \,|\, \psi \rangle = 1.$$

Hence, (2) $\implies$ (1). To show the other direction, suppose that U sends normalized vectors to normalized vectors. By scaling, we observe that $|U|\psi\rangle| = ||\psi\rangle|$ for all $|\psi\rangle \in V$. We now show that U sends orthogonal vectors to orthogonal vectors. Let $|\psi\rangle, |\varphi\rangle$ be orthogonal vectors. We wish to show that $U|\psi\rangle$ and $U|\varphi\rangle$ are orthogonal as well. We compute:

$$\begin{aligned}
|\,|\psi\rangle\,|^2 + |\,|\varphi\rangle\,|^2 &= \langle \psi + \varphi \,|\, \psi + \varphi \rangle \\
&= \langle U(\psi + \varphi) \,|\, U(\psi + \varphi) \rangle \\
&= \langle U\psi \,|\, U\psi \rangle + \langle U\varphi \,|\, U\varphi \rangle + \langle U\psi \,|\, U\varphi \rangle + \langle U\varphi \,|\, U\psi \rangle \\
&= |\,|\psi\rangle\,|^2 + |\,|\varphi\rangle\,|^2 + 2\Re\left(\langle U\psi \,|\, U\varphi \rangle\right)
\end{aligned}$$

where $\Re(\cdot)$ denotes the real part of a complex number. Thus, we conclude that $\Re\left(\langle U\psi \,|\, U\varphi\rangle\right) = 0$. However, chaning $|\varphi\rangle$ by a phase, we can assume without loss of generality that $\langle U\psi \,|\, U\varphi\rangle$ is real, and hence we conclude that $\langle U\psi \,|\, U\varphi\rangle = 0$. Thus, we conclude that $\langle U\psi \,|\, U\varphi\rangle = \langle \psi \,|\, \varphi\rangle$ whenever ψ and φ are equal or orthogonal. Letting ψ, φ run over an orthonormal basis, we thus conclude that the equation $\langle U\psi \,|\, U\varphi\rangle = \langle \psi \,|\, \varphi\rangle$ holds on a basis. Extending via linearity we conclude it holds everywhere, which is exactly the statement that $U^\dagger = U^{-1}$, as desired. □

Our second comment is in its heart a way of compact packaging the data of an observable. Given a Hilbert space V, instead of working with a choice of orthonormal basis B and a function $v : B \to \mathbb{R}$ we can work instead with a single operator $H : V \to V$. This is done by defining

$$H(b) = v(b) \cdot b$$

for all $b \in B$. The set B can now be recovered as the eigenvectors of H, and the measured results of the observable correspond to the eigenvalues. It is from this repackaging that the states in B get the name eigenstate. This packaging is useful because the space of linear operators $H : V \to V$ has more structure than the space of orthonormal bases of B paired with functions $v : B \to \mathbb{R}$. For example, we can now add two observables together, or tensor two observables on smaller systems to obtain an observable on a larger system. These sorts of operations will be very important going forward. In fact, the operator H will often have a simple form, and even computing what the elements of B are can be highly complex.

In a similar vein to our characterization of unitary operators, we give a characterization of those linear operators which arrise from observables:

Proposition 2.2 (Spectral theorem)**.** *Let $H : V \to V$ be a linear transformation. The following are equivalent:*

1. *There exists an observable (B, v) such that $H(b) = v(b) \cdot b$ for all $b \in B$;*
2. *$H = H^\dagger$.*

If any of the three equivalent conditions are met, we call H a Hermitian matrix.

Proof. We do (1) $\implies$ (2) first. From Exercise [ref], we know that $H^\dagger$ can be computed as the conjugate transpose relative to any orthonormal basis. Choosing the orthonormal basis B, H is a real diagonal matrix. Hence, it is clearly equal to its own conjugate transpose.

We now prove the converse. We consider the map $\langle \cdot | \cdot \rangle$ as defined in the proof of Proposition 2.1. Since $\mathbb{C}$ is algebraically closed the characteristic polynomial of H must have a root, hence we know that H has some eigenvector e, with eigenvalue λ. Scaling e if neccecary, we can assume without loss of generality that $\langle e|e\rangle = 1$. Let V be the subspace of vectors

$x \in \mathbb{C}[S]$ such that $\langle e|x\rangle = 0$. This space has dimension one less than V. We know from the definiton of conjugate transpose that

$$\langle x|Hy\rangle = \langle Hx|y\rangle \ \ \forall x, y \in \mathbb{C}[S].$$

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

$$\langle e|Hx\rangle = \langle He|x\rangle = \lambda \langle e|x\rangle = 0.$$

Thus, H restricts to a map on V. Continuing this proccess of picking eigenvectors and restricting H to the subspace of vectors orthogonal to it, we find that V has an orthonormal basis of eigenvectors. Moreover, all of these eigenvectors satisfy

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

so their eigenvalues $\lambda = \overline{\lambda}$ are real. Thus, (2) $\implies$ (1) as desired. □

This concludes our treatment of the basic axioms of quantum mechanics.

2.2.6 Hamiltonians and the Schrodinger equation

We now know the basic rules of quantum mechanics. Suppose, however, that we are given some quantum mechanical system in a lab. How will it evolve in time? Certinaly it will evolve by a unitary transformation, as per the axioms. But *which* unitary? The answer to this question is the Schrodinger equation. It gives us time dynamics in quantum mechanics. Once the initial state of the universe was set, the rest of time was just an evolution by the Schrodinger equation.

At the heart of the Schrodinger equation is the *Hamiltonian* of a quantum system. The Hamiltonian is an observable. The physical quantity it coressponds to is *total energy*. States with definite total energy are known as energy eigenstates, and their energy is some real number. In line with general principles established in the previous subsection, we will think of the Hamiltonian as being a linear operator $H : V \to V$. The Schrodinger equation is defined as follows:

Definition. (Schrodinger equation) Let V be a Hilbert space, corresponding to a quantum system. Let H be a Hermitian operator, corresponding to the Hamiltonian of V. Let $|\psi(t)\rangle$ denote the state of the system at time t. We have the formula

$$|\psi(t)\rangle = e^{-iHt} |\psi(0)\rangle$$

where $e^M = \sum_{n=0}^{\infty} \frac{M^n}{n!}$ is the matrix exponential.

□

This equation deserves several comments. First, we comment on terminology. Initially words *state of the system at time t* currently have no meaning. In fact time itself is at the current moment undefined. In this way, the Schrodinger equation is defining what time is in quantum mechanics (a one dimensional real parameter) and what it means for a system to be in a state at a time. We still do need to verify that the Schrodiner equation is consistent with our intuitive notion of time. For instance, if we first evolve the system in forward by t time units and then by s time units is that the same as evolving the system forward by $t + s$ time units? Under the Schroding equation, this is the same as verifying the equation

$$e^{-iH(t+s)}\left|\psi(0)\right\rangle \stackrel{?}{=} e^{-iHt}e^{-iHs}\left|\psi(0)\right\rangle.$$

This formula follows from the well known fact about matrix exponentials, which we will not prove:

Proposition 2.3. *If A and B are commuting operators, then*

$$e^A e^B = e^{A+B}.$$

Second, we make sure that the equation as stated is consistent with the axioms of quantum mechanics as we have previously defined them. In other words, is the map $e^{-iHt} : V \to V$ really a unitary operator for every $t \in \mathbb{R}$? This follows from the following important computation:

$$\begin{aligned}
\left(e^{-iHt}\right)^\dagger &= \left(\sum_{n=0}^{\infty}\frac{(-iHt)^n}{n!}\right)^\dagger \\
&= \sum_{n=0}^{\infty}\frac{\left((-iHt)^\dagger\right)^n}{n!} \\
&= \sum_{n=0}^{\infty}\frac{(iHt)^n}{n!} \\
&= e^{iHt}.
\end{aligned}$$

The operators e^{-iHt} and e^{iHt} are inverses by Proposition [ref].

A third comment to make about the Schrodinger equation is about units. Both time and energy, austensibly, should have units. However, we have treated them as dimensionless mathematical quantities. How can this be? The answer is that implicitely we *did* choose units. When different choices of units are made, different constants need to be put into the Schrodinger equation. The version of the Schrodinger equtaion which includes units is

$$\left|\psi(t)\right\rangle = e^{-iHt/\hbar}\left|\psi(0)\right\rangle$$

where $\hbar$ is the normalized plank constant. In our original statement of the Schrodinger equation we have simply decided to use units in which the normalized plank constant is equal to 1.

[WORK: talk to a physicist who can say why the Schrodinger equation is true. I only have vague waffle.]

The Schrodinger equation tells us that all we need to do to understand the dynamics of a quantum system is solve the Schrodinger equation. Suppose now that $\left|\psi(0)\right\rangle$ is some initial state in a quantum system with extended state space V and Hamiltonian H. Suppose that we have a decomposition $\left|\psi(0)\right\rangle = \sum_{x\in B} c_x \left|x\right\rangle$ where B is the set of energy eigenstates of H. Then, the Schrodinger equation would tell us that

$$\left|\psi(t)\right\rangle = \sum_{x\in B} e^{-iv(b)t}c_x\left|x\right\rangle$$

where $v(b)$ is the eigenvalue corresponding to v. In this way, we see that by writing $\left|\psi(0)\right\rangle$ in terms of an energy eigenbasis we can exactly solve the Schrodinger equation.

In this way, solving quantum dynamics correponds exactly to finding the eigenvectors of the Hamiltonian. Or, in other words, diagonalizing the Hamiltonian. This task, while conceptually easy, can be very difficult in specific cases. Diagonalizing matrices has never been so exciting!

History and further reading:

[WORK: there are people who can do a history of quantum mechanics way better than me]
A fantastic place to first learn about quantum mechanics and its principles is the popular science book "Quantum computing since Democritus" [Aar13]. A more formal, but still excellent, introduction to finite-dimensional quantum theory is Nielsen-Chuang's book "Quantum computation and quantum information" [NC10]. Past this there are many great textbooks which go into full depth on infinite-dimensional quantum theory and advanced properties of quantum systems. A good physics-oriented text is Shankar's "Principles of quantum mechanics" [Sha12], and a good math-oriented text is Hall's "Quantum theory for mathematicians" [Hal13].

Exercises:

2.1. .[WORK: show that the adjoint really is the conjugate transpose] [WORK: change verbiage above from "conjugate transpose" to "adjoint"]

[WORK: need to add somewhere that global phases don't matter, clear up this ambiguity]

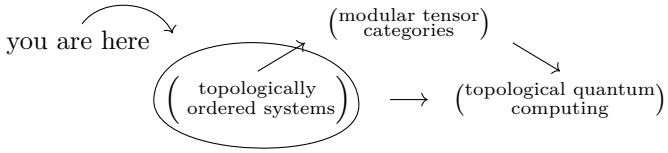
3 Topological quantum order

3.1 Overview

3.1.1 Introduction

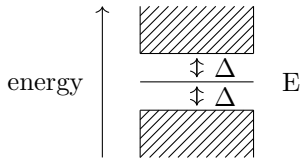
[WORK: balance generality and concreteness. I'll want to work with the definition of TO given by Bravyi and Hastings. This has the problem that it doesn't include the most physically realistic TO Hamiltonian, the honeycomb model! The honeycomb model only gives TC in its 4-th order perturbation theory. Something to deal with in the treatment - the big ideas are more important than the details. However, without the details thinigs can easily get way off track.]

In this chapter we will be giving a detailed analysis of topological quantum order, a particular type of topological quantum system. We recall below how this fits into the general framework of this book:



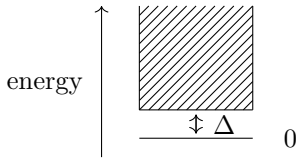
Topological quantum systems are distinguished by the fact that their states don't depend on local properties - they depend only on global topological properties of the system. One way of getting this sort of topological invariance is through *discreteness*. If a system is discrete, all of its parts are in a sense *far away* from each other. Things which are far away cannot be continusly deformed from one to another - local changes can't change discrete objects. A real-number valued invariant could move all over the place and depend heavily on local properties of a system, but an integer-valued invariant is *neccecarily* topological invariant.

We demonstrate this below in its most basic form. Suppose that V is a Hilbert space and $H : V \to V$ is a Hermitian operator. This represents a quantum system and its Hamiltonian. Let $|\psi\rangle$ be an energy eigenstate with energy E. Suppose further that the E-eigensapce of H is one dimensional, and that every other eigenvalue E' on H satisfies $|E' - E| \geq \Delta$ for some real number $\Delta > 0$. This situation is demonstrated in the below graph:



This energy gap around E adds a sort of discretness to the spectrum of H. Suppose that the system is in state $|\psi\rangle$ and we distort it a small amount. Typically, *this will not affect the state*. The state $|\psi\rangle$ would need to jump all the way to some other state, but all other states have significantly different energies. In particular, if the perturbation applied to $|\psi\rangle$ has magnitutde significatly less than Δ, then $|\psi\rangle$ cannot change. This connection between gaps in energy spectra and topological states is so essential that many physicists use the terms *topological system* and *gapped system* interchangably.

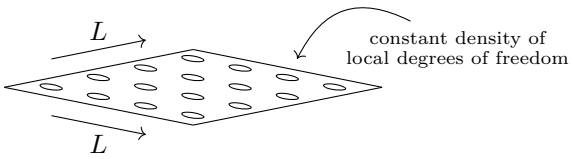
So, in practice, how do we make sure that the perturbations being applied to $|\psi\rangle$ are always much smaller than Δ? We make the system *cold*. Roughly we say that a system has *temperature* T if the states of the Hamiltonian being occupied all have energy $< T$, and perturbations from the environment have magnitute $\approx T$. We renormalize our Hamiltonain so that the lowest energy eigenstate has energy 0. We call the lowest energy eigenstates the *ground states* of the system. We now assume that the ground state space is one dimensional, so there is a unique ground state. We assume that the next lowest energy eigenvalue is $\Delta > 0$. This gives us a new picture:



So long as the temperature is much smaller than the energy gap ($T \ll \Delta$), then our system will remain in the ground state. We say that the system (V, H) *becomes topologically ordered at low temerature.*

[WORK: here is where I should introduce TO properly]

Of course, there's a big problem in our above discussion. *Every* finite dimensional quantum system is gapped. The Hamiltonian has finitely many eigenvalues, so its spectrum is neccecarily discrete. What we should really be imagnining is an infinite family of systems, paramaterized by some real number $L > 0$ called the *linear system size*. Working in a two dimensional system, this will look like the below picture:

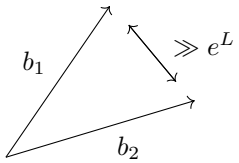


Letting $\dim(V)$ denote the dimension of V, this gives us an assymptotic formula $\dim(V) \sim e^{(\text{const})\cdot L^2}$ where the constant in the exponent depends on the density of quantum degrees of freedom in the system. Let Δ_L be the lowest nonzero energy of the Hamiltonian in the size-L system. Of course, we will always have a gap $\Delta_L > 0$. What's important is that we require that $\Delta_L > \Delta$ for some uniform $\Delta > 0$. In most quantum systems this will *not* be there case - as the system size gets larger there will be states with smaller and smaller nonzero energies.

The issue with our discussion up to now is that it is *no use* for making a topological quantum computing. There is only a single ground state, so there is no non-trivial topologically protected information. There's just a point. To make a quantum computer we will need to introduce *degeneracy* into the ground states - make the lowest energy eigenspace higher dimensional. This degenerate ground space is where we will store our information.

If we do this naively, there's an immediate issue which appears. What if a perturbation of the system keeps the vectors in the ground space, but perturbs exactly which vector in the ground space is being stored. Wouldn't this corrupt the data? The trick is choose the ground space correctly so that this does not happen. The way this works is by choosing a ground space which has a basis consiting of vectors which are in a certain sense "far apart". Because they are far apart, they cannot easily be distored from one to another.

More explicitley, let us choose standard basis S for V, inducing an isomorphism $V = \mathbb{C}[S]$. This basis should correspond to the physical degrees of freedom underlying the system. If V is made up of an L by L grid of some repeating quantum sub-system, then choosing some arbitary basis D for that subsystem a good choice for S is D^{L^2}, coming from the isomorphism $\mathbb{C}[S] \cong \mathbb{C}[D]^{\otimes L^2}$ where $\otimes$ in the exponent denotes repeated tensor product. The canonical metric on $\mathbb{C}$ induces a product metric on $V = \mathbb{C}[S]$. It is with respect to this topology that we want our basis for the ground space to be far apart. That is, we require a basis B for the ground space such that for every $b_1, b_2 \in B$, $|b_1 - b_2|$ is large. The exact scale of large depends on the topological system. At the very least it should tend to ininity with system size. In this case we will require an exponential scaling, $|b_1 - b_2| > e^{(\text{const})L}$:



[WORK: this stuff about distance is totally bogus. The real point is that if you differ at a large number of sites then it neccecarily takes a large number of local errors to make a difference! Probability gets exponentially suppressed. Global feature $\implies$ touches $>$ (const) $\cdot$ L sites.]

This allows us to state a full picture of how to store topological information in a gapped system. Suppose we have some gapped system as before with distinguished geometric basis S, Hilbert space $V = \mathbb{C}[S]$, Hamiltonian H, temperature T, topological energy gap Δ, and linear system size L. We suppose $T \ll \Delta$, $L \gg 0$. Suppose further that the information we wish to store is the ground state

$$|\psi\rangle = \sum_{x \in S} c_x |x\rangle .$$

As time goes, we image the coefficents c_x continuously varying due to noise. This noise should have magnitute $\cong T$. We control our information by repeately measuring with repsect to H. This measurement continually projects the our information back into an eigenstate. This is a mathematical mechanism for *cooling* - keeping the energy low. A few things could happen when H is measured.

1. Typically, after measuring the state will be projected back into the ground state space. The stored information will change a small continuous amount. The magnitute of this change is on the order of $T/e^{(\text{const})L}$. This is because basis vectors in the ground space are on the scale of $e^{(\text{const})L}$ times further apart than the basis vectors of $\mathbb{C}[S]$. Hence, the metric on the ground space is dialated by a factor of $e^{(\text{const})L}$, which has the effect of dampening the magnitute of the drift. Even though our stored information is always being corrupted by noise, the magnitute of this noise is tiny. Making the system size large, we can efficently make the drift arbitaraily small. For any polynomial-length algorithm, the total amount of drift is still suppressed to large enough degree that the errors are tolerable. This means that our information is *topologically protected* in this case.

2. After measurement, the state could get projected onto an energy eigenstate which is *not* a ground state. This corresponds to a spontanous jump in energy. The probability

of such a jump is suppressed by the magnitute of the gap, giving a probability on the order of T/Δ. Choosing $T \ll \Delta$, we can make this probability small. However, we cannot make it arbitrarily small, and errors of this type need to dealt with as they will surely appear in any sufficently long algorithm. The upside is that when these errors occur it is entirely detectable - the outcome of the measurement of H is some observable energy, and it can be detected when that energy becomes nonzero. When it is detected that the energy is nonzero, then the experimenters can project the system back into the ground space by applying some external probe. The experiments can choose this projection carefully so that it sends the state to the nearest ground state, keeping the information drift on the order $T/e^{(\text{const})L}$. The details of how experimenters project non-ground states into ground states depends from topological system to topological system, and is often the heart of a proposal for topological quantum computing.

All in all, we find that following the procedures outlined above we can store topological information with essentially no errors. This is topological quantum memory.

The question now is how to make a *computer* of this. How do you act on the information stored this way in a gapped system? How do we go from one state to another in a topologically protected way? There are lots of different ways to do this, each of which have many equivalent descriptions. Here I will present a framework similar to the one introduced by Aasen-Wang-Hastings [AWH22]. In this framework, we perform computations by slowly transformation which Hamiltonian H we use to cool the system.

Suppose we have some state $|\psi\rangle$ we want to perform our computation on. We will choose some a family of Hamiltonians H_t, one for each time $t \in [0, 1]$. We will require that $H_0 = H_1 = H$ is our original Hamiltonian. We will continuously transform which Hamiltonian we use to cool the system. That is, at every time step t, we measure the system with repsect to the Hamiltonian H_t. Assuming that the Hamiltonians vary slowly enough, our comments above apply. Namely, at time t either the state will stay a ground state of H_t with minimal drift or it will spontanously jump to an excited state. In the case that it jumps to an excited state, we can apply an external probe to project it back into a ground state. Letting $|\psi(t)\rangle$ denote the state at time t, we find that $|\psi(1)\rangle$ will be some new ground state of H, which is well-defined up to errors on the scale $T/e^{(\text{const})L}$.

The beautiful observation is that $|\psi(1)\rangle$ does not need to be equal to $|\psi(0)\rangle = |\psi\rangle$. If the path taken by the Hamiltonains is non-trivial it can have a non-trivial action on the ground states, and serve as a source of computation. This is topological quantum computation. This sort of continuous evolution of a Hamiltonian while keeping a state in the ground state is known as an *adiabatic* evolution of the Hamiltonian. An important point to emphaize is that for the above procedure to work, the Hamiltonians H_t must all have energy gaps, and these gaps must all be bounded below. Namely, $> \Delta$ for a fixed Δ. This model of computation can be summarized as saying that computations are performed by adiabatically transforming the Hamiltonian along non-trivial paths in the configuration space of all possible gapped Hamiltonians.

This already allows us to make interesting comments about the nature of topological quantum computing. To make a powerful quantum computer, there needs to be a lot of different loops that the Hamiltonian can go around, corresponding to a lot of possible different gates that can be applied. This means that the path-connected component of the original Hamiltonian in the configuration space of all possible gapped Hamiltonians has to have lots of non-trivial loops - its fundamental group needs to be large. Choosing gapped Hamiltonains whose path connected component in the space of gapped Hamiltonians has interesting topology is the art of topological quantum computing. It is here that we can

get the definition of what a topological order is. It is a path connected component in the configuration space of gapped Hamiltonians. Or, equivalently, an equivalence class of gapped Hamiltonian up to continuous deformation.

Note that the exact definition of gapped Hamiltonian is subtle, because really we are talking about infinite families of Hamiltonians paramaterized by system size, and so our above definiitons of topological order are only approximate. The point is that topological order captures the inherent algebraic structure and nontrivial topology with a gapped Hamiltonian, while forgetting the details of how that Hamiltonian is defined.

[WORK: How should I define topological order, as opposed to simply "gapped Hamiltonian"? What am I missing? Is this something I even want to define it? Add a subsection?]

[WORK: The papers [CDH$^+$20, BHM10, BH11] all agree on two axioms of TQO, TQO-1 and TQO-2. The exact implementation of these axioms are different, but their philosophy is here. Bring them in.

TQO-1 = ground states are error correcting code (topological protection)

TQO-2 = local ground state coincides with global one (allows for quasiparticle picture)

]

3.2 Discrete gauge theory

3.2.1 Ordered media on a lattice

Above we defined topological order. The best way to demonstrate the general prinmciples of topological order is to give a good family of examples. The examples we will give in this section come from *discrete gauge theory*. At its heart, discrete gauge theory is a quantum version of the notion of ordered media we defined in Chapter [ref] section [ref]. While mathematically unnececary, the next two subsections give physical motivation for why the formulas for discrete gauge theory have to be like they are, and why their analysis behaves like it does. Those who feel comfortable working with unmotivated formulas should skip to subsection [ref].

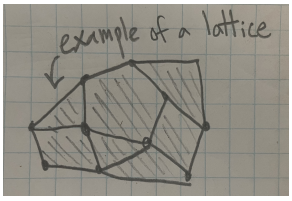
We will go from ordered media to discrete gauge theory in two steps:

Step 1: Put ordered media on a lattice;

Step 2: Make it quantum.

This first subsection is focused on Step 1. We will do Step 2 in the next subsection.

The first natural question to ask is *what is a lattice*. For our purpose a lattice is something like the picture below:

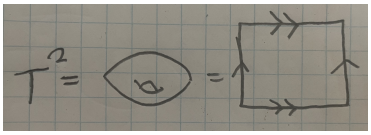


A lattice is a collection of vertices, edges, and faces connected in some way. To keep in line with the terminology common in topological quantum information, we refer to the faces of our lattices using the French term *plaquette*. Formally, by lattice we mean "simplicial

2-complex" though there is no need to go into details because we will never be dealing with the subtleties in the definition. Often times we will need to deal with *directed* lattices. These are lattices in which every edge has a direction, which we represent as an arrow on that edge.

Before putting ordered media on a lattice, a good question is *why* we would want to do this. There are two primary reasons. The first is that this will make this Hilbert spaces involved all finite dimensional. This is very important because we have only established quantum mechanics in the finite dimensional case, and working with the continuum limit can be highly complex. The second reason is that in practice, many of the systems physicists deal with are on lattices. For example, the chip of a quantum computer will store its information at finitely many sites, which can correspond to the vertices of some lattice. Many topological systems also arrise from materials which have crystal structures, which are modeled well by a lattice with atoms at the vertices and edges representing the geometry of the crystal.

The best setting for putting our ordered media on a lattice is by first putting on a torus. This helps for several reasons. Firstly, a torus is compact and hence it will add even more finiteness to the problem. Secondly, a torus has nontrivial topology which is useful for seeing the characteristic phenomina of topological order. Thirdly, a torus has no boundary, which helps because boundaries in topological order are subtle and require more work to describe. We denote the torus by T^2, and identify it with a square having its opposite sides glued:



Ordered media on the torus corresponds to continuous maps $\phi : T^2 \to M$ where M is some fixed order space. The steps to transforming a state ϕ into a lattice version of itself go as follows:

Step 1(a): Choose a directed lattice on the torus;

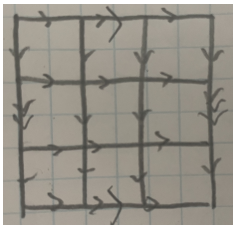
Step 1(b): Choose a basepoint $m \in M$. Make *local twists* around each vertex so that $\phi(v) = m$ for all vertices v in the lattice.

Step 1(c): On every edge, write down the winding number of ϕ along that edge, as an element of $\pi_1(M, m)$;

Step 1(d): Forget ϕ, and remember only the assignment of group elements in $\pi_1(M, m)$ to edges in the lattice.

These steps deserve explanation. Step 1(a) is clear: we choose an arbitrary lattice on the torus. Typically we will choose the square lattice on the torus:

Step 1(b) requires more explanation. The picture to imagine is that we take the state ϕ and twist its values in small neighborhoods around each vertex to enforce the condition $\phi(v) = m$. Formally, this means choosing another state $\tilde{\phi}$ such that $\tilde{\phi}(v) = m$ for every vertex v of the lattice, and $\tilde{\phi} = \phi$ outside of some chosen small neighborhoods around each vertex. The fact that we can always choose such as state $\tilde{\phi}$ is a consequence of general mathematical principles in homotopy theory. Of course, different choices of $\tilde{\phi}$ will change

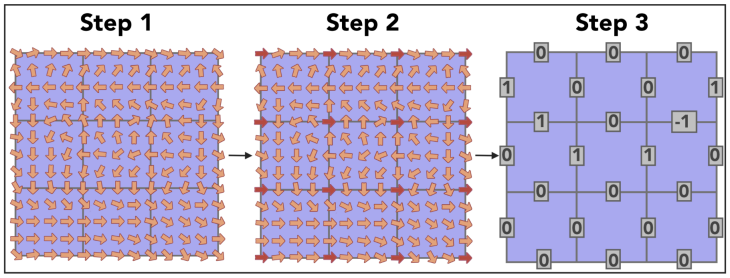


the final result of our lattice encoding. However because any two choices of $\tilde{\phi}$ can only differ by local changes they can't be *too* different, in a way we will quantify later in the subsection.

Step 1(c) is straightforward. Every edge can be thought of as a path. Pushing forward with ϕ, this gives us a path in M. Since the edge starts and ends at vertices and ϕ sends all vertices to m, this means that the push forward of our edge gives a loop in M based at m. Hence, it gives an element of $\pi_1(M, m)$. We can record this element and attach it as a piece of data associated to the edge.

Step 1(d) is entirely book keeping. It records the fact that we have successfully transformed our continuous data ($\phi : T^2 \to M$) into discerete data (an assignement of group elements to edges in a lattice).

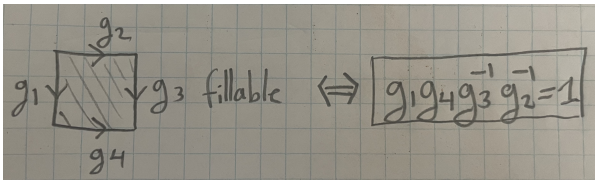
A worked example is shown below in the case that $M = S^1$ is the circle:



We now analyse our encoding of states in ordered media into assignements of group elements in $\pi_1(M, m)$ to edges in the lattice. The first fact from homotopy theory we will use is that these group elements determine the state ϕ exactly up to deformations localized within each face. Taking a limit of denser and denser lattices, this means that the group elements will specify ϕ up to increasingly local deformations. The intiution is that by taking an infinite lattice limit we should recover ϕ up to "infinitely local deformations", i.e., we recover it exactly. In this way we did a good job with our lattice encoding.

We observe that not every assignement of group elements to edges appears in our construction. There are implicit conditions. In particular, imagine taking the product of the group elements on edges along some contractible loop, taking inverses appropriately so that all the arrows are pointing in the same direction. This product will be equal to the group element associated with the loop around this whole path. The winding number along any contractible path under a continuous map should be trivial. Hence, the product of these group elements should be trivial. In particular, given any plaquette, the ordered product of group elements along its edges should be zero:

Moreover, *any* coloring of the edges of the lattice by elements of $\pi_1(M, m)$ will come from

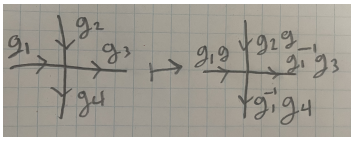


some map ϕ so long as it satisfies the condition above. This is one of the key formulas of the theory. It is in a real sense a lattice version of the continuity condition, since it is *equivalent* to the condition of continuity in the infinite lattice limit. This lattice version of continutity is called *flatness*. Flatness conditions are the most common sort of compatibility conditions which appear when you have local degrees of freedom valued in some group, making this lattice situation very general.

The last thing do deal with in analysing our system is deformation. When analysing states in ordered media, a huge amount of our time was spent on performing continuous deformations. Topological information is defined to be information which is invariant under continuous deformation. What does this correspond to in the lattice model?

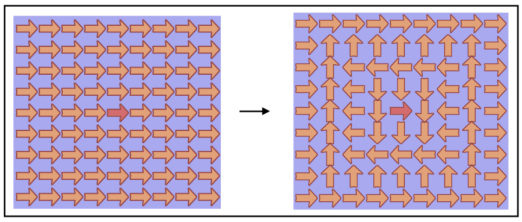
Suppose we are given an ordered media state ϕ and its corresponding lattice coloring. If we deform ϕ in some small neighborhood within a face, this will not change the values along the edges and hence will not change the coloring. If we deform ϕ in some small neighborhood around the interior of some edge this also won't change the coloring, because this will correspond to deforming the loop in M induced by going along that edge, and elements of the fundamental group are invariant under deformations of this sort. Another way of seeing that the coloring can't change is that flatness must be preserved - if the group element on the deformed edge changed, it would ruin flatness on the faces it bounds.

Finally, we can consider deforming ϕ around some vertex. This certainly *can* impact the coloring. An easy way to compute how it must impact the coloring is by using the fact that the flatness condition must be preserved. Suppose that an incoming edge labled by g_1 changes to $g_1 g$ after the deformation. Enforcing flatness along all of the faces touching the vertex allows one to conclude that all incoming edges g_k will get changed to $g_k g$, and all outgoing edges g_k will get changed to $g^{-1} g_k$, as shown below:



Another way of seeing this result is by anlysing what a deformation of ϕ does. The value $\phi(v)$ can move along some loop, starting and ending at m. This loop induces some element of the fundamental group, $g \in \pi_1(M, m)$. Performing this deformation exactly acts by precomposing/postcomposing the adject edges with $g/\ g^{-1}$ accordingly. We can see below a concrete example for $G = S^1$:

Hence, we have a picture for ordered media on the lattice: states correspond to flat colorings of elements of $\pi_1(M, m)$ on a fixed lattice, and continuous deformations correspond to certain vertex actions by elements of $\pi_1(M, m)$.



3.2.2 From ordered media to gauge theory

In the previous subsection we showed how to put ordered media on a lattice. In this section we show how to make it quantum, turning it from a classical field theory to a quantum gauge theory. The idea of this jump is as follows. In Section [ref] we obtained an equivalence

$$\binom{\text{topological information}}{\text{in ordered media}} = (\text{states}) \,/\, \binom{\text{continuous}}{\text{deformation}}.$$

It is neccecary to mod out by continuous deformation because there is topoloigcal information in states, but also local degrees of freedom. For instance, the group element assigned to any indivudal edge in ordered media on a lattice can be changed by a gauge transformation and hence is not topologically invariant. The idea of going from ordered media to gauge theory is as follows: gauge theory is what results from ordered media when quantum fluxtuations become so strong that local degrees of freedom are completely washed out and only the topology remains.

The fluxtuations are quantum because we will imagine that our states will evolve in such a way that they are in a superposition of gauge transformations having been applied and not having been applied. Our states in gauge theory will be *equal superpositions over all possible deformations* of a given state. In this way, we are using quantum mechanics as a physical mechanism for quotients. Equivalence classes under deformation will be physically realized as equal superpositions over all possible representatives.

This can all be made completely rigorous. Choose a lattice on the torus, an order space M, and a basepoint m. We define a Hilbert space

$$\mathcal{N} = \bigotimes_{\text{edges}} \mathbb{C}[G].$$

We canonically identify the standard basis of $\mathcal{N}$ with G-colorings of the lattice. Let C be an equivalence class of flat G-colorings of $\mathcal{N}$ up to gauge transformations. There is a corresponding state

$$|C\rangle = \sum_{\gamma \in C} \frac{1}{\sqrt{|C|}} |\gamma\rangle \,.$$

This state is a normalized equal superposition of representatives of C. This defines a sub-Hilbert space

$$\mathcal{C} = \text{span}\,\{\,|C\rangle |\, C \in (\text{flat } G\text{-colorings})/(\text{gauge transformations})\}\,.$$

This Hilbert space $\mathcal{C}$ stores the information in our gauge theory.

So far our system is relatively trivial - it is just a Hilbert space, with no Hamiltonian. We connect it back to our original picture of topological order. The space $\mathcal{C}$ is the collection

of ground states in a topologically ordered system. Above it there is a whole spectrum of other states. This fuller picture with a Hamiltonian adds all of the subtlety and intrigue to the system.

In particular, we observed in Chapter [ref] section [ref] we observed the importants of quasiparticles in ordered media. These formed the heart of our information processing. Similarly, in gauge theory there will be quasiparticles as well which appear higher up in the spectrum of the Hamiltonian. Some of these quasiparticles will correspond to the classical quasiparticles in ordered media, but others are entirely new features of the system which did not exist before. We will analyse all this in more in the subsection that follows.

3.2.3 Kitaev quantum double model

[WORK: not sure if this is readable to someone who skipped the first two sections, but it should be. Something to keep an eye on.]

[WORK: Use $\mathfrak{D}(G)$ as notation for the doubled quantum order associated to G.]

In this section we will give the Hamiltonian formulation of discrete gauge theory. Seeing as we have moved passed ordered media, we will no longer be working with order spaces and base points. Instead, we will choose an abstract finite group G which replaces $\pi_1(M, m)$. The general picture for creating our Hamiltonian is simple, and follows a very general pattern in quantum theory: instead of enforcing properties rigidly as conditions, we will enforce them enforce properties energetically as terms in a Hamiltonian. The formulation we give below is known as the *Kitaev quantum double model of discrete gauge theory*. It was introduced in Kitaev's seminimal paper on topological quantum information [ref]. It has been studied extensively in the literature by many authors [add more refs].

