The Algebraic Theory of Topological Quantum Information

by Milo Moses

California Institute of Technology

January 17, 2025

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.

For 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 directly 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. Alexei Kitaev and Daniel Ranard now for advising me. Maybe Sam Packman for being a peer mentor?

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 rigorous mathematical treatment, our different choice of topics, 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

0 Preface **3**

1 Overview **7**
1.1 Conceptual introduction . . . 7
1.1.1 Motivation and applications . . . 7
1.1.2 Mathematical picture . . . 9
1.1.3 History of the subject . . . 9
1.2 Technical introduction . . . 12
1.2.1 Principles of topological quantum information . . . 12
1.2.2 Defects in ordered media . . . 15
1.2.3 The fundamental group . . . 19
1.2.4 Topological classical computation . . . 23

2 Quantum mechanics **33**
2.1 Overview . . . 33
2.1.1 Introduction . . . 33
2.1.2 Experimental motivation . . . 33
2.2 Axiomatic development . . . 34
2.2.1 Probability theory . . . 34
2.2.2 Basis-dependent quantum mechanics . . . 36
2.2.3 Measurement . . . 37
2.2.4 Incomplete measurement . . . 39
2.2.5 Basis-independent quantum mechanics . . . 40
2.2.6 Hamiltonians and the Schrodinger equation . . . 43

3 Topological quantum order **47**
3.1 Overview . . . 47
3.1.1 Introduction . . . 47
3.2 Discrete gauge theory . . . 51
3.2.1 Ordered media on a lattice . . . 51
3.2.2 From ordered media to gauge theory . . . 55
3.2.3 Kitaev quantum double model . . . 56
3.3 The toric code . . . 59
3.3.1 Simplified Hamiltonian . . . 60
3.3.2 Exact solution of the toric code . . . 63
3.3.3 Toric code as a topologically ordered system . . . 64
3.4 Anyons . . . 64
3.4.1 Topological quantum information in excited states . . . 64
3.4.2 Definition and principles of anyons . . . 67
3.4.3 Anyons in the toric code . . . 69
3.4.4 Anyons in discrete gauge theory . . . 69

4 Category theory **72**
4.1 Overview . . . 72
4.1.1 Introduction . . . 72
4.1.2 Definition and important obervations . . . 73
4.2 Structures in category theory . . . 76

4.2.1 Products and universal properties . . . 76
4.2.2 Functors and natural transformations . . . 80
4.2.3 Linear categories . . . 84
4.3 Monoidal categories . . . 87
4.3.1 Motivation, definition, and string diagrams . . . 87
4.3.2 Braided monoidal categories . . . 90
4.3.3 Examples, equivalences, and MacLane's coherence theorem . . . 93
4.3.4 Pivotal monoidal categories . . . 99

5 Modular categories **108**
5.1 Overview . . . 108
5.1.1 Introduction . . . 108
5.1.2 Using the final product . . . 109
5.2 First properties . . . 110
5.2.1 Definition . . . 110
5.2.2 Anyons in modular categories . . . 112
5.2.3 States in modular categories and unitarity . . . 114
5.2.4 Topological charge measurement . . . 117
5.3 The modular category toolkit . . . 121
5.3.1 Duality . . . 122
5.3.2 Trace . . . 123
5.3.3 Quantum dimension and Frobenius-Perron dimension . . . 125
5.3.4 Twist . . . 130
5.3.5 Functors, natural transformations, and equivalence . . . 134
5.3.6 Deligne tensor product . . . 134
5.4 The category of G-graded G-representations . . . 137
5.4.1 Overview . . . 137
5.4.2 $\mathbb{C}$-linear structures . . . 138
5.4.3 Spherical fusion structures . . . 141
5.4.4 Braiding and modularity . . . 143
5.5 The modular representation . . . 146
5.5.1 Definition . . . 146
5.5.2 Torus perspective . . . 148
5.5.3 Bruguieres's modularity theorem and the Verlinde formula . . . 150
5.5.4 Proof of modularity . . . 155
5.5.5 Vafa's theorem, unitarity of S-matrix, and the Chiral central charge . 158
5.6 Skeletonization . . . 161
5.6.1 Principle . . . 161
5.6.2 F-symbols . . . 161
5.6.3 R-symbols . . . 161
5.6.4 θ-symbols . . . 161
5.6.5 Reconstruction theorem . . . 161
5.7 Quantum double modular categories . . . 161
5.7.1 The Drinfeld center . . . 161
5.7.2 Muger's theorem . . . 163
5.7.3 Discrete gauge theory as a quantum double and Morita equivalence . 163
5.7.4 Factorizability and time reversal symmetry . . . 164
5.7.5 Levin-Wen model . . . 164

5.8 Unitarity 164
5.8.1 Characterization of unitarizability 164
5.8.2 Unitary braidings 165
5.8.3 Uniqueness of unitary structure 165
5.8.4 Skeletonization of unitarity 166
5.9 Number theory in modular categories 166
5.9.1 Techniques and first results 166
5.9.2 Galois conjugation 166
5.9.3 Ocneanu rigidity 166
5.9.4 Rank-finiteness theorem 166
5.9.5 Schauenberg-Ng theorem 166

6 Further structure **170**
6.1 Overview 170
6.1.1 Introduction 170
6.2 Boundaries and domain walls 171
6.2.1 Physical picture 171
6.2.2 Boundaries and domain walls in the toric code 172
6.2.3 The algebraic theory of gapped boundaries 172
6.2.4 Lagrangian algebras and algebra objects 173
6.2.5 Module categories and boundaries in the Levin-Wen model 174
6.2.6 The Drinfeld center via bimodules 181
6.2.7 Muger's theorem and Lagrange's theorem for fusion categories 183
6.2.8 Skeletonization of gapped boundaries 184
6.3 Symmetry enriched topological order 184
6.3.1 Physical picture 184
6.3.2 Haldane spin chain 184
6.3.3 Twist defects in the toric code 184
6.3.4 The algebraic theory of SET phases 185
6.3.5 Gauging symmetries 188
6.3.6 Obstruction theory, anomalies, and zesting 189
6.3.7 G-crossed modularity 190
6.3.8 Skeletonization of SET phases 190
6.4 Fermionic topological order 190
6.4.1 Physical picture 190
6.4.2 Kitaev spin chain 190
6.4.3 The algebraic theory of fermionic topological order 190
6.4.4 The 16-fold way on the trivial fermionic theory 190
6.4.5 Modular representations of fermionic topological order 190
6.4.6 Super-groups and Deligne's theorem 191

7 Topological quantum computation **195**
7.1 Overview 195
7.1.1 Introduction 195
7.1.2 Universality 196
7.2 Computation with Fibonacci anyons 198
7.2.1 Methodology 198
7.2.2 The Jones invariant 198

7.2.3 Proof of universality . . . 198
7.3 Computation with doubles of finite groups . . . 199
7.4 Computation with the toric code . . . 201
7.5 Computation with Ising anyons . . . 201
7.6 Computation with Majorana zero modes . . . 201

A Odds and ends **204**
A.1 Topological quantum field theories . . . 204
A.1.1 Overview . . . 204
A.1.2 Dehn twists in the toric code . . . 205
A.1.3 Defining TQFT . . . 205
A.2 Quasitriangular weak Hopf algebras . . . 208
A.3 Quantum groups . . . 209
A.4 Subfactors . . . 209
A.5 Vertex operator algebras . . . 209

B Anyon data **211**
B.1 Low-rank modular categories . . . 211
B.2 Abelian modular categories . . . 211
B.3 Group-theoretical modular categories . . . 211
B.4 Miscellaneous examples . . . 211

1 Overview

1.1 Conceptual introduction

1.1.1 Motivation and applications

We 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.

The title of this book refers to "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 system 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 captures 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 [**?**], 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 [**?**, **?**]. Since then topological quantum computing has grown

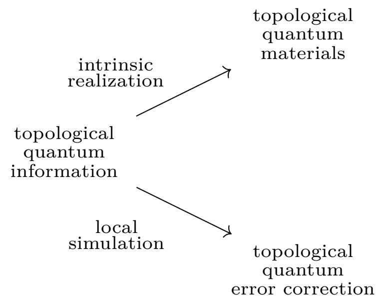


Figure 1.1: The two major branches of topological quantum information.

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 (≈5 degrees Kelvin) and large magnetic fields (≈15 Teslas) [**?**]. 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. This sort of artificial construction typically takes place within a noisy non-topological quantum computer. 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 the 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 [**?**]. Some proposed applications include processing classical information using topological defects in magnetic devices (with the end goal of making high-speed low-energy transmissions) [**?**, **?**], creating highly sensitive photodetectors (with the end goal of making night-vision goggles or sensors) [**?**], creating technolgies with high thermoelectric effect (with the end goal of making efficient fridges or electric generators) [**?**], creating highly-efficient transistors [**?**], and engineering tiny electrical components [**?**, **?**].

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 [?], topological insulators [?], fractional Chern insulators [?], Weyl/Dirac semimetals [?], topological superconductors [?], and many more. 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, helping readers think both concretely and conceptually about these materials and their applications.

1.1.2 Mathematical picture

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, we will focus on *(2+1)-dimensional* topological order - topologically ordered systems in 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 exhibit (2+1)D topological order.

$$\boxed{\text{All systems in this book are two-dimensional unless stated otherwise.}}$$

Topological quantum systems can be described in many different ways. In this book we will take an *algebraic* approach. This means we focus on the big-picture structure of the information, based on symbolic equations and relationships. The algebraic structure which houses the data of a (2+1)D topologically ordered system is known as a *modular category*. These algebraic structures are the main mathematical object of this text. Once one has a modular category it is easy to manipulate the stored information to predict the result of computations. This gives the overall schema of our discussion, illustrated visually below:

$$\begin{tikzcd} & \left(\substack{\text{modular}\\ \text{categories}}\right) \arrow[dr] & \\ \left(\substack{\text{topologically}\\ \text{ordered systems}}\right) \arrow[ur] \arrow[rr] & & \left(\substack{\text{topological quantum}\\ \text{computing}}\right) \end{tikzcd}$$

In chapter **??** we describe topological order. In chapter 5 we describe topological order algebraically in terms of modular categories. In chapter **??** we describe further algebraic structures which lie beyond plain modular categories, which allow us to describe more complex behaviors in topological order. Finally, in chapter **??** 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 2 which establishes the theory of finite dimensional quantum systems and Chapter 4 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* [?]. 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.

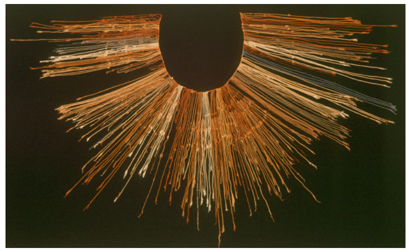


Figure 1.2: An incan quipu

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 [**?**] 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 [**?**] and the theory of point defects by Tony Skyrme [**?**] 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 [**?**] and the theory of phase transitions in the xy model proposed by Kosterlitz-Thouless [**?**]. 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 [**?**] and the subsequent discovery of the fractional quantum Hall effect in 1982 [**?**] 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 Frank Wilczek [**?**, **?**], Duncan Haldane [**?**, **?**], 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 [**?**]. 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 [**?**]. This marked the first major progress in the field since Alexander's invariant in 1928 [**?**]. 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 [?]! 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 [?], and there was debate about whether scalable quantum error correction was possible [?]. This led to two independent proposals for topological quantum computation in the same year. One was by the mathematician Michael Freedman [?]. His vision was clear. A recent paper had shown that computing the Jones invariant of knots was in general an NP-hard problem [?]. 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 [?]. 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 [?].

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 [?]. 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 [?]. 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 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 homogenous, essentially identical everywhere, at the exception of finitely many localized regions. These regions will differ substantially from the 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. 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.

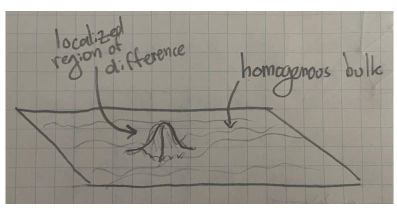


Figure 1.3: A quasiparticle in a two dimensional system

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

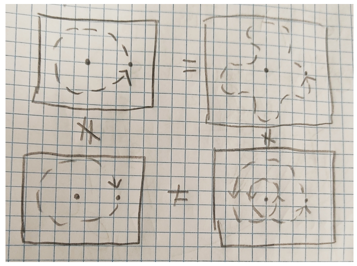


Figure 1.4: Samples of braids quasiparticles can take around one another

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 *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, make 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 feature* of a topological system.