Choose a directed lattice on the torus. Let

$$\mathcal{N} = \bigotimes_{\text{edges}} \mathbb{C}[G]$$

be the HIlbert space of our quantum system. The space $\mathcal{N}$ has a canonical basis given by $\prod_{\text{edges}} G$, which we identify with G-colorings of the lattice. Given a G-coloring γ, we will denote the corresponding state in $\mathcal{N}$ by $|\gamma\rangle$. For every plaquette p in the lattice, we define an operator on $\mathcal{N}$ by

$$B_p |\gamma\rangle = \begin{cases} |\gamma\rangle & \gamma \text{ flat at } p \\ 0 & \text{otherwise.} \end{cases}$$

We observe immediately that

$$\sum_{\text{plaquettes } p} (1 - B_p) |\gamma\rangle = 0 \iff |\gamma\rangle \text{ is flat.}$$

It is in this way that we can enforce properties energetically by adding them as terms to a Hamiltonian. If we chose the Hamiltonian to be $\sum_{\text{plaquettes } p}(1 - B_p)$, then the lowest energy eigenspace would exactly correspond to the space spanned by flat G-colorings. For every vertex v and group element $g \in G$, we define an operator on $\mathcal{N}$ by

$$A_{v,g} |\gamma\rangle = |\gamma \text{ acted on by the } g \text{ gauge action at } v\rangle .$$

For any $|\psi\rangle \in \mathcal{N}$, we call $|\psi\rangle$ *gauge invariant at* v if $A_{v,g} |\psi\rangle = |\psi\rangle$ for all $g \in G$. We call $|\psi\rangle$ gauge invariant if it is gauge invariant at v for all vertices v. We define

$$A_v = \frac{1}{|G|} \sum_{g \in G} A_{v,g}.$$

We define the Hamiltonian of our system to be

$$H = \sum_{\text{vertices } v} (I - A_v) + \sum_{\text{plaquettes } p} (I - B_p)$$

where I is the identity operator. We summarize the basic properties of this Hamiltonian below:

Proposition 3.1. *The following properties of the Kitaev quantum double Hamiltonian hold:*

(a) The operators A_v, B_p, and H are Hermitian for all vertices v and plaquettes p;

(b) The formula $A_{v,g}^\dagger = A_{v,-g}$ holds for all vertices v and $g \in G$;

(c) All of the operators in the set $\{A_v, B_p\}_{v \in vertices, p \in plaquettes}$ commute with every other operator in the set;

(d) The eigenstates of H are simultaneous eigenstates of the operators A_v, B_p;

(e) The eigenvalues of the A_v, B_p are all 0 or 1;

(f) The lowest eigenvalue of H is 0, and the 0-eigenspace of H is

$$\mathcal{C} = span\{\, |C\rangle |\, C \in \textit{(flat } G\textit{-colorings)/(gauge transformations)}\}\,.$$

where for we define the ket

$$|C\rangle = \sum_{\gamma \in C} \frac{1}{\sqrt{|C|}} |\gamma\rangle$$

for any equivalence class C of G-colorings of the lattice up to gauge transformations.

Proof. .[WORK: do proof] □

In particular, the above proposition tells us exactly that we have acheived our goal of realizing a Hamiltonian whose ground states capture the topological information in a lattice-version of ordered media. The term "double" in the Kitaev quantum double model refers to the fact that there are two families of terms in H - one family of type A_v and one family of type B_p. We can readily compute the dimension of the ground space as follows:

Proposition 3.2. *Choose a vertex v in the lattice. Every G-coloring of the lattice induces an assignment of lattice loops on the torus based at v to elements of G, based on taking the oriented winding number along that loop relative to the coloring. This restricts to a map*

$$(\textit{flat } G\textit{-colorings}) \to \mathrm{Hom}(\pi_1(T^2, v), G)$$

where $\mathrm{Hom}(\cdot, \cdot)$ *denotes the space of group homomorphisms between two groups. Any two flat G-colorings which differ by gauge transformations will induce the same map in* $\mathrm{Hom}(\pi_1(T^2, v), G)$*, up to global conjugation by an element of G. This induces a bijection*

$$(\textit{flat } G\textit{-colorings})/(\textit{gauge transformations}) \to \mathrm{Hom}(\pi_1(T^2, v), G)/\left(\begin{smallmatrix}\textit{simultaneous}\\ \textit{conjugation}\end{smallmatrix}\right).$$

The set of vectors $|C\rangle_{C \in (\textit{flat } G\textit{-colorings})/(\textit{gauge transformations})}$ *is linearly independent. Hence, there is a canonical isomorphism*

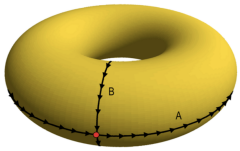
$$\mathcal{C} \to \mathbb{C}[\mathrm{Hom}(\pi_1(T^2, v), G)/\left(\begin{smallmatrix}\textit{simultaneous}\\ \textit{conjugation}\end{smallmatrix}\right)]$$

given by taking winding numbers.

Proof. .[WORK: give proof. I'm scared this could be too hard. It's already] □

The final step in using the above formula is to compute the fundamental group of the torus:

Proposition 3.3. $\pi_1(T^2, v) \cong \mathbb{Z}^2$ *for any vertex* v*. The two loops shown below are generators for* $\pi_1(T^2, v)$*:*



Proof. .[WORK: proof] □

One last observation to make about this ground space is that its ground states really are globally different:

Proposition 3.4. *Let* L *be length of the shortest non-contractible loop on the lattice. Let* γ_0, γ_1 *be non-gauge equivalent flat* G*-colorings of the lattice. There are at least* L *edges at which* γ_0 *and* γ_1 *assign different values.*

Proof. .[WORK: do proof] □

In particular, if we choose the square lattice on the torus, then the length L of the shortest non-contractible loop is obvioulsy a good measure of linear system size. Proposition [ref] tells us that the number of local changes requires to go from one ground state to another is on the order of L. This is exactly the sort of condition we needed in Section [ref] to conclude topological protection in the ground states. Of course, the smallest non-zero eigenvalue of H is at least 1, which is bounded away from zero and hence there is a system-size independent gap between the ground states and the other states. Hence, we see that H is a good topologically ordered Hamiltonian.

The excited states of H will be described localized excitations with quasiparticle behavior. Given a state $|\psi\rangle \in \mathcal{N}$, we will say that a state has an *excitation at vertex* v if $A_v |\psi\rangle = 0$ and we will say that is *unnoccupied at* p if $A_v |\psi\rangle = 1$. We say that $|\psi\rangle$ has an *excitation at plaquette* p if $B_p |\psi\rangle = 0$ and that it is *unnocupied at* p if $B_p |\psi\rangle = 1$. By Proposition [ref], every energy eigensate is either occupied or unoccupied at every vertex/plaquette. The regions in which $|\psi\rangle$ is unnoccupied are all essentially identical, leading to a homogenous

bulk. The sites at which $|\psi\rangle$ is occupied are different, and behave as quasiparticles. We will define operators which move these excitations around.

[WORK: Add something about local indistinguishability of ground states - reinforce this "homogenous bulk" idea.

More than this, it is important to note that earlier we are giving a rigorous definition of topological order. It is not immediately obvious that the KQDM satisfies this definition. This is the main content of the paper [CDH$^+$20]. Should I include a proof? At the very least there should be some mention of how this fits into the definition. In fact, this should be a big point. The KQDM is being introduced with the main goal of giving an example of TO. Needs to talk about how it is topological.]

[WORK: Maybe also reinforce that this could be done on *any manifold*, and the gound states would be the same?]

3.3 The toric code

[WORK: Maybe this section can be re-done. We know that the total space $\mathcal{N}$ can be decomposed as a direct sum

$$\mathcal{N} = \bigoplus_{\lambda} \mathcal{N}_\lambda$$

as a direct sum over syndromes, by general principles of diagonalizable matrices. To prove that all of the $\mathcal{N}_\lambda$ have an even # of excited terms in H of both A_v and B_p type is easy. Proving that they all have the same dimension involves the simple observation that applying σ_X and σ_Z between two excited terms will make them both ground states. Simple counting recovers the fact that the ground state is 4-dimensional.

The beauty of this approach is that it is immediately grounded. We have a Hamiltonian, we want to solve it - i.e. we want to compute the dimensions of the $\mathcal{N}_\lambda$, and explicitely have a way of creating those basis states. The proof in a real sense is using the quasiparticle nature of the A_v and B_p excitations. Namely they are being moved along paths to annhilate with one another.

Every operator can be decomposed as a sum of Pauli operators. Hence, unerstanding how Paulis act on $\mathcal{N}$ lets understand how every operator acts on $\mathcal{N}$. Paulis act on $\mathcal{N}$ by creating/moving/fusing vertex/plaquette excitations. Hence, understanding vertex/plaquette excitations tells you everything you need to know about the toric code. Saying it this way makes everything feel very grounded, and it doesn't bring in anyons unnececarily early into the picture. We can talk about anyons after. Highlight the fact that they behave like quasiparticles and that they will become objects of independent interest, but that isn't the point yet.

]

3.3.1 Simplified Hamiltonian

In this section we move on to analyzing the Kitaev quantum double model for $G = \mathbb{Z}_2$, which is known as the *toric code*. The name toric code comes from the fact that the toric code was first introduced as an error correcting code, and was only later recast as a topologically ordered system [refs]. The toric code is still the basis for many of the most popular error correcting codes [refs]. In a real sense the toric code is the simplest nontrivial topological order. It is a fantastic example which demonstrates almost all of the

phenomina of topological order with relatively little work involved. The toric code, and more generally $\mathbb{Z}_2$ discrete gauge theories, can be found in all sorts of systems such as [WORK: give examples].

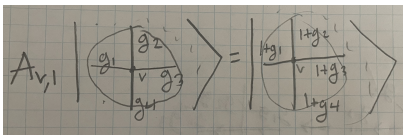
We describe the model now. Because $G = \mathbb{Z}_2$ is abelian, we will switch to additive notation for our group operation. We choose a *non-oriented* lattice structure on the torus. This lattice does not need to be oriented because changing the direction of edges in the lattice corresponds to taking inverses, and $g = g^{-1}$ for every element $g \in \mathbb{Z}_2$. We define

$$\mathcal{N} = \bigotimes_{\text{edges}} \mathbb{C}[\mathbb{Z}_2] = \bigotimes_{\text{edges}} \mathbb{C}^2.$$

Here, we identify $\mathbb{C}[\mathbb{Z}_2]$ with $\mathbb{C}^2$ for convenience, endowing $\mathbb{C}^2$ with a canonical basis $\{|0\rangle, |1\rangle\}$. We call $\mathbb{C}^2$ a *qubit*, in analogy to "bits" for classical computing. It is a standard two-level quantum system. Most quantum computers are based on qubits, which makes the toric code especially accessable to practical implementation as an error correcting code. The definition of the Hilbert space $\mathcal{N}$ can be summarized as putting a qubit on every edge of the lattice. The Hamiltonian is

$$H = \sum_{\text{vertices } v} (1 - A_v) + \sum_{\text{plaquettes } p} (1 - B_p).$$

We unpack the general definitions of A_v and B_p for the toric code. The operator $A_{v,0}$ is the identity. The operator $A_{v,1}$ acts by a gauge transformation,



Defining

$$\begin{aligned} \sigma_X : \mathbb{C}^2 &\to \mathbb{C}^2 \\ |0\rangle &\mapsto |1\rangle \\ |1\rangle &\mapsto |0\rangle \end{aligned}$$

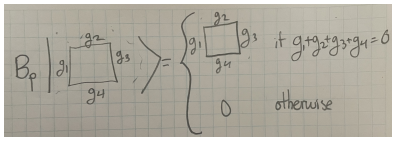
we thus find that

$$A_{v,1} = \bigotimes_{\substack{\text{edges} \\ \text{touching } v}} \sigma_X, \qquad\qquad A_v = \frac{1}{2}\left(I + A_{v,1}\right).$$

Moving on to B_p, we recall that

In the present case, B_p has a more workable expressing that is symmetric to our description of B_p. Define

$$\begin{aligned} \sigma_Z : \mathbb{C}^2 &\to \mathbb{C}^2. \\ |0\rangle &\mapsto |0\rangle \\ |1\rangle &\mapsto -|1\rangle \end{aligned}$$



Philosophically, it is useful to interpret σ_Z as acting as $|g\rangle \mapsto \chi(g)\,|g\rangle$ where $\chi : \mathbb{Z}_2 \to \mathbb{C}^\times$ is the unique nontrivial character of $\mathbb{Z}_2$, $\chi(0) = 1$, $\chi(1) = -1$. Since χ is a group isomorphism, for any $g_1, g_2, g_3, g_3 \in G$ we have an equivalence

$$g_1 + g_2 + g_3 + g_3 = 0 \iff \chi(g_1)\chi(g_2)\chi(g_3)\chi(g_4) = 1.$$

Defining an auxillary $B_{p,1}$, we thus find the following expression for B_p:

$$B_{p,1} = \bigotimes_{\substack{\text{edges} \\ \text{bounding } p}} \sigma_Z, \qquad\qquad B_p = \frac{1}{2}\left(I + B_{p,1}\right).$$

For simplicity, we will often rewrite the Hamiltonian as

$$H = \frac{1}{2} \sum_{\text{vertices } v} (1 - A_{v,1}) + \frac{1}{2} \sum_{\text{plquettes } p} (1 - B_{p,1}).$$

The matrices σ_X and σ_Z we defined are known as *Pauli matrices*. They are extremely common across formulae in quantum mechanics - this is another reason that the toric code is so ammenable to error correction applications. The basic properties of these matrices are summarized below:

Proposition 3.5.

(a) The operators σ_X and σ_Z are simultaneously unitary and Hermitian;

(b) $\sigma_X^2 = \sigma_Z^2 = I$;

(c) $\sigma_X \sigma_Z = -\sigma_Z \sigma_X$;

Proof. .[WORK: do proof] □

An important thing to note is that $A_{v,1}$ and $B_{p,1}$ commute, despite the fact that σ_X and σ_Z anticommute. The fact that they commute follows from Proposition [ref], though it fruitful to reavulate that proposition in this present context. The important fact is that given any vertex v on the exterior of any face touching p, there are an *even number* of edges which both touch v and bound p. Hence, the number of tensor factors in which $A_{v,1}$ and $B_{p,1}$ anticommute is even, and hence overall they commute.

The last step in reinterpreting our general theory of Kitaev quantum double models to the toric code is computing the ground space. We observe that since $\mathbb{Z}_2$ is abelian acting by conjugation does nothing, and hence

$$\mathrm{Hom}(\pi_1(T^2, v), \mathbb{Z}_2) / \left(\tbinom{\text{simultaneous}}{\text{conjugation}}\right) = \mathrm{Hom}(\pi_1(T^2, v), \mathbb{Z}_2).$$

Seeing as we are no longer modding out by conjucation, the group operation on $\mathbb{Z}_2$ extends to a group operation on $\mathrm{Hom}(\pi_1(T^2, v), \mathbb{Z}_2)$. Hence this space forms an abelian group, which we denote

$$H^1(T^2, \mathbb{Z}_2) = \mathrm{Hom}(\pi_1(T^2, v), \mathbb{Z}_2) = (\text{flat } \mathbb{Z}_2\text{-colorings})/(\text{gauge transformations}).$$

[WORK: maybe set notation and write out four elements explicitely? Might be too much.]

This is the *cohomology group of T^2 with coeffecients in $\mathbb{Z}_2$*. Since $\pi_1(T^2, v) \cong \mathbb{Z}^2$, we conclude that

$$H^1(T^2, \mathbb{Z}_2) \cong \mathbb{Z}_2^2.$$

Hence, we obtain the following:

Proposition 3.6. *The 0-eigenspace of H is four dimensional. It is spanned by the vectors*

$$|C\rangle = \frac{1}{\sqrt{|C|}} \sum_{\gamma \in C} |\gamma\rangle$$

for $C \in H^1(T^2, \mathbb{Z}_2)$.

Proof. .[WORK: do proof] □

3.3.2 Exact solution of the toric code

When given a quantum system, the first thing to do with it is to *solve it*. This means diagonalizing the Hamiltonian. In this case of the toric code, the diagonalization of $\mathcal{N}$ is the direct sum decomposition

$$\mathcal{N} = \bigoplus_{E \in \mathbb{R}} \mathcal{N}_E$$

where $\mathcal{N}_E$ is the energy E eigenspace,

$$\mathcal{N}_E = \{|\psi\rangle \,|,\, H\,|\psi\rangle = E\,|\psi\rangle\}.$$

Solving the toric code amounts to explicitely describing $\mathcal{N}_E$ for each E. In particular, this means computing the dimension of each space. The Hamiltonian for the toric code is

$$H = \sum_v (1 - A_v) + \sum_p (1 - B_p).$$

Since the A_v and B_p all commute with each other, they are *simultaneously diagonalizable*. This is a huge help in our analysis. We introduce some notation to take advantage of this insight. We define a *syndrome* on the toric code to be a map

$$\lambda : (\text{faces}) \sqcup (\text{vertices}) \to \{\pm 1\}.$$

We define the syndrome λ subspace of $\mathcal{N}$ to be

$$\mathcal{N}_\lambda = \{|\psi\rangle \in \mathcal{N} |\ A_{v,1}\,|\psi\rangle = \lambda(v)\,|\psi\rangle\,,\ B_{p,1}\,|\psi\rangle = \lambda(p)\,|\psi\rangle\ \forall v, p\}$$

We define the energy E_λ of a syndrome λ by the formula

$$E_\lambda = \sum_v \frac{1}{2}(1 - \lambda(v)) + \sum_p \frac{1}{2}(1 - \lambda(p)).$$

The fact that the operators A_v, B_p, and H are simultaneously diagonalizable is codified in the following observations:

Proposition 3.7. *We have that*

$$\mathcal{N} = \bigoplus_{syndromes\ \lambda} \mathcal{N}_\lambda, \qquad \mathcal{N}_E = \bigoplus_{\substack{syndromes\ \lambda \\ E_\lambda = E}} \mathcal{N}_\lambda.$$

Proof. This follows immediately from the above discussion. □

We can now solve the toric code:

Proposition 3.8. *We have that*

$$\dim(\mathcal{N}_\lambda) = \begin{cases} 4 & \text{if } \prod_v \lambda(v) = \prod_p \lambda(p) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. .[WORK: do proof] □

Corollary 3.1. *We have that*

$$\dim(N_E) = [WORK : write\ formula]$$

Proof. . [WORK: do proof] □

[WORK: this section will have some commentary about how Pauli operators are being used to fuse X-type and Z-type excitations. The way this commentary sounds should depend on the way the proof looks. I might want to include this lemma before the proof:

Given an edge e in the lattice and an operator $U : \mathbb{C}^2 \to \mathbb{C}^2$, denote by $(U)_e : \mathcal{N} \to \mathcal{N}$ the operator which applies U on the tensor factor of $\mathbb{C}^2$ at edge e. We compute the following:

Lemma 3.1. *For any vertex v, edge e, plaquette p, we have*

$$A_v(\sigma_X)_e = (\sigma_X)eA_v, \qquad B_p(\sigma_Z)_e = (\sigma_Z)eB_p,$$

$$A_v(\sigma_Z)_e = \begin{cases} -(\sigma_Z)_e A_v & \text{if } e \text{ touches } v \\ (\sigma_Z)_e A_V & \text{otherwise} \end{cases}$$

and

$$B_p(\sigma_X)_e = \begin{cases} -(\sigma_X)_e B_p & \text{if } e \text{ bounds } p \\ (\sigma_X)_e B_p & \text{otherwise} \end{cases}$$

]

3.3.3 Toric code as a topologically ordered system

.[WORK: prove that toric code satisfies axioms of TO.]

[WORK: This section will really dig into how the Pauli algebra acts on states]

[WORK: this section can also show that *global* errors (e.g. σ_X all the way around a torus) acts non-trivially. Maybe give a proof? Make a little quantum computer? If I do, I should reformulate it in in the "adiabatically changing Hamiltonian" way to tie it into the way I talked about it in the introduction.]

3.4 Anyons

3.4.1 Topological quantum information in excited states

Let us recap our current picture of topological quantum information. We introduced topological order, and argued as a general principle that its ground states are invariant under local deformations. That is, if we start with a ground state in a topologically ordered system, apply some local operator, and then project back onto ground states, then we will get back to the state we started with up to some phase. This lets us store information in ground states. This information can be used as a place to store stable information, and can be acted on by global operators to perform computations such as in proposition [ref].

We now take this perspective to its logical extreme. The dimension of the ground state space depends only on the topological order of the system and the global topology of the physical space. For instance, toric code topological order on a torus will always have a four dimensional ground space, independent of system size or choice of microscopic lattice.

To make a computer, however, we need to be able to store arbitrarily large amounts of information. This means that either we will need to work with increasingly complex topological orders or increasingly complex surfaces. There are only a handful of topological orders known to be physically realizable, so working with increasinlgy complex topological orders is out of the question. Hence, once needs to work with increasingly complex surfaces. By working on high-genus surfaces, the ground state space can be made as large as possible. This gives the following picture for a topological quantum computer:

[WORK: add picture, a-la Freedman et al.]

This approach is potentially possible, and we will explore it more in section [ref]. However, no matter the implimentation it adds a great deal of complexity. Adding genus onto a computer chip is hard work. It would be much better to work with a state with the least complex topology possible, preferably a plane, sphere, or torus.

It is for this reason that we turn to a key idea in the theory of topological order: *being careful, it is possible to store topologically protected information in the excited states of a topologically ordered system.*

[WORK: picture of spectrum diagram, with excited states boxed. "Use these to store information!"]

Using the excited states of a topologically ordered system to store information comes with several obstacles:

1. It requires careful study. This isn't a fundamental problem, but it is relevant to us since we are about to embark on that study;

2. It requires a more powerful control over the topologically ordered system than working only with ground states. This can make the approach impossible in some physical systems;

3. It introduces non-topological local degrees of freedom. This non-topological information needs to be worked around so that proper fault-tolerant computations can be performed.

We now recall our procedure for storing information in ground states. The key point is that we have a projector $\mathcal{P} : \mathcal{N} \to \mathcal{N}_{g.s.}$. This projector satisfies the relation that $\mathcal{P}\mathcal{O}\mathcal{P} = \lambda \cdot \mathcal{P}$ for any local operator $\mathcal{O}$, for some $\lambda \in \mathbb{C}$. Our physical picture for topological quantum computing is that we are continually measuring with respect to $\mathcal{P}$, and hence constantly projecting into the ground space. The formula $\mathcal{P}\mathcal{O}\mathcal{P} = \lambda \cdot \mathcal{P}$ says that even if noise is applied between rounds of projection it is okay because our state will only change by a phase and hence will still store the same information.

As we leave the ground states, this protocol breaks down. We cannot continually project into ground states because that would destroy any information we are storing in excited states! If we don't have any sort of projector, however, errors will accumulate and we will lose all of the fault-tolerance of topological quantum computing. The answer is to find a new subspace $\mathcal{N}' \subset \mathcal{N}$ to store our information in, so that the orthogonal projector $\mathcal{P}_{N'} : \mathcal{N} \to \mathcal{N}'$ satisfies a formula similar to $\mathcal{P}_{N'}\mathcal{O}\mathcal{P}_{N'} = \lambda \cdot \mathcal{P}_{N'}$.

A first guess might to constantly measure with respect to the Hamiltonian, as before, and then project into a different energy eigenspace. We have a decomposition of $\mathcal{N}$ by diagonalizing the Hamiltonian, $\mathcal{N} = \bigoplus_{E \in \mathbb{R}} \mathcal{N}_E$. We can try storing our information in $\mathcal{N}_E$, for some fixed $E > 0$ independent of system size.

We demonstrate how this fails using the toric code, working with $E = 4$. A generic state $|\psi\rangle$ in $\mathcal{N}_{E=4}$ might look like this one:

[WORK: add picture, two sites with X-excitations, two sites with Z-excitations.]

The fact that there are exactly four terms in the Hamilotian that are violated corresponds exactly to the fact that the energy of the state is $E = 4$. We now consider applying σ_X to $|\psi\rangle$ at an edge adjacent to one of the X-excitations:

[WORK: add picture. Applying $(\sigma_X)_e$ moves the X-excitation.]

This new state with the X-excitation moved still has the same number of anyons, and hence $(\sigma_X)_e |\psi\rangle$ still leaves in $\mathcal{N}_E$. Hence, $\mathcal{P}_E(\sigma_X)_e\mathcal{P}_E |\psi\rangle = (\sigma_X)_e |\psi\rangle$ does *not* differ by a scalar. Even worse, despite the consant application of the projector $\mathcal{P}_E$, local errors can accumate to become global errors. If we keep applying σ_X on edges around some loop then this will never be detected by $\mathcal{P}_E$, and this will be the same as acting by some non-trivial global operator.

[WORK: add picture of local noise accumulating to be a global error.]

In summary, storing information in an excited energy level of a topologically ordered system does not result in information which is resistant to local noise. The problem is that the terms which violate the ground-state condition in the Hamiltonian can *drift*, moving around the physical space in an uncrolled fashion without changing the energy of the system.

The solution to this problem is to *constrain the drift*. This works as follows. We work in the Kitaev quantum double model based on some finite group G. Define a *region* in a space to be a compact connected subset of it. Choose n disjoint regions $R_1 ... R_n$ on the torus T^2. We define the space

$$\mathcal{N}_{R_1,R_2...R_N} = \left\{ |\psi\rangle \in \mathcal{N} |\ A_v |\psi\rangle = B_p |\psi\rangle = |\psi\rangle\,,\ \forall v, p \notin \bigcup_{i=1}^{n} R_i \right\}.$$

This space consists of states which satisfy the condition to be in the ground state of $H = \sum_v (1 - A_v) + \sum_p (1 - B_p)$ outside of the regions $R_1 ... R_n$, but is allowed to do whatever

it wants within the regions. This is shown visually below:

[WORK: add picture]

The space $\mathcal{N}_{R_1,R_2...R_N}$ contains all ground states, but also a large amount of excited states. The regions $R_1...R_n$ constrain the drift of excitations. To illustrate the power of this space, consider the example of the toric code. Suppose we have our same state $|\psi\rangle$ as below with energy $E = 4$, but we consider it instead as a subspace of $\mathcal{N}_{R_1,R_2,R_3,R_4}$ for some regions $R_1, ...R_4$ containing the four excited operators. Applying σ_X to an edge can still change the state, and so we don't have the formula $\mathcal{P}_{N'}\mathcal{O}\mathcal{P}_{N'} = \lambda \cdot \mathcal{P}_{N'}$, but local errors *cannot* accumlate to become global errors! If the excited term starts to drift, it will eventually leave the region in started in and hence will no longer be in the subspace $\mathcal{N}_{R_1,R_2,R_3,R_4}$, so projecting back into it will fix the error. This is shown pictorally below:

[WORK: add picture]

In this way, local operators can change the information stored in the system but it can only change it to a controlled degree. There is still global information within $\mathcal{N}_{R_1,R_2...R_n}$ which is roughly invariant under local operators. Getting this global information out in such a way that the answer does not depend on whatever local operators are applied to the system is non-insurmountable challenge. This is the heart of point (3) in the obstacts of working with excited states: it introduces non-topological degrees of freedom which need to be worked around.

[WORK: notation is a bit junky because I'm working with $R_1, R_2...R_n$ all the time. It would be nicer in some ways if I worked with just one region R, and I dropped the condition that it be connected. This makes the definition of "anyon" a bit more janky though. Not sure what to do.]

[WORK: So far I haven't defined what an anyon is for topological orders other than the KQDM. One easy way to do this is by putting some set L of sites, choosing $d > 0$, defining $\mathcal{N} = \bigotimes_{\ell \in L} \mathbb{C}^d$. Then we have $H = \sum_i H_i$, $[H_i, H_j] = 0$, $H_i^2 = 1$, H_i localized to some region U_i. This is a commuting local projector Hamiltonian. It is easy to define anyons in a model like this one. I'm not sure if this would be informative or distracting.

Actually, on second thought, something like this might actually be neccecary for the definition of TO. Hence, we might have it ready-to-use for this section.]

3.4.2 Definition and principles of anyons

With the discussion in the previous section, we can start to see how our picture for topological quantum computing is similar to the picture for topological classcial computing described in chapter [ref]. The regions $R_1, R_2...R_n$ are localized regions of difference within a homogenous bulk. The bulk is homogenous because the wavefunction is groundstate of the Hamiltonian in those regions, and TQO-2 implies that all of these ground states are locally indistinugishable. The regions $R_1, R_2...R_n$ are different because they are allowed to be excited. Hence, the regions $R_1...R_n$ behave as *quasiparticles*. We will show that these quasiparticles can be pair-created, braided, and fused, just like in topological classical computing. The major difference between our scheme for topological quantum computing and topological classical computing is that instead of our quasiparticles being defects in ordered media, they are localized excitations in a topological order. This leads us to the following definition:

Definition. An *anyon* is a localized excitation in a topologically ordered system.

In our present context, this localization is best viewed not as an unavoidable physical reality but as a design decision for building a topological quantum computer. States $|\psi\rangle$ in

topologically ordered systems have terms in the Hamiltonian that the violate and ones they don't. By circling regions around the terms they don't and constraining the excitation to those regions by repeatedly applying the projector $\mathcal{P}_{\mathcal{N}_{R_1,R_2\ldots R_n}}$, we localize the excitation.

To store cohrent topological quantum information in anyons, there are a few key principles one must follow. The first principle is straightforward:

Anyons should be kept far apart

This is motivated as follows. Suppose that the anyons were kept in close proximity to one another. Then local noise could affect two anyons at once:

[WORK: add picture of R_1, R_2 with some local noise operator $\mathcal{O}$ touching both]

Our picture of our system is that there is contantly local noise being applied, and that we are contantly projecting into the space $\mathcal{N}_{R_1,R_2\ldots R_n}$. The fault-tolerant information we want to get at is exactly the information which is invariant under this noisy picture. That is, information which does not change when local operators from $\mathcal{N}_{R_1,R_2\ldots R_n}$ to itself is applied. We call this topological information.

Some of this topological information can be measured using local observables. Because physics is local, any realistic observable should be local. Suppose we have a local Hermitian operator $\pi : \mathcal{N}_{R_1,R_2\ldots R_n} \to \mathcal{N}_{R_1,R_2\ldots R_n}$ which commutes with every noise operator $\mathcal{N}_{R_1,R_2\ldots R_n} \to \mathcal{N}_{R_1,R_2\ldots R_n}$. Then π can be physically measured *and* the result of that measurement is invariant under noise. Hence, it gives topological information. We all such observables π which are locally supported and commute with every noise operator *local topological observables*. We image that the outcomes of local topological measurements are readily available to experimenters - they can be measured with physical devices in a way that does not depend on noise.

This allows us to break-down the information in our system:

[WORK:

Four-square diagram for information in $\mathcal{N}_{R_1,R_2\ldots R_n}$.

Collumns: measurable by local topological observables. (yes/no)

Rows: invariant under local noise. (yes/no)

C-yes R-no: Impossible.

C-no R-no: Non-topological information.

C-yes R-yes: Classical information / local topological information

C-no R-no: Topological quantum information / global information

Add little arrows going to each box explaining it.]

[WORK:

Measuring under all topological observables should be called a "topological charge measurement". This leads to harmony with the language used in the MTC section.

] We now break down this general picture into exact mathematical statements.

[WORK: at this point I need to read Kitaev's arguement in more detail.

The first step is to go $\mathcal{N}_{R_1,\ldots R_n} = \bigoplus_{i=1}^{N} \mathcal{N}_i$ where $\mathcal{N}_i$ indexes over classical information. This is easy. The non-trivial step is to observe that there exists some finite set $\mathcal{L}$ such that the terms $\mathcal{N}_i$ can be rearranged as

$\mathcal{N}_{R_1,\ldots R_n} = \bigoplus_{(A_i)_{i=1}^n \in \mathcal{L}^n} \mathcal{N}_{A_1,A_2\ldots A_n}$.

Each A_i is the result of a measurement localized around R_i. The set $\mathcal{L}$ is the set of anyon types, and given some state $|\psi\rangle \in \mathcal{N}_{A_1,A_2\ldots A_n}$, we call A_i the type of the anyon at R_i. Anyon types = topological classical information.

Now, the next step is to observe that there is a non-canonical tensor decomposition

$$\mathcal{N}_{A_1,A_2\ldots A_n} = \mathcal{N}^{loc}_{A_1,A_2\ldots A_n} \otimes \mathcal{N}^{top}_{A_1,A_2\ldots A_n}$$

of $\mathcal{N}_{A_1,A_2\ldots A_n}$ into a local part and a topological part. It satisfies the condition that every local noise operator $\mathcal{O}$ on $\mathcal{N}_{A_1,A_2\ldots A_n}$ can be decomposed as $\mathcal{O} = \mathcal{O}' \otimes \mathrm{id}$, and hence the information in the topological part remains unchanged. Moreover, it is maximal subject to this condition. Moreover, we have a splitting

$$\mathcal{N}^{loc}_{A_1,A_2\ldots A_n} = \mathcal{N}^{loc}_{A_1} \otimes \mathcal{N}^{loc}_{A_2} \ldots \otimes \mathcal{N}^{loc}_{A_n}.$$

Information of which direct summand I'm in = topological classical information

Information left over = tensor product of local and topological. Cannot be distinguished by the non-canonical nature of this tensor decomposition. Needs subtle techniques (i.e. fusion of anyons) to be measured. It would be fantastic if all of this could be written up correctly and codified into propositions.]

[WORK: I want to get to the fact that anyons are moved by unique operators, and hence we can ignore the specific choice of operator and just move the anyons.]

3.4.3 Anyons in the toric code

[WORK: do it first with toric code. Everything is painfully simple and obvious here.

The problem is that adding more anyons does not encode more information, so its hard to get the points of TQC across.

Hopefully this is a very short subsection.]

3.4.4 Anyons in discrete gauge theory

[WORK:

Here we go from KQDM to G-crossed G-representations. By the end we should have the category $\mathfrak{D}(G)$ as a set, with morphisms motivated.

A lot of the intricate setup has been done in the previous sections, so I think this can be relatively contained. It would be nice to have proofs. Even if this section is more intricate that should be included in most lectures series, I'd say its nice to have nonetheless as a reference.]

History and further reading:

The term topological order was first used in 1972 by Kosterlitz and Thouless to describe topological classical systems of the sort discussed in Chapter [ref] [KT18] . The term has since evolved, and was re-coined in 1989 by Xiao-Gang Wen to describe the sort of topological classical systems defined in this chapter [Wen89].

The history anyons is distinct from the history of topological order. It was first noted in 1976 in a paper of Leinass and Myrheim that the classification of particles in terms of fermions and bosons broke down in two dimensions [LM77]. The subject of anyons was then taken over by Wilczek who published a series of seminal papers on the topic [Wil82a, Wil82b, ASW84]. It was in these papers that Wilczek observed that anyons were present in the quantum Hall effect, and hence connected the theory of anyons and topological order together.
[WORK: what is the history of gauge theory, and when was it introduced to the picture? A great reference is the de Wild Propitius and Bais survey. Also should mention Kitaev's paper again.]

Exercises:

3.1. For vertices v and plaquettes p, define

$$A'_{v,1} = \bigotimes_{\substack{\text{edges} \\ \text{touching } v}} \sigma_Z, \qquad A'_v = \frac{1}{2}\left(I + A'_{v,1}\right),$$

$$B'_{p,1} = \bigotimes_{\substack{\text{edges} \\ \text{bounding } p}} \sigma_X, \qquad B'_p = \frac{1}{2}\left(I + B'_{p,1}\right),$$

and

$$H' = \sum_{\text{vertices } v} (1 - A'_v) + \sum_{\text{plaquettes } p} (1 - B'_p).$$

Define $M : \mathbb{C}^2 \to \mathbb{C}^2$ by $M(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $M(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Show that

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

and 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 σ_X with σ_Z. For example, conclude that the codespace of H' is 4 dimensional.

4 Category theory

4.1 Overview

4.1.1 Introduction

There is a lot of math in the world. The development of the subject has spanned thousands of years, and has enjoyed a large uptick in the last two hundred or so. This has given ample time for the most important ideas to rise to the top. Among these important concepts there is one which is the focus of chapter: **composition**.

Let A, B, C be sets. Let $f : A \to B$ and $g : B \to C$ be functions. The *composition* of f and g is the function $g \circ f : A \to C$ defined by the formula $(g \circ f)(x) = g(f(x))$ for all $x \in A$. More generally, composition is the act of doing one process followed by a second process. Composition is distinguished in its importance for two reasons:

1. Composition is ubiquitous;
2. A very large number of more complicated structures can be described in terms of composition.

These two primary reasons of importance lead to several emergent applications of composition:

1. It's a good organization principle - thinking in terms of composition gives a unifed approach to disperate subjects, which highlights the universality latent within mathematics;
2. It's a good compression technique - in a composition-forward approach there's no need to remember details about objects or functions between them, only the way that those functions compose is used;
3. Sometimes composition rules are the only data we have, making a composition-forward technique the only approach possible.

This third point is the situation we find ourselves in with tthe algebraic theory of topological quantum information. We're trying to give a usable mathematical description of topologically ordered systems. The way that we find ourselves doing this is by focusing on anyons (the local quasiparticle excitations in topological order). Doing this we run into three important ponts:

1. Describing anyons exactly is hard. They are emergent phenomina, found within highly-entangled energy eigenstates of arbitrarily complicated gapped Hamiltonians.
2. Describing the possible ways that anyons can transform is hard. This involved specifying intricate unitary operators on high-dimensional Hilbert spaces.
3. Describing the ways that these transformations compose with one another is always relatively simple. It can be done using explicit-to-describe rules, which are independent of system size or choice of gapped Hamiltonian.

What to do in this situation is clear: we will take a composition-first approach to anyons.

We give some examples to demonstrate our point. Suppose we want to discuss braiding anyons in the toric code. We can abstractly talk about a syndrome of the toric code in which there is one X-type particle and one Z-type particle:

[WORK: write out state.]

On these states we can talk about braiding. We use the same sorts of spactime diagrams as before to represent these transformations:

[WORK: write out state.]

Without talking about the fact that transformations of this type are realized explicitely using Pauli operators, we can still abstractly discuss the way they compose with each other:

[WORK: write out composition line]

[WORK: add more complicated example coming from whatever case of Kitaev quantum double I describe explicitely in the TO chapter]

The mathematical objects which allows one to speak intelligently about composition-first appraoches is known as a *category*. The composition-first approach to mathematics is known as *category theory*. Of course, to describe anyons we will need more than just the structure of composition. We will also need a way to encode what happens we we put anyons together, braid them, and fuse them. There structures are all completely compatible with the compostion-first approach, and correspond to adding extra structures onto the category. The categories describing anyons will all their extra structures is known as a *modular tensor category*, and will be the subject of much of this book. This chapter deals with introducing category theory, as well as some of the structures which will be important for discussing anyons and modular tensor categories.

4.1.2 Definition and important obervations

As discussed before, a category is the structure which allows for a composition-first approach to map. Before going forward lets give a formal definition of category:

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

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

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

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

Such that:

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

$$f \circ \mathrm{id}_A = f, \qquad \mathrm{id}_A \circ g = g.$$

□

The rest of this section will contain a loosely-related series of five observations about this definition:

Observation 1: *The structure of this definition is very typical of algebra.*

Roughly, algebra is defined to be the study of algebraic structures. An algebraic structure, roughly, is defined to be some collection structures on some space, with rules outlining how the structures interact with each other. The general way of defining algebraic structures is to first list the structures, and then list the axioms of how these structures inteact with each other. We will see many definitions of this sort throughout the rest of the book, so it is good to get used to it now.

Observation 2: *In this text we have already seen many examples of categories.*

We list some of them below:

- **Set**, the category of sets. The objects are sets and the morphisms are functions.
- **Top**, the category of topological spaces. The objects are topological spaces and the morphisms are continuous functions.
- $\mathbf{Vec}_k$, the category of finite dimensional vector spaces over a field k. The objects are finite dimensional vector spaces over k and the morphisms are linear operators.
- **Grp**, the category of finite groups. The objects are finite groups and the morphisms are group homomorphisms.
- **Hilb**, the category of quantum systems. The objects are finite dimensional Hilbert spaces and the morphisms are unitary operators.
- **Prob**, the category of probability spaces. The objects are finite dimensional real vector spaces with distinguished bases and the morphisms are operators which send normalized vectors to normalized vectors.
- $\mathbf{Ord}_M$, the category associated with ordered media with order space M. The objects are continuous maps $\phi : \mathbb{R}^2 \to M$ and the morphisms are continuous deformations.
- $\mathfrak{D}(G)$, the category associated with discrete gauge theory based on the finite group G. The objects are G-graded G-representations and the morphisms are linear maps which respect both the G-grading and the G-action.

Observation 3: *The objects and morphisms of a category do not have much complexity implicit to them. All of the interesting structure is encoded within the composition structure.*

This is despite the fact that when we listed our examples in Observation 2 we only described the objects and morphisms, and not the compositoin structure. The reason for this is that the composition structure between morphisms in all of our examples is clear. In all our examples the objects are sets with extra strcture, and the morphisms are maps of sets. The composition structure is inhereted from the composition structure on functions between sets.

Going further, however, we observe that objects in abstract categories are *not* required to be sets and the morphisms are *not* required to be functions of sets. Most of our examples

of categories will have objects which are sets and morphisms which are functions of sets, but there will be notable counterexamples. It is important to remember that there are some categories for which there is no interpreation of morphisms as functions between sets [Fre70].

Observation 4: *A category isn't just a space with a good notion of composition - it also has identity maps.*

These identity maps are important, and we include them in the definition purposefully. There are two primary reasons: firstly that all of the relevant examples of categories will have identity maps, and secondly that most interesting properties of categories only make sense because of the identity maps. Hence if we didn't require identity maps then we would find ourselves constantly requiring them as a condition, which is a waste of space.

It is important to take a closer look at what the identity map means, though. The identity map is trying to capture a very general phenominon about transformations: *there is always the trivial transformation which results from doing nothing.* This do-nothing map is the identity. In the category of sets, the identity maps on the set A is given by the formula $\mathrm{id}_A(x) = x$ for all $x \in A$. The fact that these maps are the identities in the category of sets is the reason that the identity axiom for categories is defined like it is. Really, there is an implicit lemma hidden in the definition of category:

Lemma 4.1. *Let A be a set. For all sets B and for all $f : A \to B$, $g : B \to A$ we have*

$$f \circ \mathrm{id}_A = f, \qquad \mathrm{id}_A \circ g = g.$$

In particular, id_A satisfies the axiom of an identity in the category of sets, and hence **Set** *forms a category.*

Proof. .[WORK: do proof] □

These sorts of implicit lemmas are everywhere in category theory. Whenever a composition-forward definition is given in category theory, there is the assumption that it agrees with the standard definition at least in the category of sets. For instance, we make the following definition:

Definition (Isomorphism)**.** Let $\mathscr{C}$ be a category, let $A, B \in C$ be objects, and let $f : A \to B$ be a morphism. We say that f is an *isomorphism* if there exists a morphism $f^{-1} : B \to A$ such that $f^{-1} \circ f = \mathrm{id}_A$ and $f \circ f^{-1} = \mathrm{id}_B$. We call f^{-1} the *inverse* of f. In this case, we say that A and B are *isomorphic objects.*

□

The implicit lemma in this definition is as follows:

Lemma 4.2. *Let A, B be sets, and let $f : A \to B$ be a function. The map f is a bijection if and only if there exists a function $f^{-1} : B \to A$ such that $f^{-1} \circ f = \mathrm{id}_A$ and $f \circ f^{-1} = \mathrm{id}_B$. In particular, a function f in the category* **Set** *is an isomorphism if and only it is a bijection.*

Proof. .[WORK: do proof] □

Observation 5: *Statements in category theory can be very broadly applied.*

This is in some sense obvious by the fact that there are so many different examples of categories, but it's good to state the observation explicitely. Here's a good example:

Proposition 4.1. *Let $\mathscr{C}$ be a category. Identities in $\mathscr{C}$ are unique. Explicitely, let $A \in \mathscr{C}$ be an object and let $\mathrm{id}_A, \tilde{\mathrm{id}}_A : A \to A$ be morphisms satisfying the identity axiom. We have that $\mathrm{id}_A = \tilde{\mathrm{id}}_A$.*

Proof. . Using the fact that $\mathrm{id}_A \circ f = f$ and $f \circ \tilde{\mathrm{id}}_A = f$ for any $f : A \to A$, we compute that

$$\mathrm{id}_A = \mathrm{id}_A \circ \tilde{\mathrm{id}}_A = \tilde{\mathrm{id}}_A$$

as desired. □

This has broad application. For instance: why are identity elements in groups unique? Le G be a group and let $1, 1' \in G$ be identity elements. We find that $1 = 1 \cdot 1' = 1'$ as desired. Going further, here is another proposition in category theory:

Proposition 4.2. *Let $\mathscr{C}$ be a category. Let A, B be objects and let $f : A \to B$ be an isomorphism. The inverse of f is unique. That is, let $f^{-1}, \tilde{f}^{-1}$ be morphisms satisfying the definition of the inverse of f. We have that $f^{-1} = \tilde{f}^{-1}$.*

Proof. Using the associativity axiom, we compute

$$f^{-1} = f^{-1} \circ \mathrm{id}_B = f^{-1} \circ (f \circ \tilde{f}^{-1}) = (f^{-1} \circ f) \circ \tilde{f}^{-1} = \mathrm{id}_A \circ \tilde{f}^{-1} = \tilde{f}^{-1}$$

as desired. □

This is very general. Why are inverses unique in groups? Why are inverses of matrices unique? Abstractly, why should the inverse of any reversible process be unique? Proposition 4.2 gives the answer.

4.2 Structures in category theory

[WORK: this section should include all of the structures which are neccecary for the rest of the book, and are too cumbersome to define on-site. It should also read as an introducting to how to think in the language of categories. Here is the running list of neccecary topics

- Products/coproducts/biproducts;
- zero objects;
- $\mathbb{C}$-linear structure;
- Functors, natural equivalence, equivalence of categories, NOT Yoneda lemma;

]

[WORK: maybe use homotopy theory as a reccuring motivating example?]

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

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

Such that:

1. The composition maps $\circ : \mathrm{Hom}(B, C) \times \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C)$ are bilinear maps of vector spaces for all $A, B, C \in \mathscr{C}$.

□

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

□

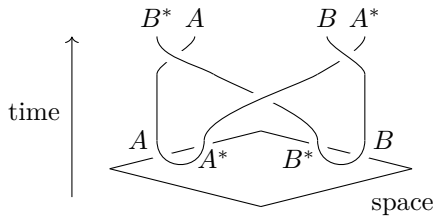
[WORK: do I need to define $\mathbb{C}$-linear natural transformation?]

4.3 Monoidal categories

4.3.1 Motivation, definition, and string diagrams

The goal of this sectio is to introduce the language neccecary for a proper detailed discussion of modular tensor categories. Despite the fact that the language of composition is very useful for MTCs, there are still many concepts in MTC theory which require more structure than just composition. In the sections that follow we will introduce these structures one-by-one, giving motivation and proving basic properties along the way.

By the end of our discussion, we will be able to discuss situations like these, where we create and braid quasiparticles:

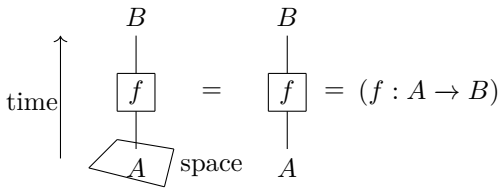


This sort of diagram will take place in some category $\mathscr{C}$. The labeles A, B, A^*, B^* represent objects in $\mathscr{C}$. The objects (A, A^*) form a particle/antiparticle pair, and the objects (B, B^*) form a particle/antiparticle pair. Naively, we could interpret this diagram as follows. To begin, there are no particles. Then, we have creation maps create_{A,A^*} and $\mathrm{create}_{B^*,B}$ which pairs of particles and their antiparticles. Then we have three different braids, braid_{A^*,B^*}, braid_{A,B^*}, and $\mathrm{braid}_{A^*,B}$. The overall process is the composition of these:

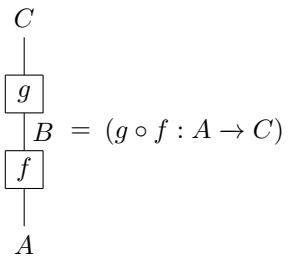
$$(\mathrm{braid}_{A^*,B}) \circ (\mathrm{braid}_{A,B^*}) \circ (\mathrm{braid}_{A^*,B^*}) \circ (\mathrm{create}_{B^*,B}) \circ (\mathrm{create}_{A,A^*}).$$

These creation maps and braiding maps are exactly the sort of maps which we will be introducing as extra structures on our category during this chapter. One lingering problem, however, is that the naive approach to formalising these diagrams in category theory results in long chains of composition. These long chains of composition hide the real structure of the problem, and make processes like the one in diagram [ref] much harder to parse. It is for this reason that we introduce a *graphical language for category theory*. This graphical language makes the diagrams like [ref] rigorous mathematical notion which describe well-defined morphisms. These diagrams are known as *string diagrams*.

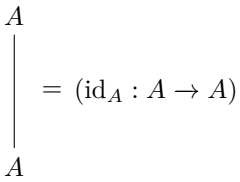
The main principle of string diagrams is that morphisms are represented as follows:



The direction of time going from bottom to up and the space being two-dimensional slices is the same in every diagram, and hence is left implicit from here on out. Composition can be expressed cleanly in this langauge as stacking, for all $f : A \to B$, $g : B \to C$:



Accordingly, the identity map has a simple implementation:



We now give our first major example of adding structure, and how that structure can be interpreted in terms of string diagrams. This structure is that of a *monoidal category*. For technical reasons we only define *strict* monoidal categories for now - we will come back to the general definition later. Monoidal categories give a way to put objects together. For instance, in diagram [ref] we had four particles all together. We need to way to discuss composite-particle systems. In quantum mechanics, forming a composite system is done by taking the tensor product. Hence, we will use the notation $\otimes$ for joining particles in our current setting. We will even use the term "tensor product" to discuss it. In general, joining two systems is one way of going from pairs of systems to individual systems:

$$\begin{aligned}(\text{systems}) \times (\text{systems}) &\to (\text{systems}).\\ (\text{system 1}, \text{system 2}) &\mapsto (\text{system 1}) \otimes (\text{system 2})\end{aligned}$$

In the world of category theory, we only require some basic properties of this joining. Namely, it should be functorial and satisfy some simple conditions:

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

1. A category $\mathscr{C}$;
2. (Tensor product) A functor $\otimes : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$;
3. (Unit) A distinguished element $\mathbf{1} \in \mathscr{C}$;

Such that:

1. (Unit axiom) Let $A, A' \in \mathscr{C}$ be objects and let $f : A \to A'$ be a morphism. We have

$$A \otimes \mathbf{1} = \mathbf{1} \otimes A = A, \qquad f \otimes \mathrm{id}_{\mathbf{1}} = \mathrm{id}_{\mathbf{1}} \otimes f = f.$$

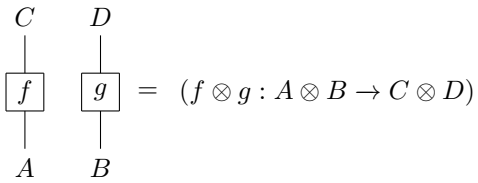
2. (Associativity) Let $A, B, C, A', B', C' \in \mathscr{C}$ be objects, and let $f : A \to A'$, $g : B \to B'$, $h : C \to C'$ be morphisms. We have

$$(A \otimes B) \otimes C = A \otimes (B \otimes C), \qquad (f \otimes g) \otimes h = f \otimes (g \otimes h).$$

□

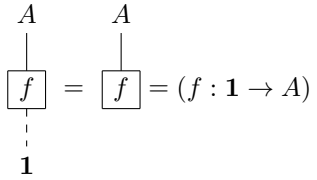
The object $\mathbf{1} \in \mathscr{C}$ is important. Just like how groups of symmetries always include the "do-nothing" symmetry, strict monoidal categories should always include the unit. In this case, $\mathbf{1} \in \mathscr{C}$ represents the empty particle - no particle at all. In every particle theory there should be the possibility of not having any particles. Joining the empty particle with any other particle should obviously do nothing, hence the axiom $1 \otimes A = A \otimes 1 = A$.

We can now work strict monoidal categories into our graphical language. The tensor product of two objects is represented by putting two lines adjacent to one another. For instance, let $\mathscr{C}$ be a strict monoidal category, let $A, B, C, D \in \mathscr{C}$ be four objects, and let $f : A \to C$, $g : B \to D$ be morphisms. We have



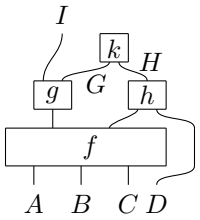
$= \quad (f \otimes g : A \otimes B \to C \otimes D)$

The monoidal unit $\mathbf{1}$ is distinguished in monoidal categories, and hence is represented with a special line. We will either use a dotted line, or no line at all:



$= \quad (f : \mathbf{1} \to A)$

We *do not* require that the lines drawn in string diagrams be straight. They can curve any amount so long as it is clear that they are directly connecting an output to an input. The lines cannot cross each other or double back. Additionally, when it is clear from context, we *do not* require ourselves to include every label. For example, the following is a valid diagram in all strict monoidal categories $\mathscr{C}$, where $A, B, C, D, E, F, G, H \in \mathscr{C}$ are objects, and $f : A \otimes B \otimes C \to E \times F$, $g : E \to I \otimes G$, $h : F \otimes D \to H$, and $k : G \otimes H \to \mathbf{1}$ are morphisms:



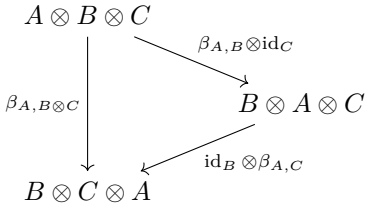
4.3.2 Braided monoidal categories

We continue our definitions of structures on monoidal categories, and their expression in the language of string diagrams. Our next definition is that of a strict *braided* monoidal category:

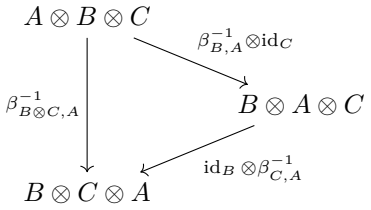
Definition (Strict braided monoidal category)**.** A strict braided monoidal category is the following data:

1. A strict monoidal category $\mathscr{C}$;
2. (Braiding) Isomorphisms $\beta_{A,B} : A \otimes B \to B \otimes A$ for all $A, B \in \mathscr{C}$ which form a natural isomorphism between the functors $\mathscr{C} \times \mathscr{C} \to \mathscr{C}$ given by $(A, B) \mapsto A \otimes B$ and $(A, B) \mapsto B \otimes A$.

Such that for all $A, B, C \in \mathscr{C}$, the diagrams



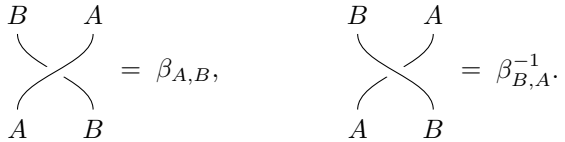
and



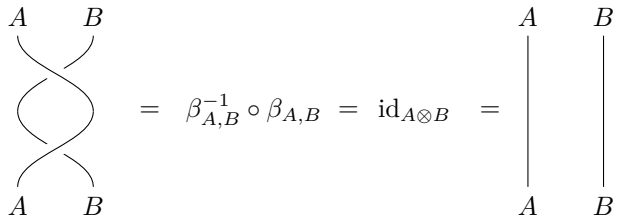
commute.

□

The idea for how to implement braided monoidal categories in the language of string diagrams is to introduce a special symbol for the braiding map $\beta_{A,B}$. Namely, we define graphically overcrossing and undercrossing as follows:

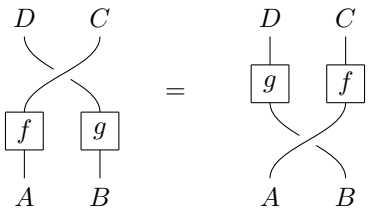


The fact that overcrossing and undercrossing are related by an inverse encodes the following key fact that



We can now describe the conditions on a strict braided monoidal category in a graphical way. The fact that β is a natural transformation can be reinterpreted as follows:

Lemma 4.3. *Let $\mathscr{C}$ be a strict braided monoidal category. For all $A, B, C, D \in \mathscr{C}$ and $f : A \to C$, $g : B \to D$, we have the following equality of string diagrams:*



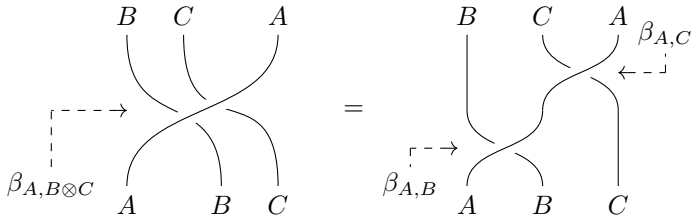
The same formula holds replacing overcrossing with undercrossing on both sides.

Proof. Consider the morphism $(f, g) : (A, B) \to (C, D)$ in $\mathscr{C} \times \mathscr{C}$. The naturality of β implies the following commutative square:

$$\begin{array}{ccc} A \otimes B & \xrightarrow{f\otimes g} & C \otimes D \\ \downarrow{\scriptstyle \beta_{A,B}} & & \downarrow{\scriptstyle \beta_{C,D}} \\ B \otimes A & \xrightarrow{g\otimes f} & D \otimes C \end{array}$$

exanding this square in diagramatic language gives the first part of the proposition. Reversing the direction of the arrows by taking inverses gives the second part. □

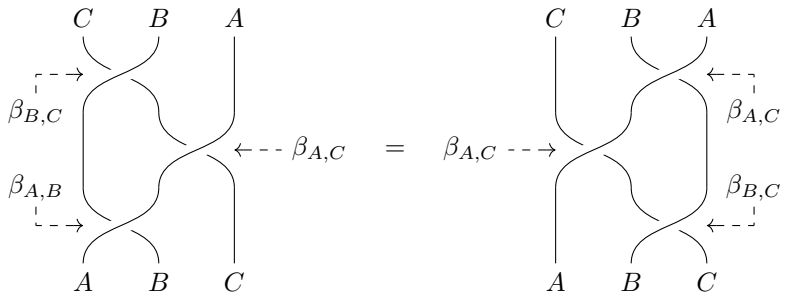
The coherence axiom can be stated diagrammatically as follows,



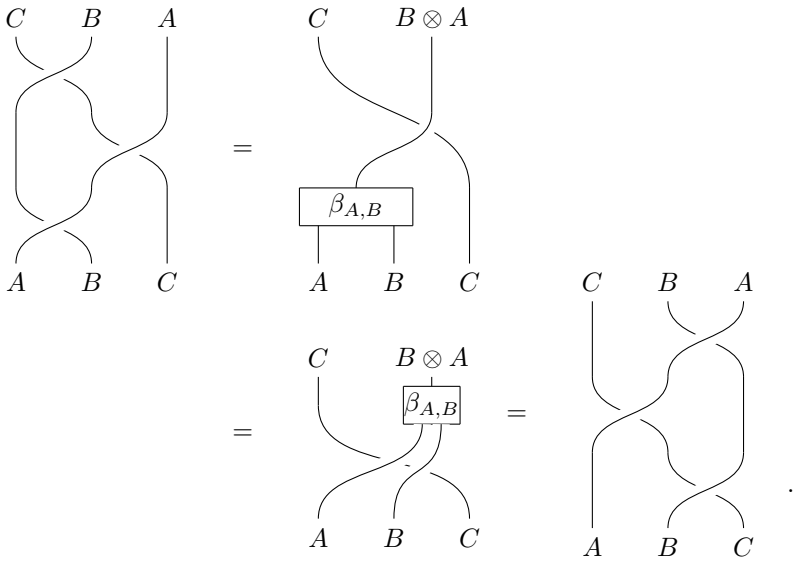
and similarly with replacing overcrossing with undercrossing. The importance of this axiom is that it means that our graphical langauge can express braid diagrams without other ambiguity. We can safely deform strings behind braids and not need to worry about whether we are applying $\beta_{A,B\otimes C}$ or $(\mathrm{id}\, B \otimes \beta_{A,C}) \circ (\beta_{A,B} \otimes \mathrm{id}_C)$.

A fundamental result about braided monoidal categories is that the coherence condition given is enough to rearrange braids at will. In particular, we have the following key proposition:

Proposition 4.3 (Yang-Baxter equation)**.** *Let $\mathscr{C}$ be a strict braided monoidal category. Let $A, B, C \in \mathscr{C}$ be objects. We have*



Proof. We offer a graphical proof, using first the coherence condition and then naturality:



□

We get the following corrolary:

Corollary 4.1. *Let $\mathscr{C}$ be a strict braided monoidal category. Let $A \in \mathscr{C}$ be an object. The map*

$$\begin{aligned} B_n &\to \mathrm{Aut}(A^{\otimes n}) \\ \sigma_i &\mapsto \mathrm{id}_{A^{\otimes i-1}} \otimes \beta_{A,A} \otimes \mathrm{id}_{A^{n-i-1}} \end{aligned}$$

is a homomorphism of groups.

Proof. We saw in Proposition [ref] that the relations on B_n are generated by the conditons $\sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_i\sigma_{i+1}\sigma_i$. These conditions are satisfied by the braiding by Proposition [ref]. Hence, the map is a homomorphism of groups. □

4.3.3 Examples, equivalences, and MacLane's coherence theorem

In this section we will give concrete examples of monoidal categories and braided monoidal categories. What we will find, however, is that these examples will all demonstrate the same subtle problem. For example, here is a category which we would want to give as an example of a monoidal category:

$$\mathscr{C} = \mathbf{Set},\ \otimes = \text{Cartesian product.}$$

The Cartesian product is certainly functorial. Namely, given morphisms $f : A \to C$ and $g : B \to D$ we get a morphism

$$\begin{aligned}(f \times g) : A \times B &\to C \times D. \\ (a, b) &\mapsto (f(a), g(b))\end{aligned}$$

However we get a key issue $(A \times B) \times C \neq A \times (B \times C)$. We have an isomorphism

$$\begin{aligned}\alpha : (A \times B) \times C &\to A \times (B \times C), \\ ((a, b), c) &\mapsto (a, (b, c))\end{aligned}$$

but this isomorphism is *not* an equality. This means that **Set** does not satisfy the definiton of a strict monoidal category! In general, all the examples we would want to give of monoidal categories fail to be strict monoidal categories. In this section we discuss a method for loosening the definition of monoidal category so that **Set** and other examples can be included in the definition.

For this reason, we give the following warning: **This section is not neccecary for a conceptual understanding of the subject matter. It is material of technical importance, and thus of interest to those who want a correct formal understanding of the mathematics at play.**

This is because, despite the fact that we will loosen the notation of strict monoidal category to a more general sort of possibly non-strict category, we will do the following:

We assume monoidal categories are strict whenever it is convenient.

The fact that this does not cause issues is a corrollary of MacLane's coherence theorem. We will discuss these issues in detail in this section.

The most naive way of loosening the definition of monoidal category is to only enforce the condition $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$ instead of equality. However, this leads to a problem. The associativity axiom on morphisms $(f \otimes g) \otimes h = f \otimes (g \otimes h)$ no longer makes sense because there is no way of comparing morphisms on $(A \otimes B) \otimes C$ and $A \otimes (B \otimes) C$. In general category theory fashion, we should choose specific isomorphisms $\alpha_{A,B,C} : (A \otimes B) \otimes C \xrightarrow{\sim} A \otimes (B \otimes C)$ and require that those isomorphisms satisfy certain coherence conditions. This leads us to our definition of a non-strict monoidal category:

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

1. A category $\mathscr{C}$.
2. (Tensor product) A functor $\otimes : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$.

3. (Unit) A distinguished element $\mathbf{1} \in \mathscr{C}$.

4. (Associator) A natural isomorphism

$$\alpha : - \otimes (- \otimes -) \xrightarrow{\sim} (- \otimes -) \otimes -,$$

where $-\otimes(-\otimes-)$ denotes the functor $\mathscr{C}\times\mathscr{C}\times\mathscr{C} \to \mathscr{C}$ sending (A, B, C) to $A\otimes(B\otimes C)$, and similarly for $(- \otimes -) \otimes -$.

5. (Left unitor) A natural isomorphism $\lambda : \mathbf{1} \otimes - \xrightarrow{\sim} -$, where $\mathbf{1} \otimes -$ denotes the functor $\mathscr{C} \to \mathscr{C}$ sending A to $\mathbf{1} \otimes A$, and $-$ denotes the identity.

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

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

1. (Triangle identity) The diagram

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

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

2. (Pentagon identity) The diagram

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

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

□

With this more general definition, we now have many examples of monoidal categories:

Proposition 4.4. *The following collections of data form monoidal categories*

*(i) The category $\mathscr{C} =$ **Set**, with tensor product $\otimes =$ Cartesian product, monoidal unit $\mathbf{1} = \{*\}$, associator*

$$\begin{aligned}\alpha_{A,B,C} : A \times (B \times C) &\xrightarrow{\sim} (A \times B) \times C, \\ (a,(b,c)) &\mapsto ((a,b),c)\end{aligned}$$

and unitors

$$\begin{aligned}\lambda : \mathbf{1} \otimes A &\to A & \qquad \rho : A \otimes \mathbf{1} &\to A. \\ (*, a) &\mapsto a & \qquad (a, *) &\mapsto a\end{aligned}$$

(ii) The plain category $\mathscr{C} = \mathbf{Vec}_{\mathbb{C}}$, with its standard tensor product, monoidal unit $\mathbf{1} = \mathbb{C}$, associator

$$\begin{aligned}\alpha_{A,B,C} : A \times (B \times C) &\xrightarrow{\sim} (A \times B) \times C, \\ a \otimes (b \otimes c) &\mapsto (a \otimes b) \otimes c\end{aligned}$$

and unitors

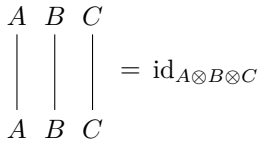
$$\begin{aligned}\lambda : \mathbf{1} \otimes A &\to A & \qquad \rho : A \otimes \mathbf{1} &\to A. \\ 1 \otimes a &\mapsto a & \qquad a \otimes 1 &\mapsto a\end{aligned}$$

(iii) The category $\mathscr{C} = \mathbf{Set}$ with tensor product $\otimes$ = Disjoint union and $\mathbf{1} = \{\}$, with a standard choice of associators and unitors;

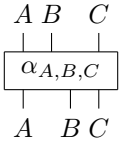
(iv) The category $\mathscr{C} = \mathbf{Vec}_{\mathbb{C}}$ with tensor product $\otimes$ = Direct sum, and $\mathbf{1} = 0$, with a standard choice of assoicators and unitors.

Proof. These facts are staightforward to verify, and are left as an exercise to the reader. □

In expanding our definition from strict monoidal category to monoidal category, however, we have introduced a subtle problem. The diagram



no longer makes sense! The map $\mathrm{id}_{A\otimes B\otimes C}$ no longer exists, because $A \otimes B \otimes C$ no longer exists. One must make a choice of $(A \otimes B) \otimes C$ or $A \otimes (B \otimes C)$. These maps may be isomorphic, but they have no need to be equal! The correct diagram would be



All string diagrams would now need α maps thrown in at key points to make a well-defined language. This is exceedingly complicated, and has deep issues that need to be adressed. Hence, we maintain that our graphical langauge only applies to strict monoidal categories.

This means that we haven't really gotten anywhere. We defined the notion of a non-strict monoidal category so that we could include our favorite examples, but then we observed that string diagrams still fail to describe those examples! This seemingly bad situation is rectified by the following theorem, which we first state informally.

MacLane's cohrence theorem: *every monoidal category is equvialent to a strict monoidal category.*

This gives us a workflow for the book. We will frame our discussion so that it applies to arbitrary monoidal categories. That way, all our usual examples are included. Then, when we want to use string diagrams, we use MacLane's coherence theorem to pass to an equivalent strict category, in which our diagrams make sense. Then, when we are done using the diagram, we pass the conclusion of the argument through the equivalence! We will be using this subtle technique repeatedly throughout the book. To save time and energy, we won't explicitely mention it. We will implicitely pass to an equivalent strict category without making any special note.

Sometimes we will want to pass to a strict monoidal category even before string diagrams come into play. For instance, in Proposition [ref] we proved that every strict braided monoidal category $\mathscr{C}$ comes paired with a group homomorphism

$$B_n \to \mathrm{Aut}\left(A^{\otimes n}\right)$$

for all $A \in \mathscr{C}$, $n \geq 1$. Once we generalize strict braided monoidal categories to possibly non-strict braided monoidal categories, this proposition will become false. The object $A^{\otimes n}$ does not exist - a choice of parenthesization needs to be made. Every time that an element of the braid group acts on $A^{\otimes n}$, the parentheses need to be re-arranged using associators, then the braiding map β can be applied, and then the parentheses need to be re-arranged back into their original position using associators again.

Not only does this non-strict version of Proposition [ref] take more time and space to set-up, but it also leads to potential thorny issues. There are multiple ways to rearange parentheses from one starting point to the other. How do we know that they will all give the same map, and hence into a well-defined homomorphism from B_n? It follows from general combinatorial principles and a repeated application of the pentagon identity.

This is indicative of the general feeling of working with non-strict monoidal categories. Statements and proofs which were obvious for strict monoidal categories become needlessly unintuitive for non-strict monoidal categories. Hence, it is much better to pass to a strict monoidal category using MacLane's coherence theorem at our first convenience.

Of course, all of this discussion rests on the notion of *equivalent* in MacLane's coherence theorem being well defined, so that we can pass information back and forth through the equivalence. Our notation of equivalence is modeled after the more general notation of equivalence of categories - a pair of functors whose compositions are both naturally isomorphic to the identity. To translate to the present setting, we need a good notion of monoidal functor and monoidal natural transformation so that the equivalence can pass through information about the monoidal structure.

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

1. A functor $F : \mathscr{C} \to \mathscr{D}$.
2. A morphism $\epsilon : 1_{\mathscr{D}} \to F(1_{\mathscr{C}})$.
3. A natural isomorphism $\mu : F(-) \otimes_{\mathscr{D}} F(-) \xrightarrow{\sim} F(- \otimes_{\mathscr{C}} -)$.

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

1. (Associativity) The diagram

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

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

2. (Unitality) The diagrams

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

   and

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

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

□

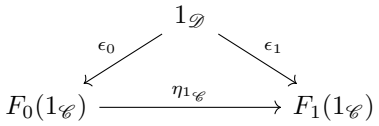
Definition (Monoidal natural transformation)**.** A monoidal natural transformation between two monoidal functors (F_0, μ_0, ϵ_0) and (F_1, μ_1, ϵ_1) between monoidal categories $(\mathscr{C}, \otimes_{\mathscr{C}}, \mathbf{1}_{\mathscr{C}})$ and $(\mathscr{D}, \otimes_{\mathscr{D}}, 1_{\mathscr{D}})$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

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

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

   commutes.

2. (Compatibility with unit) The diagram



commutes.

□

We can now define monoidal equivalence. A *monoidal equivalence* between two monoidal categories $\mathscr{C}, \mathscr{D}$ is a pair of monoidal functors $F : \mathscr{C} \to \mathscr{D}$, $G : \mathscr{D} \to \mathscr{C}$ such that $G \circ F$ is monoidally naturally isomorphic to $\mathrm{id}_{\mathscr{C}}$ and $F \circ G$ is monoidally naturally isomorphic to $\mathrm{id}_{\mathscr{D}}$. We say two categories are monoidally equivalent if there is a monoidal equivalence between them. We can now state MacLane's coherence theorem:

Theorem 4.1 (MacLane's coherence theorem,)**.** *Every monoidal category is monoidally equivalent to a strict monoidal category.*

As we add more structure, it will be a non-trivial task to verify that we can still apply MacLane's coherence theorem. In particular, we will need to strengthen our notion of equivalence to make sure it is strong enough to pass through information about our additional structures. We can see this in the case of braidings already.