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

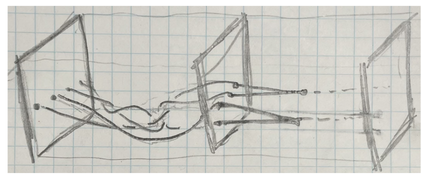


Figure 1.5: A schematic of topological quantum computing

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 1.5.

Example 1.2.1. 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 [**?**]. 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 done by initializing some prescribed state and then braiding its quasiparticles in the correct fashion. 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:

$$\underline{\text{input}} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \underline{\text{output}}$$

$$\begin{matrix}\text{positive}\\\text{integer}\end{matrix} \xrightarrow{\begin{matrix}\text{efficient}\\\text{classical}\\\text{algorithm}\end{matrix}} \text{braid} \xrightarrow{\begin{matrix}\text{braiding}\\\text{quasiparticles}\\\text{in Fibonacci}\\\text{particle theory}\end{matrix} + \begin{matrix}\text{recording}\\\text{probability of}\\\text{annhilation}\end{matrix}} \text{real number} \xrightarrow{\begin{matrix}\text{efficient}\\\text{classical}\\\text{algorithm}\end{matrix}} \begin{matrix}\text{factorization}\\\text{of input}\end{matrix}$$

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 [**?**]. 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.

To make a real topological quantum computer, one would need to create a physical topological system which is described by the Fibonacci theory. In the realm of materials, the most promising approach seems to be specially tuned versions of the fractional quantum Hall system [**?**]. 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 [**?**, **?**, **?**]. 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 topological 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 subtleties 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 our discussion is taken from an excellent review article by Mermin [**?**].

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*. As an input to our construction we will take a topological space called the *order space* of our theory. To simply notation, we fix the convention

$$M \text{ is a path-connected topological space, the order space.}$$

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 applications of 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 is also naturally occuring helium-3. At cold temperatures helium-3 undergoes a phase transition, becoming a superfluid. There are several different superfluid phases helium-3 can go into: the B-phase, dipole-locked A-phase, and dipole-free A-phase. The dipole-locked A-phase is well modeled by ordered media with order space $M = \mathrm{SO}(3)$, where $\mathrm{SO}(3)$ is the space of rotations in three dimensional space. The dipole-free A-phase is well modeled by ordered media with order space $M = \mathrm{SO}(3) \times \mathrm{SO}(3)/H$, where H is the subgroup of $SO(3) \times SO(3)$ generated by rotations across the z-axis of any degree, and simultaneous rotations of 180° on both copies of $\mathrm{SO}(3)$ around any axis.

- **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 they will have the same symmetry group as a rectangle which is enough for the model to be accurate. The order space M of the model is equal to the space of possible orientations of a rectangle in three dimensions. Note that in this space every orientation is equal to its 180° rotation across any axis of the rectangle, since the rectangle is symmetric under such rotations.

We now seek extend our model of ordered media and perform a detailed analysis of it. To do this, we will need to use notions from topology such as a *continuous deformation* of a system and the *inside* of a loop in $\mathbb{R}^2$. While these notions are certainly intuitive, they can be shockingly hard to prove. The fact that every loop in $\mathbb{R}^2$ partitions space into an *inside* and an *outside* is known as the Jordan curve theorem. The proof of this trivial seeming statement is famously tricky [**?**]. Thus, we adopt the following policy:

> Seeing as the primary focus of this text is algebra we opt to leave our topology non-rigorous, focusing instead on principles and techniques. We only return to mathematical rigor once the subject has become sufficiently algebraic.

We now add a picture of *dynamics* into our model - how states will be change through time. In particular, we imagine that as time passes the system changes continuously. Suppose that $\phi_t : \mathbb{R}^2 \to M$ is the state of the system at time t. If t_0, t_1 are similar times we require

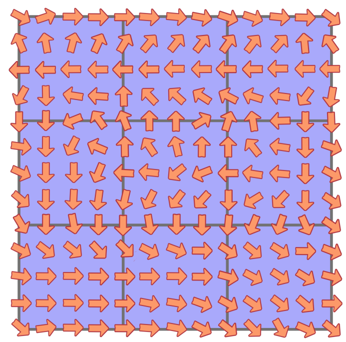


Figure 1.6: The xy-model of a 2D electron gas

$\phi_{t_0}(x)$ and $\phi_{t_1}(x)$ will be close. Formally, we say that a family of states ϕ_t for $0 \le t \le T$ form a valid trajectory in time if the map

$$\begin{aligned} \phi_\cdot : \mathbb{R}^2 \times [0,T] &\to M \\ (x,t) &\mapsto \phi_t(x) \end{aligned}$$

is continuous. We also call ϕ_- a continuous deformation from ϕ_0 to ϕ_T, because the trajectory in time continuously changes the initial state ϕ_0 until it becomes the final state ϕ_T.

Remark 1.2.2. It is a general fact from topology that every pair of maps $\phi_0, \phi_1 : \mathbb{R}^2 \to M$ can be continuously deformed from one to the other. Intuitively, this means that as our system evolves it can transition continuously from any state to any other state. In this way, our system does not store any information which is invariant under continuous deformations. That is, it does not hold any *topologically invariant* information.

In light of remark 1.2.2, we find our ordered media system is not complicated enough to build a computer yet because it cannot store information. We rectify this 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 use the term defect.

A defect is a point at which we 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 $\phi : \mathbb{R}^2 \backslash S \to M$ is a continuous map.

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*. Following our general stance on topological rigor, we omit the precise definition of defect-mobile deformation.

The vision for building our computer is that the experimenter should have control of the trajectories of the defects, but no control over the rest of the system. This means that the system will trasform under defect-mobile deformations with definite defect paths chosen by the experimenter, but the details of the rest of the deformation is arbitarily and

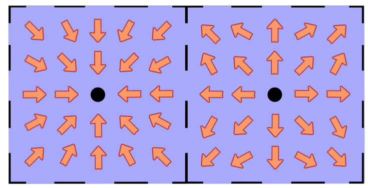


Figure 1.7: Two defects in the xy-model

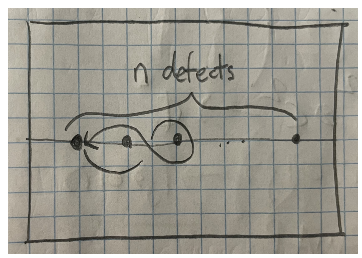


Figure 1.8: Defects on a line, with a sample trajectory of one particle around the others.

uncontrollable. The principle that the details of the deformation are uncontrollable comes from the fact that we expect the individual objects making up the ordered media to by noisy - the are prone to uncontrolled transformations and errors. The defects, however, are made up of many objects and are stabilized by the assumption that there is a physical mechanism which forces most nearby objects to have similar states.

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 topologically-distinct states of this system:

$$\binom{\text{information storage}}{\text{space}} = \binom{\text{states with } n \text{ defects}}{\text{arranged in a line}} \Big/ \binom{\text{defect-fixed}}{\text{deformation}}$$

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. This process is described visually in Figure 1.5

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

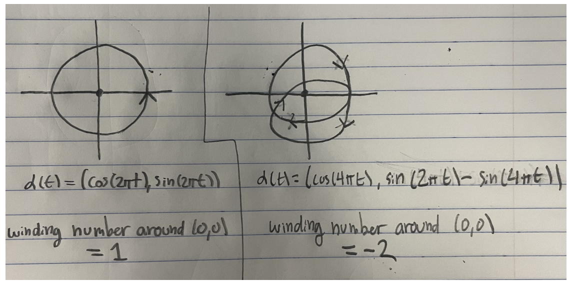


Figure 1.9: Examples of loops in $\mathbb{R}^2$.

works.

1.2.3 The fundamental group

To understand topological computation we will need to put in some real work analysing defects in ordered media. Our main technical ingredient will be a construction from topology known as the *fundamental group*. In this section we will define the fundamental group and apply it to ordered media.

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. Formally, we define a loop in a topological space M to be a continuous map $\alpha : [0,1] \to M$ such that $\alpha(0) = \alpha(1)$.

A clever observation is that the space of loops can be endowed with the structure of a group. A group, by definition, has a group operation. A natural choice of group operation on the space of loops is *composition*. Given two loops we can compose them by first following one loop and then following the other.

Importantly, composing loops has a subtlety. To compose, we glue the endpoint of one loop to the start point of the other. However, loops do not have marked start and end points so this composition rule is not well-defined! To fix this issue, we work with loops that do have a distinguished start and end point. Formally, we define a *based loop* in a topological space M to be a pair (α, m) where $m \in M$ is a point known as the *basepoint* of the loop, and $\alpha : [0,1] \to M$ is a continuous map such that $\alpha(0) = \alpha(1) = m$. The composition of based loops is well-defined. Given two based loops α_0, α_1 in M with basepoint $m \in M$, we define their composition to be

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

The reason we need to add the factors of two 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 by a factor of two. This composed map is continuous at $s = 1/2$ because the left and right limits of $(\alpha_1 \circ \alpha_0)(s)$ are both equal to m.

Despite being well-defined, composition does *not* endow the space of based loops in a topological space with the structure of a group. The issue that the axioms of associativity, unit, and inverse all fail to hold. A clever way to fix these problems and to make the resulting group more universal is to only consider equivalence classes of based loops up to deformations which preserve the basepoint. This means that if there is a continuous deformation between two loops which leaves the basepoint fixed along the entire deformation, then the two loops are considered to be equivalent. It is not difficult to verify that the composition rule for based loops is well-defined on such equivalence classes, and gives rise to the *fundamental group of a topological space M with basepoint $m \in M$*:

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

We denote the equivalence class of the based loop α by $[\alpha] \in \pi_1(M, m)$. The identity element in the fundamental group is the equivalence class of the trivial loop $\alpha(s) = m$ which stays at its basepoint and doesn't move. Inverses are given by reversing orientation. That is, the inverse of $[\alpha]$ is the equivalence class of $\alpha^{-1}(s) = \alpha(1 - s)$.

Example 1.2.3. The good first fundamental group to compute is $\pi_1(\mathbb{R}^2, 0)$. Suppose that α is a loop in $\mathbb{R}^2$ based at 0. The define $\alpha_t(s) = t\cdot\alpha(s)$ for $0 \leq t \leq 1$. The maps $\alpha_t : [0, 1] \to \mathbb{R}^2$ are loops based at 0 becasue $\alpha_t(0) = t \cdot \alpha(0) = 0$ and $\alpha_t(1) = t \cdot \alpha(1) = 0$. Hence, the family of loops α_t provides a basepoint preserving deformation from $\alpha_1 = \alpha$ to the constant map $\alpha_0 = 0$. Hence, all loops in $\mathbb{R}^2$ based at 0 are equivalent to the constant map in the fundamental group so $\pi_1(\mathbb{R}^2, 0) = 0$. Applying translations, we find more generally that $\pi_1(\mathbb{R}^2, m) = 0$ for any $m \in \mathbb{R}^2$.

Example 1.2.4. Another important important fundamental group to compute is $\pi_1(\mathbb{R}^2\backslash\{p\}, m)$ for distinct points, $p, m \in \mathbb{R}^2$. Every loop α in $\mathbb{R}^2$ goes around p some total number of times, which we call the *winding number* of α around p. We count counterclockwise trajectories around p as positive and clockwise trajectories around p as negative, so that the winding number is an integer in $\mathbb{Z}$. Composing loops corresponds to adding winding numbers. It can be shown that the winding number provides a complete characterization of loops in $\mathbb{R}^2\backslash\{p\}$, and thus we arrive at an isomorphism of groups $\pi_1(\mathbb{R}^2\backslash\{p\}, m) \cong \mathbb{Z}$. The loops in figure 1.9 have their winding numbers given as an illustration of the concept.

Remark 1.2.5. A point to emphasize is that $\pi_1(M, m)$ does *not* capture the space of loops in M based at m up to arbitrary deformation - it only captures the space of loops in M based at m under basepoint preservind deformations, by definition. Sometimes there are ways of deforming continuously between two loops, but such a deformation must neccecarily move the basepoint. The space of loops in M based at m under arbitrary deformations is equal to the space of *conjugacy classes*[1] in $\pi_1(M, m)$:

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

The intuition for this formula is as follows. Let α be a loop based at m. Let α' be the same loop but with a different choice of basepoint m'. 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 $\alpha = \epsilon^{-1} \circ \alpha' \circ \epsilon$, as depicted in figure 1.10. Hence, choosing different basepoints amounts to conjugation on the level of loops.

[1] Recall that a conjugacy class in a group G is an equivalence class of elements $g \in G$ under the equivalence relation where g is equivalent to h whenver there exists k for which $g = khk^{-1}$.

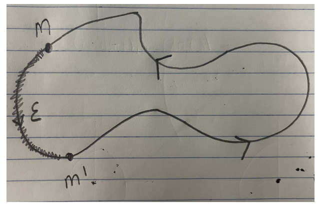


Figure 1.10: Illustration of why changing basepoints behaves as conjugation on loops .