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

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

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

1. (Hexagon identities) The diagrams

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

and

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

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

□

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

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

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

□

Thankfully, there is no notion of braided monoidal natural transformation - any monoidal natural transformation will automatically repsect the braiding. Hence, we can define two braided monoidal categories to be equivalent if there are braided monoidal functors between them which have compositions which are naturally isomorphic to the identity. Hence we can state a braided MacLane coherence theorem:

Theorem 4.2 (Braided MacLane coherence theorem)**.** *Every braided monoidal equivalent is equivalent as a braided monoidal category to a strict braided monoidal category.*

Proof. .[WORK: I bet the proof is not that bad. Include it if so.] □

As we go through this text, we will define increasingly more structure on monoidal categories. We will be implicitely assuming theorems which assert that every structured monoidal categories is equivalent to a structure monoidal category whose underlying monoidal category is strict. Importantly, we will assume that this equivalence respects the relevant structure. We will not state these theorems as we go along the way, but they are true and neccecary for our discussion. [WORK: Is this accurate? What is a good reference for this sort of coherence theorem? Will I talk about it more in the "Yoneda perspective" chapter?]

4.3.4 Pivotal monoidal categories

So far we have defined a language for putting particles together and braiding them. The next frontier is to introduce a langauge for creating and fusing particles/antiparticles. Categories with a mechanism for creating and fusing particles/antiparticles is known as a *pivotal monoidal category*.

In any realistic system, every particle will have a dual *antiparticle*. Particle/antiparticle pairs can always spontaneously be created from the vaccuum. Often, particles/antiparticles can annhilate each other to go back to the vaccum. This process of annhilation is much more subtle however, because a particle/antiparticle pair could also fuse to make a particle which is *not* the vacuum. We delay the subtleties of fusion to our chapter on modular tensor categories. In a category with duals, every object $A \in \mathscr{C}$ will have a dual object which we denote $A^* \in \mathscr{C}$. For now, we introduce categories with maps for annhilation/creation which we call *evaluation* and *coevaluation* respectively:

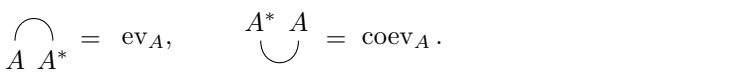
Definition (Right-rigid monoidal category)**.** A right-rigid monoidal category is the following data:

1. A monoidal category $\mathscr{C}$.
2. Objects A^* for all $A \in \mathscr{C}$.
3. Morphisms $\mathrm{ev}_A : A \otimes A^* \to 1$, and $\mathrm{coev}_A : 1 \to A^* \otimes A$ for all $A \in \mathscr{C}$.

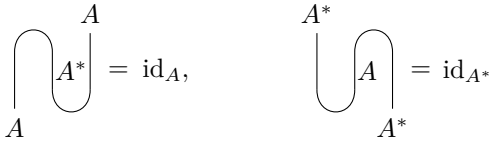
Such that $(\mathrm{ev}_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_A \otimes \mathrm{coev}_A) = \mathrm{id}_A$ and $(\mathrm{id}_{A^*} \otimes \mathrm{ev}_A) \circ (\mathrm{coev}_A \otimes \mathrm{id}_{A^*}) = \mathrm{id}_{A^*}$ for all $A \in \mathscr{C}$.

□

We implement right-rigid monoidal categories in string diagrams as follows. We denote evaluation and coevaluation as follows:



The compatibility conditions are stated graphically as follows:



We now note that particle/antiparticle pairs could also be created on the other side. This gives a left-rigid monoidal category, defined similarly:

Definition (Left-rigid monoidal category)**.** A left-rigid monoidal category is the following data:

1. A monoidal category $\mathscr{C}$.
2. Objects A^* for all $A \in \mathscr{C}$.
3. Morphisms $\mathrm{ev}_A : A^* \otimes A \to 1$, and $\mathrm{coev}_A : 1 \to A \otimes A^*$ for all $A \in \mathscr{C}$.

Additionally, a rigid category is required to satisfy the property that $(\mathrm{id}_A \otimes \mathrm{ev}_A) \circ (\mathrm{coev}_A \otimes \mathrm{id}_A) = \mathrm{id}_A$ and $(\mathrm{ev}_A \otimes \mathrm{id}_{A^*}) \circ (\mathrm{id}_{A^*} \otimes \mathrm{coev}_A) = \mathrm{id}_{A^*}$ for all $A \in \mathscr{C}$.

□

In a left-rigid monoidal category, graphical cups and caps can be defined just like in right-rigid monoidal categories.

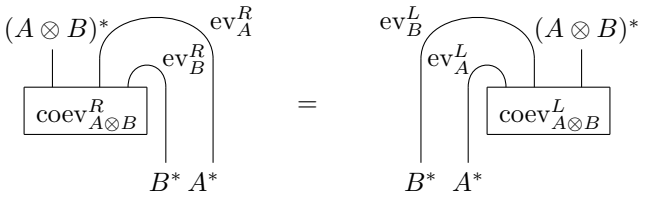
This leads us to our main definition of the section. We want to discuss categories which have a full theory of particles/antiparticles. This means that they should be able to create particle/antiparticle pairs on both sides, leading to a left-rigid and right-rigid structure on $\mathscr{C}$. As per usual, there should be some compatibility conditions between these two rigid structures. We give this full definition now:

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

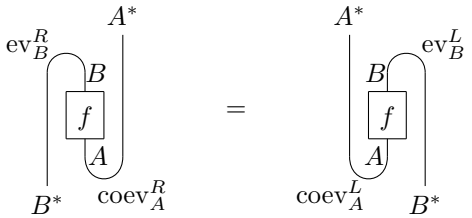
1. A monoidal category $\mathscr{C}$;
2. A right-rigid structure $(\mathrm{ev}^R, \mathrm{coev}^R)$ on $\mathscr{C}$;
3. A left-rigid structure $(\mathrm{ev}^L, \mathrm{coev}^L)$ on $\mathscr{C}$.

Such that:

1. The right-duals and left-duals of all objects are equal;
2. For all $A, B \in \mathscr{C}$, we have an equality of morphisms $B^* \otimes A^* \to (A \otimes B)^*$,



3. For all $A, B \in \mathscr{C}$ and $f : A \to B$,

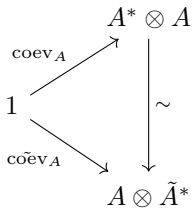


□

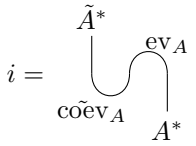
Now that we have given our main definitions, we prove some basic properties of rigid and pivotal categories.

The first thing to observe is that even though there is a lot of structure involved in the definition of a rigid monoidal category, most of it is in a real sense innessential. That is, we could have chosen different duals and the result would have been essentially the same:

Proposition 4.5. *Let $\mathscr{C}$ be right (resp. left) rigid monoidal category. Let $A \in \mathscr{C}$ be an object, and let $(\tilde{A}^*, \tilde{\mathrm{ev}}_A, \tilde{\mathrm{coev}}_A)$ be another triple satisfying the axioms of rigidity. There is a unique morphism $i : A^* \to \tilde{A}^*$ making the diagram*

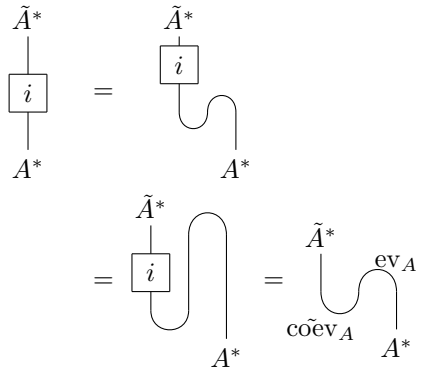


commute (resp. reverse order of tensor factors). This unique morphism is an isomorphism, and it is given by

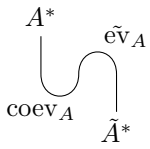


Remark. This proposition can be summarized by saying that *duals are unique up to unique isomorphism.*

Proof. By the computation



we find that i is unique, and it has the desired formula. To prove that i is an isomorphism we observe that the map



serves as an inverse. This gives a proof of the result. □

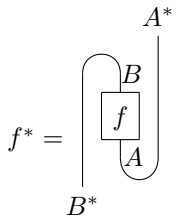
We now discuss the correct notion of functors between rigid and pivotal categories. Let $F : \mathscr{C} \to \mathfrak{D}$ be a functor between pivotal categories. Given an object $A \in \mathscr{C}$, the evaluation and coevaluation maps naturally extend through the functor to endow $F(A^*)$ with the structure of a dual for A. Thus, by Proposition [ref], we have a canonical isomorphism $F(A^*) \cong F(A)^*$. This isomorphism exists without needing to add any extra conditions on F. In this way, the correct notion of functor between right/left rigid categories is just functor! There is, however, extra an compatibility condition needed for pivotal category. Both the left-rigid *and* right-rigid structures induce isomorphisms $F(A^*) \cong F(A)^*$. These induced isomorphisms should be the same. This is known as a pivotal functor.

Another important thing to know about rigid monoidal categories is that duality is *functorial*. That is, the duals of objects induce functors:

Proposition 4.6. *Let $\mathscr{C}$ be right (resp. left) rigid monoidal category. Define a monoidal category $\overline{\mathscr{C}}$ as follows. The underlying category on $\overline{\mathscr{C}}$ is the opposite category for $\mathscr{C}$. The tensor product is given by $A \overline{\otimes} B = B \otimes A$, and the monoidal unit is $\mathbf{1} \in \mathscr{C}$. This gives a well-defined monoidal category.*

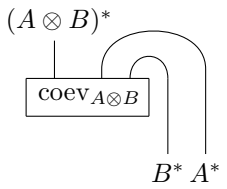
(i) The right (resp.left) rigid structure on $\mathscr{C}$ induces a left (resp. right) rigid structure on $\overline{\mathscr{C}}$;

(ii) Given any morphism $f : A \to B$ in $\mathscr{C}$, define



to be the dual for f (resp. same diagram using left rigidity). The assignment $A \mapsto A^*$, $f \mapsto f^*$ induces a functor from $\mathscr{C}$ to $\overline{\mathscr{C}}$ which we denote $(-)^*$.

(iii) Given any objects $A, B \in \mathscr{C}$, define the map



from $B^* \otimes A^*$ to $(A \otimes B)^*$ (resp. same diagram using left rigidity). These maps endows $(-)^*$ with the structure of a monoidal functor.

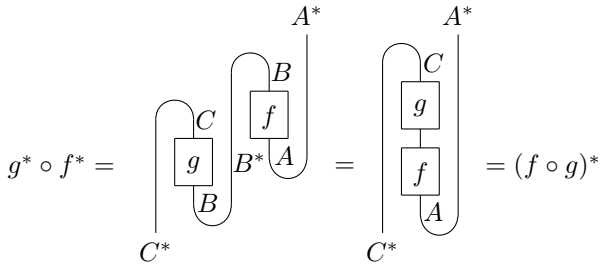
(iv) The functor $(-)^*$ is fully faithful. If $\mathscr{C}$ is a pivotal category, then then functor above is an equivalence of monoidal categories between $\mathscr{C}$ and $\overline{\mathscr{C}}$.

Remark. This proposition can be used to motivate the axioms of a pivotal category. Both the right and left rigid structures in a pivotal category induce functors $\mathscr{C} \to \overline{\mathscr{C}}$. The coherence condition is that these two functors should be equal.

Proof. We do only the proofs for right-rigid categories. The left-rigid proof is identitical.

(i) This follows immediately from the definitions;

(ii) Functoriality is the condition that $(f \circ g)^* = g^* \circ f^*$. The follows from the following argument:



(iii) This is an unlightening and straightforward computation;

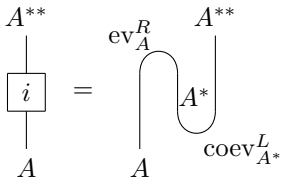
(iv) We first prove that $(-)^*$ is fully faithful. Given any objects $A, B \in \mathscr{C}$ and any morphism $g : B^* \to A^*$, the morphism

[WORK: add formula.]

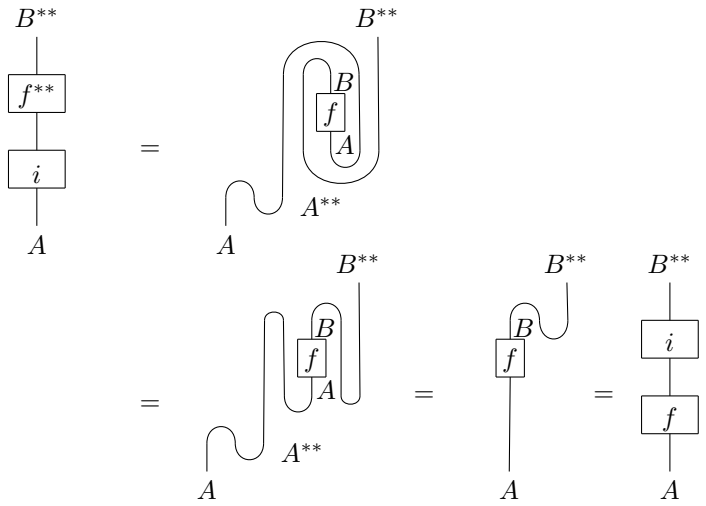
has the property that $f^* = g$. Hence, $(-)^*$ is bijective on hom-spaces as desired.

We now show that $(-)^*$ is an equivalence of categories with $\mathscr{C}$ is pivotal. By part (i), $\overline{\mathscr{C}}$ is a pivotal monoidal category. Hence duality once again induces a monoidal functor, this time $\overline{\mathscr{C}} \to \overline{\overline{\mathscr{C}}}$. Clearly, by our definition of $\overline{\mathscr{C}}$, $\overline{\overline{\mathscr{C}}} = \mathscr{C}$. Hence we have a pair of functors $\mathscr{C} \to \overline{\mathscr{C}}$ and $\overline{\mathscr{C}} \to \mathscr{C}$, each given by duality. Proving this proposition hence amounts to showing that the double dual map is monoidally naturally isomorphic to the identity.

To do this, we define a natural isomorphism explicitely by the isomorphisms $i : A \xrightarrow{\sim} A^{**}$



for all $A \in \mathscr{C}$. To show that these morphisms induce a natural transformation, we observe that for all $f : A \to B$

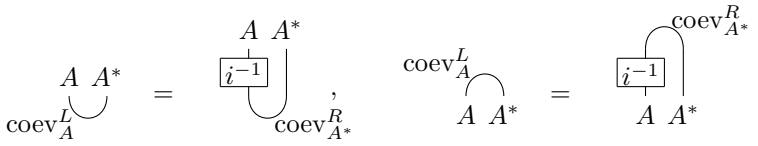


The fact that $\mathscr{C}$ is compatible with the tensor product is a straightforward computation, using the fact that computing the tensor product using right-rigidity and left-rigidity gives the same answer, and compatibility of $\mathscr{C}$ with the unit is immediate.

□

As a key part of Proposition [ref], we showed that every pivotal structure on a right-rigid monoidal category induces a natural isomorphism between the identity functor and the double dual functor. This gives an alternate description of pivotal categories which is useful in some applications:

Corollary 4.2. *Let $\mathscr{C}$ be a right-rigid monoidal category. Let $i : \mathrm{id}_{\mathscr{C}} \xrightarrow{\sim} (-)^{**}$ be a monoidal natural isomorphisms between the identity functor and the double dual functor. The maps*



induce a pivotal structure on $\mathscr{C}$. Moreover, this assignement induces a bijection between pivotal structures on $\mathscr{C}$ and monoidal natural isomorphisms $\mathrm{id}_{\mathscr{C}} \xrightarrow{\sim} (\mathrm{id}_{\mathscr{C}})^{**}$.

Proof. Proving that the maps provided satisfy the axioms of a left-rigid structure is immediate. Proving that they satisfy the axioms of a pivotal structure comes from running the arguments in the proof of proposition [ref] in reverse. The operations of inducing a monoidal natural isomorphism from a pivotal structure and inducing a pivotal structure from a monoidal natural isomorphism are inverses of one another. Hence, they induce a bijection between the two types of structures as desired. □

History and further reading:

Category theory was first introduced and formalized by Saunders Mac Lane and Samuel Eilenberg in 1945 [EM45]. Of course, the ideas underlying category theory were present earlier and can be traced back arbitrarily far. In the subsequent decades the formalism of category theory spread far and wide, bringing with it the discovery of many deep theorems. The first major explicit appearance of category theory in physics was Vladimir Drinfeld's work on so-called *quantum groups* in the early 1980s [Dri86]. Quantum groups are certain kinds of mathematical objects righly related to content in this book. They were introduced as tools to help generate exactly-solvable models in condensed matter physics. Very quickly quantum groups were absorbed into the theory of the ideas of string theory of topological quantum field theory, which were both new at the time [BPZ84, Wit88]. The physics in this area has since become and remained extremely categorical in nature [Lur08, BDSPV15].

There are many excellent introductory texts to category theory. Some authors find it fruitful to reformulate all of quantum mechanics, and especially quantum information, in terms of category theory. A good source outlining this approach and introducing category theory through it is Coecke-Kissinger's textbook [CK18]. The Kong-Zhang textbook [KZ22] gives an introduction to category theory in the context of topological order. A good general-purpose textbook on category theory is Fong-Spivak [FS19], and a classical but slightly dated reference is [ML13].

Exercises:

4.1. .[WORK: If $\mathscr{C}$ is a category with products, then the product forms a monoidal structure (with a good **1** given of course), and same for coproducts.]

4.2. .[WORK: Show that endofunctors form a *strict* monoidal category.]

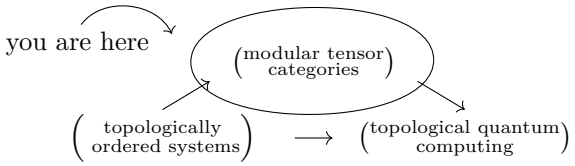
4.3. .[WORK: Add an exercise giving some compatibility conditions between monoidal/rigid structures and direct sums. Namely, they distribute nicely.]

5 Modular categories

5.1 Overview

5.1.1 Introduction

In this chapter we will be giving a detailed analysis of modular categories, the abstract algebraic structures used to describe anyons in topological order. We recall below how this fits into the general framework of this book:



Describing exactly what an anyon and how it can transform in terms of states and unitary operators on a Hilbert space can be difficult. However, describing abstractly how these transformations compose with one another can be done realtively simply. Hence we take a composition-first category-theoretic approach to anyons. We will make heavy use of the diagramatic language of braided monoidal categories established in Chapter [ref]. Concretely, we will think of a modular category as being the category with the following data:

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

Up to topological equivalence, there are not that many things that a collection of anyons can do. The most basic thing is to move anyons around each other - this is known as braiding. If the anyons touch each other then they can congeal into a single composite anyon - this is known as fusion. Even if there are no anyons in a system, however, there is always something possible. Anyons can be spontaneously created, so long as every anyon which is created comes along with its corresponding antiparticle. This is known as *pair-creation*. These three operations are the fundamental structures which we will building into modular categories:

1. braiding;
2. fusion;
3. pair-creation.

One potentially useful way of thinking about modular categories comes from analogy with classical physics. We saw in Chapter [ref] that topological classical systems have an algebraic description in terms of finite groups. Namely, quasiparticles in the system of ordered media with order space M is algebraically characterized by the fundamental group $\pi_1(M, m)$ of M relative to some basepoint $m \in M$. Seeing as topological order is a vast quantum generalization of classical ordered media, we can think of modular categories as being a vast quantum generalization of finite groups. Every finite group induces a modular category, by

first constructing the Kitaev quantum double model based on that finite group and then describing its anyons. Most modular categories, however, lie beyond this description.

[WORK: There's an issue in this treatment. There is one piece of data beyond the scope of an modular categories - the chiral central charge. This is a remnant of the fact that the bulk-to-boundary correspondane is not exact because the boundary can have stacked E_8 phases, see [Bon21]. Of course this is not something to dive into now. However, I want to be maximally honest - point out that there is a unique piece of topologically invariant information beyond the scope of modular categories. Maybe include somewhere (as an exercise?) the treatment of chiral central charge mod 8? I think this would make for a good footnote. I'm realizing now that the fact that the chiral central charge is a root of unity is part of Vafa's theorem. So, it makes the most sense for this to be in the number theory section.]

5.1.2 Using the final product

Before developping the theory of modular categories, it is good to get a feel for what using the final product is like. A modular category itself will be a big infinite thing, with infinitely many objects and infinitely many morphisms between those objects. However, all modular categories are in a real sense *finitely generated*. What we mean by this is that plugging in a finite number of objects and morphisms, the rest of the obejcts and morphisms can be recovered by the abstract rules encoded in the formalism. For example, consider the 3-strand braid group B_3. This group has ininitely many elements and the group operation $\cdot : B_3 \times B_3 \to B_3$ takes a-priori an infinite amount of data to describe. However, the presentation

$$B_3 = \langle \sigma_1, \sigma_2 \,|\, \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \rangle$$

gives completely finite description of B_3. It is important to note, however, that this presentation would *not* have been enough to recover B_3 if we had just been told that B_3 is a monoid. The fact that B_3 is a group implied the existence of elements σ_1^{-1}, σ_2^{-1}, and defined how they interacted with σ_1, σ_2. We see in this way that the axioms of a group not only serve as a restriction on what mathematical objects are allowed to be groups, but they also serve as a compression technique. They give the rules by which a minimal collection of data can be used to generate the rest.

In a similar way, the axioms of modular categories are not only neccecary by the fact that they restrict which categories can be modular categories, but they are also vital in the fact that they allow us to generate a full description of anyons from a minimal collection of data. For practically-minded readers, this can be viewed as the main motivation for defining modular categories at all, instead of just working with important examples.

The final challenge in going from modular categories to their description in terms of a finite set of data is in comming up with an efficient standard way of descrbing morphisms in a modular category. This is done using skeletonization, as discussed in section [ref].

In the end, the data of a modular category will look like what we have below for the toric code:

[WORK: add toric code modular category data]

Or, for a more complicated example, we can consider the data for $G = S_3$:

[WORK: add $G = S_3$ modular category data]

A large table of these descriptions are found in Chapter [ref]. We now give a worked example of how this data is used to compute observable quantities.

[WORK: add good example, computing some probability of annhilation]

5.2 First properties

5.2.1 Definition

In this section we finally define modular categories, which are the main mathematical content of this book. Seeing as lots of data is involved, we spread out the definition over a series of steps as to not overload the senses. These intermediate definitions are also important in their own right, because they will be used in other places in the algebraic theory of topological phases.

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

1. A category $\mathscr{C}$;
2. The structure of a right-rigid monoidal category on $\mathscr{C}$;
3. The structure of a $\mathbb{C}$-linear category on $\mathscr{C}$.

Such that:

1. The tensor product functor $\otimes : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$ induces bilinear maps hom-spaces;
2. There is an equivalence $\mathscr{C} \cong \mathbf{Vec}_{\mathbb{C}}^n$ as $\mathbb{C}$-linear categories;
3. $\mathrm{End}_{\mathscr{C}}(\mathbf{1}) \cong \mathbb{C}$ as $\mathbb{C}$-vector spaces

□

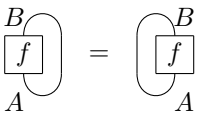
A fusion category is part of the way towards having all of the requisite structures of a modular category: it has a method for fusion inherited from the tensor product, and it has half of a method for pair-creation coming from right-rigidity. The $\mathbb{C}$-linearity allows us to think of hom-spaces as vector spaces, which allows us to treat hom-spaces as quantum systems. The condition (1) is a comptability between the $\mathbb{C}$-linear structure and the monoidal structure. The conditions (2)-(3) are strong niceness and finiteness conditions - we will explain them in detail later. We now move one step closer to our definition of modular category:

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

1. A fusion category $\mathscr{C}$;
2. A left-rigid structure on $\mathscr{C}$.

Such that:

1. The left-rigid and right-rigid structures on $\mathscr{C}$ satisfy the axioms of a pivotal structure on $\mathscr{C}$;
2. For every object $A \in \mathscr{C}$ and for every morphism $f : A \to A$, we have



□

A spherical fusion category now has a structure for fusion, and a full structure for pair-creation. The 2nd condition is known as the *spherical axiom*. We will explain this axiom in more detail later.

Adding on a braiding, we can get all of the structures of a modular category. However, adding this structure still misses one key structure of being a modular category. Hence, we call it *pre-modular*:

Definition (Pre-modular category)**.** A pre-modular category is the following data:

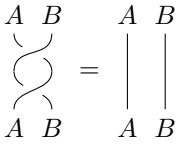
1. A spherical fusion category $\mathscr{C}$;
2. A braided structure on $\mathscr{C}$.

No extra compatibility conditions are required.

□

This definition now has all of the structure we wanted it to have: fusion, pair-creation, and braiding. The final axiom is a non-degeneracy condition. It is subtle in its interpretation, and we will explain it several different ways throughout this chapter:

Definition (Modular category)**.** A modular category is a pre-modular category satisfying the following condition. Let $A \in \mathscr{C}$ be an object. If



for all $B \in \mathscr{C}$, then $A \cong \mathbf{1}$.

□

5.2.2 Anyons in modular categories

Modular categories are supposed to be theories of anyons in topological order. So, now that we have the definition of modular category, it is natural to ask: what do anyons mathematically correspond to, in modular categories? The answer lies within the condition in a fusion category $\mathscr{C}$ that there is an equivalence $\mathscr{C} \cong \mathbf{Vec}_{\mathbb{C}}^n$ as $\mathbb{C}$-linear categories. We explore the importance of this condition.

Suppose we are given an object $V = (V_1, V_2 ... V_n) \in \mathbf{Vec}_{\mathbb{C}}^n$. For all $1 \leq i \leq n$, let $\mathbb{C}_i \in \mathbf{Vec}_{\mathbb{C}}^n$ denote the object which has dimension zero in every index $j \neq i$ and is equal to $\mathbb{C}$ in index i. We observe the isomorphism

$$\begin{aligned} V &\cong \bigoplus_{i=1}^{n} (0 ... V_i ... 0) \\ &\cong \bigoplus_{i=1}^{n} (0 ... \mathbb{C}^{\dim(V_i)} .. 0) \\ &\cong \bigoplus_{i=1}^{n} \dim(V_i) \cdot \mathbb{C}_i \end{aligned}$$

where $\dim(V_i)\cdot(\mathbb{C}_i) = \mathbb{C}_i \oplus \mathbb{C}_i ... \oplus \mathbb{C}_i$, $\dim(V_i)$ many times. This computation shows that any object in $\mathbf{Vec}_{\mathbb{C}}^n$ can be decomposed into irriducible components $\mathbb{C}_i$. These objects $\mathbb{C}_i$ are in a real sense the building blocks of $\mathbf{Vec}_{\mathbb{C}}^n$. They will correspond physically to anyons. More concretely, we make the following definition:

Definition. A *simple object* A in a fusion category $\mathscr{C}$ is an object which has no direct sum decomposition into smaller objects. That is, $A \ncong B \oplus C$ for any non-zero objects $B, C \in \mathscr{C}$ where $\oplus$ denotes the biproduct in $\mathscr{C}$.

Our physics-math dictionary is that anyon types correspond to isomorphism classes of simple objects.

We now state the basic proposition which ensures that the neccecary properties from $\mathbf{Vec}_{\mathbb{C}}^n$ follow through the equivalence of categories.

Proposition 5.1. *Let $\mathscr{C}$ be a fusion category. The biproduct of any two elements in $\mathscr{C}$ exists, and $\mathscr{C}$ has a zero object. Let $\mathcal{L}$ denote the set of isomorphism classes of simple objects in $\mathscr{C}$. The set $\mathcal{L}$ is finite. Choose an object $X \in \mathscr{C}$. There exist unique nonnegative integers $c_{[A]}$, $[A] \in \mathcal{L}$ such that*

$$X \cong \bigoplus_{[A]\in\mathcal{L}} N_{[A]} \cdot A.$$

Proof. We first show that $\mathscr{C}$ has biproducts. Let $F : \mathscr{C} \to \mathbf{Vec}_{\mathbb{C}}^n$, $G : \mathbf{Vec}_{\mathbb{C}}^n \to \mathscr{C}$ be a pair of functors which induces an equivalence of categories, for some $n \geq 1$ Let $A, B \in \mathscr{C}$ be objects. Since G and F are fully faithfull, the universal property of the direct sum $F(A) \oplus F(B)$ guarantees that $G(F(A) \oplus F(B))$ will be a direct sum of $G(F(A))$ and $G(F(B))$. Since $G(F(A)) \cong A$ and $G(F(B)) \cong B$, we conclude that $\mathscr{C}$ has biproducts. The object $G(0)$ is a zero object for $\mathscr{C}$.

We now prove that $\mathscr{C}$ has finitely many isomorphism classes of simple objects. It is clear that an object $A \in \mathscr{C}$ is simple if and only fi $F(A) \in \mathbf{Vec}_{\mathbb{C}}^n$ is simple. Thus, since G serves as an inverse, F establishes a bijection between isomorphism classes of simple obejcts in $\mathscr{C}$ and isomorphism classes of simple objects in $\mathbf{Vec}_{\mathbb{C}}^n$. Every simple obejct in $\mathbf{Vec}_{\mathbb{C}}^n$ will be isomorphic to $\mathbb{C}_i$ for some $1 \leq i \leq n$. Hence, there are n simple objects in $\mathbf{Vec}_{\mathbb{C}}^n$. Hence, there are n simple objects in $\mathscr{C}$, which is finite.

The unique direct sum decomposition is clearly true in $\mathbf{Vec}_{\mathbb{C}}^n$. It is immediate that it passes to a unique direct sum decomposition in $\mathscr{C}$. □

The set of simple objects has an alternative description, known as Schur's lemma:

Proposition 5.2 (Schur's Lemma)**.** *Let $\mathscr{C}$ be a fusion category. An object $A \in \mathscr{C}$ is simple if and only if its endomorphism ring* $\mathrm{End}(A)$ *is one-dimensional. Additionally, if $A, B \in \mathscr{C}$ are nonisomorphic simple objects then* $\mathrm{Hom}(A, B) = 0$.

Proof. Let $F : \mathscr{C} \to \mathbf{Vec}_{\mathbb{C}}^n$, $G : \mathbf{Vec}_{\mathbb{C}}^n \to \mathscr{C}$ be a pair of $\mathbb{C}$-linear functors which establishes an equivalence between $\mathscr{C}$ and $\mathbf{Vec}_{\mathbb{C}}^n$ as $\mathbb{C}$-linear categories. The simple objects in $\mathbf{Vec}_{\mathbb{C}}^n$ are all isomorphic to $\mathbb{C}_i$ for some $1 \leq i \leq n$. We compute that

$$\dim\left(\mathrm{Hom}_{\mathbf{Vec}_{\mathbb{C}}^n}\left(\bigoplus_{i=1}^n n_i\mathbb{C}_i, \bigoplus_{i=1}^n m_i\mathbb{C}_i\right)\right) = \sum_{i=1}^n n_i m_i.$$

As a corrolary of this formula, we find that if $A = \bigoplus_{i=1}^n n_i\mathbb{C}_i$ then $\dim(\mathrm{End}_{\mathbf{Vec}_{\mathbb{C}}^n}(A)) = \sum_{i=1}^n n_i^2$. Clearly, this dimension is equal to one if $A = \mathbb{C}_i$ for some $1 \leq i \leq n$, and is greater

than one otherwise. As a second corrolary, we compute that $\mathrm{Hom}(\mathbb{C}_i, \mathbb{C}_j) = 0$ whenever $i \neq j$.

The functor G induces a bijection between isomorphism classes of simple objects in $\mathbf{Vec}_{\mathbb{C}}^n$ and isomorphism classes of simple objects in $\mathbf{Vec}_{\mathbb{C}}^n$, and it induces vector space isomorphisms on hom spaces. This means that the results for $\mathbf{Vec}_{\mathbb{C}}^n$ translate to the desired result on $\mathscr{C}$. $\square$

As an immediate application of Schur's lemma, we observe that the monoidal unit $\mathbf{1}$ is a simple object in every fusion category. By our physics-math dictionary, this means that $\mathbf{1}$ corresponds to an anyon type. This type is the *vaccuum* type - empty space. The anyon $\mathbf{1}$ is the trivial no-anyon type.

Another application of Schur's lemma is to make a first verification that simple objects are a good choice of mathematical characterization of anyons. If A, B are distinct anyon types, then there should not be any physical process which goes from one to another. There is no physical mechanism for locally turning one anyon type into another. This is captured by the formula $\mathrm{Hom}(A, B) = 0$. Similarly, given an anyon A, there is no nontrivial action that can be locally performed on A. This comes from the fact that information is topologically protected, and thus cannot be changed by acting on a single particle - topological information processing requires global braiding between multiple particles. This is encoded in the fact that $\mathrm{Hom}(A, A) \cong \mathbb{C}$ is one dimensional and hence consists only of trivial phase gates.

Expanding our physics-math dictionary, we say that for every anyon A its *antiparticle* is the dual A^* which comes from right-rigidity. This gives a valid anyon type by the following computation:

Proposition 5.3. *Let $\mathscr{C}$ be a fusion category. If $A \in \mathscr{C}$ is a simple object, then so is A^*.*

Proof. By Proposition [ref] duality induces a bijection on hom-spaces. Since composition is bilinear, this bijection is an isomorphism of vector spaces. Hence, for all $A \in \mathscr{C}$ there is an isomorphism $\mathrm{Hom}(A, A) \cong \mathrm{Hom}(A^*, A^*)$. Hence, $\dim \mathrm{Hom}(A, A) = 1$ if and only if $\dim \mathrm{Hom}(A^*, A^*) = 1$ so the result follows by Schur's lemma. $\square$

An important part of of understanding simple objects in modular categories is making sense of the direct sum decompositions coming from Proposition [ref]. Let $\mathscr{C}$ be a fusion category with simple objects $A, B \in \mathscr{C}$. Consider the decomposition

$$A \otimes B \cong \bigoplus_{[C] \in \mathcal{L}} N_C^{A,B} \cdot C$$

where $N_C^{A,B} \geq 0$ are nonnegative integers, and $\mathcal{L}$ is the set of isomorphism classes of simple objects. The integers $\{N_C^{A,B}\}_{[C] \in \mathcal{L}}$ are known as fusion coefficents, because they specify the behavior of A and B when they fuse.

The tensor product $\otimes$ physically corresponds to joining anyons, forming a composite anyon configuration. The object $A \otimes B$ corresponds to the configuration with one A-type anyon and one B-type anyon. The direct sum decomposition is physically interpreted as saying that when $A \otimes B$ are fused, the possible results of that fusion are all of the anyon types $[C] \in \mathcal{L}$ for which $N_C^{A,B} \neq 0$.

[WORK: add nontrivial example from Kitaev quantum double model]

A more detailed understanding of the physical meaning of the direct sum will have to wait for later.

This concludes our basic picture of anyons in fusion categories.

5.2.3 States in modular categories and unitarity

It is now worth reflecting on what exactly states correspond to in modular categories. In particular, objects in modular categories are *not* quantum systems. They don't have vector space structure. The spaces with vector space structure are the hom-spaces, by $\mathbb{C}$-linearity. Objects will correspond to anyon configurations. States will correspond to normalized vectors in certain hom-spaces. In particular:

$$\begin{pmatrix}\text{states of topological order } \mathscr{C} \\ \text{on the sphere} \\ \text{with anyon configuraiton } A_1, A_2 ... A_n\end{pmatrix} = \begin{pmatrix}\text{normalized vectors in the Hilbert space} \\ \text{Hom}_{\mathscr{C}}(\mathbf{1}, A_1 \otimes A_2 ... \otimes A_n)\end{pmatrix}$$

where by "anyon configuration $A_1, A_2 ... A_n$" we mean that the state has anyons present in n sites, arranged left to right on a one dimensional subspace of $\mathbb{R}^2$, with corresponding anyon type $A_1, A_2 ... A_n$. For the sake of concreteness, one can imagine that at the point $(i, 0) \in \mathbb{R}^2$ thee state has an anyon of type A_i.

The remainder of this subsection is a series of loosely-related observations about this choice of state space:

Observation 1: *The physical space is a sphere.*

It is not immediately clear where in the formula $\text{Hom}(\mathbf{1}, A_1 \otimes A_2 ... \otimes A_n)$ we chose the sphere as the physical space. To make it make sense, we observe as a special case of the general formula that

$$\dim \begin{pmatrix}\text{Hilbert space of topological order } \mathscr{C} \\ \text{on the sphere } S^2 \\ \text{with exactly one anyon of type } A\end{pmatrix} = \dim \text{Hom}(\mathbf{1}, A) = \begin{cases} 1 & A = \mathbf{1} \\ 0 & \text{otherwise.} \end{cases}$$

Hence, the state formula tells us that if the sphere has exactly one anyon on it then that anyon type must be trivial. Moreover, there is unique state on the sphere with no anyons.

This is consistent with our general principles about topological order on the sphere.

[WORK: sketch nice argument for why there is a unique ground state on the sphere. What I'm struggling with here is why an anyon type in a region must neccecarily be detectable by its surrounding region.]

This gives us a framework for extending our state-space/hom-space correspondances to physical spaces other than the sphere. In particular, we find the following:

$$\begin{pmatrix}\text{states of topological order } \mathscr{C} \\ \text{on the infinite flat plane } \mathbb{R}^2 \\ \text{with anyon configuraiton } A_1, A_2 ... A_n\end{pmatrix} = \begin{pmatrix}\text{normalized vectors in the Hilbert space} \\ \text{Hom}_{\mathscr{C}}\left(\bigoplus_{[B] \in \mathcal{L}} B, A_1 \otimes A_2 ... \otimes A_n\right)\end{pmatrix}$$

where $\mathcal{L}$ is the set of isomorphism classes of simple objects in $\mathscr{C}$. Replacing $\mathbf{1}$ with $\bigoplus_{[B] \in \mathcal{L}} B$ reflects the differences between the sphere and the infinite flat plane.

[WORK: sketch nice argument for why states on infinite flat plane are determined by their overall charge. The subtelty here is exactly the same as the one for the sphere. Think about it then put it down.]

[WORK: What happens for higher genus surfaces? I should add a few words about them. Zhenghan says all of this is contained in Turaev's book about the Reshetikhin-Turaev construction.]

Observation 2: *The anyons are always assumed to be arranged in a line.*

The anyon configurations are always assumed to be linear. The main reason to do this is because it makes the mathematics much simpler. If we kept track of the positions of each

of the anyons in two dimensional space it would add more pieces of data and structures to keep track of. Seeing as every anyon configuration can be pushed onto a one-dimensional space, only working with a one-dimensional configuration does not affect the generality of the answers and hence it is very much prefered.

Observation 3: *The formula* $\mathrm{Hom}_{\mathscr{C}}(\mathbf{1}, A_1 \otimes A_2 ... \otimes A_n)$ *encodes the fact that states can be specified by their history.*

A good first question to ask when seeing the Hilbert space $\mathrm{Hom}_{\mathscr{C}}(\mathbf{1}, A_1 \otimes A_2 ... A_n)$ is *why* this should describe a state with anyon configuration $A_1 ... \ A_n$. The answer is that states can be described their history. [WORK: give good example of making a state by specifying its history; argue why it has to be this way in general.].

Observation 4: *In the definition of an modular category hom-spaces are vector spaces and not Hilbert spaces, so this choice of physics-math correspondance is incorrect as literally written.*

To make this definition work, all of the hom-spaces of the modular category $\mathscr{C}$ should be equipped with Hilbert space structures. Furthermore, the natural operators we wish to perform like braiding should all be unitary with respect to these inner products. This amounts to adding a large number of compatibility conditions on the Hilbert space structures. A modular category with this choice of structure is known as a *unitary* modular category. We give the formal definition below:

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

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

Such that:

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

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

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

2. $\left(f^\dagger\right)^\dagger = f$ for all $f \in \mathrm{Hom}(A, B)$, $A, B \in \mathscr{C}$.
3. $(f \circ g)^\dagger = g^\dagger \circ f^\dagger$ for all $f \in \mathrm{Hom}(B, C)$,$g \in \mathrm{Hom}(A, B)$, $A, B, C \in \mathscr{C}$.
4. $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$ for all $f \in \mathrm{Hom}(A, B)$,$g \in \mathrm{Hom}(C, D)$, $A, B, C, D \in \mathscr{C}$.
5. $(\mathrm{coev}_A)^\dagger \circ (f \otimes \mathrm{id}_{A^*}) \circ \mathrm{coev}_A = \mathrm{tr}(f)$ for all $A \in \mathscr{C}$

□

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

Proposition 5.4. *Let* $\mathscr{C}$ *be a unitary fusion category. The maps* $\mathrm{ev}_A^L = (\mathrm{coev}_A)^\dagger$ *and* $\mathrm{coev}_A^L = (\mathrm{ev}_A)^\dagger$ *give a left-rigid structure on* $\mathscr{C}$*. This left-rigidity endows* $\mathscr{C}$ *with the structure of a spherical fusion category.*

Proof. .[WORK: This is actually subtler than I expected. Either give a proof here, or postpone it to the unitarity section.] □

We can now define unitary modular categories. The compatibility conditions for the twist are chosen so that the definition of trace as a modular category and the definition of trace as a unitary fusion category coincide. [WORK: The definition below is outdated. It uses the twist-theoretic definition of modular categories. Should be re-done.]

Definition (Unitary pre-modular category)**.** A unitary modular category is the following data:

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

Such that:

1. Forgetting the left-rigid structure and braiding, $(\mathscr{C}, \dagger)$ forms a unitary fusion category.
2. $\left(\mathrm{ev}_A^R\right)^\dagger = \mathrm{coev}_A^L$;
3. $\left(\mathrm{coev}_A^R\right)^\dagger = \mathrm{ev}_A^L$;
4. $(\beta_{A,B})^\dagger = \beta_{B,A}^{-1}$.

□

Definition (Unitary modular category)**.** A unitary modular category is a unitary pre-modular category which satisfies the non-degeneracy axiom of a modular category.

For this reason, the correct algebraic structure to underlie the theory of topological order is not a modular category, but a unitary modular category. We have chosen to not emphasize this before because the difference between unitary modular categories and non-unitary modular categories is very small. [WORK: talk about uniqueness + positive q.d. criterion this will make more sense once we write the actual section about unitarity. A good thing to emphaize is that unitary modular categories don't let you use less data in your definition, and you can still do essentially everything you want to do. It's just way more cumbersome. They're all equivalent but you still have to choose, c.f. the fact that the category of vector spaces and Hilbert spaces with linear maps as morphisms are equivallent].

5.2.4 Topological charge measurement

When two anyons are fused together, they will form a superposition of other anyon types. Measuring the result of the fusion will collapse the answer into a specific anyon type. The outcome of this measurment is an observable quantity, which allows for the measurement of topological quantum information. In many cases this is the *only* local observable quanitity. We give the formalism behind computing these probabilities now.

[WORK: do this right - I don't know it well but it shouln't be hard to learn. Don't introduce anything too general, like trace or whatnot. Just quantum dimension, which should already have been introduced in previous chapter.]

[WORK: The correct reference for this subsection is [Bon21]. The paper [CCW17] claims to introduce the term topological charge measurement and gives a nice formal treatmenet. Clarifying the situation seems important.]

5.3 The modular category toolkit

In this section, we will introduce and prove the basic facts about the most important structures in the theory of modular categories. These facts and structures are the tools used for solving problems about the algebraic theory of anyons.

[WORK: I don't have a section on fusion coefficients yet. I guess this isn't a problem, because there isn't that much to say. I would like to have the associativity of fusion cooficients and the fact that braiding $\implies$ commutative said somewhere explicitely, though. Find a place?]

5.3.1 Trace

The first structure to define in the theory of modular categories is the *trace*. Let $\mathscr{C}$ be a spherical fusion category. Given any object $A \in \mathscr{C}$ and any endomorphism $f : A \to A$, we define the *trace of* f by the following formula:

$$\mathrm{tr}(f) = A^* \left(\boxed{f} \right)^{A}_{A}$$

Initially, the trace is a morphism, $\mathrm{tr}(f) : \mathbf{1} \to \mathbf{1}$. However, we will choose to think of the trace of a morphism as a *complex number*, $\mathrm{tr}(f) \in \mathbb{C}$. This can be done because the definition of a fusion category $\mathrm{End}(\mathbf{1}) \cong \mathbb{C}$. This isomorphism can be made canonical by identifying an endomorphism $g \in \mathrm{End}(\mathbf{1})$ with the unique $\lambda \in \mathbb{C}$ such that $g = \lambda \cdot \mathrm{id}_{\mathbf{1}}$.

The trace is used mainly as a tool for linearization. Morphisms and objects are hard to describe, but the trace is a complex number.

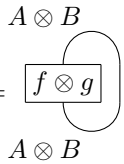
Proposition 5.5. *Let $\mathscr{C}$ be a spherical fusion category. For all $A, B \in \mathscr{C}$, $f \in \mathrm{End}(A)$ the following claims are all true:*

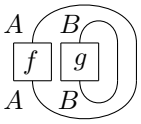
1. $\mathrm{tr} : \mathrm{End}(A) \to \mathbb{C}$ *is a linear map of vector spaces,*
2. $\mathrm{tr}(f^*) = \mathrm{tr}(f)$,
3. $\mathrm{tr}(f \oplus g) = \mathrm{tr}(f) + \mathrm{tr}(g)$ *for all* $g \in \mathrm{End}(B)$,
4. $\mathrm{tr}(f \otimes g) = \mathrm{tr}(f) \cdot \mathrm{tr}(g)$ *for all* $g \in \mathrm{End}(B)$,
5. $\mathrm{tr}(h \circ g) = \mathrm{tr}(g \circ h)$ *for all* $g : A \to B$, $h : B \to A$.
6. *Trace is preserved by functors. That is, let $\mathscr{C}, \mathscr{D}$ be spherical categories with traces $\mathrm{tr}_{\mathscr{C}}, \mathrm{tr}_{\mathscr{D}}$ respectively. Let $F : \mathscr{C} \to \mathscr{D}$ be a pivotal functor. We have that $\mathrm{tr}_{\mathscr{C}}(f) = \mathrm{tr}_{\mathscr{D}}(F(f))$;*

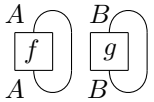
Proof. We prove the claims one by one.

1. This follows immediately from the bilinearity of composition.
2. This is a straightforward computation.
3. .[WORK: do proof. This uses facts about the direct sum we haven't established yet.]

4. Using Proposition [ref] we compute

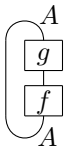
$\mathrm{tr}(f \otimes g) =$ 

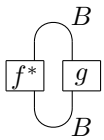
$=$ 

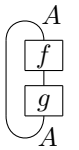
$=$ 

$= \mathrm{tr}(f) \cdot \mathrm{tr}(g).$

5. Using Proposition [ref] we find that

$\mathrm{tr}(f \circ g) =$ 

$=$ 

$=$ 

$= \mathrm{tr}(g \circ f).$

6. .[WORK: do the proof. It's not very hard, but involves a diagram and uses pivotality of the functor.]

This completes the proof. □

With these properties in hand, we can explicitely compute the trace using a straightforward procedure:

Corollary 5.1. *Let $f : A \to A$ be an endomorphism in a fusion category $\mathscr{C}$. Fix a decomposition $A \cong \bigoplus_{i \in I} A_i$ of A into simple objects A_i. Moreover, we take the decomposition such that if $A_i \cong A_j$ then $A_i = A_j$. We can decompose*

$$\mathrm{Hom}(A, A) \cong \mathrm{Hom}(\bigoplus_{i \in I} A_i, \bigoplus_{i \in I} A_i) = \bigoplus_{i \in I, j \in I} \mathrm{Hom}(A_i, A_j).$$

Let M be the matrix whose collums and rows are labeled by I, and whose (i, j) entry is 0 if $A_i \ncong A_j$ and $\lambda \cdot d_{A_i}$ if $A_i = A_j$, where $\lambda \in \mathbb{C}$ is the unique value such that the $\mathrm{Hom}(A_i, A_j)$ component of f is $\lambda \cdot \mathrm{id}_{A_i}$. We have that

$$\mathrm{tr}_{\mathscr{C}}(f) = \mathrm{tr}_{\mathbf{Vec}}(M).$$

Proof. Suppose that $A = A_0 \oplus A_1$ is the direct sum of two objects, not neccecarily simple. By proposition [ref] we have a canonical decomposition

$$(A_0 \oplus A_1) \otimes (A_0 \oplus A_1)^* \cong (A_0 \otimes A_0^*) \oplus (A_0 \otimes A_1^*) \oplus (A_1 \otimes A_0^*) \oplus (A_1 \otimes A_1^*).$$

Suppose that $h : A \to A$ is an endomorphism. We can decompose $h = h_{A_0,A_0} + h_{A_0,A_1} + h_{A_1,A_0} + h_{A_0,A_1}$ as a sum of morphisms which restrict to maps $A_i \to A_j$. We find that $\mathrm{coev}_{A \oplus B}$ restricts to a map whose codomain is $(A_0 \otimes A_0^*) \oplus (A_1 \otimes A_0)^*$ and similarly ev

restricts to a map whose domain is $(A_0 \otimes A_0^*) \oplus (A_1 \otimes A_0)^*$, since $\mathrm{coev}_{A\oplus B} = \mathrm{coev}_A \oplus \mathrm{coev}_B$ and $\mathrm{ev}_{A\oplus B} = \mathrm{ev}_A \oplus \mathrm{ev}_B$.

Hence, in the definition of trace, we find that the cross terms $h_{A_0,A_1} + h_{A_1,A_0}$ act by zero since they send the codomain of $\mathrm{coev}_{A\oplus B}$ to elements with no effect on the map $\mathrm{ev}_{A\oplus B}$. Moreover, we compute in this way that $\mathrm{tr}(h) = \mathrm{tr}(h_{A_0,A_0}) + \mathrm{tr}(h_{A_1,A_1})$.

In this way, the trace splits over direct sums and only picks out diagonal elements. Applying this result inductively reduces the proof to the case that A is a simple object. This follows directly from the definition of quantum dimension. □

5.3.2 Duality

Duality is baken into our definition of modular categories as a fundamental part of the structure. It acts in a very controlled way on fusion cooefficients:

Proposition 5.6. *Let $\mathscr{C}$ be a fusion category and let $A, B, C \in \mathscr{C}$ be simple objects. We have the following:*

(i) (Anti-involution) $N_C^{A,B} = N_{C^*}^{B^*,A^*}$;

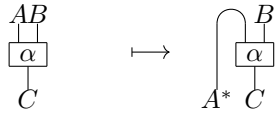
(ii) (Frobenius reciprocity) $N_C^{A,B} = N_B^{A^*,C} = N_A^{C,B^*}$.

Proof. Part (i) follows from the fact that the duality functor is fully faithful and monoidal from propositon [ref], so

$$N_C^{A,B} = \dim \mathrm{Hom}(C, A \otimes B) = \dim \mathrm{Hom}(A^* \otimes B^*, C^*) = N_{C^*}^{B^*,A^*}.$$

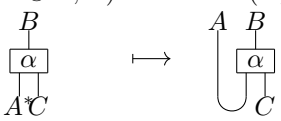
Part (ii) follows from the following computation. Consider the map

$$i : \mathrm{Hom}(A, B \otimes C) \longrightarrow \mathrm{Hom}(A^* \otimes C, B)$$



Since composition is bilinear, i is a linear map. The map

$$\mathrm{Hom}(A^* \otimes C, B) \longrightarrow \mathrm{Hom}(A, B \otimes C)$$



serves as an inverse for i by rigidity. Hence, we conclude that

$$N_C^{A,B} = \dim \mathrm{Hom}(C, A \otimes B) = \dim \mathrm{Hom}(A^* \otimes C, B) = N_B^{A^*,C}.$$

The third equality in Frobenius reciprocity follows from an identical argument, and hence we conclude the proof. □

In particular, we can describe the fusion rules of a simple object with its dual:

Corollary 5.2. *Let $\mathscr{C}$ be a fusion category. Let $A, B \in \mathscr{C}$ be simple objects. We find that*

$$N_{\mathbf{1}}^{A,B} = N_{\mathbf{1}}^{B,A} = \begin{cases} 1 & B \cong A^* \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. This follows from Frobenius reciprocity and Schur's lemma:

$$N_{\mathbf{1}}^{A,B} = N_A^{A^*,\mathbf{1}} = \dim(\mathrm{Hom}(A, A^*)) = \begin{cases} 1 & B \cong A^* \\ 0 & \text{otherwise.} \end{cases}$$

□

Specializing even more, we get the following corollary:

Corollary 5.3. *If $\mathscr{C}$ is a fusion category, then $A \cong A^{**}$ for all $A \in \mathscr{C}$.*

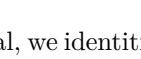
Proof. Since $N_{\mathbf{1}}^{A^*,A^{**}} > 0$, we conclude that $A^{**} \cong A$ by the $(iii) \implies (i)$ implication in proposition [ref]. □

However, despite this corollary, we *cannot* conclude that every fusion category admits a pivotal structure. The isomorphism $A \cong A^{**}$ may fail to form a monoidal natural transformation. It is an open problem whether or not every fusion category admits a pivotal structure, and it is furthermore an open problem whether every pivotal fusion category admits a spherical structure [ENO05].

5.3.3 Quantum dimension and Frobenius-Perron dimension

.[WORK: include something about global quantum dimension $\mathcal{D}$.]

Our next tool to discuss is the *quantum dimension*. Given any spherical fusion category $\mathscr{C}$ and any object $A \in \mathscr{C}$, we define its quantum dimension using the following formula:

$d_A =$ 

As usual, we identitfy d_A with a complex number via the canonical isomorphism $\mathrm{End}(\mathbf{1}) \cong \mathbb{C}$. The quantum dimension is clearly equal to the trace of the identity map on A, $d_A = \mathrm{tr}(\mathrm{id}_A)$. The first properties of quantum dimension follow from our general analysis of trace:

Proposition 5.7. *For every spherical fusion category $\mathscr{C}$ and any objects $A, B \in \mathscr{C}$, we have the following formulas:*

(i) *If $A \cong B$, then $d_A = d_B$;*

(ii) $d_{A \oplus B} = d_A + d_B$;

(iii) $d_{A \otimes B} = d_A \cdot d_B$;

(iv) $d_{A^*} = d_A$.

(v) $d_A \neq 0$.

Proof.

(i) Let $f : A \cong B$ be an isomorphism. Using Proposition [ref] we find

$$d_A = \mathrm{tr}(\mathrm{id}_A) = \mathrm{tr}(f^{-1} \circ f) = \mathrm{tr}(f \circ f^{-1}) = \mathrm{tr}(\mathrm{id}_B) = d_B.$$

(ii) This follows from proposition [ref].

(iii) This follows from proposition [ref].

(iv) This follows from proposition [ref].

(v) From proposition [ref], we know that $A \otimes A^* \cong \mathbf{1} \oplus X$ for some $X \in \mathscr{C}$ which does not have any factors of $\mathbf{1}$ in its direct sum decomposition. The map $\mathrm{coev}_A^R : \mathbf{1} \to A \otimes A^*$ is thus a non-zero scalar times the inclusion $\mathbf{1} \hookrightarrow \mathbf{1} \oplus X$, and the map $\mathrm{ev}_A^L : A \otimes A^* \to \mathbf{1}$ is a non-zer scalar times the projection $\mathbf{1} \oplus X \to \mathbf{1}$. Since inclusion composed with projection is the identity, we find that $\mathrm{ev}_A^L \circ \mathrm{coev}_A^R$ is a non-zero scalar times the identity, as desired.

□

The above propositions tell us that the values d_A as A ranges over isomorphism classes of simple objects determs all the other values of d_A. Moreover, proposition [ref] tells us that the quantum dimensions of simple objects determines the trace of *every* endomorphism! Hence, computing d_A for each isomorphism class $[A] \in \mathcal{L}$ is an important step in analysing an modular category. The following formula and its linear-algebraic reformulaion are the primary insight in performing the computation:

Proposition 5.8. *Let $\mathscr{C}$ be a spherical fusion category.*

(i) Let $A, B \in \mathscr{C}$ be simple objects. We have that

$$d_A d_B = \sum_{[C] \in \mathcal{L}} N_C^{A,B} d_C.$$

(ii) Let $A \in \mathscr{C}$ be a simple object. Define an operator

$$\begin{aligned} N^A : \mathbb{C}[\mathcal{L}] &\to \mathbb{C}[\mathcal{L}]. \\ |[B]\rangle &\mapsto \sum_{[C] \in \mathcal{L}} N_C^{A,B} \, |[C]\rangle \end{aligned}$$

Define $\mathbf{d} = \sum_{[B] \in \mathcal{L}} d_B \, |[B]\rangle \in \mathbb{C}[\mathcal{L}]$. We have that

$$N^A \mathbf{d} = d_A \mathbf{d}.$$

Proof. From proposition [ref], we have an isomorphism

$$A \otimes B \cong \bigoplus_{[C] \in \mathcal{L}} N_C^{A,B} \cdot C$$

and thus

$$\mathrm{tr}(\mathrm{id}_{A \otimes B}) = \mathrm{tr}(\mathrm{id}_{\bigoplus_{[C] \in \mathcal{L}} N_C^{A,B} \cdot C}).$$

Expanding using the rules in proposition [ref] gives part (i). Part (ii) follows from expanding the definition of the linear operator and applying part (i). □

We now make commentary about the above proposition. It tells us that d_A is an eigenvalue of N^A. Since N^A is an operator with integer coefficients, this immediately tells us that d_A is the root of polynomial with integer coeffients. Namely, the characteristic polynomial of N^A. We can even be more precise about the nature of d_A:

[WORK: On the MathOverflow question "Modular Tensor Categories: Reasoning behind the axioms", a commentator said "You also have to assume that the categorical dimensions arising from the pivotal structure are all real. This is called the spherical axiom". Why is this the same thing as the spherical axiom? What is the motivation? I should include this as a remark on the below proposition.]

Corollary 5.4. *Let $\mathscr{C}$ be a spherical fusion category. The quantum dimensions of all simple objects in $\mathscr{C}$ are real numbers.*

Proof. .[WORK: do proof.] □

The question is whether or not the quantum dimensions are *positive* real numbers. We recall that we defined a unitarizable spherical fusion category to be one in which the quantum dimensions are all positive. It is at this point that this becomes relevant. In particular, if $\mathscr{C}$ is unitarizable then its quantum dimensions are eigenvalues of N^A, and their corresponding eigenvector $\mathbf{d}$ has positive real entries. There is a theorem about eigenalues of non-negative matrices with positive eigenvectors:

Theorem 5.1 (Frobenius-Perron theorem, [EGNO16])**.** *Let B be a square matrix with nonnegative real entries.*

(i) B has a non-negative real eigenvalue. The largest non-negative real eigenvalue $\lambda(B)$ of B dominates the absolute values of all other eigenvalues μ of B: $|\mu| \leq \lambda(B)$. Moreover, there is an eigenvector of B with non-negative entries and eigenvalue $\lambda(B)$.

(ii) If B has strictly positive entries then $\lambda(B)$ is a simple positive eigenvalue, and the corresponding eigenvector can be normalized to have strictly positive entries. Moreover, $|\mu| < \lambda(B)$ for any other eigenvalue μ of B.

(iii) If a matrix B with non-negative entries has an eigenvector v with strictly positive entries, then the corresponding eigenvalue is $\lambda(B)$.

We call the largest positive real eigenvalue of a matrix its *Frobenius-Perron eigenvalue*. The Frobenius-Perron theorem tells us the following:

Corollary 5.5. *Let $\mathscr{C}$ be a unitarizable spherical fusion category. Let $A \in \mathscr{C}$ be a simple object. The quantum dimension d_A is equal to the Frobenius-Perron eigenvalue of N^A.*

Proof. Since $\mathscr{C}$ is unitarizable, the vector $\mathbf{d} = \sum_{[B]\in\mathcal{L}} d_B \, |[B]\rangle \in \mathbb{C}[\mathcal{L}]$ has positive entries and has eigenvalue d_A. Hence, d_A is the Frobenius-Perron eigenvalue of N^A as desired. □

In this chapter we will mostly work with generic spherical fusion categories with no conditions on unitarizability. Hence, it is useful to make the following definition. Let $A \in \mathscr{C}$ be a simple object in a spherical fusion category. We define

$$\mathrm{FPdim}(A) = (\text{Frobenius-Perron eigenvalue of } N^A).$$

When $\mathscr{C}$ is unitarizable, $\mathrm{FPdim}(A) = d_A$. Many formulas about quantum dimension in the unitary world apply to the Frobenius-Perron dimension in the non-unitary world.

An interesting observation is that the definition of quantum dimension strongly uses the spherical structure on $\mathscr{C}$. However, the Frobenius-Perron dimension only uses the fusion coeffients, and those are well-defined in any fusion category. Hence, the Frobenius-Perron dimension also derives utility from being applicable in a broader set of situations than the quantum dimension.

We now give an alternate interpretation of the Frobenius-Perron dimension in terms of growth in tensor powers. This sort of alternate perspective of dimension applies to several types of objects outside the scope of tensor category theory [COT24].

Proposition 5.9. *Let $\mathscr{C}$ be a fusion category, and let $A \in \mathscr{C}$ be a simple object.*

(i) $\mathrm{FPdim}(A) = \lim_{n\to\infty} \dim(\mathrm{Hom}(A^{\otimes n}, A^{\otimes n}))^{1/(2n)}$

(ii) $\mathrm{FPdim}(A) = \lim_{n\to\infty} \dim(\mathrm{Hom}(\mathbf{1}, A^{\otimes n}))^{1/n}$

(iii)

$$\mathrm{FPdim}(A) = \lim_{n\to\infty} (\#\text{ of simple objects in the direct sum decomposition of } A^{\otimes n})^{1/n}.$$

Proof. .[WORK: I can do a good part of this when $\mathscr{C}$ is unitarizable, so that its largest eigenvalue is strictly larger than all of the others. When there are multiple large eigenvalues all of the same size then the proofs go wrong. Is there something about the structure of N^A I can exploit? Are these theorems true for fusion categories, or do I need to pass to unitarizable fusion categories?] □

This proposition can be interpreted as saying that the simple object A has $\mathrm{FPdim}(A)$ internal degrees of freedom "on average". Elements of the vector space $\mathrm{Hom}(\mathbf{1}, A^{\otimes n})$ correspond to states in the system with n anyons of type A arranged in a line. If the internal configuration space of each anyon was $\mathrm{FPdim}(A)$-dimensional, then the overall dimension would be $\mathrm{FPdim}(A)^n$. By Proposition [ref], $\mathrm{FPdim}(A)^n$ is approximately $\mathrm{Hom}(\mathbf{1}, A^{\otimes n})$ for large n. Hence, each anyon has approximately $\mathrm{FPdim}(A)$ internal degrees of freedom. Of course, $\mathrm{FPdim}(A)$ has no reason to be an integer! In the Fibonacci theory $\mathrm{FPdim}(\tau) = \phi = 1.61....$ Frobenius-Perron dimension just gives an average amount for large values.

[WORK: re-do this explanation way better + add diagram for it.]

5.3.4 Twist

In this section we will discuss *twists*. The twist is a subtle concept, which we have not explicitely mentioned up to now. The idea is that anyons can *rotate in place*. Since the space of endomorphisms of an anyon is one dimensional, this rotation must act by a phase. This phase is physically relevant, and can be measured in experiment.

For example, consider the Y-type on the toric code. It consists of the fusion of an X-type anyon and a Z-type anyon, as shown below:

[WORK: add figure of Y as a thick X and Z together; could be hard to draw these nice]

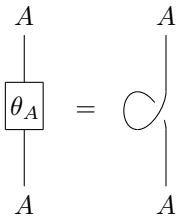
Twisting Y in place will correspond to twisting X and Z around each other. This twsiting thus results in a phase of -1. In general, we can imagine anyons as having some thickness to them. Anyons are not localized at points - they are localized at small regions. Twisting this region all the way around can be viewed visually as

[WORK: twisted anyon.]

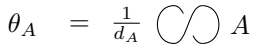
This is the twist. One way of working with the twist is to work with thickened diagrams, where strings are replaced with ribbons. While popular in some parts of the literature, we will continue to work with string diagrams for simplicity. The key observation is that the twist can be constructed using string diagramatic structures we already have as follows:

[WORK: twist as a swirl diagram, compared with ribbon.]

Hence, letting $\mathscr{C}$ be a pre-modular fusion category, we *define* the twist θ_A of an object $A \in \mathscr{C}$ to be

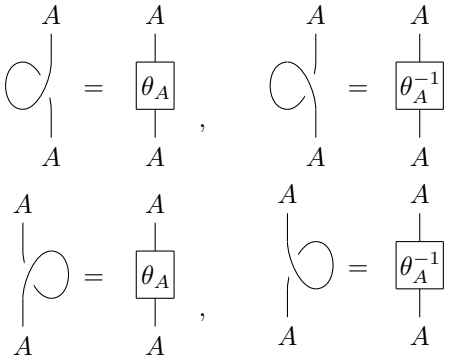


For every simple object $A \in \mathscr{C}$, the map $\theta_A \in \mathrm{End}(A)$ can be identified with the unique complex number λ such that $\theta_A = \lambda \cdot \mathrm{id}_A$. Equivilantly, we can identify θ_A with the complex number $\lambda = \mathrm{tr}(\theta_A)/d_A$ which gives the graphical formula

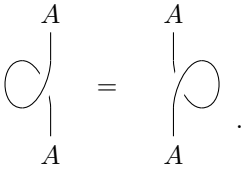


We can reinterpret all other twist-like maps in terms of θ:

Lemma 5.1. *Let $\mathscr{C}$ be a pre-modular fusion category. We have that*



Proof. To begin we show that



When A is simple, this follows from the spherical axiom. Taking the trace of both sides gives the same formula for θ_A as a figure-eight. Additionally, pushing through duals it is clear that both sides in the above proposed equality are natural isomorphisms. Natural isomorphisms are determined by their action on simple objects because they commute with direct sums. Hence, we conclude that the sides are equal for all objects.

To get that the two reversed formulas are equal to θ_A^{-1}, it suffices to compose with θ_A and use string-diagram manipulations to show that it results in the identity. This is a simple exercise and is left as an exercise to the reader. □

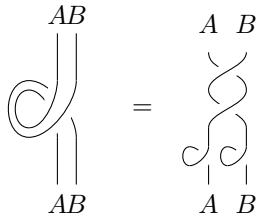
We now characterize the key properties of the twist:

Proposition 5.10. *Let $\mathscr{C}$ be a pre-modular fusion category. The twists θ induce a monoidal natural isomorphism $\mathrm{id}_{\mathscr{C}} \xrightarrow{\sim} \mathrm{id}_{\mathscr{C}}$. Additionally, θ satisfies the identity*

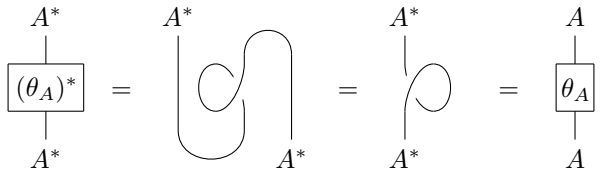
$$\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$$

for all $A, B \in \mathscr{C}$, and $\theta_{A^*} = (\theta_A)^*$.

Proof. Naturality of θ follows from pushing through duals. The formula $\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$ comes from manipulating string diagrams to get the equation

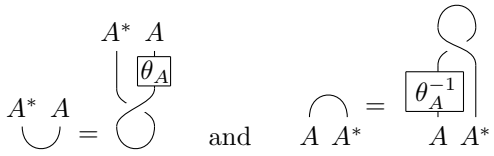


Finally, $\theta_{A^*} = (\theta_A)^*$ comes from the string-diagram manipulation and proposition [ref]:



as desired. □

The naive reason to care about twists is that they descrbe a physically relevant quantity and hence should be studied. The more subtle reason to care about twists is that they are the most efficient way of encoding the spherical structure on $\mathscr{C}$. A spherical structure is first and foremost a pivotal structure, meaning that it has a right and left rigid structure which are compatible. Given a spherical structure one can always obtain twists. Conversely, given a right-rigid structure and twists one can recover the left-rigid structure via the formulas

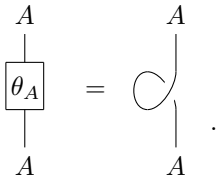


In this way, giving a spherical structure on a right-rigid monoidal category is the *same* as giving a twist structure. This is codified in the following lemma:

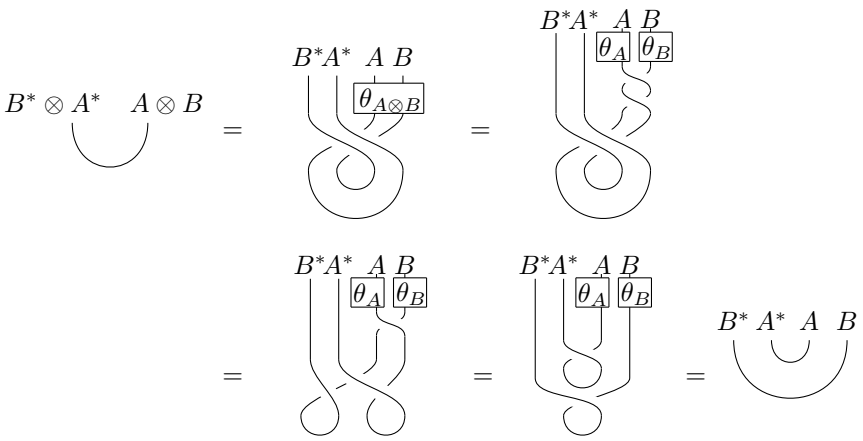
Proposition 5.11 (Deligne's twisting lemma, [Yet92])**.** *Let $\mathscr{C}$ be a right-rigid braided monoidal category. Every pivotal structure on $\mathscr{C}$ naturally gives a twist natural transformation $\theta : \mathrm{id}_{\mathscr{C}} \to \mathrm{id}_{\mathscr{C}}$. This assignment induces a canonical bijection between the set of pivotal structures on $\mathscr{C}$ and the set of natural isomorphism $\theta : \mathrm{id}_{\mathscr{C}} \to \mathrm{id}_{\mathscr{C}}$ satisfying $\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$ for all $A, B \in \mathscr{C}$.*

Moreover, restricting the assignment to the space of spherical structures on $\mathscr{C}$ induces a canonical bijection between the set of spherical structures on $\mathscr{C}$ and the set of isomorphisms $\theta : \mathrm{id}_{\mathscr{C}} \to \mathrm{id}_{\mathscr{C}}$ satisfying $\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$ for all $A, B \in \mathscr{C}$ and $\theta_{A^*} = (\theta_A)^*$.

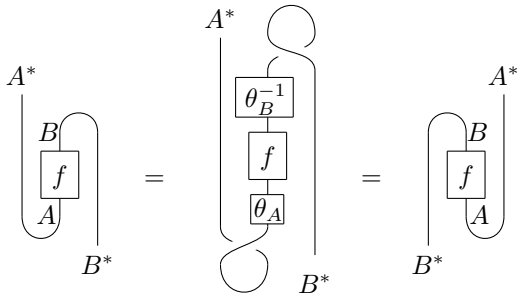
Proof. We already showed in proposition [ref] that every spherical category gives a twist natural transformation satisfying the desired axioms. Restriciting the proof to only a possibly non-spherical pivotal category still gives a twist natural transformation satisfying $\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$ for all $A, B \in \mathscr{C}$. The heart of the proof is showing that the formulas [ref] induce pivotal and spherical structures with the twist satisfies the right axioms. The process of inducing a pivotal structure and inducing a twist are inverses to one another because



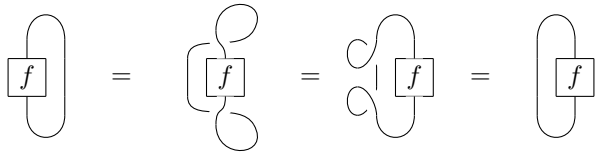
To begin, we assume that $\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$ and we seek to prove that the corresponding ev^L, coev^L maps induce a pivotal structure. We first axiom of pivotality follows from use of the axiom $\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$:



The second axiom of pivotality follows from the use of the naturality of θ:



Finally, we assume that $(\theta_A)^* = \theta_{A^*}$ and we seek to prove the spherical axiom. Taking the dual of theta we can get all of the equalities in Lemma [ref]. Applying them we get that



as desired. □

5.3.5 Functors, natural transformations, and equivalence

In this section, we will talk about functors, natural transformations, and equivalences between fusion, spherical, pre-modular, and modular categories. Given a topological order, there is *not* a unique modular category describing it. There is a unique modular category *up to equivalence*. Hence, the notion of equivalence of categories is baked into our physics-math correspondance so it is important that we state it explicitely.