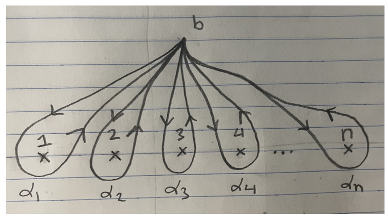


Figure 1.11: Defects arranged in a line with distinguished counterclockwise loops around each defect.

We can now 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 $S \subset \mathbb{R}$ 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 $(\phi \circ \alpha)(0) = (\phi \circ \alpha)(1) = \phi(b)$. The equivalence class of this loop up to basepoint preserving deformation is an element of $\pi_1(M, \phi(b))$. Given any state ϕ and given any loop α based at b, we denote the corresponding element of $\pi_1(M, \phi(b))$ by $\phi_*(\alpha)$, which we call 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 and do not go around any other defects. This setup is depicted in figure 1.11.

Given any ordered media state ϕ on this system, we can take the winding numbers $\phi_*(\alpha_i) \in \pi_1(M, \phi(b))$ of each loop α_i. Applying a defect-fixed deformation could change the values $(\phi_*(\alpha_i))_{i=1}^n$ by a simultaneous conjugation on each component, because the defect-fixed deformation could change the value $\phi(b)$ assigned to the basepoint. Up to this global conjugation, however, the values $(\phi_*(\alpha_i))_{i=1}^n$ give a complete characterization of the information in ϕ which is invariant under defect-fixed deformations.

We now consider the behavior of these winding numbers $\phi_*(\alpha_i)$ under defect-mobile deformation. A defect mobile homotopy will have the effect of moving the defects around each other. Suppose that we have winding numbers $\phi_*(\alpha_i) = g_i \in \pi_1(M, \phi(b))$ for each $1 \leq i \leq n$. Let $\tilde{\phi}$ be a state which is obtained by performing a defect-mobile deformation which moves defect i above and around defect $i + 1$, and which moves defect $i + 1$ below

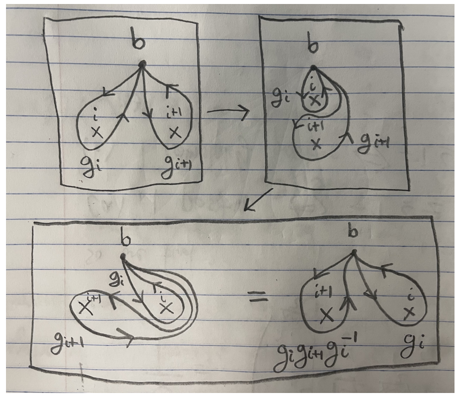


Figure 1.12: Illustration of the effect of exchanging defects on winding numbers.

and around defect i. This swap will result in a new state $\tilde{\phi}$ which is well-defined up to defect-fixed deformation. Denote the winding numbers $\tilde{\phi}_*(\alpha_i) = \tilde{g}_i \in \pi_1(M, \phi(b))$.

At every step along the defect-mobile deformation from ϕ to $\tilde{\phi}$ a loop can be drawn around defect i connecting it to the basepoint b so that these loops change continuously and never cross defect $i+1$. This means that the loop α_i at the beginning of the defect-mobile deformation is continuously deformed to the loop α_{i+1} after the deformation, and thus $\tilde{g}_{i+1} = g_i$. We observe additionally that the defect-mobile homotopy made no changes outside of a region localized around the defects i and $i+1$ so the total winding number around defects i and $i+1$ must be preserved. Thus, $\tilde{g}_i\tilde{g}_{i+1} = g_i g_{i+1}$. Combining these formulas, we conclude moving defect i above and around defect $i+1$ has the following effect on winding numbers:

$$\tilde{g}_{i+1} = g_i, \qquad \tilde{g}_i = g_i g_{i+1} g_i^{-1}.$$

The above process is illustrated in figure 1.12. If instead defect i moves below and around defect $i+1$, the corresponding change in winding numbers is

$$\tilde{g}_{i+1} = g_{i+1}^{-1} g_i g_{i+1}, \qquad \tilde{g}_i = g_{i+1}.$$

The last ingredient we discuss are the locally measurable quantities in our system. Winding numbers are useful invariants of a state under defect-fixed deformation, but they are dependent on the choice of basepoint used. This means that the information encoded in the winding number is spread out over the whole region between the defect and the basepoint. This nonlocal nature makes it hard or impossible to measure in most reasonable physical implementations. A more readily measurable quantity is the winding number of a defect up to arbitrary deformation. That is, the conjugacy class in $\pi_1(M, \phi(b))$ associated to the defect. This conjugacy class can be computed using loops that are arbitararily close to the defect. Thus, it is a local quantity and can be effectively measured in physical implementations.

It is also desirabe to have a mechanism for reading out some non-local information about states in ordered media. A good way to do this is by fusing defects. Fusing defects is the process where nearby defects are brought close together until they act like a single defect. Fusion must preserve total winding number, and thus if two defects with winding number g_1, g_2 are fused then their resulting winding number is $g_1 g_2$. The conjugacy classes of g_1 and g_2 are not enough to determine the conjugacy class of $g_1 g_2$, and thus fusing two defects and then measuring the conjugacy class of their winding number gives access to more informaiton. In a sense, it gives access to the non-local information which was being stored between the two defects which are fused.

A sample measurement pattern is as follows. Suppose that ϕ is a state with n defects arranged in a line as before, and let us denote the winding numbers $\phi_*(\alpha_i) = g_i$. Local measurements give us access to the conjugacy classes of all of the elements g_i. By fusing the defects into the left-most defect one by one, we can access the conjugacy classes of g_1, $g_1 g_2$, $g_1 g_2 g_3$,... all the way up to $g_1 g_2 g_3 ... g_n$. In favorable situations these measurements can give a large amount of non-local information.

1.2.4 Topological classical computation

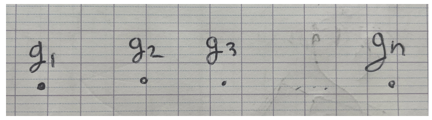
We are now ready to describe the theory of topological classical computation. In the subsection 1.2.3, we showed how all the topological information about defects in ordered media is controlled by the fundamental group $G = \pi_1(M, m)$ of the order space M relative to some basepoint $m \in M$. This is the heart of the algebraic theory of topological computing. Even though our physical model is complicated, most information theoretic properties can understrood by analysing the algebraic structure G. In fact, we can now 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. This gives the following schematic for our discussion:

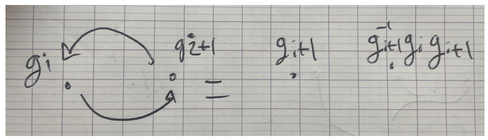
$$\begin{tikzcd} & (\text{groups}) \arrow[dr] & \\ (\text{ordered media}) \arrow[ur] \arrow[rr] & & \left(\substack{\text{topological classical}\\ \text{computing}}\right) \end{tikzcd}$$

That is, our construction of topological classical computers from ordered media *factors through* group theory. This schematic is similar to the overall structure of this book, which we said before is summarized by this diagram:

$$\begin{tikzcd} & \left(\substack{\text{modular}\\ \text{categories}}\right) \arrow[dr] & \\ \left(\substack{\text{topologically}\\ \text{ordered systems}}\right) \arrow[ur] \arrow[rr] & & \left(\substack{\text{topological quantum}\\ \text{computing}}\right) \end{tikzcd}$$

Remark 1.2.6. Just like how groups are the structures which control the algebraic theory of ordered media, modular categories are the structure which control the algebraic theory topologically ordered systems. In fact, this analogy this analogy can be made precise. The idea is that ordered media can be *quantized*, turning it from a classical to a quantum system. This quantized version of ordered media is known as *discrete gauge theory*. Quantization is a subtle procedure, which we will discuss in section **??**. When the group $G = \pi_1(M, m)$ is infinite the quantization procedure goes wrong, because there are divergences in the formulas. Hence, quantization of ordered media only works for finite groups. The algebraic structure controlling the quantized version of ordered media based on a finite group G is $\mathfrak{D}(G)$, where $\mathfrak{D}(G)$ is a modular category constructed using the finite group G. So, in a real sense, modular categories can be seen as vast quantum generalizations of finite groups. This is often a useful perspective to take.





We now set up topological classical computing with ordered media, along the same lines as our abstract setup in subsection 1.2.1. Our system consists of n defects on a straight line. These defects are labeled with group elements $g_i \in G$, for $1 \leq i \leq n$. These labels correspond to winding numbers around loops:

Braiding g_i under and around 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. The types of the defects are local observables which can be measured by the experimenter.

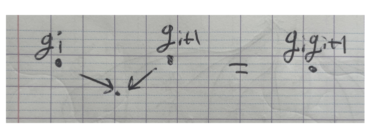
Our previous discussion of braiding was heuristic, but we are now ready to put it on firm footing. We first try to capture our intuitive notion of braiding from before. Intutively, we consider a braiding operation to be some way of moving n points arrangened on a line in $\mathbb{R}^2$ around each so that the end position of each point is equal to the start position of some other point. For example, moving one point under and around another point is a braiding operation. Continuous deformations do not change the effect of braiding operations on topological information, so long as they do not change the initial or final positions of any of the points. Thus, for any integer $n \geq 1$ we define the *braid group on n stands*:

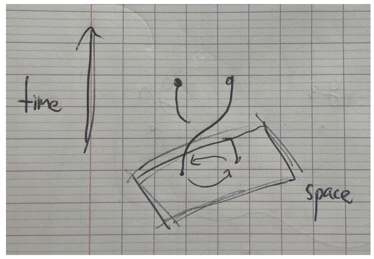
$$B_n = (\text{braiding operations on } n \text{ points})/(\substack{\text{endpoint-preserving} \\ \text{continuous deformations}}).$$

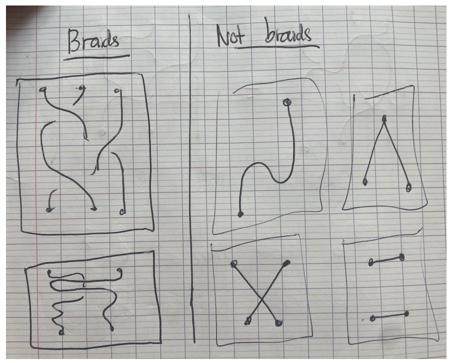
We call elements of B_n *braids*. We call the trajectories of the individual points through time *strands*. We can also define the *pure braid group on n strands P_n* to be the subset of braids such that the final position of every point is equal to its initial position. Elements of P_n are called *pure braids*.

To facilitate our discussion of braids, we use a graphical notation which tracks the trajectories of the points through time. For instance, the braiding operation in the two-strand braid groupB_2 which moves one point above and around the other point is represented through the following diagram:

The braid group is called a group because it has a natural group structure on it induced by composition. Given any two braiding operations on n points, composing them will give another braiding operation! Composition is well-defined on equivalence classes under continuous deformation, and thus it gives a well-defined group structure. The unit element

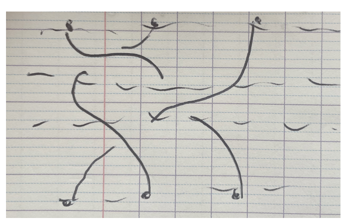






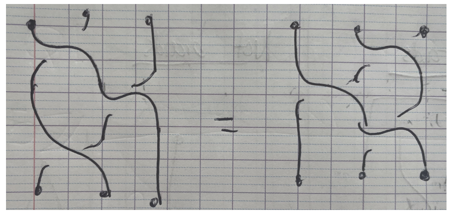
for this group structure is the equivalence class of the braiding operation which does not move the points at all, and the inverse of a braid comes from taking a braiding operation and then reversing its direction in time. This turns B_n into a group, and P_n into a normal subgroup.

The key insight in putting the braid group on a rigorous algberaic footing is to observe that every braid can be obtained by repeatedly composing nearest-neighbor swaps between points. This is done by chopping it its spacetime diagram into slices which each contain an individual swap, as shown below:



If two crossings happen at the same time and hence cannot be seperated by chopping, then the braid is first deformed so that the crossings happen at seperate times and then the braid is chopped. This decomposition observation has a quite concrete implication for the group theory of B_n. For every $1 \leq i \leq n-1$, define the braid σ_i to be the equivalence class of the braiding operation which moves point i above and around point $i+1$. By chopping braidins into indivudal swaps, we conclude that B_n is generated as a group by the braids σ_i, $1 \leq i \leq n-1$.

These generators σ_i, $1 \leq i \leq n-1$, satisfy several relations in B_n. The obvious relations



between them is that σ_i commutes with σ_j whenever $|i-j| \geq 2$. This is because in this case σ_i and σ_j act on different strands, and hence can be deformed past each other without issues. The subtle relation is what happens when $j = i+1$. In this case, we observe the following equality of braids:

Algebraically, this is the identity

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}.$$

These relations we have obtained on the generators σ_i of B_n, in fact, generate the space of all relations between the σ_i. This means that we have the following presentation for the group B_n:

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

We do not prove that this presentation of B_n is correct, because our notions from topology are not rigorous enough to allow for such a proof. Instead, we take this presentation as an alternative algebraic definition of the braid group! At this point 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 records the fact that moving defects by braids acts on the stored information in the way we expect:

Proposition 1.2.7. *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 $\mathrm{Sym}(G^n)$ *of set-wise permutations of the Cartesian product G^n.*

Proof. To prove this proposition we need to check that the group elements $\rho_n(\sigma_i) \in B_n$ satisfy the equations in the presentation of the braid group. The relation $\rho_n(\sigma_i)\rho_n(\sigma_j) = \rho_n(\sigma_j)\rho_n(\sigma_i)$ for $|i-j| \geq 2$ follows from the fact that $\rho_n(\sigma_i)$ and $\rho_n(\sigma_j)$ act on disjoint factors of G in G^n.

The relation $\rho_n(\sigma_i)\rho_n(\sigma_{i+1})\rho_n(\sigma_i) = \rho_n(\sigma_{i+1})\rho_n(\sigma_i)\rho_n(\sigma_{i+1})$ follows evaluating both permutations on a sample element $(g_i)_{i=1}^n \in G^n$ and verifying that they give the same result. Namely, we compute that

$$\begin{aligned}
&\rho_n(\sigma_i)\rho_n(\sigma_{i+1})\rho_n(\sigma_i)(...g_i, g_{i+1}, g_{i+2}...)\\
=&\rho_n(\sigma_i)\rho_n(\sigma_{i+1})(...g_{i+1}, (g_{i+1}^{-1}g_i g_{i+1}), g_{i+2}...)\\
=&\rho_n(\sigma_i)(...g_{i+1}, g_{i+2}, (g_{i+2}^{-1}g_{i+1}^{-1}g_i g_{i+1}g_{i+2})...)\\
=&(...g_{i+2}, (g_{i+2}^{-1}g_{i+1}g_{i+2}), (g_{i+2}^{-1}g_{i+1}^{-1}g_i g_{i+1}g_{i+2})...)
\end{aligned}$$

and

$$\begin{aligned}
&\rho_n(\sigma_{i+1})\rho_n(\sigma_i)\rho_n(\sigma_{i+1})(...g_i, g_{i+1}, g_{i+2}...)\\
=&\rho_n(\sigma_{i+1})\rho_n(\sigma_i)(...g_i, g_{i+2}, g_{i+2}^{-1}g_{i+1}g_{i+2}...)\\
=&\rho_n(\sigma_{i+1})(...g_{i+2}, (g_{i+2}^{-1}g_i g_{i+2}), (g_{i+2}^{-1}g_{i+1}g_{i+2})...)\\
=&(...g_{i+2}, (g_{i+2}^{-1}g_{i+1}g_{i+2}), (g_{i+2}^{-1}g_{i+1}^{-1}g_i g_{i+1}g_{i+2}).
\end{aligned}$$

Thus, the map ρ_n is a well-defined group homomorphism. □

The final ingredient we need for our computer is the ability to create pairs of defects. Just like how a pair of defects with winding numbers g and g^{-1} could spontaneously fuse to give a defect with winding number $gg^{-1} = 1$, the opposite process could start with a state with no defects and create a pair of defects with winding numbers g and g^{-1}. We can now give the full list of operations which we require the experimenter to be able to perform for building a topological classical computer using ordered media:

1. The ability to create an ordered media state with no defects;
2. The ability to create pairs of defects with specified winding numbers;
3. The ability to perform defect-mobile deformations with specified defect trajectories;
4. The ability to measure the conjugacy class of the winding number associated to a defect.

Before giving a general prescription of how to make a computer based on finite group G, we give a worked example. In this example, we use the group $G = A_5$ of all even permutations on five letters. We recall the basic features of the alternating group. It is a normal subgroup of the group $\mathrm{Sym}(\{0,1,2,3,4\})$ of permutations on a five-element set. There is a canonical group homomorphism

$$\mathrm{sign} : \mathrm{Sym}(\{0,1,2,3,4\}) \to \mathbb{Z}_2$$

which sends a permutation in $\mathrm{Sym}(\{0,1,2,3,4\})$ to its sign, a $\mathbb{Z}_2$-valued invariant. The alternating group A_5 is defined to be the kernel of this map, $A_5 = \ker(\mathrm{sign})$. In our context, the simplest way to define the sign is as follows. We observe that the symmetric group is the group obtained from taking the braid group and only remembering the endpoints of the braids, and not the exact way they bend around each other. Alternatively, the symmetric group is the group obtained from the braid group and identifying overcrossings with undercrossings. It is now a clear topological fact about braids that the number of overcrossings minus the number of undercrossings is an invariant of the braid - this can be also checked algebraically via the presentation we gave before. Thus, once overcrossings and undercrossings have been identifeid, we find that the total number of crossings is a $\mathbb{Z}_2$-valued invariant. This is the sign.

The set of all permutations on five letters has $5! = 120$ elements. Since A_5 is the kernel of a surjective map onto a two-element group, its order is $120/2 = 60$. We write the elements of A_5 using cycle notation. We denote by $(i_0, i_1 ... i_n)$ the cyclic permutation which sends i_0 to i_1, i_1 to i_2, all the way until i_n which sends to i_0. The notation $(i_0 ... i_n)(j_0 ... j_m)$ refers to the composition of cycles, where first we permute by $(i_0 ... i_n)$ and then by $(j_0 ... j_m)$. With this notation in mind, we can move on to making the computer.

Our information is stored in pairs of defects whose overall winding number is trivial. In particular, we choose the following perscription for our binary zero and one states:

$$|0\rangle = \boxed{\underset{(04321)}{\times} \quad \underset{(04321)^{-1}}{\times}}\,, \qquad |1\rangle = \boxed{\underset{(03124)}{\times} \quad \underset{(03124)^{-1}}{\times}}\,.$$

To encode n bits of information we thus use $2n$ defects, put into pairs with opposite winding number. The fact that we can create a state with these pairs comes from points (1) and (2) of our assumptions on the experimenter.

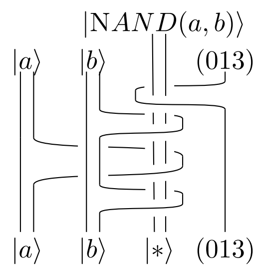
We now describe the implementarion of logic gates on our computer. Our basic logic gate is the NAND gate, defined by the truth table

$$\mathrm{N}AND(a, b) = \begin{cases} 0 & a = b = 1 \\ 1 & \text{otherwise.} \end{cases}$$

We implement the NAND gate as follows. We define a new state:

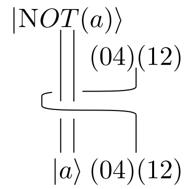
$$|*\rangle = \boxed{\underset{(02143)}{\times} \quad \underset{(02143)^{-1}}{\times}}\,.$$

It is straightforward to verify that the following braid relation:

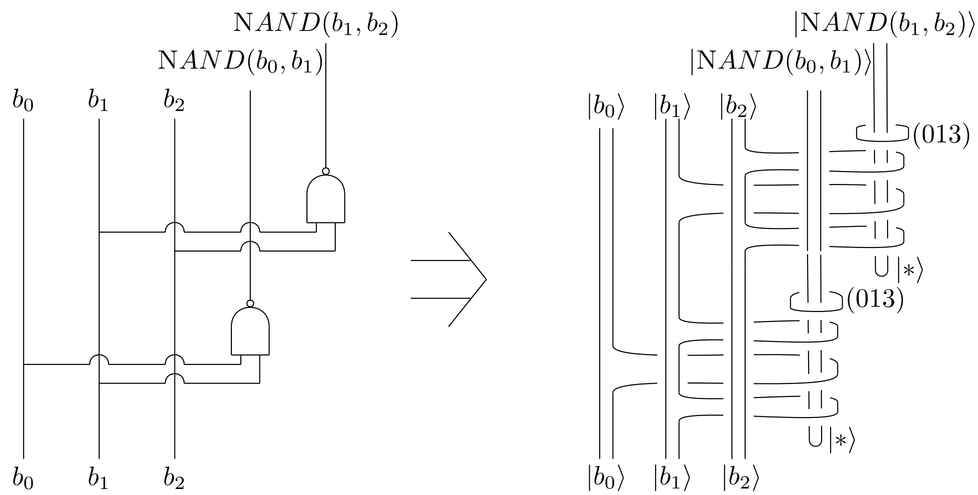


That is, braiding $|a\rangle$ and $|b\rangle$ in the fashion described in the above picture around the non-computational state $|*\rangle$ has the effect of replacing the state $|*\rangle$ with $|\mathrm{N}AND(a, b)\rangle$.

Similarly, one can verify the following protocol for implementing the NOT gate, which flips the value of a bit from 0 to 1 and vice-versa:



It is a well-known fact from computer science that the NAND gate and NOT gate can be used together to implement any boolean circuit. That is, every function $f : \{0,1\}^n \to \{0,1\}^n$ can be computed by taking the input bits, computing the NAND or NOT of these input bits in new registers, and the repeatedly computing more NANDs and NOTs in successive layers. A typical conversion from a standard boolean circuit to a topological circuit using $G = A_5$ woud look like this:



The general method for making a topological classical computer follows in complete analogy from the case of $G = A_5$. To begin, one chooses a conjugacy class C in G with more than one element. This is possible whenever G is non-abelian. Then, we choose two distinct elements g_0, g_1 in G. We define a computational state $|0\rangle$ to be a pair of defects with winding number g_0, g_0^{-1} and we define $|1\rangle$ to be a pair of defects with winding number g_1, g_1^{-1}. Then, we find a scheme for implementing the NAND and NOT gates by braiding around some other defect, possibly including extra defects which are included just for the purpose of imeplementing the gate. We then use the NAND and NOT gates to implement all boolean circuits.

Let us analyse the above proposal in more detail. Suppose we want to implement the NAND gate of two bits b_0, b_1. The first step is to chose some group element $h \in C$, and initialize a pair of defects with winding numbers h, h^{-1}. Then, we procedure to braid the defects $|b_0\rangle$ and $|b_1\rangle$ around the h, h^{-1} defect pair, as well as creating other auxillary defects and braiding them around the h, h^{-1} pair. At the end of the process, the h defect will have a new winding number, $f(g_{b_0}, g_{b_1}) h f(g_{b_0}, g_{b_1})^{-1}$. Here, $f : \{0,1\}^2 \to G$ is some function which is a product of the inputs g_{b_0}, g_{b_1}, their inverses, and fixed elements of G, any of which may appear multile times in the product. The condition we want is that

$$f(g_{b_0}, g_{b_1}) h f(g_{b_0}, g_{b_1})^{-1} = \begin{cases} g_0 & \text{if } \mathrm{N}AND(b_0, b_1) = 0 \\ g_1 & \text{if } \mathrm{N}AND(b_0, b_1) = 1. \end{cases}$$

Since g_0, g_1, and h are all in the same conjugacy class, a function f with the above property must exist. The only question is whether or not it is expressible as a product of the inputs g_{b_0}, g_{b_1}, their inverses, and fixed elements of G. If so, then a universal topological classical computing scheme is possible.

Clearly, if G is abelian then the above scheme will not work. This is because we will not even be able to do the first step of the algorithm, which is to pick a conjugacy class with at least two elements. However, just being nonabelian is not enough. The group needs to be *sufficiently non-abelian* so that conjugation is powerful enough to implement the NAND gate. It turns out that a sufficient condition is that G is a non-abelian *simple* group. We recall that a simple group is a group with no proper non-zero normal subgroups.

In this case we have the following important result, which paired with the above discussion immediately tells us that non-abelian simple groups can be used to make a universal classical computer:

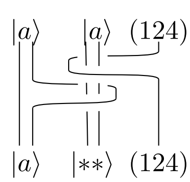
Theorem 1.2.8 (Mochon; Maurer-Rhodes)**.** *Let G be a non-abelian simple group. Every function $f(g_1, g_2 ... g_n) : G^n \to G$ can be expressed as the product of the inputs $\{g_i\}$, their inverses $\{g_i^{-1}\}$, and fixed elements of G, any of which may appear multiple times in the product.*

Proof. The original proof is in a paper of Maurer-Rhodes [**?**]. The connection to topological computing was dicovered in [**?**], where a new constructive proof was also given. □

Remark 1.2.9. In light of Theorem 1.2.8, it is natural to see why we chose the group A_5 in our example of topological classical computing. The group A_5 of order 60 is the smallest non-abelian simple group! This concludes our overview of the subject.