Functors which do not induce equivalences of categories are also physically relevant. In certain contexts, a functor $F : \mathscr{C} \to \mathfrak{D}$ is used to model a *phase transition* from $\mathscr{C}$ to $\mathfrak{D}$. We will see a lot more functors and natural transformations between modular categories throughout the book, especially in chapter [ref].

Even though structures in categories require a lot of compatibility conditions, the conditions on the functors do not. This means that we have the following:

- The correct notion of functor between fusion categories is $\mathbb{C}$-linear monoidal functor. There is no compatibility condition required between the $\mathbb{C}$-linear structure and the monoidal structure. The correct notion of natural transformation between $\mathbb{C}$-linear monoidal functors is a monoidal natural transformation.

- The correct notion of functor between spherical fusion categories is $\mathbb{C}$-linear pivotal monoidal functor. There is no compatibility condition required between the $\mathbb{C}$-linear structure and the pivotal monoidal structure. The correct notion of natural trasnformation is monoidal natural transformation.

- The correct notion of functor between pre-modular categories is $\mathbb{C}$-linear pivotal braided monoidal functor. There is no compatibility condition required between the $\mathbb{C}$-linear structure, pivotal monoidal structure, or braided monoidal structure. The correct notion of natural transformation is monoidal natural transformation.

- The correct notions of functors/natural transformations for modular categories are the same as for pre-modular categories.

[WORK: this section is very short. I don't have much to say, actually. Should this be moved? Maybe I keep a very short section? I don't know.]

5.3.6 Deligne tensor product

In the theory of any class of mathematical object, an important consideration is the ways in which examples can be put together to give new examples. In the case of fusion categories, this basic operation is known as the *Deligne tensor product*. Given any fusion categories $\mathscr{C}$, $\mathscr{D}$, their Deligne tensor product $\mathscr{C} \boxtimes \mathscr{D}$ is a new fusion category. The Deligne tensor product of spherical fusion categories will be equipped with the structure of a spherical fusion category, and the Deligne tensor product of (pre-)modular categories will be equipped with the structure of a (pre-)modular category.

Physically, the Deligne tensor product corresponds to *stacking*. Consider two sheets of material. We choose two modular categories $\mathscr{C}$, $\mathscr{D}$. We enodow the top sheet with the structure of a topologically ordered quantum system described by $\mathscr{C}$ and we endow the bottome with the structure of a topologically ordered quantum system described by $\mathscr{D}$. The algebraic description of this bilayer system is $\mathscr{C} \boxtimes \mathscr{D}$. This can be viewed as the physical definition of $\mathscr{C} \boxtimes \mathscr{D}$.

[WORK: add bilayer system diagram]

We now mathematically define the Deligne tensor product.

Definition. Let $\mathscr{C}, \mathscr{D}$ be a $\mathbb{C}$-linear categories, isomorphic as a $\mathbb{C}$-linear categories to $\mathbf{Vec}_{\mathbb{C}}^n$, $\mathbf{Vec}_{\mathbb{C}}^m$ respectively. We define a Deligne tensor product of $\mathscr{C}$ and $\mathscr{D}$ to be be the following data:

1. A $\mathbb{C}$-linear category $\mathscr{C} \boxtimes \mathscr{D}$;
2. A $\mathbb{C}$-linear functor $\mathscr{C} \times \mathscr{D} \to \mathscr{C} \boxtimes \mathscr{D}$.

Such that:

1. Every object $X \in \mathscr{C} \boxtimes \mathscr{D}$ has a direct sum decomposition

$$X \cong \bigoplus_{i=1}^{n} A_i \boxtimes B_i$$

   for some $n \geq 1$, $A_i \in \mathscr{C}$, $B_i \in \mathscr{D}$.

2. There is an equality of vector spaces

$$\mathrm{Hom}_{\mathscr{C}\boxtimes\mathscr{D}}(A \boxtimes B, A' \boxtimes B') = \mathrm{Hom}_{\mathscr{C}}(A, A') \otimes \mathrm{Hom}_{\mathscr{D}}(B, B').$$

3. Given any $A, A', A'' \in \mathscr{C}$, $B, B', B'' \in \mathscr{D}$, $f : A \to A'$, $f' : A' \to A''$, $g : B \to B'$, $g' : B' \to B''$, the diagram

$$A \boxtimes B \xrightarrow{f\boxtimes g} A' \boxtimes B' \xrightarrow{f'\boxtimes g'} A'' \boxtimes B''$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \underset{(f'\circ f)\boxtimes(g'\circ f)}{\curvearrowright}$$

commutes.

We know state the main existence/uniqueness result about the Deligne tensor product:

Proposition 5.12. *Let $\mathscr{C}, \mathscr{D}$ be $\mathbb{C}$-linear categories isomorphic as $\mathbb{C}$-linear categories to $\mathbf{Vec}_{\mathbb{C}}^n$ and $\mathbf{Vec}_{\mathbb{C}}^m$ respectively. There exists a Deligne product $\mathscr{C} \boxtimes \mathscr{D}$ for $\mathscr{C}$ and $\mathscr{D}$. Moreover, given any other deligne tensor product $\mathscr{C} \boxtimes' \mathscr{D}$ of $\mathscr{C}$ and $\mathscr{D}$ there exists a unique functor $F : \mathscr{C} \boxtimes \mathscr{D} \to \mathscr{C} \boxtimes' \mathscr{D}$ making the diagram*

$$\begin{array}{ccc} \mathscr{C} \times \mathscr{D} & \longrightarrow & \mathscr{C} \boxtimes \mathscr{D} \\ & \searrow & \downarrow F \\ & & \mathscr{C} \boxtimes' \mathscr{D} \end{array}$$

commute. This functor is an equivalence of categories.

Proof. It is clear that $\mathbf{Vec}_{\mathbb{C}}^n \boxtimes \mathbf{Vec}_{\mathbb{C}}^m = \mathbf{Vec}_{\mathbb{C}}^{nm}$. Every equivalence of categories $\mathscr{C} \to \mathscr{C}'$ induces an equivalence of categories $\mathscr{C} \boxtimes \mathscr{D} \to \mathscr{C}' \boxtimes \mathscr{D}$. Hence, since $\mathfrak{D}$ and $\mathfrak{D}$ are equivalent to $\mathbf{Vec}_{\mathbb{C}}^n$ and $\mathbf{Vec}_{\mathbb{C}}^m$ respectively, their Deligne tensor product exists and is equivalent to $\mathbf{Vec}_{\mathbb{C}}^{nm}$.

Any functor making the diagram commute must send $A \boxtimes B$ to $A \boxtimes' B$. The definition of Deligne tensor produce tells us this is enough to conclude that the map is an equivalence of categories, since axiom 3 this map is always a functor, axiom 2 implies it is fully faithful, and axiom 1 implies it is essentially surjective, and hence we can apply proposition [ref]. □

Now that we have defined the Deligne tensor product of $\mathbb{C}$-linear categories equivalent to $\mathbf{Vec}_{\mathbb{C}}^n$, we move on to defining the Deligne tensor product of fusion categories, spherical fusion categories, pre-modular categories, and modular categories.

Proposition 5.13. *The following claims are all true.*

(i) Let $\mathscr{C}$, $\mathscr{D}$ be fusion categories. On the level of objects, define a monoidal structure $\mathscr{C} \boxtimes \mathscr{D}$ by the formula

$$(A \boxtimes B) \otimes (A' \boxtimes B') = (A \otimes A') \boxtimes (B \otimes B').$$

Along with a natural choice of action of the tensor product on morphisms, unit $\mathbf{1}_{\mathscr{C} \boxtimes \mathscr{D}} = \mathbf{1}_{\mathscr{C}} \boxtimes \mathbf{1}_{\mathscr{D}}$, and a natural choice of associator and unitors, this induces the structure of a monoidal category on $\mathscr{C}$.

Define a right-rigid structure on $\mathscr{C} \boxtimes \mathscr{D}$ as follows. The dual of an object $A \boxtimes B$ is $A^* \boxtimes B^*$. Define $\mathrm{ev}_{A \boxtimes B} = \mathrm{ev}_A \boxtimes \mathrm{ev}_B$, $\mathrm{coev}_{A \boxtimes B} = \mathrm{coev}_A \boxtimes \mathrm{coev}_B$. This induces a well-defined right-rigid structure on $\mathscr{C} \boxtimes \mathscr{D}$.

The above definitions induce the structure of a fusion category on $\mathscr{C} \boxtimes \mathscr{D}$.

(ii) Let $\mathscr{C}, \mathscr{D}$ be spherical fusion categories. The evaluation and coevaluation maps $\mathrm{ev}^L_{A \boxtimes B} = \mathrm{ev}^L_A \boxtimes \mathrm{ev}^L_B$ and $\mathrm{coev}^L_{A \boxtimes B} = \mathrm{coev}^L_A \boxtimes \mathrm{coev}^L_B$ induce a left-rigid structure on $\mathscr{C} \boxtimes \mathscr{D}$. Along with the canonial structure of a fusion category on $\mathscr{C} \boxtimes \mathscr{D}$, this induces the structure of a spherical fusion category on $\mathscr{C} \boxtimes \mathscr{D}$.

(iii) Let $\mathscr{C}, \mathscr{D}$ be pre-modular categories. The braiding map $\beta_{\mathscr{C} \boxtimes \mathscr{D}} = \beta_{\mathscr{C}} \boxtimes \beta_{\mathscr{D}}$ induces the structure of a pre-modular category on $\mathscr{C} \boxtimes \mathscr{D}$. The product $\mathscr{C} \boxtimes \mathscr{D}$ is modular if and only if $\mathscr{C}, \mathscr{D}$ are both modular.

Proof. Given any of the above structures, all of the axioms on $\mathscr{C}\boxtimes\mathscr{D}$ immediately follow from their respective axioms on $\mathscr{C}$ and $\mathscr{D}$. Hence, the proof is an exercise is recalling definitons which we omit. □

5.4 The category of G-graded G-representations

5.4.1 Overview

We've talked about a lot of general theory of modular categories. It's time for us to focus on our main family of *examples*. Namely, the categories $\mathfrak{D}(G)$ of G-graded G-representations. These categories describe discrete gauge theory based on the finite group G.

Before we can prove that $\mathfrak{D}(G)$ is a modular category, we need to endow $\mathfrak{D}(G)$ with the neccecary structures. In particular, we will endow $\mathfrak{D}(G)$ with $\mathbb{C}$-linear, monoidal, braided, right-rigid, and left-rigid structures. We will need to show that all of these structures are comptabile with each other in the neccecary ways, and that $\mathfrak{D}(G)$ satisfies the non-degeneracy axiom. We will use this as an oppurtunity to introduce tools of general use for proving that categories satisfy the axioms of a modular category.

Additionally, we will also study two categories similar to $\mathfrak{D}(G)$ which will serve as extra examples to get our grip on definitions. These categories will also appear later as relevant in and of themselves. The first is $\mathbf{Vec}_G$, the category of G-graded vector spaces. It is defined as follows:

[WORK: define $\mathbf{Vec}_G$ in terms of objects and composition.]

Our second structure of interest is $\mathrm{Rep}(G)$, the category of G-representations. It is defined as follows:

[WORK: define $\mathrm{Rep}(G)$ in terms of objects and composition.]

We will show that both $\mathbf{Vec}_G$ and $\mathrm{Rep}(G)$ can be naturally equipped with the structures of spherical fusion categories. We then show that $\mathrm{Rep}(G)$ admits a braiding which turns it into a pre-modular category. This braiding is symmetric in the sense that $\beta_{B,A}\circ\beta_{A,B} = \mathrm{id}_A\otimes\mathrm{id}_B$ for all $A, B\in\mathscr{C}$, and hence $\mathrm{Rep}(G)$ is not a modular category. The category $\mathbf{Vec}_G$ is shown to not admit a braiding whenever G is non-abelian.

5.4.2 Higher linear algebra

.[WORK: In this section we define the $\mathbb{C}$-linear structures on $\mathbf{Vec}_G$, $\mathrm{Rep}(G)$, and $\mathfrak{D}(G)$. Our goal is to show that they are all equivalent to $\mathbf{Vec}_{\mathbb{C}}^n$ for some $n\geq 1$.

It seems like the best approach is through higher linear algebra. Namely, we show that if $\mathscr{C}$ is abelian, $\mathbb{C}$-linear, semisimple, and has finitely many isomorphism classes of simple obejcts then it must be isomorphism to $\mathbf{Vec}_{\mathbb{C}}^n$. Its a good time to wax philosophical about higher linear algebra and 2-vector spaces. However, its not clear that this approach actually helps at all. It might be easier to immediately note that everybody is the direct sum of irriducibles, prove a Schur's lemma, and call it a day. Of course these approaches are all equivalent but its not clear what's best.]

5.4.3 Spherical fusion structures

.[WORK: show that the categories have duals and monoidal structure. This should be pretty easy and painless. Pentagon identity should follow from the pentangon identity on $\mathbf{Vec}_{\mathbb{C}}$.]

5.4.4 Braiding and modularity

.[WORK: Introduce braidings. Show that Rep(G) is symmetric. Show that $\mathbf{Vec}_G$ does not admit a braiding if G is not abelian and does admit a symmetric braiding if G is abelian. Show that $\mathfrak{D}(G)$ admits a non-degenerate braiding.]

5.5 The modular representation

5.5.1 Definition

In this chapter we are going to talk about the *modular representations* of modular categories. Here's the point. Let $\mathscr{C}$ be a modular category. Let $\mathcal{L}$ be the set of isomorphism classes of simple objects of $\mathscr{C}$. We will define a group homomorphism

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

assocociated to $\mathscr{C}$, where $\mathrm{SL}_2(\mathbb{Z})$ is the group of 2-by-2 matrices with integer coefficients and unit determinant. The group $\mathrm{SL}_2(\mathbb{Z})$ is sometimes known as the *modular group*, due to its connection with moduli spaces of elliptic curves. Hence, $\rho_{\mathscr{C}}$ is known as the *modular representation* of $\mathscr{C}$.

The goal of this chapter is to introduce $\rho_{\mathscr{C}}$, show it is well defined, and then prove a series of theorems related to $\rho_{\mathscr{C}}$.

Before defining $\rho_{\mathscr{C}}$, we recall the basic group theory of $\mathrm{SL}_2(\mathbb{Z})$. It is generated by the matrices

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

These two matrices satisfy the relations $s^2 = -1$ and $(st)^3 = -1$, where 1 is used the represent the identity matrix. These relations generate $\mathrm{SL}_2(\mathbb{Z})$, in the sense that we have the following presentation:

Proposition 5.14. *The following presentation is valid:*

$$\mathrm{SL}_2(\mathbb{Z}) = \left\langle s, t \,\middle|\, s^4 = 1,\ (st)^3 = s^2 \right\rangle.$$

Proof. This is a standard fact about $\mathrm{SL}_2(\mathbb{Z})$. Se for instance [WORK: ref]. □

Hence, to define a homomorphism $\rho_{\mathscr{C}} : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Aut}(\mathbb{C}[\mathcal{L}])$ it suffices to choose automorphisms $\rho_{\mathscr{C}}(s)$, $\rho_{\mathscr{C}}(t)$ of $\mathbb{C}[\mathcal{L}]$, and show that they satisfy the relations $\rho_{\mathscr{C}}(s)^4 = 1$ and $(\rho_{\mathscr{C}}(s)\rho_{\mathscr{C}}(t))^3 = \rho_{\mathscr{C}}(s)^2$. Since $\mathbb{C}[\mathcal{L}]$ has a canonical basis, we can think of its automorphisms as being matrices with rows and collumns labeled by $\mathcal{L}$. We define an operator $S : \mathbb{C}[\mathcal{L}] \to \mathbb{C}[\mathcal{L}]$ via the matrix coeffients

$S_{A,B} =$ 

We next define the matrix $T : \mathbb{C}[\mathcal{L}] \to \mathbb{C}[\mathcal{L}]$ to be the diagonal matrix with $([A],[A])$-entry θ_A, for all $[A] \in \mathcal{L}$.

As currently stated, the S and T matrices defined do not satify $S^4 = 1$ and $(ST)^3 = S^2$. They only satisfy these formula up to phases in $\mathbb{C}$. They still need to be normalized before we can defined $\rho_{\mathbb{C}}$. The normalization factors come in terms of the *Gauss sums*,

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

We can now state the main theorem of this chapter:

Theorem 5.2. *Let $\mathscr{C}$ be a modular category. The values $p_{\mathscr{C}}^{+}$ and $p_{\mathscr{C}}^{-}$ are nonzero, and the map*

$$\begin{aligned} \rho_{\mathscr{C}} : \mathrm{SL}_2(\mathbb{Z}) &\to \mathrm{Aut}(\mathbb{C}[\mathcal{L}]) \\ s &\mapsto \frac{1}{\mathcal{D}} \cdot S \\ t &\mapsto \left(p_{\mathscr{C}}^{-}/p_{\mathscr{C}}^{+}\right)^{1/6} \cdot T \end{aligned}$$

is a group homomorphism.

We will prove this theorem and motivate why it should be true over the course of this chapter. We will also prove key facts about the image and kernel of this representation, as well as other formulas of interest relating to twists, S-matrix entries, and Gauss sums.

5.5.2 Torus perspective

It's good to reflect on why MCs have $\mathrm{SL}_2(\mathbb{Z})$ representations assocated with them in the first place. Not only does the representation exist, but it is so fundamental to the modular category that it is chosen as the namesake. This begs the question. What's going on?

The answer has to do with topological phases on the torus.

[WORK: add torus]

Every modular category $\mathscr{C}$ is supposed to describe a topological order. Up to now we have only considered what happens when this topological order is applied to an infnitely large flat sheet. We have not examined what happens when this topological order is put on a space with nontrivial topology. For instance, the torus. Suppose we analyse the system of $\mathscr{C}$ applied to the torus. This amounts to breaking up the torus into some microscopic lattice and applying some Hamiltonian. This Hamiltonian will have group states $V_{\text{g.s.}}^{T^2}$, which are independent of the choice of microscopic realization of $\mathscr{C}$.

Suppose we start with a torus, cut it across, twist one of its legs, then glue it back together, as shown below:

[WORK: add Dehn twist picture.]

If the initial torus has some state $|\psi\rangle \in V_{\text{g.s.}}^{T^2}$ on it, then applying this procedure would give back another group state, though possibly a different one. The key phenominon is that continues transformations on physical space correspond to linear transformations on state space:

[WORK: add schematic.]

We can make this more formal as follows. We define the *mapping class group* of a topological space X as follows:

$$\mathrm{MCG}(X) = (\text{homeomorphisms } X \to X)/(\text{continuous deformations}).$$

If two homeomorphisms can be continuously deformed from one another then they will act the same on the ground states $V_{\text{g.s.}}^{T^2}$. This is because ground states are topologically

protected and hence slowly changing the diffeomorphism cannot affect them. Hence, we get a well-defined group homomorphism

$$\rho_{\mathscr{C}}^{T^2} : \mathrm{MCG}(T^2) \to \mathrm{Aut}\left(V_{\mathrm{g.s.}}^{T^2}\right).$$

This homomorphism connects back to our modular representation as follows:

- **Claim 1:** $\mathrm{MCG}(T^2) \cong \mathrm{SL}_2(\mathbb{Z})$;
- **Claim 2:** $V_{\mathrm{g.s.}}^{T^2} \cong \mathbb{C}[\mathcal{L}]$;
- **Claim 3:** $\rho_{\mathscr{C}}^{T^2} \cong \rho_{\mathscr{C}}$, passing through the identifications in claims 1 and 2.

In general, we see that associated to every modular category $\mathscr{C}$ there should not only be a modular representation, but also a representation of $\mathrm{MCG}(\Sigma)$ for many other choices of topological space Σ. For instance, if $\Sigma = \Sigma_g$ is the g-holed torus then putting $\mathscr{C}$ on Σ_g we get a map

$$\rho_{\mathscr{C}}^{\Sigma_g} : \mathrm{MCG}(\Sigma_g) \to \mathrm{Aut}(V_{\mathrm{g.s.}}^{\Sigma_g}).$$

[WORK: maybe say a few words about these representations. I'm sure they must have an explicit description in terms of generators and relations. A good reference (though a bit early) is this one: [Lyu95]]

We now examine and motivate claims 1-3.

Claim 1: $\mathrm{MCG}(T^2) \cong \mathrm{SL}_2(\mathbb{Z})$. This claim is best seen by thinking of the torus as a a gluing diagram,

[WORK: add gluing diagram]

[WORK: add diagram with s acting by rotating by 90 degrees. Clearly, $s^4 = 1$.]

[WORK: add diagram with t as a shift. $(st)^3 = s^2$ can be left as an exercise.]

[WORK: writing presentation for $MCG(T^2)$, note that it is the same as $\mathrm{SL}_2(\mathbb{Z})$.

Claim 2: $V_{\mathrm{g.s.}}^{T^2} \cong \mathbb{C}[\mathcal{L}]$.

[WORK: explain this. Cut into cylinder, label by charge on boundary]

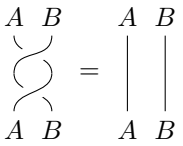
Claim 3: $\rho_{\mathscr{C}}^{T^2} \cong \rho_{\mathscr{C}}$.

[WORK: Showing that the Dehn twist acts diagonally by θ_A is obvious. θ_A and Dehn twist are both defined as a 2π twist. For S we need another argument, more subtle but not too hard. I think Simon has it.]

[WORK: Finish by saying this is something like TQFTs. TQFT = bundled collection of mapping class group representations. Link this to TQFT appendix.]

5.5.3 Bruguieres's modularity theorem and the Verlinde formula

In this section we prove Bruguieres's modularity theorem. This theorem asserts that, given a pre-modular category $\mathscr{C}$, the S-matrix S is invertible if and only if $\mathscr{C}$ is modular. Historically, this theorem is backwards. The original definition of modular category included that the S-matrix should be invertible. This was the only definition of modular category, until Bruguieres proved in [ref] that the invertability of the S-matrix is equivalent to $\mathscr{C}$ having the non-degenerate braiding property that if



for all $B \in \mathscr{C}$ then $A \cong \mathbf{1}$. We are thus stating a historically incorrect definition of modular category, and Bruguieres's modularity theorem tells us that this is equivalent to the original definition. The proof of the modularity theorem relies on the *Verlinde algebra* of $\mathscr{C}$. This algebra will be of use for us in proving other theorems in the future, in particular the Verlinde formula in section [ref].

We define an *algebra* over $\mathbb{C}$ to a vector space V paired with a bilinear map $\cdot : V \times V \to V$ called multiplication, such that multiplication is associative and has a unit. An algebra is called *commutative* if its multiplication is commutative.

We define the Verlinde algebra $K_{\mathbb{C}}(\mathscr{C})$ of $\mathscr{C}$ as follows:

$$K_{\mathbb{C}}(\mathscr{C}) = \left\{ \mathbb{C}[\mathcal{L}] \text{ with algebra structure } |[A]\rangle \cdot |[B]\rangle = \sum_{[C]\in\mathcal{L}} N_C^{A,B} |[C]\rangle \right\}.$$

We additionally define the function algebra

$$\mathbb{C}[\mathcal{L}]^{\text{func}} = \left\{ \mathbb{C}[\mathcal{L}] \text{ with algebra structure } \left(\sum_{[A]\in\mathcal{L}} c_A |[A]\rangle\right) \cdot \left(\sum_{[A]\in\mathcal{L}} c'_A |[A]\rangle\right) = \sum_{[A]\in\mathcal{L}} c_A c'_A |[A]\rangle \right\}.$$

Lemma 5.2. *Both $K_{\mathbb{C}}(\mathscr{C})$ and $\mathbb{C}[\mathcal{L}]^{func}$ are commutative algebras.*

Proof. The fact that $K_{\mathbb{C}}(\mathscr{C})$ is associative follows from the associativity of the tensor product. Its unit is $|[\mathbf{1}]\rangle$. It is commutative because $\mathscr{C}$ is braided. The fact that $\mathbb{C}[\mathcal{L}]^{\text{func}}$ is a commutative algebra is a standard exercise in algebra. Its unit is $\sum_{[A]\in\mathcal{L}} |[A]\rangle$. □

We now state and prove the core theorem which underlies the core properties of the S matrix:

Proposition 5.15. *The map*

$$\begin{aligned} \mathcal{S} : K_{\mathbb{C}}(\mathscr{C}) &\to \mathbb{C}[\mathcal{L}]^{func} \\ |[A]\rangle &\mapsto \sum_{[B]\in\mathcal{L}} \frac{1}{d_B} S_{B,A} |[B]\rangle \end{aligned}$$

is a morphism of algebras.

Proof. Since it was defined on a basis, $\mathcal{S}$ is clearly a linear map. We now verify that $\mathcal{S}$ preserves multiplication. In the below computation, we identity endomorphisms of simple objects with the unique scalar they are times the identity. We let A, B, D be simple objects.

$$\left(\tfrac{1}{d_D}S_{D,A}\right)\left(\tfrac{1}{d_D}S_{D,B}\right) = \left(A \otimes \overset{D}{\underset{D}{\cap}} \right) \cdot \left(B \otimes \overset{D}{\underset{D}{\cap}} \right) = \left(\begin{array}{c} D \\ B \otimes \\ A \otimes \\ D \end{array} \right)$$

$$= \left(A \otimes B \otimes \overset{D}{\underset{D}{\cap}} \right) = \sum_{[C]\in\mathcal{L}} N_C^{A,B} \cdot \left(C \otimes \overset{D}{\underset{D}{\cap}} \right)$$

$$= \sum_{[C]\in\mathcal{L}} N_C^{A,B} \left(\tfrac{1}{d_D}S_{D,C}\right).$$

Note our key use of the fact that

$$B \oplus C \otimes \overset{A}{\underset{A}{\cap}} = B \otimes \overset{A}{\underset{A}{\cap}} + C \otimes \overset{A}{\underset{A}{\cap}}$$

which follows from the facts that $\mathrm{id}_{B\oplus C}$ can be decomposed as projection onto B plus projection onto C, and composition is bilinear. We now conclude that

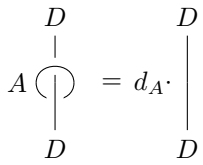
$$\begin{aligned}
\mathcal{S}\left(|[A]\rangle\right) \cdot \mathcal{S}\left(|[B]\rangle\right) &= \sum_{[D]\in\mathcal{L}} \left(\frac{1}{d_D}S_{D,A}\right)\left(\frac{1}{d_D}S_{D,B}\right)|[D]\rangle \\
&= \sum_{[D]\in\mathcal{L}} \left(\sum_{[C]\in\mathcal{L}} N_C^{A,B} \left(\frac{1}{d_D}S_{D,C}\right)\right)|[D]\rangle \\
&= \mathcal{S}\left(|[A]\rangle \cdot |[B]\rangle\right)
\end{aligned}$$

as desired. □

By Proposition [ref], we have constructed a map of algebras $\mathcal{S} : K_{\mathbb{C}}(\mathscr{C}) \to \mathbb{C}[\mathcal{L}]^{\mathrm{func}}$. As a map of vector spacces, $\mathcal{S}$ is equal to the S-matrix up to a rescaling of rows by nonzero factors. Hence, it is clear that the S-matrix is invertible if and only if the algebra map $\mathcal{S}$ is invertible. We now use special properties of the map $\mathcal{S}$ to prove the main theorem of the section:

Theorem 5.3 (Bruguieres's modularity theorem)**.** *Let $\mathscr{C}$ be a pre-modular category. The braiding on $\mathscr{C}$ satisfies the non-degenerate braiding axiom if and only if the S-matrix is invertible.*

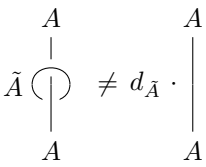
Proof. We observe that $\mathscr{C}$ has a degenerate braiding if and only if there exists some $A \ncong \mathbf{1}$ such that



for all $D \in \mathscr{D}$. If such an element A exists, then clearly $\mathcal{S}(|[A]\rangle) = d_A \mathcal{S}(|[1]\rangle)$. Hence, two linearly independent vectors map to linearly dependent vectors and thus $\mathcal{S}$ is not invertible. Thus, the invertibilty of the $\mathcal{S}$-matrix implies that the braiding is non-degenerate.

We now prove the converse, and hence we suppose that $\mathscr{C}$ has nondegenerate braiding. The proof is in two main steps. First, we prove that $|[\mathbf{1}]\rangle$ is in the image of $\mathcal{S}$. Then, we use the fact that $|[\mathbf{1}]\rangle$ is in the image of $\mathcal{S}$ to construct the rest of the image, which proves that $\mathcal{S}$ is surjective hence invertible.

Part 1: $|[\mathbf{1}]\rangle$ is in the image of $\mathcal{S}$. Since $\mathscr{C}$ has nondegenerate braiding, for all simple objects $A \ncong \mathbf{1}$ there exists some simple object $\tilde{A}$ such that



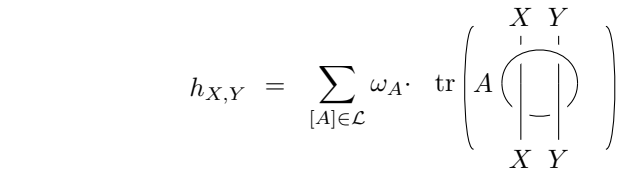
Thus, the vector $\mathcal{S}(|[\tilde{A}]\rangle) - \frac{S_{A,\tilde{A}}}{d_A}\mathcal{S}(|[\mathbf{1}]\rangle)$ has a cooficient zero of for $|[A]\rangle$ but a non-zero cooficient for $|[\mathbf{1}]\rangle$. Thus, using the product structure on $\mathbb{C}[\mathcal{L}]^{\text{func}}$, we find that the vector

$$\prod_{\substack{[A]\in\mathcal{L}\\ A\ncong\mathbf{1}}} \left(\mathcal{S}(|[\tilde{A}]\rangle) - \frac{S_{A,\tilde{A}}}{d_A}\mathcal{S}(|[\mathbf{1}]\rangle)\right)$$

has a cooficient of zero for all $|[A]\rangle$, $A \ncong \mathbf{1}$, but a non-zero cooficient of $|[\mathbf{1}]\rangle$. Hence, it is a scalar multiple of $|[\mathbf{1}]\rangle$. Since $\mathcal{S}$ is a morphism of algebras, it is in the image of $\mathcal{S}$. Hence, $|[\mathbf{1}]\rangle$ is in the image of $\mathcal{S}$.

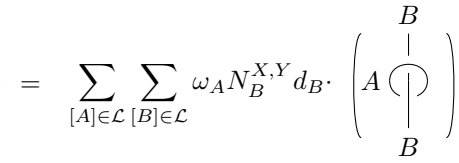
This completes the first part of the proof. We now use the fact that $|[\mathbf{1}]\rangle$ is in the image of $\mathcal{S}$ to construct the rest of the vectors.

Part 2: $\mathcal{S}$ is surjective. Let $\omega = \sum_{[A]\in\mathcal{L}} \omega_A |[A]\rangle \in K_{\mathbb{C}}(\mathscr{C})$ be a vector such that $\mathcal{S}(\omega) = |[\mathbf{1}]\rangle$, which exists by part 1 of the proof. We now compute the quantity

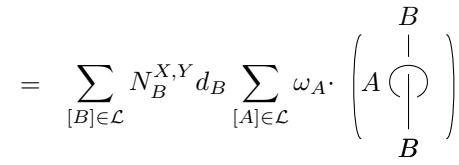


two ways, for all simple objects $X, Y \in \mathscr{C}$. The first way folllows by expanding $X \otimes Y$ as a direct sum and using the fact that $\mathcal{S}(\omega) = |[\mathbf{1}]\rangle$:

$$h_{X,Y} = \sum_{[A]\in\mathcal{L}} \sum_{[B]\in\mathcal{L}} \omega_A N_B^{X,Y} d_B \cdot$$



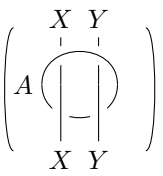
$$= \sum_{[B]\in\mathcal{L}} N_B^{X,Y} d_B \sum_{[A]\in\mathcal{L}} \omega_A \cdot$$



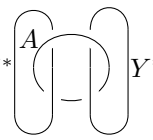
$$= N_{\mathbf{1}}^{X,Y} d_1 = \begin{cases} 1, & X \cong Y^* \\ 0, & \text{otherwise.} \end{cases}$$

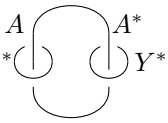
In our second way of computing $h_{X,Y}$, we relate the string diagram trace to S-matrix values:

$$\mathrm{tr}$$



$$=$$





$$= \tfrac{1}{d_A} S_{X,A} S_{Y,A}$$

and thus, combining our two computations, we find

$$h_{X,Y} = \sum_{[A]\in\mathcal{L}} \frac{\omega_A}{d_A} S_{X,A} S_{Y,A} = \begin{cases} 1 & X \cong Y^* \\ 0 & \text{otherwise.} \end{cases}$$

We now define the vector

$$\omega^{(X)} = \sum_{[A]\in\mathcal{L}} \frac{\omega_A}{d_A} S_{A,X^*} \left|[A]\right\rangle$$

for all simple objects $X \in \mathscr{C}$. We compute

$$\begin{aligned} \mathcal{S}(\omega^{(X)}) &= \sum_{[A]\in\mathcal{L}} \frac{\omega_A}{d_A} S_{A,X^*} \left(\sum_{[Y]\in\mathcal{L}} \frac{1}{d_Y} S_{A,Y} \left|[Y]\right\rangle \right) \\ &= \sum_{[Y]\in\mathcal{L}} \frac{1}{d_Y} \left(\sum_{[A]\in\mathcal{L}} \frac{\omega_A}{d_A} S_{A,X^*} S_{A,Y} \right) \left|[Y]\right\rangle \\ &= \sum_{[Y]\in\mathcal{L}} \frac{h_{X^*,Y}}{d_Y} \left|[Y]\right\rangle = \frac{1}{d_X} \left|[X]\right\rangle . \end{aligned}$$

Hence $|[X]\rangle$ is in the image of $\mathcal{S}$ for $[X] \in \mathcal{L}$, as desired.

□

5.5.4 Verlinde formula

In this section, we prove the *Verlinde formula*. This formula was first conjectured by Verlinde [Ver88], and proven the following year by Moore-Seiberg [MS89]. There are now many Verlinde-type formulas. Most imporantly, there is one for vertex operator algebras [Hua08] and one in algebraic geometry [Fal94]. With proposition [ref] in hand, the proof is very quick:

Theorem 5.4 (Verlinde formula)**.** *Let $\mathscr{C}$ be a modular category.*

(i) For all simple objects $A, B, C \in \mathscr{C}$,

$$N_C^{A,B} = \sum_{[E] \in \mathcal{L}} \frac{S_{A,E} S_{B,E} \left(S^{-1}\right)_{C,E}}{d_E}$$

where $(S^{-1})_{C,E}$ denotes the (C,E)-coefficeint of the inverse of the S matrix.

(ii) For all simple objects $A \in \mathscr{C}$, the matrix

$$D^A = S N^A S^{-1}$$

is diagonal with $([B],[B])$-entry $S_{A,B}/d_B$, where $N^A = (N_C^{A,B})_{([B],[C]) \in \mathcal{L}^2}$ is the fusion matrix of A.

Proof. We begin by proving part (ii). The main observation of the proof is that that the operator $N^A : \mathbb{C}[\mathcal{L}] \to \mathbb{C}[\mathcal{L}]$ is exactly left multiplication by A in $K_{\mathbb{C}}(\mathscr{C})$. Proposition [ref] says that $\mathcal{S}$ is a morphism of algebras, and hence we can commute N^A past $\mathcal{S}$, and turn it into multiplication by A in $\mathbb{C}[\mathcal{L}]^{\text{func}}$. Hence, using the appropriate multiplication in the appropriate algebra, we find

$$\begin{aligned}
\left(\mathcal{S} N^A \mathcal{S}^{-1}\right) |[B]\rangle &= \mathcal{S}\left(|[A]\rangle \cdot_{K_{\mathbb{C}}(\mathscr{C})} \mathcal{S}^{-1}(|[B]\rangle)\right) \\
&= \mathcal{S}(|A\rangle) \cdot_{\mathbb{C}[\mathcal{L}]^{\text{func}}} |[B]\rangle \\
&= \frac{S_{A,B}}{d_B} |[B]\rangle .
\end{aligned}$$

Thus, $\mathcal{S} N^A \mathcal{S}^{-1}$ is diagonal with $([B],[B])$ entry $S_{A,B}/d_B$. Scaling rows of $\mathcal{S}$ does not change the effect of diagonalizition. Hence, we conclude that $S N^A S^{-1}$ is diagonal as well, with the same entries, and thus our proof of (ii) is complete.