Exercises:

1.1. Verify the protocol for copying the value of a bit using a $G = A_5$ topological classical computer,



where

$$|{*}{*}\rangle = \boxed{\overset{\times}{(02431)} \quad \overset{\times}{(02431)^{-1}}}$$

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

1.3. WORK: definition of the braid group as a fundamental group.

1.4. WORK: It is a theorem that for any non-solvable finite group G, there exists a normal subgroup P of G and a normal subgroup N of P such that P/N is simple. Use this to deduce a universal classical computation scheme based on any non-solvable group.

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 small 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

Lemma 2.1.1. *ike* probability theory, but based on the 2-norm instead of the 1-norm?... Quantum mechanics is what inevitably results." - Scott Aaronson[2]

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.

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

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. Thus, we fix the notation throughout this section:

$$S \text{ is a finite set.}$$

A convement notation for proability distribution is the language of weighted sums. The state $\sum_{x\in S} p_x |x\rangle$ denotes the state with probability $p_x \geq 0$ of having outcome $|x\rangle$, where $\sum_{x\in S} p_x = 1$. The notation $|-\rangle$ for states is known as a *ket*. This is part of so-called *Dirac notation* (or *bra-ket notation*), which is widespread in quantum theory. We use it here to help ease our transition from probability theory to quantum mechancis.

Example 2.2.1. 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. In Dirac notation, we would write

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

[2] Page 112 of Aaronson's "Quantum Computing since Democritus" [?]

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

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

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. They ket insight is that probabilistic processes are *linear.* That is, valid assignments of distributions on S to distributions on S' coming form probability theory will all be restrictions of linear mapas $\mathbb{R}[S] \to \mathbb{R}[S']$.

Example 2.2.2. 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. In this computation, we used the fact that there is a *linear map* result : $\mathbb{R}[\{\text{Ticket } 1, \text{Ticket } 2\}] \to \mathbb{R}[\text{win}, \text{lose}]$. 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 2.2.3 (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 2.2.4 (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. The numbers c_x are not probabilities. They are called *amplitudes*. We say that the state $|\psi\rangle = \sum_{x\in S} c_x |x\rangle$ is in a *superposition* of the different basis states $|x\rangle$.

Remark 2.2.5. In the case where the elements of 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 particle-like state. This is the essence of wave-particle duality in quantum mechanics.

Remark 2.2.6. 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 the energy of this state, it will collapse onto some energy eigenstate. It will collapse onto $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ 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.

Example 2.2.7. A more subtle restricition on the definition of observes is illustrated 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 do not add to one and hence do not give a valid probability distribution. This means that our proposed definition of an observable was invalid.

They key algebraic requirement illustrated by example 2.2.7 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 specifed 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. For simplicity, for all states $|\psi\rangle$, $|\varphi\rangle$ we use the notation

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

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.

Example 2.2.8. 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 value is 10J. This will collapse the state onto $\frac{1}{\sqrt{2}}\,|1\rangle - \frac{i}{\sqrt{2}}\,|2\rangle$.

Algebraically, the result of a measurement will be an orthogonal projection onto the space of states which the observed value of the observable, scaled so that the resulting state is normalized. To state this axiom it is good to introduce some notation.

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

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

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:

Definition 2.2.9. A (finite-dimensional) Hilbert space $(V, \langle \cdot \mid \cdot \rangle)$ is a (finite-dimensional) vector space V, along with a map $\langle \cdot \mid \cdot \rangle : V \times V \to \mathbb{C}$, such that

1. $\langle \cdot, \cdot \rangle$ is linear in the first argument;
2. $\langle x, y \rangle = \overline{\langle y, x \rangle}$ for all $x, y \in V$;
3. If x is non-zero, then $\langle x, x \rangle > 0$.

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

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

.

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 $|\psi\rangle = \sum_{b\in B} c_b \left|b\right\rangle$, then

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

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

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

where $\otimes$ is the tensor product. For those unfamilar with the tensor product, this could be taken as a *definition.* 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 2.2.10 (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

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

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

Remark 2.2.11. The space of operators which send normalized states to normalized states has a very concise charactarization in terms of the *adjoint.* Let V be a Hilbert space, and let $M : V \to V$ be an operator. The adjoint is denoted $M^\dagger$, and is defined to be the unique operator on V such that

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

for all $|\varphi\rangle \in V$. It is verified in Exercise [ref] that this formula always specifies a unique well-defined operator. In fact, the adjoint can be constructed quite succinctly. Relative to any orthonormal basis of V, the adjoint $M^\dagger$ is equal to the *conjugate transpose* of M relative to that basis.

Proposition 2.2.12. *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. ☐

Remark 2.2.13. In a similar spirit to how transformations in quantum mechanics can be characterized as unitary transformations, we can give an alternate characterization of 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 $b \in B$. In the case that v is injective, the set B can now be recovered as the eigenvectors of H, and the values $v(b)$ 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 computing what the elements of B are can be highly complex.

Proposition 2.2.14 (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 2.2.12. 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 2.2.15. (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.

Remark 2.2.16. This equation deserves several comments. First, we comment on terminology. Initially the 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 Schrodinger equation, this is the equation

$$e^{-iH(t+s)}\,|\psi(0)\rangle = e^{-iHt}e^{-iHs}\,|\psi(0)\rangle\,,$$

which follows from proposition 2.2.17.

Proposition 2.2.17. *If A and B are commuting operators, then*

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

Remark 2.2.18. We also need make sure that the Schrodinger equation is consistent with the axioms of quantum mechanics as we have previously developped them. In particular, is it true that 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 2.2.17.

Remark 2.2.19. It is worthwhile to take note of the *units* in the Shrodinger equation. 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

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

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.

Remark 2.2.20. 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 $|\psi(0)\rangle$ is some initial state in a quantum system with extended state space V and Hamiltonian H. Suppose that we have a decomposition $|\psi(0)\rangle = \sum_{x \in B} c_x |x\rangle$ where B is the set of energy eigenstates of H. Then, the Schrodinger equation would tell us that

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

where $v(b)$ is the eigenvalue corresponding to v. In this way, we see that by writing $|\psi(0)\rangle$ 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: I should learn the history of quantum mechanics better. Maybe give references to the many good history books on this topic.

A fantastic place to first learn about quantum mechanics and its principles is the popular science book "Quantum computing since Democritus" [**?**]. A more formal, but still excellent, introduction to finite-dimensional quantum theory is Nielsen-Chuang's book "Quantum computation and quantum information" [**?**]. 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" [**?**], and a good math-oriented text is Hall's "Quantum theory for mathematicians" [**?**].

Exercises:

2.1. WORK: show that the adjoint really is the conjugate transpose

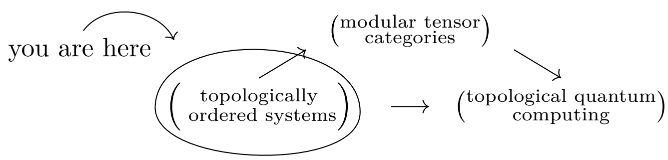
WORK: I need to add somewhere that global phases don't matter, clear up this ambiguity

3 Topological quantum order

3.1 Overview

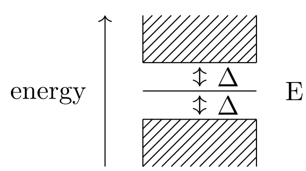
3.1.1 Introduction

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



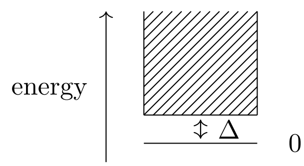
Topological quantum systems are distinguished by the fact that their states don't depend on local properties - they depend only on global topological properties of the system. One way of getting this sort of topological invariance is through *discreteness*. If a system is discrete, all of its parts are 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* topologically 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-eigenspace 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:

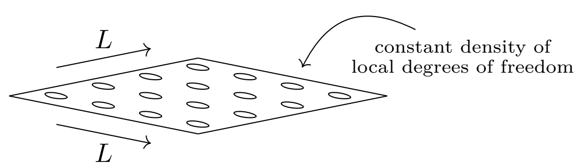


So long as the temperature is much smaller than the energy gap ($T\mathcal{L}\delta$), then our system will remain in the ground state. We say that the system (V, H) *becomes topologically ordered at low temerature.*

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

[WORK: The issue of topological order at nonzero temperature is actually quite subtle. Seeing as in two dimensions there are no self-correcting codes, we can conclude that all topological order is *unstable* at nonzero temperature - it needs the external probes to drive it into the ground state: [**?**]. Another good discussion of topological order at nonzero temperature is [**?**].]

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:

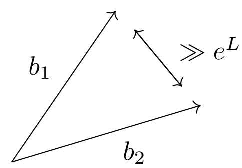


Letting $\dim(V)$ denote the dimension of V, this gives us an assymptotic formula $\dim(V) \sim e^{(\text{const})\cdot L^2}$ where the constant in the exponent depends on the density of quantum degrees of freedom in the system. Let δ_L be the lowest nonzero energy of the Hamiltonian in the size-L system. 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 $>$ $(\text{const}) \cdot L$ sites.

Explicitely, this condition says that there exists a basis $|\psi_i\rangle$ such that

$$\langle \psi_i \,|\, \mathcal{O} \,|\, \psi_j \rangle = 0$$

for all $i \neq j$ and local operators $\mathcal{O}$. Paired with the error correcting code property, these conditions can be succinctly summarized as

$$\langle \psi_i \,|\, \mathcal{O} \,|\, \psi_j \rangle = \lambda \delta_{i,j}$$

Here's a good reference which talks about when all this stuff is physical possible and is fault tolerant - [**?**].]

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 $T\mathcal{L}\delta$, $L \gg 0$. 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 $e^{(\mathrm{const})L}$ times further apart than the basis vectors of $\mathbb{C}[S]$. Hence, the metric on the ground space is dialated by a factor of $e^{(\mathrm{const})L}$, 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 arbitarally 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 $T\mathcal{L}\delta$, 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 $T/e^{(\mathrm{const})L}$. 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 [**?**]. 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 $T/e^{(\mathrm{const})L}$.

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 Hamiltoninan"? What am I missing? Is this something I even want to define it? Add a subsection?]

[WORK: The papers [**?**, **?**, **?**] 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].

[WORK: There's a subtlety that this quantization procedure only works for finite groups. Infinite groups add divergences into the formulas which cause them to fail. There are also deeper physical reasons for this, though. A lack of discreteness on the level of the input group G is associated with *gapless modes* on the level of quantum field theory[**?**]. More generally, though, a lack of discreteness is bad because you lost fault tolerance. The reason that discreteness has to be enfored strictly as a finiteness condition is that we don't just need G to be discrete; we need it's quantum double $\mathfrak{D}(G)$ to be discrete. Just like how in Pontryagin duality discreteness is dual to compactness, in generalized quantum group duality discreteness is dual to compactness. Since $\mathfrak{D}(G)$ is built out of the group and its dual it will be discrete if and only if G is discrete *and* compact, i.e., finite. [**?**]]

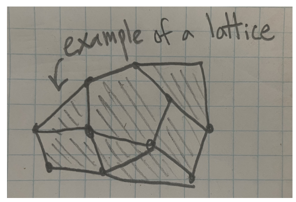
We will go from ordered media to discrete gauge theory in two steps:

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.

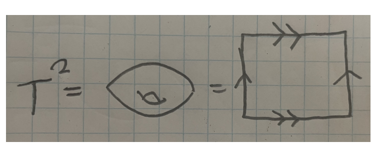
The first natural question to ask is *what is a lattice.* For our purpose a lattice is something like the picture below:



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:

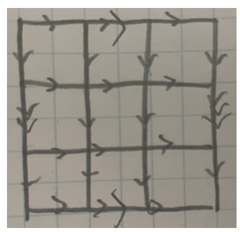
Step 1(a): Choose a directed lattice on the torus;

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:



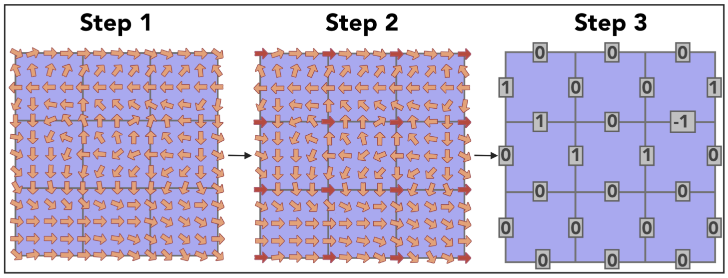
Step 1(b) requires more explanation. The picture to imagine is that we take the state ϕ and twist its values in small neighborhoods around each vertex to enforce the condition $\phi(v) = m$. Formally, this means choosing another state $\tilde{\phi}$ such that $\tilde{\phi}(v) = m$ for every vertex v 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).

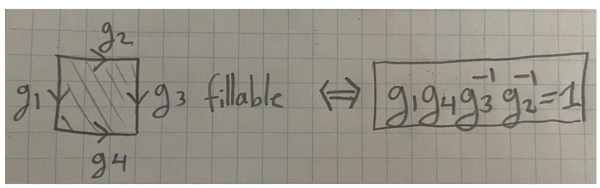
A worked example is shown below in the case that $M = S^1$ is the circle:

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:

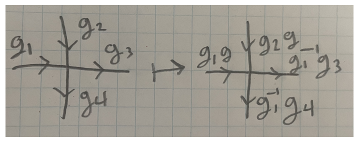


Moreover, *any* coloring of the edges of the lattice by elements of $\pi_1(M, m)$ will come from some map ϕ so long as it satisfies the condition above. This is one of the key formulas of the theory. It is in a real sense a lattice version of the continuity condition, since it is *equivalent* to the 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.

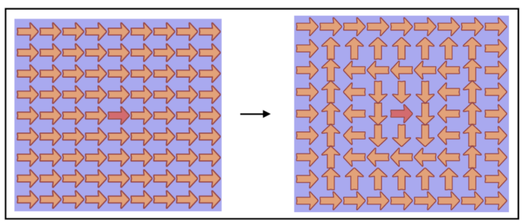
The last thing do deal with in analysing our system is deformation. When analysing states in ordered media, a huge amount of our time was spent on performing continuous deformations. Topological information is defined to be information which is invariant under continuous deformation. What does this correspond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

$$\left(\begin{smallmatrix}\text{topological information}\\ \text{in ordered media}\end{smallmatrix}\right) = (\text{states}) \,/\, \left(\begin{smallmatrix}\text{continuous}\\ \text{deformation}\end{smallmatrix}\right).$$

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

$$\mathbb{C} = \text{span}\left\{ |C\rangle \middle| C \in (\text{flat } G\text{-colorings})/(\text{gauge transformations}) \right\}.$$

This Hilbert space $\mathbb{C}$ 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 $\mathbb{C}$ 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 3.2.1. *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 $A^\dagger_{v,g} = A_{v,-g}$ 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

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

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 3.2.2. *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*

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

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

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

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

$$\mathbb{C} \to \mathbb{C}[\mathrm{Hom}(\pi_1(T^2, v), G)/\binom{\textit{simultaneous}}{\textit{conjugation}}]$$

given by taking winding numbers.

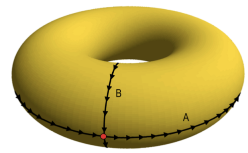
Proof. .[WORK: give proof. I'm scared this could be too hard. It's already] □

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

Proposition 3.2.3. *$\pi_1(T^2, v) \cong \mathbb{Z}^2$ 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 3.2.4. *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 [?]. 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. The ones that jump to mind are dimer models - [**?**, **?**]].

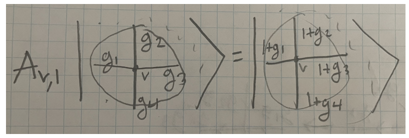
We describe the model now. Because $G = \mathbb{Z}_2$ is abelian, we will switch to additive notation for our group operation. We choose a *non-oriented* lattice structure on the torus. This lattice does not need to be oriented because changing the direction of edges in the lattice corresponds to taking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



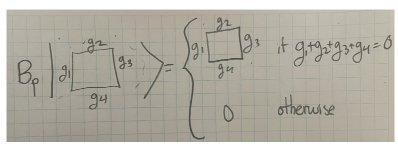
Defining

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

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 3.3.1.

(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] $\square$

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

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

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 3.3.2. *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] $\square$

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 3.3.3. *We have that*

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

Proof. This follows immediately from the above discussion. ☐

We can now solve the toric code:

Proposition 3.3.4. *We have that*

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

Proof. .[WORK: do proof] ☐

Corollary 3.3.5. *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 3.3.6. *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

[WORK:

I've realized that I was wrong about anyons. I thought that they were localized excitations in a topologically ordered system. I was wrong. Anyons are *stable* localized excitations in a topologically ordered system. This stability is what ensures that they will have a well-defined type. This correct definition should make the presentation a lot easier!]

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 3.4.1. 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 $\mathcal{P}_{\mathcal{N}_{R_1, R_2 ... R_n}}$, 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:

$$\boxed{\text{Anyons should be kept far apart}}$$

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 $\mathcal{N}_{R_1, R_2 ... R_n}$. 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 $\mathcal{N}_{R_1, R_2 ... R_n}$ 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.]

[WORK: The notion of anyon types is explaned well by Kawagoe and Levin [**?**]:

quote: We begin with the idea of "anyon types." ... anyon excitation of type a, type b, type c, etc.]

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] [**?**] . 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 [**?**].

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 [**?**]. The subject of anyons was then taken over by Wilczek who published a series of seminal papers on the topic [**?**, **?**, **?**]. 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

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

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

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 progress 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 performing one process followed by performing a second process. Composition is distinguished in its importance for two reasons:

1. Composition is ubiquitous;
2. Many complicated structures can be described in terms of composition.

These two primary sources 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-first 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 about an object of study, making a composition-first technique the only approach possible.

This third point is the situation we find ourselves in with the algebraic theory of topological quantum information. We're trying to give a usable mathematical description of topologically ordered systems. The way we do this is by focusing on anyons (local quasiparticle excitations in topological order). In doing so 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 ways anyons can transform is hard. This involves specifying intricate unitary operators on high-dimensional Hilbert spaces.
3. Describing how these transformations compose with one another is relatively simple. It can be done using explicit-to-describe rules, which are independent of the system size or choice of gapped Hamiltonian.

What to do in this situation is clear: we will take a composition-first approach to anyons. The mathematical structure which allows for an intelligent discussion of composition 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 type of category which fully describes anyons is known as a *modular tensor category*, and these categories 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 mathematics. Before going forward lets define what a category is:

Definition 4.1.1 (Category)**.** A category is the following data:

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

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

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

Such that:

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

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

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

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

Remark 4.1.2. The structure of definition 4.1.1 is very typical of algebra. Roughly, algebra is defined to be the study of algebraic structures. An algebraic structure is some collection operations on some space, with rules outlining how these operations interact with each other. The general way of definding an algebraic structure is to first list its operations, and then list the axioms of how these operations 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.

Example 4.1.3. In this text we have already seen many examples of categories. We list some of them here:

- **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 groups. The objects are 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.

Warning 4.1.4. One subtelty of the defintions in example 4.1.3 is that the collection of objects in some of these definitions are not sets. For instance, the collection of all sets does not itself form a set, due to logical paradoxes such as Bertrand's paradox. A more proper treatment of category theory would restrict to smaller categories (such as the category *finSet* of finite sets) where the collection of objects does really form a set. Alternatively, one can introduce the notation of a *class*, with is a collection of sets defined by some unambiguous property that all objects share. The collection of all objects in **Set** is not a set, but it is a class. In this framework, we call categories whose collection objects and whose hom spaces are all sets a *finite category.* The concerned reader can make all of our discussion correct by restricting to the case of small categories, and defining **Set** to be the space of all sets whose cardinality is at most the size of the real numbers, and in general restricting any definition of a category (such as **Grp**) to spaces whose underlying set whose cardinality has at most the size of the real numbers.

Remark 4.1.5. 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 example 4.1.3 we only described the objects and morphisms, and not the composition 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, we remark that objects in abstract categories are *not* required to be sets and the morphisms are *not* required to be functions of sets. It is important to be aware of the fact that there are some categories for which there is no interpreation of morphisms as functions between sets [**?**].

Remark 4.1.6. We will make several notational shorthands when dealing with categories. We will conflate a category and its set of objects whenever convenient. That is, we will label a category by its set of objects. Additionally, instead of writing "$\mathrm{Hom}_{\mathcal{C}}(A, B)$" we will write "$\mathrm{Hom}(A, B)$" when $\mathcal{C}$ is clear, and we will write "$f : A \to B$" to mean "$f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$". Additionally, we will use a single quantifier to instanciate multiple objects simultaneously. For example, we will use "$\forall f : A \to B$ in $\mathcal{C}$" to mean "$\forall A, B \in \mathcal{C},$ and $\forall f : A \to B$".

Remark 4.1.7. 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 $x \in A$ by lemma 4.1.8. 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.

Lemma 4.1.8. *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. The associativity axiom is satisfied because composition of set functions is associative, and for all $f : A \to B$, $g : B \to A$,

$$(f \circ \mathrm{id}_A)(x) = f(\mathrm{id}_A(x)) = f(x),$$

$$(\mathrm{id}_A \circ g)(x) = \mathrm{id}_A(g(x)) = g(x),$$

so the identity axiom is satisfied. □

Definition 4.1.9 (Isomorphism)**.** Let $\mathcal{C}$ 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*.

Lemma 4.1.10. *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. Suppose that f is a bijection. Then, we can define a map $f^{-1} : B \to A$ which sends $b \in B$ to the unique element $f^{-1}(b)$ such that $f(f^{-1}(b)) = b$, which exists since f is surjective and is unique because f is injective. By definition of f^{-1}, $f \circ f^{-1} = \mathrm{id}_B$. To show that the composition the other direction is the identity, we observe that for all $a \in A$

$$f(f^{-1}(f(a)) = f(a),$$

so $f^{-1}(f(a)) = a$ by the injectivity of f. Thus, f has an inverse. Conversely, suppose that f has an inverse f^{-1}. Then, $f(a) = f(a')$ implies $a = f^{-1}(f(a)) = f^{-1}(f(a')) = a'$ so f is injective. Additionally, for all $b \in B$ we have $b = f(f^{-1}(b))$ so f is surjective. Thus, f is a bijection. We have proved both directions, so our proof is complete. $\square$

Remark 4.1.11. Just like how the category-theoretic definitions of identity maps and isomorphisms are modeled after the abstract properties of identity maps and isomorphisms in the category of sets, many other definitions will be implicitely modeled after the abstract properties of the category of sets or vector spaces. Accompanied with most definitions, there is often an implicit lemma that the usual examples satisfy the axioms of the definition. Going forward, we will rarely remark on these implicit lemmas.

Proposition 4.1.12. *Let $\mathcal{C}$ be a category. Identities in $\mathcal{C}$ are unique. Explicitely, let $A \in \mathcal{C}$ 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. $\square$

Proposition 4.1.13. *Let $\mathcal{C}$ 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. $\square$

Remark 4.1.14. 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. For instance, look at proposition 4.1.13. It applied equally well for showing that inverse elements in groups are unique and for showing that inverses of matrices are unique. Abstractly, proposition 4.1.13 demonstrates why the inverse of any reversible process is unique.

4.2 Structures in category theory

4.2.1 Products and universal properties

In this section we will work on defining important structures in category, with a focus on the broadly applicable principles behind the definitions. In this first subsection we focus on products, our first example of a definition via universal property.

Definition 4.2.1 (Product)**.** Let $A, B \in \mathcal{C}$ be objects in a category. A *product* of A and B is the following data:

1. An object $A \times B \in \mathcal{C}$;
2. A morphism $\pi_A : A \times B \to A$;
3. A morphism $\pi_B : A \times B \to B$;

such that for all other objects $C \in \mathcal{C}$ with morphisms $f_A : C \to A$, $f_B : C \to B$, there exists a unique morphism $f : C \to A \times B$ such that the diagram

$$\begin{tikzcd}
& C \arrow[ddl, "f_A"'] \arrow[d, dashed, "f"] \arrow[ddr, "f_B"] & \\
& A \times B \arrow[dl, "\pi_A"] \arrow[dr, "\pi_B"'] & \\
A & & B
\end{tikzcd}$$

commutes.

Remark 4.2.2. At first glance, the categorical definition of a product may look strange. For a first level of comfort, one should observe that the categorical notion of product agrees with the usual notion of Cartesian product in the category **Set**, by proposition 4.2.3. More generally, the same argument as in proposition 4.2.3 can be used to show that the Cartesian product endowed with the product topology is a product in the category **Top**, the direct sum of vector spaces is a product in the category $\mathbf{Vec}_k$ for all fields k, the Cartesian product endowed with component-wise multiplication is a product in the category **Grp**, and so on.