We now move on to proving part (i). Expanding the formula $N^A = S^{-1} D^A S$, we find

$$
\begin{aligned}
N^A\,|[B]\rangle &= S^{-1}D^A S\,|[B]\rangle \\
&= S^{-1}\left(\sum_{[E]\in\mathcal{L}} \frac{S_{A,E}S_{B,E}}{d_E}\,|[E]\rangle\right) \\
&= \sum_{[E]\in\mathcal{L}} \frac{S_{A,E}S_{B,E}}{d_E}\left(\sum_{[C]\in\mathcal{L}} (S^{-1})_{C,E}\,|[C]\rangle\right).
\end{aligned}
$$

Comparing coeffients with the definition of N^A, we conclude the result.

□

5.5.5 Proof of modularity

In this section we prove that the S-matrix and T-matrix indeed give a representation of the modular group. That is, we will prove Theorem [ref]. At its heart, the fact that the modular representation of modular category is a homomorphisms comes down to proving a series of relations between the coeffients of the S-matrix and the coeffients of the T-matrix. That is, we are proving a series of relations between braiding and twisting. The general method is to take traces of certain diagrams, and then compute those traces in two ways. One way will involve more twists and the other will involve more braiding. This will give some algebraic relation, and choosing the right diagrams we will get enough algebraic relations to deduce Theorem [ref].

We begin with the most fundamental relationship between S-matrix and T-matrix entries:

Lemma 5.3. *Let $\mathscr{C}$ be a pre-modular category. We have that*

$$S_{A,B} = \theta_A^{-1}\theta_B^{-1}\sum_{[C]\in\mathcal{L}} N_C^{A,B}\theta_C d_C$$

and

$$S_{A^*,B} = \theta_A\theta_B\sum_{[C]\in\mathcal{L}} N_C^{A,B}\theta_C^{-1} d_C.$$

Proof. By Proposition [ref], we have $\beta_{B,A}\circ\beta_{A,B} = (\theta_A^{-1}\otimes\theta_B^{-1})\circ\theta_{A\otimes B}$. Taking the trace of this formula we get

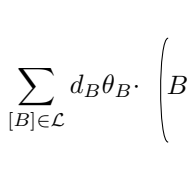
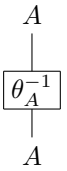
$$S_{A,B} = \theta_A^{-1}\theta_B^{-1}\operatorname{tr}(\theta_{A\otimes B}).$$

Now, since θ is a natural transformation it splits over direct sums. Traces split over direct sums as well by proposition [ref] and hence $\operatorname{tr}(\theta_{A\otimes B}) = \sum_{[C]\in\mathcal{L}} N_C^{A,B}\theta_C d_C$. This concludes the proof of the first formula.

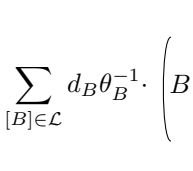
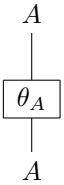
For the second formula, we observe that replacing overcrossings with undercrossings in the definition of $S_{A,B}$ has the effect of taking the dual of one of elements, replacing it with $S_{A^*,B}$. Hence $\operatorname{tr}(\beta_{A,B}^{-1}\circ\beta_{B,A}^{-1}) = S_{A^*,B}$. Thus, taking the trace of the formula $\beta_{A,B}^{-1}\circ\beta_{B,A}^{-1} = \theta_{A\otimes B}^{-1}\circ(\theta_A\otimes\theta_B)$ yields the desired result. □

Before continuing to our proof of theorem [ref] we observe a key lemma:

Lemma 5.4. *Let $\mathscr{C}$ be a pre-modular category. Let $A \in \mathscr{C}$ be a (possibly non-simple) object. We have that*

$$\sum_{[B]\in\mathcal{L}} d_B\theta_B \cdot$$  $$= p^+_{\mathscr{C}} \cdot$$ 

and

$$\sum_{[B]\in\mathcal{L}} d_B\theta_B^{-1} \cdot$$  $$= p^-_{\mathscr{C}} \cdot$$ 

Proof. We only prove the first formula - the second follows by a formally dual argument. We restrict to the case that A is simple. Seeing as both sides are linear with respect to direct sums, the case that A is simple will immedaitely imply the general case. Since A is simple, it suffices to prove that the traces of both sides are equal. The trace on the left hand side has the effect of replacing the diagram with $S_{A,B}$. Hence, we compute as follows using Lemma [ref] and the fact that $\sum_{[C]\in\mathcal{L}} N_C^{A,B} d_B = d_A d_C$ from proposition [ref]:

$$\begin{aligned}
\sum_{[B]\in\mathcal{L}} d_B\theta_B S_{A,B} &= \sum_{[B]\in\mathcal{L}} d_B\theta_B \left(\theta_A^{-1}\theta_B^{-1} \sum_{[C]\in\mathcal{L}} N_C^{A,B}\theta_C d_C \right) \\
&= \theta_A^{-1} \sum_{[C]\in\mathcal{L}} \theta_C d_C \left(\sum_{[B]\in\mathcal{L}} N_C^{A,B} d_B \right) \\
&= \theta_A^{-1} d_A \sum_{[C]\in\mathcal{L}} \theta_C d_C^2 = p^+_{\mathscr{C}}\theta_A^{-1} d_A.
\end{aligned}$$

This result is exact the trace of the right hand sides of the lemma. Hence, the proof is complete. □

We now give the heart of the proof of theorem [ref]:

Theorem 5.5. *Let $\mathscr{C}$ be a pre-modular category. Define the charge conjugation operator $\check{C} : \mathbb{C}[\mathcal{L}] \to \mathbb{C}[\mathcal{L}]$ to the matrix with $([A], [A^*])$ coefficient 1 for all $[A] \in \mathcal{L}$, and all other coefficients zero.*

(i) $\check{C}S = S\check{C}$, $\check{C}T = T\check{C}$, *and* $\check{C}^2 = 1$;

(ii) $(ST)^3 = p^+_{\mathscr{C}} S^2$;

(iii) $(ST^{-1})^3 = p^-_{\mathscr{C}} S^2 \check{C}$.

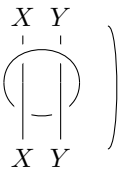
If $\mathscr{C}$ is modular, then

(iv) $S^2 = p_{\mathscr{C}}^+ p_{\mathscr{C}}^- \check{C}$.

Proof. Part (i) follows from the fact that $S_{A^*,B^*} = S_{A,B}$, $\theta_{A^*} = \theta_A$, and $A^{**} \cong A$. Parts (ii) and (iii) have formally dual proofs, which arise from replacing θ with θ^{-1} at every opportunity. Part (iv) follows algebraically from combining formulas (ii) and (iii) whenever S is invertible, which is always the case when $\mathscr{C}$ is modular by theorem [ref].

Hence, it suffices to prove part (ii). The proof comes from comuting the quantity

$$h_{X,Y} \;=\; \sum_{[A]\in\mathcal{L}} d_A\theta_A \cdot \operatorname{tr}\Bigg($$

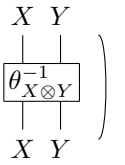


$$\Bigg)$$

two ways.

In the first way of computing $h_{X,Y}$, we use lemma [ref]. We find the following:

$$h_{X,Y} \;=\; p_{\mathscr{C}}^+ \cdot \;\operatorname{tr}\Bigg($$



$$\Bigg) = p_{\mathscr{C}}^+ \theta_X \theta_Y S_{X^*,Y}$$

In our second way of computing $h_{X,Y}$, we use computation of the trace of two lines through a loop in the proof of Theorem [ref]. We find this way that

$$h_{X,Y} = \sum_{[A]\in\mathcal{L}} \theta_A S_{X,A} S_{Y,A}.$$

Thus, we find that $\sum_{[A]\in\mathcal{L}} \theta_A S_{X,A} S_{Y,A} = p_{\mathscr{C}}^+ \theta_X \theta_Y S_{X^*,Y}$. Thinking of these quantites as the $([X],[Y])$ entries in operators $\mathbb{C}[\mathcal{L}] \to \mathbb{C}[\mathcal{L}]$, we get the equation

$$STS = p_{\mathscr{C}}^+ TST\check{C}.$$

.[WORK: This formula is WRONG. It should be

$$STS = p_{\mathscr{C}}^+ T^{-1} S T^{-1}.$$

From this we get

$$(ST)^3 = p_{\mathscr{C}}^+ S^2$$

as desired. I'm not sure where I went wrong, but something is off in here.] □

We now know that the S and T matrices give a modular representation *up to phase*! We still need to work out the details of the phases. A key part is the following computation:

Corollary 5.6. *Let $\mathscr{C}$ be a modular category. The quantities $p_{\mathscr{C}}^+$ and $p_{\mathscr{C}}^-$ are nonzero, and*

$$p_{\mathscr{C}}^+ p_{\mathscr{C}}^- = \mathcal{D}^2.$$

Proof. The values $p_{\mathscr{C}}^+$ and $p_{\mathscr{C}}^-$ must be nonzero because S is invertible and $S^2 = p_{\mathscr{C}}^+ p_{\mathscr{C}}^- \check{C}$. The formula $S^2 = p_{\mathscr{C}}^+ p_{\mathscr{C}}^- \check{C}$, when expanded, says that

$$\sum_{[C]\in\mathcal{L}} S_{C,A} S_{C,B} = \begin{cases} p_{\mathscr{C}}^+ p_{\mathscr{C}}^- & A \cong B^* \\ 0 & \text{otherwise.} \end{cases}$$

Applying this formula to $A = B = \mathbf{1}$, we find

$$\sum_{[C]\in\mathcal{L}} S_{C,\mathbf{1}} S_{C,\mathbf{1}} = \sum_{[C]\in\mathcal{L}} d_C^2 = p_{\mathscr{C}}^+ p_{\mathscr{C}}^-$$

as desired. □

Now, it is clear that we can normalize the representation appropriately and conclude theorem [ref], as desired.

5.5.6 Vafa's theorem, unitarity of S-matrix, and the Chiral central charge

In this section we discuss some finer points of the structure of the modular representation. In particular, we will prove that modular representation of every modular category is *unitary*. That is, the S and T matrices are both unitary operators on $\mathbb{C}[\mathcal{L}]$ when it is endowed with its canonical inner product coming from its basis

We begin with the matrix T. For a diagonal matrix to be unitary, it is neccecary and sufficient for its diagonal entries to have absolute value 1. We will prove something even stronger: that all of the entries are roots of unity! We recall that a number $z \in \mathscr{C}$ is called a root of unity if $z^n = 1$ for some integer $n \geq 1$. We begin with a key topological lemma which will underscore our proof:

Lemma 5.5 (Lantern identity)**.** *Let $\mathscr{C}$ be a pre-modular category. Let $A, B, C \in \mathscr{C}$ be objects. As maps $A \otimes B \otimes C \to A \otimes B \otimes C$, we have the identity*

$$\theta_{A\otimes B} \circ \theta_{A\otimes C} \circ \theta_{B\otimes C} = \theta_{A\otimes B\otimes C} \circ (\theta_A \otimes \theta_B \otimes \theta_C).$$

Proof. In the language of string diagrams, this formula becomes

[WORK: add diagram.]

It is a matter of elementary manipulations to convince one's self that these two diagrams are equal. An alternate algebraic approach is to expand the relation both sides using the formula $\theta_{X\otimes Y} = (\beta_{Y,X} \circ \beta_{X,Y}) \circ (\theta_X \otimes \theta_Y)$, cancel $\theta_A^2 \otimes \theta_B^2 \otimes \theta_C^2$, and compare the resulting braids using the hexagon and naturality. □

We state one more linear-algebraic lemma neccecary for the proof:

Lemma 5.6. *Let $n \geq 1$ be an integer and let $M : \mathbb{R}^n \to \mathbb{R}^n$ be a linear operator whose (a, b) entry is $M_{a,b}$. Suppose that all off diagonal entries of M are positive, and that $\sum_{b=1}^n M_{a,b} < 0$ for all $1 \leq a \leq n$. Then, M is invertible.*

Proof. .[WORK: This follows from the Gershgorin circle theorem, but that's way to general for our purposes. Find a nice proof which is appropriate for the situation.] □

Theorem 5.6 (Vafa)**.** *Let $\mathscr{C}$ be a pre-modular category. The values θ_A are roots of unity for all simple object $A \in \mathscr{C}$.*

Remark. This theorem is interesting in part due to its history. [WORK: add history.]

Proof. To begin, we choose a simple obejct A. We observe that every endomorphism of $A \otimes A^* \otimes A$ induces a linear map

$$\mathrm{Hom}(A, A \otimes A^* \otimes A) \to \mathrm{Hom}(A, A \otimes A^* \otimes A)$$

by postcomposition. We now consider the lantern identity (proposition [ref]) on the stands A, A^*, A,

$$\theta_{A\otimes A^*} \circ \theta_{A\otimes A} \circ \theta_{A^*\otimes A} = \theta_{A\otimes A^*\otimes A} \circ (\theta_A \otimes \theta_{A^*} \otimes \theta_A).$$

viewed as an equality of linear operators on $\mathrm{Hom}(A, A \otimes A^* \otimes A)$. We compute the determinant of both sides. We first compute the determinant of $\theta_{A\otimes A^*}$. The eigenvalues of the operator $\theta_{A\otimes A^*}$ are the twists θ_B. The dimension of the θ_B eigenspace is exactly the dimension of the subspace of $\mathrm{Hom}(A, A\otimes A^*\otimes A)$ in which $A\otimes A^*$ fuse to B. The dimension of this space is $N_B^{A,A^*} N_A^{B,A} = (N_B^{A,A^*})^2$. The determinant is equal to the product of the eigenvalues counted with multiplicity, and hence

$$\det \theta_{A\otimes A^*} = \prod_{[B]\in\mathcal{L}} \theta_B^{\left(N_B^{A,A^*}\right)^2}.$$

Continuing this way for all the other twists and plugging them into the lantern identity we get

$$\prod_B \theta_B^{2\left(N_B^{A,A^*}\right)^2 + \left(N_B^{A,A}\right)^2} = \theta_A^{4\cdot \dim \mathrm{Hom}(A, A\otimes A^*\otimes A)}.$$

We now define the coefficients

$$M_{A,B} = \begin{cases} 2\left(N_B^{A,A^*}\right)^2 + \left(N_B^{A,A}\right)^2 & A \ncong B \\ 2\left(N_B^{A,A^*}\right)^2 + \left(N_B^{A,A}\right)^2 - 4 \cdot \dim \mathrm{Hom}(A, A\otimes A^*\otimes A) & A \cong B. \end{cases}$$

We observe that all of the off-diagonal entries of $M_{A,B}$ are positive and

$$\begin{aligned} \sum_{[B]\in\mathcal{L}} M_{A,B} &= \sum_{[B]\in\mathcal{L}} 2\left(N_B^{A,A^*}\right)^2 + \left(N_B^{A,A}\right)^2 - 4 \cdot \dim \mathrm{Hom}(A, A\otimes A^*\otimes A) \\ &= -\dim \mathrm{Hom}(A, A\otimes A^*\otimes A) < 0. \end{aligned}$$

Thus, by lemma [ref], we conclude that the matrix $M = (M_{A,B})_{([A],[B])\in\mathcal{L}^2} : \mathbb{C}[\mathcal{L}] \to \mathbb{C}[\mathcal{L}]$ is invertible. Let $\tilde{M}$ be the adjugate of M. That is, an integer valued matrix such that $M \cdot \tilde{M} = \tilde{M} \cdot M = n$ where $n = \det M$. We find for all simple objects A that

$$\theta_A^n = \prod_{[C]\in\mathcal{L}} \left(\prod_{[B]\in\mathcal{L}} \theta_B^{M_{C,B}} \right)^{\tilde{M}_{A,C}} = 1,$$

and hence θ_A is a root of unity as desired.

□

We immediately get several corollaries from this theorem. The first is that braiding enough times gets you back where you started:

Corollary 5.7. *Let $\mathscr{C}$ be a pre-modular category. There exists an integer $n \geq 1$ such that*

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

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

Proof. Choose $n \geq 1$ so that $\theta_C^n = 1$ for all simple objects $C \in \mathscr{C}$, which exists by Vafa's theorem (theorem [ref]). Seeing that $\beta_{B,A} \circ \beta_{A,B} = \theta_{A \otimes B} \circ (\theta_A^{-1} \otimes \theta_B^{-1})$, in the direc sum decomposition $A \otimes B \cong \bigoplus_{[C] \in \mathcal{L}} N_C^{A,B} \, |[C]\rangle$ the transformation $\beta_{B,A} \circ \beta_{A,B}$ acts by the scalar $\theta_C/(\theta_A \theta_B)$ on every $|[C]\rangle$ summand. Thus, $(\beta_{B,A} \circ \beta_{A,B})^n$ acts by $(\theta_C/(\theta_A \theta_B))^n = 1$ and thus $(\beta_{B,A} \circ \beta_{A,B})^n$ is the identity as desired. □

Corollary 5.8. *Let $\mathscr{C}$ be a modular category. The quantity $p_{\mathscr{C}}^-/p_{\mathscr{C}}^+$ is a root of unity.*

Proof. We take determinants. From $S^2 = p_{\mathscr{C}}^+ p_{\mathscr{C}}^- \check{C}$ we find that $\det(S)^2 = \pm p_{\mathscr{C}}^+ p_{\mathscr{C}}^-$, since $\det \check{C} = \pm 1$. From the formula $(ST)^3 = p_{\mathscr{C}}^+ S^2$ we find that

$$\left(p_C^+ / \det(S)\right)^2 = \det(T)^6$$

so $p_C^+/p_C^- = \pm \det(T)^6$. By Vafa's theorem $\det(T)$ is a root of unity. Hence, we conclude that p_C^+/p_C^- is a root of unity as desired. □

We take a moment to observe that the quantity $p_{\mathscr{C}}^-/p_{\mathscr{C}}^+$ is of great interest to physicists. It is related to the *chiral central charge* c_{top} of the theory by the formula

$$p_{\mathscr{C}}^-/p_{\mathscr{C}}^+ = e^{-\frac{2\pi i c_{\mathrm{top}}}{4}}.$$

[WORK: probably say a bit more? Maybe there will be a better spot somewhere else.]

We now move on to proving that the S matrix is unitary. The main technical ingredient is as follows:

Proposition 5.16. *Let $\mathscr{C}$ be a modular category. For all simple objects $A, B \in \mathscr{C}$ we have that $S_{A^*,B} = \overline{S_{A,B}}$.*

Proof. By the Verlinde formula [ref], we know that for all simple objects A there exists a vector $\mathbf{v}_B \in \mathbb{C}[\mathcal{L}]$ such that

$$N^A \mathbf{v}_B = \frac{S_{A,B}}{d_B} \mathbf{v}_B$$

for all simple objects A. Namely, $\mathbf{v}_B$ is the $[B]$-collumn of the S matrix. Let $\mathbf{v}_B^*$ be the row vector which is the Hermitian adjoint to $\mathbf{v}_B$. We have that

$$\mathbf{v}_B N^A \mathbf{v}_B = \frac{S_{A,B}}{d_B} |\mathbf{v}_B|^2.$$

Now, we observe that by Frobenius reciprocity (proposition [ref]) $(N^A)^\dagger = N^{A^*}$. Hence,

$$\begin{aligned}\mathbf{v}_B N^A \mathbf{v}_B &= \left(N^{A^*}\mathbf{v}_B\right)^* \mathbf{v_B} \\ &= \left(\frac{S_{A^*,B}}{d_B}\mathbf{v}_B\right)^* \mathbf{v_B} \\ &= \frac{\overline{S_{A^*,B}}}{d_B}|\mathbf{v}_B|^2.\end{aligned}$$

Comparing, we get the desired result.

□

We now get the following theorem:

Theorem 5.7 (Etingof-Nikshych-Ostrik)**.** *Every matrix in the image of the modular represention* $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Aut}(\mathbb{C}[\mathcal{L}])$ *is a unitary operator on* $\mathbb{C}[\mathcal{L}]$.

Proof. We already know by theorem [ref] and corollary [ref] that the normalized T-matrix is unitary. It thus suffices to show that the modular S matrix is unitary. From theorem [ref] we have that $\left(\frac{1}{\mathcal{D}}S\right)^{-1} = (\frac{1}{\mathcal{D}}S)\cdot\check{C}$. By proposition [ref] $(\frac{1}{\mathcal{D}}S)\cdot\check{C} = (\frac{1}{\mathcal{D}}S)^\dagger$ and thus $\frac{1}{\mathcal{D}}S$ is unitary as desired. □

5.6 Skeletonization

5.6.1 Principle

.[WORK: lots of big choices need to be made here. Do I call this the skeletonization, or do I call it something else? Do I work with multiplicity-free categories, or do I allow multiplicity? I don't know what the correct statements are or what the proofs look like so this section might be a tough one.]

5.6.2 F-symbols

5.6.3 R-symbols

5.6.4 θ-symbols

5.6.5 Reconstruction theorem

5.7 Quantum double modular categories

5.7.1 The Drinfeld center

A quantum double modular category is a special type of modular category. They are particularly important because many of the constructions of topological order only deal with quantum double modular categories. For instance, there are constructions of modular categories/topological order coming from the theory of tensor networks [ref], subfactors [ref], vertex operator algebras [ref], [WORK: add more sources]. All of these constructions only give quantum double modular categories. Hence, understanding quantum doubles is key to understanding how topological order work in practice.

At the heart of quantum doubles is a construction known as the *Drinfeld center*. In its most basic form the Drinfeld center induces an assignment

$$\mathcal{Z} : (\text{monoidal categories}) \to (\text{braided monoidal categories}).$$

In our context, we care about a more structured version of the Drinfeld center. It is a theorem of Muger that the Drinfeld center induces an assignment as follows:

$$\mathcal{Z} : (\text{spherical fusion categories}) \to (\text{modular categories}).$$

This theorem is fantastic because it allows one to construct modular categories using much less data than would otherwise be neccecary. Without needing a braiding, non-degenerate or otherwise, the Drinfeld center allows one to construct a modular category. This makaes the Drinfeld center an abundant source of modular categories. We call an modular category $\mathscr{C}$ a quantum double if it is of the form $\mathcal{Z}(\mathscr{C}_0)$ for some spherical fusion category $\mathscr{C}_0$. A a major goal of this chapter is to set up and prove Muger's theorem

We now define the Drinfeld center. The Drinfeld center is a somewhat direct categorification of the usual notion of center for finite groups. If G is a finite group, its center is defined as follows:

$$Z(G) = \{g \in G | gh = hg \ \forall h \in G\}.$$

The first guess at $\mathcal{Z}(\mathscr{C})$ is thus

$$\mathcal{Z}(\mathscr{C}) = \{A \in \mathscr{C} | A \otimes B \cong B \otimes A \ \forall B \in \mathscr{C}\}.$$

This is almost correct, but not quite. The issue is that $\mathcal{Z}(\mathscr{C})$ is not quite a braided monoidal category yet. Even though $A \otimes B \cong B \otimes A$ for all $A, B \in \mathcal{Z}(\mathscr{C})$, we don't have a distinguished choice of isomorphism. A braided monoidal category requires a distinugished isomorphism $\beta_{A,B} : A \otimes B \xrightarrow{\sim} B \otimes A$. Moreover, these distinguished isomorphisms are required to satisfy the hexagon equations. Hence, we make a new definition of center which keeps track of the choice of isomorphism and enforces the hexagon equation along the way:

Proposition 5.17. *The Drinfeld center $\mathcal{Z}(\mathscr{C})$ of a monoidal category $\mathscr{C}$ is a braided monoidal category defined as follows:*

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

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

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

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

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

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

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

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

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

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

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

This condition makes the second hexagon identity tautological. Similarly, the definition of tensor product given is not strictly correct - one must add the correct associator terms, making the first hexagon identity immediate. Lastly one must verify the half-braidings defined on the tensor unit/tensor product are actually half braidings, i.e., that they satisfy the hexagon condition. These follow from straightforward computations, which we leave as exercises. This completes the proof.

□

5.7.2 Muger's theorem

[WORK: through Mueger's theorem. The exposition will greatly differ based on what the proof looks like, which I haven't done before.]

5.7.3 Discrete gauge theory as a quantum double and Morita equivalence

We saw in chapter [ref] that $\mathbf{Vec}_G$ anad $\mathrm{Rep}(G)$ are both naturally spherical fusion categories. Thus, Muger's theorem tells us that $\mathcal{Z}(\mathbf{Vec}_G)$ and $\mathcal{Z}(\mathrm{Rep}(G))$ are both modular categories. Hence, given a finite group G we have three different modular categories we can associate to it: $\mathfrak{D}(G)$, $\mathcal{Z}(\mathbf{Vec}_G)$, $\mathcal{Z}(\mathrm{Rep}(G))$. The amazing fact is that these are all the same category:

Proposition 5.18. *Let* G *be a finite group. There are equivalences of modular categories* $\mathfrak{D}(G) \cong \mathcal{Z}(\mathbf{Vec}_G) \cong \mathcal{Z}(\mathrm{Rep}(G))$.

Proof. .[WORK: do proof. Shouldn't be too hard.] □

We now make a few comments about this theorem. The first is that it proves that $\mathfrak{D}(G)$ is a quantum double modular category. Secondly, it gives a second proof that $\mathfrak{D}(G)$ has a non-degenearte braiding, using Muger's theorem. Thirdly, it demonstrates the concept of *Morita equivalence*.

[WORK: introduce Morita equivalence. I know that there's some important basic facts to tell - I should include those.]

5.7.4 Factorizability and time reversal symmetry

Given a modular category $\mathscr{C}$, we can forget the braiding on $\mathscr{C}$ and only remember its structure as a spherical fusion category. Hence, Muger's theorem tells us that $\mathcal{Z}(\mathscr{C})$ is canonically a modular category. It is a fantastic fact that in this case $\mathcal{Z}(\mathscr{C})$ can be explicitely computed in terms of $\mathscr{C}$. We describe this computation now.

[WORK: Define the time-reversal conjugate $\overline{\mathscr{C}}$. Setup the map $\mathscr{C} \boxtimes \overline{\mathscr{C}} \to \mathcal{Z}(\mathscr{C})$]

Proposition 5.19. *Let $\mathscr{C}$ be a pre-modular category. The canonical map $\mathscr{C} \boxtimes \overline{\mathscr{C}} \to \mathcal{Z}(\mathscr{C})$ is an equivalence of categories if and only if $\mathscr{C}$ is modular.*

Proof. .[WORK: do proof] □

This theorem is fantastic because it not only computes $\mathcal{Z}(\mathscr{C})$ for every modular category $\mathscr{C}$, but also it gives an equivalent definition of modularity. This gives us our third definition of modularity. Namely a pre-modular category $\mathscr{C}$ is modular if and only if its braidings are all non-degenerate, or equivalently if its S-matrix is non-degenerate, or equivalently if it is factorizable in the above sense.

5.7.5 Levin-Wen model

[WORK: work though the Levin-Wen model.

I think that this model is fantastic because it shows how all of the ideas of tensor category theory can manifest themselves extremely concretelely on the level of gapped Hamiltonians. Namely, the coherence relations on the category theory side correspond exactly the the formulas needed to make terms in a Hamiltonian commute with one another. It would be nice if I could give a motivation for which the category which describes the Levin-Wen model is the Drinfeld center, though I've never seen that before.]

5.8 Unitarity

5.8.1 Characterization of unitarizable modular categories

[WORK: the main theorem of this section is that a modular category is unitarizable if and only if it has positive quantum dimensions]

[WORK: there also needs to be mention of the fact that braiding is automatically unitary in a unitary category]

5.8.2 Uniqueness of unitary structure

5.8.3 Skeletonization of unitarity

5.9 Number theory in modular categories

5.9.1 .[prerequisites and introduction]

5.9.2 Galois conjugation

5.9.3 Ocneanu rigidity

5.9.4 Rank-finiteness theorem

5.9.5 Schauenberg-Ng theorem

.[WORK: Go through Schauenberg-Ng's original paper and understand the proof.

It seems on the face of it like it is a hard theorem. Certainly, it uses strongly the theory of the Drinfeld center as well as the modular representation. It is good to push this proof as far down as possible since it will use a lot of machinery. I think it can be boiled down to something elegant, though, if the machinery has been set up.]

.[WORK: this section is going to host a lot more theorems]

History and further reading:

Modular categories were born from conformal field theory in the late 1980s. In a series of papers, Moore and Seiberg analysed deeply the underlying content within conformal field theory to find what essential algebraic data lied within it [MS88, MS89]. They wrote out the axioms of this essential algebraic data in their subsequent notes on conformal field theory [MS90]. They used the name modular category to describe their data, as suggested by Igor Frenkel. This definition was then refined and re-introduced by Turaev [Tur92]. The first major application of modular categories was the Reshetikhin-Turaev construction [RT91, Tur10]. Prior to this result nobody had succeed in constructing topological quantum field theories. In this way, modular categories and the Reshetikhin-Turaev construction completed Witten's programme of quantizing Chern-Simons theory.

By the early 2000s, the proposal of topological quantum computing was attracting a lot of interest in anyons and their algebraic properties. Seeing as topological order can be described by topological quantum field theory and topological quantum field theory is essentially equivalent to modular categories, it was understood that modular categories could be used to understand topological order. This latent description of anyons in terms of modular categories was made explicit in an appendix in the seminal 2006 paper of Kitaev [Kit06]. This approach to anyons in terms of modular categories was popularized by Wang's early monograph [Wan10]. This has since become the standard approach towards the algebraic theory of topological quantum information.

Exercises:

5.1. .[WORK: apply Verlinde formula to group-theoretical modular categories to recover classical theorem by Burnside]

5.2. .[WORK: show that irriducible G-graded G-reps are equivalent to irriducible reps of centralizers of conjugacy classes]

5.3. .[WORK: is it too much to include the chiral central charge as an exercise? There's one formula as a ratio of Gauss sums and a second one from Gauss-someone-else. Show that those two are equal, and that they are equal to a root of unity?]

6 Further structure

6.1 Overview

6.2 Domain walls

6.3 Symmetry enriched topological order

6.4 Fermionic topological order

History and further reading:

[WORK: add history]

Exercises:

6.1. .[WORK: make exercises]

7 Topological quantum computation

7.1 Overview

7.1.1 Introduction

In this section we will discuss topological quantum computing, the concept of making a computer based on topological quantum systems. We recall now ow this fits into the overall framework of this book:

[WORK: add diagram]

We recall some general principles and motivations for topological quantum computing, most of which were outlined in Chapter [ref]. Seeing as we will be making repeated use of the term, we abbreviate topological quantum computing to *TQC*.

The most important idea in the subject is that TQC is inherently *fault tolerant*. Noise in the environment of a quantum computer, when properly controlled, can be made small in magniude and local in effect. By the definition of a topological system, the information in the topological computer is invariant under small local changes. Hence, the information remains invariant under noise and the computation can proceed as intended without errors. If there are errors, which is always possible with some small probability, topological quantum systems typically have mechanisms whereby the experimenter can remove the error and restore the information how it was. This is the general picture for fault tolerance in TQC. We will make this picture more precise as we give examples of methods for TQC.

We additionally recall that TQC splits into two major branches. The first is the method of finding physical materials that naturally exhibit topological quantum behavior. These systems can then be used to make a computer. The second approach is to simulate a topological quantum system on a quantum computer. This simulation is used to inheret the fault-tolerant properties of the topological quantum systems on the original quantum computer. So long as the simulation is efficient and local noise on the physical system corresponds to local noise on the simulated system, this method works as described. This gives the following diagram for TQC:

[WORK: add diagram - its already used somewhere else!]

In this chapter, we will talk about lots of different approaches to TQC. Some of them are naturally ammenable to the approach of topological quantum materials, and some of them are naturally ammenable to the approach of topological quantum error correction. We will flag these differences and the status of experimental progress as we go along.

Before moving on with our discussion of TQC, it is good to be aware of the limitations of the algebraic approach.

1. Introducing the algebraic theory is a lot of overhead for not very many examples. Overwhelmingly, proposals for TQC center around just a few algebraic models. Topological quantum error correction is mostly centered around the toric code (see section [ref]), and topological quantum materials are mostly centered around Majorana fermions (see section [ref]). The vast majority of algebraic models have no serious proposals for TQC associated with them. It is for this reason that much of the literature is focused on working out the details of small models and examples, instead of the development of general theory which is largely useless in this lens.

2. The algebraic structures fail to capture a lot of important details about proposals for TQC. It only captures the high-level information flow, and none of the microscopic features. For example, a breakthrough in the field of topological quantum error correction come with the introduction of *color codes* in 2006 [BMD06]. These color codes have very nice properties, and have been an important player in the field of TQC. However, algebraically the color code is equivalent to bilayer toric code:

$$(\text{color code}) \cong (\text{toric code}) \boxtimes (\text{toric code}).$$

The entirely of the novelty of the color code comes in its specific choice of Hamiltonian and microscopic details - there is no new algebra involved.

All this is not to say that the algebraic theory of topological quantum information is useless. It has been an important guide in the subject, and has provided footing and motivation for the continued development of TQC. Large-scale fault-tolerant quantum computation is one of the defining technological challenges of the 21st century. It seems very likely that topological methods will be part of its realization!

7.1.2 Universality

An important concept for understanding TQC methodology is *universality*. To illustrate this concept we begin with an example.

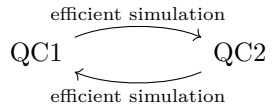
In 1994, Peter Shor developped an efficient quantum algorithm for factoring integers [Sho94]. This algorithm is important because much of modern cryptography is based on the hardness of factoring integers and similar problems. Hence, an efficient factoring algorithm could jeapordize internet security.

However, we must pose ourselves the question: what does it mean, really, for Shor to have found an efficient quantum factoring algorithm? A quantum computer is a computer whose information processing is fundamentally described by quantum mechanics. A priori there are lots of different quantum computers one could make. Which one did Shor find a factoring algorithm for? Maybe when we finally make a quantum computer it will be the type of quantum computer which cannot run Shor's algorithm so internet security will be safe.

The key in understanding this situation is the concept of universality. There are certainly quantum computers which cannot run Shor's algorithm. For instance, if a quantum computer has only a finite number of degrees of freedom to store information then it certainly cannot run large cases of Shor's algorithm because it can't even record the input! Even if a quantum computer can store arbitrarily large inputs, that doesn't mean it will have the capabilities to run Shor's algorithm because it might just not have a physical method for running the algorithm.

However, every *sufficiently powerful* quantum computer can run Shor's algorithm. Moreover, every algorithm you can run efficiently can run efficiently on one quantum computer can then be run on every other sufficiently powerful quantum computer.

Here is the explination for this phenominon. Computers can be viewed as simulation devices. Quantum computers are simultation devices which can simulate quantum systems. Suppose that you are given two quantum computers QC1 and QC2. If QC1 is sufficiently powerful, it should be able to efficienlty simulate the behavior of QC2. If QC2 is sufficiently powerful, it should be able to efficiently simulate the behavior of QC1, as illustrate below:



This gives an easy way to turn any efficient algorithm on QC1 into an efficient algorithm on QC2. First you simulate QC1, and then you run the algorithm on QC1! This means that any problem solved on one of the computers can be efficiently solved on the other. In this way these two computers are *computationally equivalent*. The non-trivial inisght is that every sufficiently powerful quantum computer is able to efficiently simulate every other sufficiently powerful quantum computer. These powerful quantum computers which can simulate every other computer are known as *universal* quantum computers. The existence of universal quantum computers is the heart of universality. What Shor did was make a factoring algorithm which could be run on any universal quantum computer.