Proposition 4.2.3. *For all pairs of sets A, B, the triple $(A \times B, \pi_A, \pi_B)$ is a product of A, B in the category* **Set***, where $A \times B$ is the Cartesian product, π_A is the projection of $A \times B$ onto the A component, and π_B is the projection of $A \times B$ onto the B component.*

Proof. Consider a set C and functions $f_A : C \to A$, $f_B : C \to B$. We can define a function $f : C \to A \times B$ by $f(c) = (f_A(c), f_B(c))$. Clearly, this morphism f satisfies $f_A = \pi_A \circ f$ and $f_B = \pi_B \circ f$. Moreover, suppose $f : C \to A \times B$ is any function with $f_A = \pi_A \circ f$ and $f_B = \pi_B \circ f$. Then, the A component of $f(c)$ is $f_A(c)$ and the B component of $f(c)$ is $f_B(c)$. Thus, $f(c) = (f_A(c), f_B(c))$. Thus, we conclude that there is a unique map $f : C \to A \times B$ making the relevant diagram commute, and since C, f_A, f_B were chosen arbitrarily we conclude the result. $\square$

Remark 4.2.4. Even though the Cartesian product is a product in the category of sets, it is *not* true that every categorical product of two sets A, B in **Set** is equal to the Carteisan product. In particular, suppose that D is a set and $i : D \xrightarrow{\sim} A \times B$ is a bijection from D to $A \times B$. Define $g_A = \pi_A \circ i$ and $g_B = \pi_B \circ i$. Then, (D, g_A, g_B) is also a product of A and B. This fact can be seen as follows. Suppose C is set, and $f_A : C \to A$, $f_B : C \to B$ are functions. We can define $f : C \to D$ by $f(c) = i^{-1}((f_A(c), f_B(c)))$. This map satisfies $f_A = g_A \circ f$ and $f_B = g_B \circ f$ since

$$g_A \circ f = (\pi_A \circ i) \circ (i^{-1}(f_A(c), f_B(c))) = f_A(c).$$

This is, however, the only freedom we have for choosing products. Every product of A, B in **Set** will be obtained by starting with $(A \times B, \pi_A, \pi_B)$ and composing with a bijection. To summarize this situation, we say that categorical products are not unique but they are *unique up to isomorphism.* Moreover, given another product (D, g_A, g_B), there is a *unique* isomorphism $i : D \to A \times B$ such that $f_A = \pi_A \circ f$ and$g_B = \pi_B \circ i$. For this reason we say that products are *unique up to unique isomorphism.* The proof for the category of sets is no easier than the general case, which is given in proposition 4.2.5

Proposition 4.2.5. *Let $A, B \in \mathcal{C}$ be objects in a category. Let (C, f_A, f_B), (D, g_A, g_B) be products of A and B. There exists a unique isomorphism $i : C \to D$ such that $f_A = g_A \circ i$ and $f_B = g_B \circ i$.*

Proof. By the universal property of (D, g_A, g_B), there exists a unique morphism $i : C \to D$ making the relevant diagram commute ($f_A = g_A \circ i$ and $f_B = g_B \circ i$). Similarly, by the universal property of C, there exists a unique morphism $j : D \to C$ making the relevant diagram commute ($g_A = f_A \circ j$ and $g_B = f_B \circ j$). Composing, we find that $j \circ i : C \to C$ makes the relevant diagram commute ($f_A = f_A \circ (j \circ i)$ and $f_B = f_B \circ (j \circ i)$). The map $\mathrm{id}_C : C \to C$, however, also makes the relevant diagram commute ($f_A = f_A \circ \mathrm{id}_C$ and $f_B = f_B \circ \mathrm{id}_C$). The universal property of the product says that there is a *unique* map making the diagram commute. Thus, we must have $j \circ i = \mathrm{id}_C$. By an analagous argument using the universal property of D, we find that $i \circ j = \mathrm{id}_D$. Thus, $j = i^{-1}$ and i is an isomorphism as desired. □

Remark 4.2.6. Definition 4.2.1 is our first example of a definition by a *universal property*. The property that the triple $(A \times B, \pi_A, \pi_B)$ is asked to satisfy in the definition is the universal property. In words, we will sometimes say that the product of A, B is universal with respect to the property of having morphisms into A and B. In light of proposition 4.2.5, the categorical definition of product is unique up to isomorphism, and in light of proposition 4.2.3 this unique product is isomorphic to the usual Cartesian product. Thus, at least for the category of sets, definition 4.2.1 is a more-complicated and less-precise way of defining the Cartesian product. There are several general reasons why one might prefer definitions by universal property:

1. Universal properties are common throughout mathematics (and specifically in the study of topological quantum information). It is good to understand their general structure;
2. WORK: make this list better. There's a very well-written list on Wikipedia.

Definition 4.2.7 (Coproduct)**.** Let $A, B \in \mathcal{C}$ be objects in a category. A *coproduct* of A and B is the following data:

1. An object $A \sqcup B \in \mathcal{C}$;
2. A morphism $i_A : A \to A \sqcup B$;
3. A morphism $i_B : B \times A \sqcup B$;

such that for all other objects $C \in \mathcal{C}$ with morphisms $f_A : A \to A \sqcup B$, $f_B : B \to A \sqcup B$, there exists a unique morphism $f : A \sqcup B \to C$ such that the diagram

$$\begin{tikzcd}
& C & \\
& A \sqcup B \arrow[u, dashed, "f"] \arrow[dr, "i_B"'] & \\
A \arrow[uur, "f_A"] \arrow[ur, "i_A"'] & & B \arrow[uul, "f_B"']
\end{tikzcd}$$

commutes.

Definition 4.2.8 (Opposite category)**.** Let $\mathcal{C}$ be a category. The *opposite category* of $\mathcal{C}$ is the category defined as follows $\mathcal{C}^{\mathrm{op}}$. The set of objects of $\mathcal{C}^{\mathrm{op}}$ is the same as the set of objects as $\mathcal{C}$, with the object $A \in \mathcal{C}$ corresponding to the object $A^{\mathrm{op}} \in \mathcal{C}^{\mathrm{op}}$. The hom-sets of $\mathcal{C}^{\mathrm{op}}$ are defined as

$$\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A^{\mathrm{op}}, B^{\mathrm{op}}) = \mathrm{Hom}_{\mathcal{C}}(B, A).$$

The morphism in $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A^{\mathrm{op}}, B^{\mathrm{op}})$ corresponding to $f \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ is denoted f^{op}. Given any $A, B, C \in \mathcal{C}$, and functions $f : A \to B$, $g : B \to C$ we define

$$f^{\mathrm{op}} \circ g^{\mathrm{op}} = (g \circ f)^{\mathrm{op}}.$$

Remark 4.2.9. The category $\mathcal{C}^{\mathrm{op}}$ is intuitively described as "reversing all the arrows in $\mathcal{C}$". It is often a useful category to consider, especially in the context of mathematical physics were we see that the opposite category can be seen as the *time reversal* of $\mathcal{C}$. That is, the physical system analogous to $\mathcal{C}$ where the arrow of time has been reversed. This is also a mathematically fruitful perspective to take, because flipping source and target for arrows is the same as changing the direction of causation.

Remark 4.2.10. Definition 4.2.7 of the coproduct is another definition by universal property. The universal property, of course, is very similar to the universal property of the product. In a formal sense it is the same universal property but with all of the arrows reversed. In particular, proposition 4.2.11 shows that products and coproducts are formally dual in the sense that products (resp. coproducts) in a category $\mathcal{C}$ correspond to coproducts (resp. products) in the opposite category $\mathcal{C}^{\mathrm{op}}$. This is a common theme in category theory. Many notions have corresponding dual notions, and the general terminology for the dual notion is to add the prefix "co-".

Proposition 4.2.11. *Let $A, B \in \mathcal{C}$ be objects in a category. Let $(A \times B, \pi_A, \pi_B)$ be a product of A, B in $\mathcal{C}$. The triple $((A \times B)^{\mathrm{op}}, \pi_A^{\mathrm{op}}, \pi_B^{\mathrm{op}})$ is a coproduct of $A^{\mathrm{op}}, B^{\mathrm{op}}$ in $\mathcal{C}^{\mathrm{op}}$. Similarly, if $(A \sqcup B, i_A, i_B)$ is a coproduct of A, B in $\mathcal{C}$ then $((A \sqcup B)^{\mathrm{op}}, i_A^{\mathrm{op}}, i_B^{\mathrm{op}})$ is a product in $A^{\mathrm{op}}, B^{\mathrm{op}}$ in $\mathcal{C}^{\mathrm{op}}$.*

Proof. We show that $((A \times B)^{\mathrm{op}}, \pi_A^{\mathrm{op}}, \pi_B^{\mathrm{op}})$ is a coproduct. Choose an arbitrary triple $C^{\mathrm{op}} \in \mathcal{C}^{\mathrm{op}}$,$f_A^{\mathrm{op}} : A^{\mathrm{op}} \to C^{\mathrm{op}}$, and $f_B^{\mathrm{op}} : B^{\mathrm{op}} \to C^{\mathrm{op}}$. Then considering the triple (C, f_A, f_B) and applying the universal property of the product, we conclude that there is a unique map $f : C \to A \times B$ making the relevant diagram for the product commute. The dual map $f^{\mathrm{op}} : (A \times B)^{\mathrm{op}} \to C^{\mathrm{op}}$ is thus the unique map making the relevant diagram for the coproduct commute, so $((A \times B)^{\mathrm{op}}, \pi_A^{\mathrm{op}}, \pi_B^{\mathrm{op}})$ is indeed a coproduct. The argument for why $((A \sqcup B)^{\mathrm{op}}, i_A^{\mathrm{op}}, i_B^{\mathrm{op}})$ is a product is analagous. $\square$

Corollary 4.2.12. *Let $A, B \in \mathcal{C}$ be objects in a category. The coproduct of A, B, if it exists, is unique up to unique isomorphism. That is, if (C, f_A, f_B), (D, g_A, g_B) are coproducts of A and B, there exists a unique isomorphism $i : C \to D$ such that $g_A = i \circ f_A$ and $g_B = i \circ f_B$.*

Proof. By proposition 4.2.11 we find that $(C^{\text{op}}, f_A^{\text{op}}, f_B^{\text{op}})$, $(D^{\text{op}}, g_A^{\text{op}}, g_B^{\text{op}})$ are products in $\mathcal{C}^{\text{op}}$. By proposition 4.2.5, we conclude that there is a unique isomorphism between C^{op} and D^{op} making the relevant diagram commute. Taking the opposite of this isomorphism, we conclude that there is a unique isomorphism between C and D making the relevant diagram commute, as desired. $\square$

Remark 4.2.13. Unlike how the product looks roughly similar in all our basic examples of categories, the coproduct can change quite dramatically. For instance, in the category **Set** the coproduct is the disjoint union by proposition 4.2.14. However, the coproduct of two vector spaces V, W in $\mathbf{Vec}_k$ is the direct sum $V \oplus W$ with i_V, i_W given by $i_V(v) = (v, 0)$, $i_W(v) = (0, v)$, for all fields k. The coproduct in **Grp** is especially exotic. Given two groups G, H, their coproduct is the *free product*, defined to be the group whose elements are formal words where each letter is either an element of G or an element of H, and two words are considered equivalent if it is possible to go from one to another by adding/removing copies of the identity elements of G, H or by replacing a product $g_1 g_2$ of adjacent elements by their product (in G or H). For example, the free product of $\mathbb{Z}$ and $\mathbb{Z}$ is the free group on two generators. The definition of free product can sometimes feel cumbersome - it is an example of a case where the universal property can be helpful. Seeing as the free product of finite groups can be infinite, we conclude that the category **finGrp** does not have coproducts. Even though coproducts are unique up to unique isomorphism if they exist, they are not gauranteed to exist.

Proposition 4.2.14. *For all pairs of sets A, B, the triple $(A \sqcup B, i_A, i_B)$ is a coproduct of A, B in the category of* **Set***, where $A \sqcup B$ is the disjoint union of A and B and i_A (resp. B) is the inclusion of A (resp. B) into $A \sqcup B$.*

Proof. Suppose C is a set and $f_A : A \to C$, $f_B : B \to C$ are maps. Then, we can define a map $f : A \sqcup B \to C$ by the formula

$$f(x) = \begin{cases} f_A(x) & \text{if } x \in A \\ f_B(x) & \text{if } x \in B. \end{cases}$$

Moreover, suppose we had any other map $f : A \sqcup B \to C$ such that $f_A = f \circ i_A$ and $f_B = f \circ i_B$. The first condition says that $f(x) = f_A(x)$ for $x \in A$ and the second condition says that $f(x) = f_B(x)$ for $x \in B$, so f must be equal to the map defined above. Thus, we conclude that $(A \sqcup B, i_A, i_B)$ as a coproduct of A, B. $\square$

4.2.2 Functors and natural transformations

Category theory philosophy tells us to care about the relationships between things (or more precisely, how those relationships compose). Moreover, category theory philosophy tells us to care about categories (any self-respecting theory should care about its central object of study). Naively combining these two principles, category theory thus suggests we should care about relationships between different categories. These relationships are called *functors.* Going further, seeing as we care about functors, a naive application of the principles of category theory suggests we should care about the relationships between different functors. These relationships are known as *natural transformations*. Thankfully, this line of reasoning does not go on indefinitely. One could try to define a notation of a relationship between natural transformations, but the resulting notion is trivial. Thus, one is left with exactly two important and fundamental notions to define: functors and natural transformations.