This sort of universality has been known for a long time. It was first proposed by pioneers of computation Alan Turing and Alonzo Church [Tur39, Cop97]:

> Church-Turing thesis: "All sufficiently powerful computational models yield efficiently intersimulable classes - there is one theory of computation".

Of course, this thesis does not account for the possibility of quantum computation. Classical and quantum computation seem to be turly distinct theories of computation, violating Church-Turing's intention. This leads to a modern revised version of the Church-Turing thesis:

> Revised Church-Turing thesis: "All sufficiently powerful classical computational models yield efficiently intersimulable classes - there is one theory of classical computation".

A quantum version of the Church-Turing thesis was introduced in an early review article on topological quantum computation by Michael Freedman, Alexei Kitaev, Michael Larsen, and Zhenghan Wang [FKLW03]. It goes as follows:

> Freedman-Church-Turing thesis: "All sufficiently powerful computational models which add the resources of quantum mechanics to classical computation yield efficiently intersimulable classes - there is one theory of quantum computation".

The goal, then, is to make a *universal* topological quantum computer. In a sense this makes designing a scheme for topological quantum computation difficult. It gives constraints, and forces a certain amount of computation power. In another sense, it is liberating. The existence of universal quantum computation means that once we have implemendent a certain amount of computational power into our proposal, we are done. There is no need to search for clever ways to add more power because or system is already universal, and hence finding more techniques in unnececary. It gives an end goal to building a quantum computer - a bell to ring when we are done.

Formally, a universal quantum computer will be one which can approximate and unitary transformation. This means that for every $n \geq 0$, the a universal quantum computer can be prepared in such a way that its information is stored in a Hilbert space V of dimension greater or equal to n. The space of possible computations on the computer should form a dense subgroup of the projective unitary group $PU(V)$.

One important question is whether a computer which is universal in the sense above can *efficiently* simulate any other computer is an important question. This is generically true by to Solovay-Kitaev theorem [Kit97, NC10]. However, a finer discussion of these points and other notions in computaional complexity is beyond the scope of this book and is unnececary for understanding the topics at hand.

[WORK: there is the general corrolation between computational power, difficulty of implimentation, and non-abelian flavor. Give the nice table and talk about it.]

[WORK: boson fermion - easy to simulate. Needs to exploit the weird, compliacated (non-abelian) nature of brading. Hence needs to be sufficiently non-abelian, hence the above picture.]

7.2 Computation with Fibonacci anyons

7.2.1 Methodology

.[WORK: I'm realizing that I don't know enough about Fibonacci anyons to write this. What's the deal with the "golden chain"? How does the relationship with $SU(2)$ work again? What's the history? What does the density of braid group reps say, exactly, and how does the proof go?]

7.2.2 The Jones invariant

.[WORK: here we can connect things to the Jones invariant. The first step is the definition via the Kauffman braket. The key part is to observe that the Skein relation can be enforced physically by finding an anyon (i.e. Fibonacci) which satisfies the Skein relation as operators on a Hilbert space! Such a Skein relation *must* exist, and hence this also explains in a fundamental way why there is a good Skein relation which gives a knot invariant. Also motivates quantum topology in a way, so maybe say a few works about quanutm topology? A good reference is [AA11] which gives a self-contained elementary proof of BQP completeness of Jones invariant.]

7.2.3 Proof of universality

.[WORK: prove that the braid group representations are dense in the appropriate sense.]

7.3 Computation with doubles of finite groups

.[WORK: need to read Mochon's papers and Zhenghan's clarifications again to write this section. Maybe have two sections, one for non-solvable and one for solvable non-nilpotent?]

.[WORK: Maybe add a little word about the idea of having $\mathbb{Z}_2$ bulk and then interfacing with S_3 islands?]

.[WORK: using gapped boundaries. This is the surface code.]

.[WORK: maybe bring up universal TQC with gapped boundaries in $\mathfrak{D}(\mathbb{Z}_3)$ and projective charge measurement somehow? It would be nice to include somewhere. Maybe have an intro about how hard you have to try to get unversal TQC with different groups, and how you can get universal TQC even with abelian groups if you try hard enough.]

]

7.4 Computation with the toric code

7.5 Computation with Ising anyons

.[WORK: universal TQC with Ising twsit defects]

7.6 Computation with Majorana zero modes

.[WORK: Theory of Majoranas, as $\mathbb{Z}_2$-crossed extensions of sVec.]

.[WORK: This section requires a real discussion of physics. There are three key systems to discuss.

1. $\nu = 5/2$ FQH. This system is described by a supermodular category, up to the typical caveat that it is only quasi-topological order and not pure topological order so some phases might not be protected. This supermodular category has Ising as a subcategory. However, the simple object which makes the nonabelian anyon in the Ising MTC is *not* "fundamental" in the system. It is composite, made out of two physically creatable anyons. In this sense $\nu = 5/2$ doesn't really have fundamental Ising anyons, only composite ones.

2. The ends of nanowires. Kitaev has his famous paper introducing this idea. These are Majorana zero modes in their purest form. This is NOT ising. It is a $\mathbb{Z}_2$-crossed extension of sVec which is algebraically essentially the same as Ising, but the distinction is that some of the phases which are well-defined in Ising are unphysical in the $\mathbb{Z}_2$-crossed extension.

3. Superconductor/topologial insulator heterostructures. If you have a sample of topological insulator and you make its boundary conditions oscillate between magnet and superconductor you get Majoranas at the interface between those boundaries. The online course on topology in condensed matter has a good section on this, and there is a lot of literature on the subject. Algebraically, this should be the $\mathbb{Z}_2$-crossed extension of sVec as well. This could be a good reference: [SA19].

Pointing out the key subtle differences between these models is of utmost importance. There should be sections summarizing each experiment and describing its algebraic theory.]

[WORK: This could become a lot of work. It is very relevant to physicists (perhaps the most relevant part of this book), but unnececary and cumbersome for mathematial thinkers. Maybe this should be its own chapter?]

History and further reading:

The idea of topological quantum computing was first introduced by 1997 by Kitaev and Freedman [Kit03, Fre98]. Soon, Freedman, Kitaev, Wang, and Larsen wrote a review article about topological quantum computing which formally started the field in 2002 [FKLW03]. In these early years, these authors and others introduced a number of techniques for universal topological quantum computation [FLW02, Moc03, BK05]. From here, the goal of research became the task of acheiving universal topologial quantum computation in the simplest possible experimental setup.

In the world of quantum materials, this has mostly taken the form of hunting for *Majorana bound states*. Majorana bound states are topological quasiparticles which are bound to defects in materials. Some theories suggest that these Majorana bound states could be braided in a fashion which allows for topological quantum computing. Algebraically, Majorana bound states behave as [WORK: what do they behave as?]. Theorists have engineered increasingly simple materials which are predicted to host Majoranas [FK08, STL$^+$10, Ali10]. Braiding Majorana bound states does not allow for universal topological quantum computation, so most proposals for Majorana quantum computing include some non-topological gates.

In the world of quantum error correction, the search for simple experimental setups has centered around the surface code. The surface code on its own is not univeral, and requires a single extra gate to be made universal. There have been a large number of proposals for how to do this final extra gate, which are more or less feasable depending on the architecture of the underlying quantum computer [BK05, BMD11, Bom15].

There are many good references for topological quantum computing. From the perspective of materials, there are several excellent review articles by Freedman, Nayak, Das Sarma, and others [NSS$^+$08, SFN15]. From the perspetive of topological quantum error correcting codes, the best approach to learn more is to delve into the general theory of quantum error correction. A good place to start is the chapter in Nielsen-Chuang [NC10]. After this there are several review articles [Ter15, Got97].

Exercises:

7.1. .[WORK: make exercises]

A Odds and ends

A.1 Topological quantum field theories

In this chapter we will be exploring topological quantum field theory, a particular way of mathematically formalizing topological order. We recall below how this fits into the general framework of this book:

[WORK: add pretty picture.]

Topological quantum field theory is not our primary approach for understanding topological order - we will mainly be performing our anlysis of topological order using modular tensor categories. For this reason, the present chapter is essentially auxillary to the rest of the book. This chapter is primarily included for the following reasons:

1. To help give a comprehensive picture of the algebraic theory of topological quantum information. Much of the work in the field is written in the language of topological quantum field theory. Not knowing topological quantum field theory can make existing in the world of topological quantum information more painful than it needs to be.

2. Topological quantum field theory makes some important ideas clear which are opaque in the language of modular tensor cateogories. For instance, the proper way of interpreting the modular representation of a modular tensor category is to use concepts of topological quantum field theory.

3. In contrast to modular tensor categories, the definition of a topological quantum field theory is very concise. This means that the fact that topological quantum field theories and modular tensor categories are equivalent is a strong indication that the definition of modular tensor category is well-chosen. As we will discuss in Chapter [ref], the definition of modular tensor category was explicitely chosen to be the way it so that they would be equivalent to topological quantum field theories.

For brevity, we will use the accronym *TQFT* to abbreviate Topological Quantum Field Theory. We will now move on to describing the big idea of TQFT. We will do this by starting with an abstract topological order $\mathscr{C}$. Of course, we haven't defined what an abstract topological order is yet. The point is that we will image that $\mathscr{C}$ is some family of gapped Hamiltonians which has topologically protected ground spaces. All the different gapped Hamiltonians should be related in the sense that they have the same underlying algebraic theory, though we haven't described what that theory is yet. That underlying algebraic theory will exactly be a TQFT. Because they are the only examples we have given, we will always image that $\mathscr{C}$ is the Kitaev quantum double model based on some finite group G, or even more specifically the toric code.

The first step in defininining TQFT is to think about $\mathscr{C}$ is a machine which takes in topological spaces and spits out quantum systems, by taking the space and putting the topological order $\mathscr{C}$ on it. For instance, if $\mathscr{C}$ is the Kitaev quantum double model based on a finite group G and the input space is a torus, then the corresponding system is the Hamiltonian $H = \sum_v (1 - A_v) + \sum_p (1 - B_p)$ defined by choosing a lattice structure on the torus and collecting flatness and gauge invaraince conditions, as pictured below:

[WORK: add picture.]

The Hilbert space $\mathcal{N} = \bigotimes_{\text{edges}} \mathbb{C}[G]$ of this system clearly depends on the choice of lattice on the torus. However, as demonstrated in proposition [ref] the ground states of $\mathcal{N}$ are $\mathcal{C} = \mathbb{C}[\text{Hom}(\pi_1(T^2, v), G)/\left(\begin{smallmatrix}\text{simultaneous}\\ \text{conjugation}\end{smallmatrix}\right)]$. Since the fundamental group is a topological invariant, we see thus that this Hilbert space does not depend on our choice of lattice - its dimension is fixed by the topology of the torus.

More generally, this is what we should expect when putting a topological order on space. The excited states will depend on the details of the gapped Hamiltonian we choose, but the ground states are a topological invariant of the space. The fact that the ground states are topologically invariant is the *defining feature* of topological order. Hence, the topological order $\mathscr{C}$ gives a well-defined assignement from topological spaces to quantum systems.

Not every topological space can host topological order, however. We recall that our definition of topological order required physical space to be *two dimensional*. Of course, there can be global curvature like in the torus. What's important is that locally the system is flat. Hence, the topological spaces on which we can apply our topological order are subspaces of $\mathbb{R}^3$ which locally look like $\mathbb{R}^2$. Topological spaces of this type are called *surfaces*. The most important examples are the g-holed surfaces, for any $g \geq 0$, called Σ_g:

[WORK: add Σ_g picture]

Hence, we find that every topological $\mathscr{C}$ induces an assignment

[WORK: add formula - surfaces get assigned to the Hilbert space of ground statees of $\mathscr{C}$ on that surface.]

This is the general picture for TQFT. A TQFT is an assignment from surfaces to vector spaces, with extra restrictioons which are required to get a reasonable theory. This sort of approach to quantum field theory can be generalized beyond TQFT. In these generalized cases, however, the assignment won't taken surfaces as inputs. Instead, it will take surfaces with detailed geometric structure which encodes the fact that the resulting quantum system will depend on distances and local geometric information. This approach is feasable in some cases but is quite technical [Seg88]. Typically in non-topological cases people opt for other techniques.

A.2 Quasitriangular weak Hopf algebras

A.3 Quantum groups

A.4 Subfactors

A.5 Vertex operator algebras

B Anyon data

B.1 Low-rank MTCs

.[WORK: list of all low-rank MTCs]

B.2 Abelian MTCs

.[WORK: classification of abelian MTCs, give data for a lot of examples]

B.3 Group-theoretical MTCs

.[WORK: give theorems to characterize all of the data for group-theoretical MTCs, give generously many examples]

B.4 Miscellaneous examples

.[WORK: miscillaneous high-rank non-abelian non-group theoretical categories of interest. Probably Haagerup and E6 subfactors [HRW08]. Maybe $SU(2)$ quantum group MTCs for various roots of unity would be nice too.]

[WORK: list of questions/comments:

- I like the term *modular category*. It's shorter than "modular tensor category" and has no ambiguity. There's some literature which uses the term modular category instead of modular tensor category. Modular tensor category is especially confusing as a term because I never define what a tensor category is. Maybe this book is a good time to change the culture on these things, and use the term modular category instead of modular tensor category...

- I'm a bit confused about the stability of topological order. When a constant-size perturbation is applied to a topologically ordered system, this will cause an exponentially small change in the ground state energy of the spectrum, and constant-size spread in the higher energy levels of the spectrum. Moreover, the size of this spread grows linearly with the eigenvalue. Hence, for any constant size perturbation, the higher end of the spectrum will start overlapping. Moreover, this will already start happening with a relatively small ($O(1)$) number of anyons. The authors of [BHM10] who discovered this result console us with the following line: "In the case when excitations of H_0 are anyons, one can infer all topological invariants such as S, R, and F-matrices by evaluating fusion and braiding diagrams with only a few particles (for example 4 particles suffice to compute all F matrices)". They then say once again very clearly that their stabiloity result only applies to states with $O(1)$-many anyons. Is this a fundamental problem? We need more than $O(1)$-many anyons to perform TQC!

  I think that the answer comes from the fact that we can re-formulate TQC in terms of defects. We can change the Hamiltonian terms so that the ground states of the new Hamitonian are anyonic excitations in the original Hamiltonian. This Hamiltonian can be adiabatically changed to perform computations. These new Hamiltonians should all exhibit the same TO as the original Hamiltonian. They will also have a gapped spectrum. Errors will only bleed into low-energy parts of this spectrum, and this can be safely dealt with by the stability theorem. I think that this is the idea. However, this feels like it will do weird things for non-abelian anyons, and there's a good change that these new Hamiltonians won't satisfy TQO-2. If you do it naively in Kitaev's original approach it won't satisfy the literal version of TQO-1 either.

- I would like to add the following principle in my discussion of anyons: *Anyons types cannot be held in coherent superpositions.*

  This principle is subtle. Important, but subtle. On the face of it, it seems like it outlaws anyon interferometry but it can be done if you put your mind to it [Bon12, WBMF23]. At this point one needs to re-define the term anyon. Anyons MUST be of pure type. Otherwise all of our statements will become discussions of "pure-type" anyons and not anyons. Also, some people might contest the principle: [Bon21]. Not sure if I want to include something controversial like this.

  The point is as follows. Define the space $\mathcal{N}_{R_1 \dots R_n} = \bigoplus_{\{A_i\} \in \mathcal{L}^n} \mathcal{N}_{A_1 \dots A_n}$. The operator $\bigoplus_{\{A_i\} \in \mathcal{L}^n} \lambda_{A_1 \dots A_n} \cdot \mathrm{id}$ is a local operator which commutes with all other local noise operators. Since in our physical picture we should imagine local noise being continually applied, this will have the unavoidable effect of de-phasing the superpositions. How can this be dealt with? Maybe the more robust statement is *Anyons types cannot be held in coherent superpositions in noisy environments.*

- What should the name for the F-symbol R-symbol θ-symbol description of an MTC be? I called it the Yoneda perspective because I think that's cute. Zhenghan seems to think that somehow this is related to skeletonization? I don't know the truth. This process was introduced in Kitaev's 2006 paper without a name. Time to think about standardizing.
- I have this very nice picture in my head about TQC in ground state degeneracies. The Hamiltonian is taken on an adiabatic path through the configuration space of possible gapped Hamiltonians. This picture includes anyons for abelian anyons, but not for non-abelian anyons. In general, this doesn't include defects because defect creation/fusion will change the ground state degeneracy and can be non-unitary. In some sense, creating/fusing defects form *nice* paths in configuration space, even if they are not continuous. Maybe we should define some sort of new topology which allows for these sorts of fault-tolerant but not-continuous paths, and it would allow for more gates. Which gates are allowed this way?

]

References

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

[AA11] Dorit Aharonov and Itai Arad. The bqp-hardness of approximating the jones polynomial. *New Journal of Physics*, 13(3):035019, 2011.

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

[AB59] Yakir Aharonov and David Bohm. Significance of electromagnetic potentials in the quantum theory. *Physical review*, 115(3):485, 1959.

[Ale28] James W Alexander. Topological invariants of knots and links. *Transactions of the American Mathematical Society*, 30(2):275–306, 1928.

[Ali10] Jason Alicea. Majorana fermions in a tunable semiconductor device. *Physical Review B—Condensed Matter and Materials Physics*, 81(12):125318, 2010.

[AMV18] NP Armitage, EJ Mele, and Ashvin Vishwanath. Weyl and dirac semimetals in three-dimensional solids. *Reviews of Modern Physics*, 90(1):015001, 2018.

[ASW84] Daniel Arovas, John R Schrieffer, and Frank Wilczek. Fractional statistics and the quantum hall effect. *Physical review letters*, 53(7):722, 1984.

[ASWZ85] Daniel P Arovas, Robert Schrieffer, Frank Wilczek, and Anthony Zee. Statistical mechanics of anyons. *Nuclear Physics B*, 251:117–126, 1985.

[AT77] PHILIP W Anderson and G Toulouse. Phase slippage without vortex cores: vortex textures in superfluid he 3. *Physical Review Letters*, 38(9):508, 1977.

[AWH22] David Aasen, Zhenghan Wang, and Matthew B Hastings. Adiabatic paths of hamiltonians, symmetries of topological order, and automorphism codes. *Physical Review B*, 106(8):085122, 2022.

[BCG+24] Sergey Bravyi, Andrew W Cross, Jay M Gambetta, Dmitri Maslov, Patrick Rall, and Theodore J Yoder. High-threshold and low-overhead fault-tolerant quantum memory. *Nature*, 627(8005):778–782, 2024.

[BDSPV15] Bruce Bartlett, Christopher L Douglas, Christopher J Schommer-Pries, and Jamie Vicary. Modular categories as representations of the 3-dimensional bordism 2-category. *arXiv preprint arXiv:1509.06811*, 2015.

[Ben73] Charles H Bennett. Logical reversibility of computation. *IBM journal of Research and Development*, 17(6):525–532, 1973.

[BGS+09] Kirill I Bolotin, Fereshte Ghahari, Michael D Shulman, Horst L Stormer, and Philip Kim. Observation of the fractional quantum hall effect in graphene. *Nature*, 462(7270):196–199, 2009.

[BH11] Sergey Bravyi and Matthew B Hastings. A short proof of stability of topological order under local perturbations. *Communications in mathematical physics*, 307:609–627, 2011.

[BHM10] Sergey Bravyi, Matthew B Hastings, and Spyridon Michalakis. Topological quantum order: stability under local perturbations. *Journal of mathematical physics*, 51(9), 2010.

[BK+01] Bojko Bakalov, Alexander A Kirillov, et al. *Lectures on tensor categories and modular functors*, volume 21. American Mathematical Society Providence, RI, 2001.

[BK05] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal clifford gates and noisy ancillas. *Physical Review A—Atomic, Molecular, and Optical Physics*, 71(2):022316, 2005.

[BK13] Sergey Bravyi and Robert König. Classification of topologically protected gates for local stabilizer codes. *Physical review letters*, 110(17):170503, 2013.

[BKK+24] Jan Balewski, Milan Kornjaca, Katherine Klymko, Siva Darbha, Mark R Hirsbrunner, Pedro Lopes, Fangli Liu, and Daan Camps. Engineering quantum states with neutral atoms. *arXiv preprint arXiv:2404.04411*, 2024.

[BKKK22] Sergey Bravyi, Isaac Kim, Alexander Kliesch, and Robert Koenig. Adaptive constant-depth circuits for manipulating non-abelian anyons. *arXiv preprint arXiv:2205.01933*, 2022.

[BMD06] Hector Bombin and Miguel Angel Martin-Delgado. Topological quantum distillation. *Physical review letters*, 97(18):180501, 2006.

[BMD11] H Bombin and MA Martin-Delgado. Nested topological order. *New Journal of Physics*, 13(12):125001, 2011.

[Bom15] Héctor Bombín. Gauge color codes: optimal transversal gates and gauge fixing in topological stabilizer codes. *New Journal of Physics*, 17(8):083002, 2015.

[Bon12] Parsa Hassan Bonderson. *Non-Abelian anyons and interferometry*. California Institute of Technology, 2012.

[Bon21] Parsa Bonderson. Measuring topological order. *Physical Review Research*, 3(3):033110, 2021.

[BPZ84] Alexander A Belavin, Alexander M Polyakov, and Alexander B Zamolodchikov. Infinite conformal symmetry in two-dimensional quantum field theory. *Nuclear Physics B*, 241(2):333–380, 1984.

[CCW17] Iris Cong, Meng Cheng, and Zhenghan Wang. Universal quantum computation with gapped boundaries. *Physical Review Letters*, 119(17):170504, 2017.

[CDH+20] Shawn X Cui, Dawei Ding, Xizhi Han, Geoffrey Penington, Daniel Ranard, Brandon C Rayhaun, and Zhou Shangnan. Kitaev's quantum double model as an error correcting code. *Quantum*, 4:331, 2020.

[CK18] Bob Coecke and Aleks Kissinger. Picturing quantum processes: A first course on quantum theory and diagrammatic reasoning. In *Diagrammatic Representation and Inference: 10th International Conference, Diagrams 2018, Edinburgh, UK, June 18-22, 2018, Proceedings 10*, pages 28–31. Springer, 2018.

[CLRL17] Ching-Kit Chan, Netanel H Lindner, Gil Refael, and Patrick A Lee. Photocurrents in weyl semimetals. *Physical Review B*, 95(4):041104, 2017.

[Cop97] B Jack Copeland. The church-turing thesis. 1997.

[COT24] Kevin Coulembier, Victor Ostrik, and Daniel Tubbenhauer. Growth rates of the number of indecomposable summands in tensor powers. *Algebras and Representation Theory*, 27(2):1033–1062, 2024.

[Dir31] Paul Adrien Maurice Dirac. Quantised singularities in the electromagnetic field. *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, 133(821):60–72, 1931.

[Dri86] Vladimir Gershonovich Drinfeld. Quantum groups. *Zapiski Nauchnykh Seminarov POMI*, 155:18–49, 1986.

[EGNO16] Pavel Etingof, Shlomo Gelaki, Dmitri Nikshych, and Victor Ostrik. *Tensor categories*, volume 205. American Mathematical Soc., 2016.

[EK09] Bryan Eastin and Emanuel Knill. Restrictions on transversal encoded quantum gate sets. *Physical review letters*, 102(11):110502, 2009.

[EM45] Samuel Eilenberg and Saunders MacLane. General theory of natural equivalences. *Transactions of the American Mathematical Society*, 58(2):231–294, 1945.

[ENO05] Pavel Etingof, Dmitri Nikshych, and Viktor Ostrik. On fusion categories. *Annals of mathematics*, pages 581–642, 2005.

[Fal94] Gerd Faltings. A proof for the verlinde formula. *Journal of Algebraic Geometry*, 3(2):347, 1994.

[FEC+21] Michael S Fuhrer, Mark T Edmonds, Dimitrie Culcer, Muhammad Nadeem, Xiaolin Wang, Nikhil Medhekar, Yuefeng Yin, and Jared H Cole. Proposal for a negative capacitance topological quantum field-effect transistor. In *2021 IEEE International Electron Devices Meeting (IEDM)*, pages 38–2. IEEE, 2021.

[FK08] Liang Fu and Charles L Kane. Superconducting proximity effect and majorana fermions¡? format?¿ at the surface of a topological insulator. *Physical review letters*, 100(9):096407, 2008.

[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.

[Fre70] Peter Freyd. Homotopy is not concrete. In *The Steenrod Algebra and Its Applications: A Conference to Celebrate NE Steenrod's Sixtieth Birthday: Proceedings of the Conference held at the Battelle Memorial Institute, Columbus, Ohio March 30th–April 4th, 1970*, pages 25–34. Springer, 1970.

[Fre98] Michael H Freedman. P/np, and the quantum field computer. *Proceedings of the National Academy of Sciences*, 95(1):98–101, 1998.

[FS19] Brendan Fong and David I Spivak. *An invitation to applied category theory: seven sketches in compositionality*. Cambridge University Press, 2019.

[goo23] Suppressing quantum errors by scaling a surface code logical qubit. *Nature*, 614(7949):676–681, 2023.

[Got97] Daniel Gottesman. *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997.

[Hal83] F Duncan M Haldane. Nonlinear field theory of large-spin heisenberg antiferromagnets: semiclassically quantized solitons of the one-dimensional easy-axis néel state. *Physical review letters*, 50(15):1153, 1983.

[Hal88] F Duncan M Haldane. Model for a quantum hall effect without landau levels: Condensed-matter realization of the" parity anomaly". *Physical review letters*, 61(18):2015, 1988.

[Hal13] Brian C Hall. *Quantum theory for mathematicians*, volume 267. Springer Science & Business Media, 2013.

[HDSHL24] Yifan Hong, Elijah Durso-Sabina, David Hayes, and Andrew Lucas. Entangling four logical qubits beyond break-even in a nonlocal code. *arXiv preprint arXiv:2406.02666*, 2024.

[HK10] M Zahid Hasan and Charles L Kane. Colloquium: topological insulators. *Reviews of modern physics*, 82(4):3045–3067, 2010.

[HRW08] Seung-Moon Hong, Eric Rowell, and Zhenghan Wang. On exotic modular tensor categories. *Communications in Contemporary Mathematics*, 10(supp01):1049–1074, 2008.

[Hua08] Yi-Zhi Huang. Vertex operator algebras and the verlinde conjecture. *Communications in Contemporary Mathematics*, 10(01):103–154, 2008.

[ITV+24] Mohsin Iqbal, Nathanan Tantivasadakarn, Ruben Verresen, Sara L Campbell, Joan M Dreiling, Caroline Figgatt, John P Gaebler, Jacob Johansen, Michael Mills, Steven A Moses, et al. Non-abelian topological order and anyons on a trapped-ion processor. *Nature*, 626(7999):505–511, 2024.

[Jon97] Vaughan FR Jones. A polynomial invariant for knots via von neumann algebras. In *Fields Medallists' Lectures*, pages 448–458. World Scientific, 1997.

[JVW90] François Jaeger, Dirk L Vertigan, and Dominic JA Welsh. On the computational complexity of the jones and tutte polynomials. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 108, pages 35–53. Cambridge University Press, 1990.

[KDP80] K v Klitzing, Gerhard Dorda, and Michael Pepper. New method for high-accuracy determination of the fine-structure constant based on quantized hall resistance. *Physical review letters*, 45(6):494, 1980.

[Kit97] A Yu Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191, 1997.

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

[Kit06] Alexei Kitaev. Anyons in an exactly solved model and beyond. *Annals of Physics*, 321(1):2–111, 2006.

[KL09] Louis H Kauffman and Samuel J Lomonaco. Topological quantum information theory. In *Proceedings of Symposia in Applied Mathematics*, volume 68, 2009.

[KT73] JM Kosterlitz and David James Thouless. Ordering, metastability and phase transitions in two-dimensional systems. *J. Phys. C*, 6:1181–1203, 1973.

[KT18] John Michael Kosterlitz and David James Thouless. Ordering, metastability and phase transitions in two-dimensional systems. In *Basic Notions Of Condensed Matter Physics*, pages 493–515. CRC Press, 2018.

[KZ22] Liang Kong and Zhi-Hao Zhang. An invitation to topological orders and category theory. *arXiv preprint arXiv:2205.05565*, 2022.

[Lan95] Rolf Landauer. Is quantum mechanics useful? *Philosophical Transactions of the Royal Society of London. Series A: Physical and Engineering Sciences*, 353(1703):367–376, 1995.

[LM77] JM Leinaas and J Myrheim. On the theory of identical particles. *Il nuovo cimento*, 37:132, 1977.

[Lur08] Jacob Lurie. On the classification of topological field theories. *Current developments in mathematics*, 2008(1):129–280, 2008.

[Lyu95] Volodymyr V Lyubashenko. Invariants of 3-manifolds and projective representations of mapping class groups via quantum groups at roots of unity. *Communications in mathematical physics*, 172:467–516, 1995.

[Mer79] N David Mermin. The topological theory of defects in ordered media. *Reviews of Modern Physics*, 51(3):591, 1979.

[ML13] Saunders Mac Lane. *Categories for the working mathematician*, volume 5. Springer Science & Business Media, 2013.

[Moc03] Carlos Mochon. Anyons from nonsolvable finite groups are sufficient for universal quantum computation. *Physical Review A*, 67(2):022315, 2003.

[Moc04] Carlos Mochon. Anyon computers with smaller groups. *Physical Review A*, 69(3):032306, 2004.

[MS88] Gregory Moore and Nathan Seiberg. Polynomial equations for rational conformal field theories. *Physics Letters B*, 212(4):451–460, 1988.

[MS89] Gregory Moore and Nathan Seiberg. Classical and quantum conformal field theory. *Communications in Mathematical Physics*, 123:177–254, 1989.

[MS90] Gregory Moore and Nathan Seiberg. Lectures on rcft. In *Physics, geometry and topology*, pages 263–361. Springer, 1990.

[MZ21] CH Marrows and K Zeissler. Perspective on skyrmion spintronics. *Applied Physics Letters*, 119(25), 2021.

[NC10] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[NSS+08] Chetan Nayak, Steven H Simon, Ady Stern, Michael Freedman, and Sankar Das Sarma. Non-abelian anyons and topological quantum computation. *Reviews of Modern Physics*, 80(3):1083–1159, 2008.

[PBD17] Benedikt Placke, Stefano Bosco, and David P DiVincenzo. A model study of present-day hall-effect circulators. *EPJ Quantum Technology*, 4:1–14, 2017.

[RB11] Nicolas Regnault and B Andrei Bernevig. Fractional chern insulator. *Physical Review X*, 1(2):021014, 2011.

[RS20] Arthur P Ramirez and Brian Skinner. Dawn of the topological age? *Physics Today*, 73(9):30–36, 2020.

[RT91] Nicolai Reshetikhin and Vladimir G Turaev. Invariants of 3-manifolds via link polynomials and quantum groups. *Inventiones mathematicae*, 103(1):547–597, 1991.

[SA17] Masatoshi Sato and Yoichi Ando. Topological superconductors: a review. *Reports on Progress in Physics*, 80(7):076501, 2017.

[SA19] Jun Ho Son and Jason Alicea. Commuting-projector hamiltonians for two-dimensional topological insulators: Edge physics and many-body invariants. *Physical Review B*, 100(15):155107, 2019.

[SBZ22] Alexis Schotte, Lander Burgelman, and Guanyu Zhu. Fault-tolerant error correction for a universal non-abelian topological quantum computer at finite temperature. *arXiv preprint arXiv:2301.00054*, 2022.

[Seg88] Graeme B Segal. The definition of conformal field theory. In *Differential geometrical methods in theoretical physics*, pages 165–171. Springer, 1988.

[SF18] Brian Skinner and Liang Fu. Large, nonsaturating thermopower in a quantizing magnetic field. *Science advances*, 4(5):eaat2621, 2018.

[SFN15] Sankar Das Sarma, Michael Freedman, and Chetan Nayak. Majorana zero modes and topological quantum computation. *npj Quantum Information*, 1(1):1–13, 2015.

[Sha12] Ramamurti Shankar. *Principles of quantum mechanics*. Springer Science & Business Media, 2012.

[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.

[Sim23] Steven H Simon. *Topological quantum*. Oxford University Press, 2023.

[Sky62] Tony Hilton Royle Skyrme. A unified field theory of mesons and baryons. *Nuclear Physics*, 31:556–569, 1962.

[ŠMYM18] Libor Šmejkal, Yuriy Mokrousov, Binghai Yan, and Allan H MacDonald. Topological antiferromagnetic spintronics. *Nature physics*, 14(3):242–251, 2018.

[STL+10] Jay D Sau, Sumanta Tewari, Roman M Lutchyn, Tudor D Stanescu, and S Das Sarma. Non-abelian quantum order in spin-orbit-coupled semiconductors: Search for topological majorana particles in solid-state systems. *Physical Review B—Condensed Matter and Materials Physics*, 82(21):214509, 2010.

[SZBV22] Alexis Schotte, Guanyu Zhu, Lander Burgelman, and Frank Verstraete. Quantum error correction thresholds for the universal fibonacci turaev-viro code. *Physical Review X*, 12(2):021012, 2022.

[Ter15] Barbara M Terhal. Quantum error correction for quantum memories. *Reviews of Modern Physics*, 87(2):307–346, 2015.

[TSG82] Daniel C Tsui, Horst L Stormer, and Arthur C Gossard. Two-dimensional magnetotransport in the extreme quantum limit. *Physical Review Letters*, 48(22):1559, 1982.

[Tur39] Alan Mathison Turing. Systems of logic based on ordinals. *Proceedings of the London Mathematical Society, Series 2*, 45:161–228, 1939.

[Tur92] Vladimir G Turaev. Modular categories and 3-manifold invariants. *International Journal of Modern Physics B*, 6(11n12):1807–1824, 1992.

[Tur10] Vladimir G Turaev. *Quantum invariants of knots and 3-manifolds*. de Gruyter, 2010.

[TVV23] Nathanan Tantivasadakarn, Ashvin Vishwanath, and Ruben Verresen. Hierarchy of topological order from finite-depth unitaries, measurement, and feedforward. *PRX Quantum*, 4(2):020339, 2023.

[VD14] Giovanni Viola and David P DiVincenzo. Hall effect gyrators and circulators. *Physical Review X*, 4(2):021019, 2014.

[Ver88] Erik Verlinde. Fusion rules and modular transformations in 2d conformal field theory. *Nuclear Physics B*, 300:360–376, 1988.

[vKCK+20] Klaus von Klitzing, Tapash Chakraborty, Philip Kim, Vidya Madhavan, Xi Dai, James McIver, Yoshinori Tokura, Lucile Savary, Daria Smirnova, Ana Maria Rey, et al. 40 years of the quantum hall effect. *Nature Reviews Physics*, 2(8):397–401, 2020.

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

[WBMF23] Zezhu Wei, Navketan Batra, VF Mitrović, and DE Feldman. Thermal interferometry of anyons. *Physical Review B*, 107(10):104406, 2023.

[Wen89] Xiao-Gang Wen. Vacuum degeneracy of chiral spin states in compactified space. *Physical Review B*, 40(10):7387, 1989.

[Wil82a] Frank Wilczek. Magnetic flux, angular momentum, and statistics. *Physical Review Letters*, 48(17):1144, 1982.

[Wil82b] Frank Wilczek. Quantum mechanics of fractional-spin particles. *Physical review letters*, 49(14):957, 1982.

[Wit88] Edward Witten. Topological quantum field theory. *Communications in Mathematical Physics*, 117(3):353–386, 1988.

[Wit89] Edward Witten. Quantum field theory and the jones polynomial. *Communications in Mathematical Physics*, 121(3):351–399, 1989.

[XSW+24] Shibo Xu, Zheng-Zhi Sun, Ke Wang, Hekang Li, Zitian Zhu, Hang Dong, Jinfeng Deng, Xu Zhang, Jiachen Chen, Yaozu Wu, et al. Non-abelian braiding of fibonacci anyons with a superconducting processor. *Nature Physics*, pages 1–7, 2024.

[Yet92] David N Yetter. Framed tangles and a theorem of deligne on braided deformations of tannakian categories. *Contemp. Math*, 134:325–350, 1992.

[ZGHS15] W Zhu, SS Gong, FDM Haldane, and DN Sheng. Fractional quantum hall states at $\nu = 13/5$ and $12/5$ and their non-abelian nature. *Physical review letters*, 115(12):126805, 2015.