Definition 4.2.15 (Functor)**.** A *functor* from a category $\mathcal{C}$ to a category $\mathcal{D}$ is the following data:

1. A function of objects $F : \mathcal{C} \to \mathcal{D}$;
2. A function of morphisms $F : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$ for all $A, B \in \mathcal{C}$;

such that for all $A, B, C \in \mathcal{C}$, $f : A \to B$, $g : B \to C$,

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

Definition 4.2.16 (Natural transformation)**.** A *natural transformation* from a functor F to a functor G between categories $\mathcal{C}, \mathcal{D}$ is a family of morphisms $\eta_A : F(A) \to G(A)$ for all $A \in \mathcal{C}$ such that the diagram

$$\begin{tikzcd}
F(A) \arrow[r, "\eta_A"] \arrow[d, "F(f)"'] & G(A) \arrow[d, "G(f)"] \\
F(B) \arrow[r, "\eta_B"'] & G(B)
\end{tikzcd}$$

commutes for all $f : A \to B$ in $\mathcal{C}$.

Example 4.2.17. A important family of examples of functors are *forgetful functors*. A forgetful functor is a functor which acts on the level of objects by taking an algebraic structure and forgetting that it satisfies certain axioms or is equipped with certain operations so that it becomes a different algebraic structure, and it acts as the identity on the level of morphisms. For instance, there is a forgetful functor $F : \mathbf{Top} \to \mathbf{Set}$ which takes a topological space and assigns to it its underlying set. There is a forgetful functor $F : \mathbf{Vec} \to \mathbf{Grp}$ which takes a vector space and assigns to it its underlying additive group. There is also a forgetful functors $F : \mathbf{Field} \to \mathbf{Grp}$ from the category of fields to the category of groups which assigns to every fields its underlying additive group. Some functors which are almost like forgetful functors also get called forgetful functors, such as the functor $F : \mathbf{Field} \to \mathbf{Grp}$ which assigns to every field its multiplicative group of non-zero elements. The inclusion functors $F : \mathbf{finSet} \to \mathbf{Set}$ and $F : \mathbf{finGrp} \to \mathbf{Grp}$ from the categories of finite sets (resp. finite groups) to to the category of all sets (resp. groups) can also be viewed as forgetful functors, where we are forgetting the fact that the input objects are finite.

Example 4.2.18. For every $n \geq 1$, there is a functor $\mathrm{GL}_n : \mathbf{Field} \to \mathbf{Grp}$ which assigns to a field k to the general linear group of n by n matrices, $\mathrm{GL}_n(k)$. This map is em functorial (that is, it can be extended to a functor) since every field homomorphism $k \to k'$ induces a group homomorphism $\mathrm{GL}_n(k) \to \mathrm{GL}_n(k')$ by acting via the field homomorphism element-wise on a matrix. It is clear that this assignment is compatible with composition, and is thus a functor. There are many natural transformations between the functors GL_n. For instance, the inverse-transpose $((-)^{-1})^T$ is a natural transformation between the functor GL_n and itself. For every field k, there is a map $((-)^{-1})^T : \mathrm{GL}_n(k) \to \mathrm{GL}_n(k)$ which acts by first taking the inverse of a matrix and then taking its transpose. These maps form a natural transformation, because for any field homomorphism $k \to k'$ there is a commutative diagram

$$\begin{tikzcd} \mathrm{GL}_n(k) \arrow[r, "((-)^{-1})^T"] \arrow[d] & \mathrm{GL}_n(k) \arrow[d] \\ \mathrm{GL}_n(k') \arrow[r, "((-)^{-1})^T"'] & \mathrm{GL}_n(k'). \end{tikzcd}$$

WORK: the determinant is also a good example, and so is the map which pads a matrix with an extra row/collumn. Lots of nice linear algebra natural transformations. Not sure how relevant they are to this book - maybe I can do something better? Perhpas the additive group of matrices, with trace as an example. Want something that I could pull on later.

Definition 4.2.19. The way that functors relate categories and natural transformations relate functors is completely analagous to the way that morphisms relate objects in a category. In particular, we observe that there is a category **Cat** whose objects are categories, and whose morphisms are functors between categories. The identity morphisms in this category are the idenity functors $\mathrm{id}_{\mathcal{C}}$, which act as the identity both on objects and on hom spaces. For any two categories $\mathcal{C} \to \mathcal{D}$, we can define a catgegory $\mathbf{Hom}(\mathcal{C}, \mathcal{D})$ whose objects are functors $\mathcal{C} \to \mathcal{D}$ and whose morphisms are natural transformations. The identity morphisms in this category are the identity natural transformations id_F from a functor to itself which acts by the identity map on $F(A)$ for objects A.

Definition 4.2.20. Two categories are called *isomorphic* if they are isomorphic in the category of categories (denoted $\mathcal{C} \cong \mathcal{D}$), and two functors are called *naturally isomorphic* if they are isomorphic in the appropriate category of functors (denoted $F \cong G$). Two categories $\mathcal{C}$, $\mathcal{D}$ are called *equivalent* if there exists functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ such that $G \circ F \cong \mathrm{id}_{\mathcal{C}}$ and $F \circ G \cong \mathrm{id}_{\mathcal{D}}$ (denoted $\mathcal{C} \simeq \mathcal{D}$).

Remark 4.2.21. If two categories are isomorphic, then they are also equivalent. There are, however, equivalent categories which are not isomorphic. Let $\mathcal{C}$ be a non-empty category for which between any two objects are is always a unique morphism. Then, by proposition 4.2.22, $\mathcal{C}$ is equivalent to the category $\mathbf{1}$ which is defined to have a unique object labeled X and whose only morphism is id_X. We need not have $\mathcal{C} \cong \mathbf{1}$, however. In particular, if $\mathcal{C}$ has at least two objects than it cannot be isomorphic to $\mathbf{1}$ since $\mathbf{1}$ has a single objects and isomorphisms of categories must be bijections of sets of objects.

As an example, given objects $A, B \in \mathcal{D}$ in a category we define a category $\mathbf{Prod}(A, B)$ as follows. The objects of $\mathbf{Prod}(A, B)$ are products (C, f_A, f_B) of A, B. A morphism between (C, f_A, f_B) and (D, g_A, g_B) is a map $h : C \to D$ such that $f_A = g_A \circ h$ and $f_B = g_B \circ h$. That is, morphisms in $\mathbf{Prod}(A, B)$ are the morphisms in $\mathcal{C}$ which respect the additional structure of the triples. By the definition of a product, there is a unique morphism between any two objects in $\mathbf{Prod}(A, B)$ so by proposition 4.2.22 we have $\mathbf{Prod}(A, B) \simeq \mathbf{1}$ whenever the product of A, B exists. Philosophicaly, this language of equivalence says that even though products are not unique, the space of possible products between any two objects is equivalent to a point.

Proposition 4.2.22. *Let $\mathcal{C}$ be a non-empty category for there is a unique morphism between any two objects. Then, $\mathcal{C} \simeq \mathbf{1}$.*

Proof. Define a functor $F : \mathbf{1} \to \mathcal{C}$ by $F(X) = C$, $F(\mathrm{id}_X) = \mathrm{id}_C$ for some $C \in \mathcal{C}$. Define a functor $G : \mathcal{C} \to \mathbf{1}$ by $G(A) = X$, $G(f) = \mathrm{id}_X$ for all $A, B \in \mathcal{C}$, $f : A \to B$. It is clear that $G \circ F = \mathrm{id}_{\mathbf{1}}$. Conversely, we can show that $F \circ G \cong \mathrm{id}_{\mathcal{C}}$. To do this, we can define a natural transformation $\eta : (F \circ G) \to \mathrm{id}_{\mathcal{C}}$ which acts on each component by the unique morphism with the correct source and target. Namely, for all $A \in \mathcal{C}$, η is the unique morphism from $(F \circ G)(A) = F(X) = C$ to $\mathrm{id}_{\mathcal{C}}(A) = A$. The relevant diagram for showing that η is a natural transformation must commute, because there is a unique morphism between any two objects in $\mathcal{C}$ and thus every diagram in $\mathcal{C}$ commutes! Thus, η is indeed a natural transformation. We can see that η is invertible, it acts by invertible maps on all components (since all maps in $\mathcal{C}$ are invertible). Thus, η is a natural isomorphism as desired, so $\mathcal{C} \simeq \mathbf{1}$. $\square$

Example 4.2.23. For all categories $\mathcal{C}$, the functor $i : (\mathcal{C}^{\mathrm{op}})^{\mathrm{op}} \to \mathcal{C}$ defined by $(A^{\mathrm{op}})^{\mathrm{op}} \mapsto A$ and $(f^{\mathrm{op}})^{\mathrm{op}} \mapsto f$ is an isomorphism of categories.

Remark 4.2.24. We can give an alternate definition of the opposite category via a universal property. Given two categories $\mathcal{C}, \mathcal{D}$, we define a *contravariant functor* $F : \mathcal{C} \to \mathcal{D}$ to be an assignment $F : \mathcal{C} \to \mathcal{D}$ of objects and $F : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(F(B), F(A))$ of morphisms for all $A, B \in \mathcal{C}$, such that for all $A, B, C \in \mathcal{C}$, $f : A \to B$, $g : B \to C$,

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

Note that a contravariant functor is not a functor. We will sometimes call a standard functor a *covariant functor* to highlight that it is not contravariant. We observe that by the definition of the opposite category, every contravariant functor $F : \mathcal{C} \to \mathcal{D}$ naturally induces a covariant functor $G : \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ by defining $G(A^{\mathrm{op}}) = F(A)$, $G(f^{\mathrm{op}}) = F(f)$. Moreover, this basic fact about the opposite category can be stated in terms of a universal property. This goes as follows. There is a canonical contravariant functor $i : \mathcal{C} \to \mathcal{C}^{\mathrm{op}}$, which takes $A \to A^{\mathrm{op}}$. This functor has the property that for any category $\mathcal{D}$ and for any contravariant functor $F : \mathcal{C} \to \mathcal{D}$, there exists a unique covaraint functor $G : \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ as defined before, making the diagram

$$\begin{tikzcd} \mathcal{C} \arrow[r, "i"] \arrow[d, "F"'] & \mathcal{C}^{\mathrm{op}} \arrow[dl, "G"] \\ \mathcal{D} & \end{tikzcd}$$

commute. Moreover, for any other pair $(\mathcal{E}, i)$ with $\mathcal{E}$ a category $j : \mathcal{C} \to \mathcal{E}$ a contravariant with the same universal property then there would be a unique isomorphism of categories $I : \mathcal{E} \to \mathcal{C}^{\mathrm{op}}$ such that $I \circ j = i$. That is, the universal property that $\mathcal{C}^{\mathrm{op}}$ turns contravariant functors into covariant functors defines $\mathcal{C}^{\mathrm{op}}$ up to unique isomorphism.

Example 4.2.25. Let $\mathcal{C}$ be a category. For all $A \in \mathcal{C}$, there is a functor $\mathrm{Hom}_{\mathcal{C}}(A, -) : \mathcal{C} \to \mathbf{Set}$ defined by $\mathrm{Hom}_{\mathcal{C}}(A, -)(B) = \mathrm{Hom}_{\mathcal{C}}(A, B)$. This map is functorial because any morphism $f : B \to C$ induces a map $\mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{C}}(A, C)$ by postcomposition. Similarly, there is a contravariant functor $\mathrm{Hom}_{\mathcal{C}}(-, A)$. If a functor $F : \mathcal{C} \to \mathbf{Set}$ is of the form $\mathrm{Hom}_{\mathcal{C}}(A, -)$ or $\mathrm{Hom}_{\mathcal{C}}(-, A)$ for some $A \in \mathcal{C}$, we call it *representable*.

Definition 4.2.26. Let $\mathcal{C}$, $\mathcal{D}$ be categories. We define the *product category* $\mathcal{C} \times \mathcal{D}$ of $\mathcal{C}$ to $\mathcal{D}$ to be the category whose objects are pairs (A, B), $A \in \mathcal{C}$, $B \in \mathcal{D}$, whose morphisms between (A, A') and (B, B') are pairs (f, g), $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, $g \in \mathrm{Hom}_{\mathcal{D}}(A', B')$, and whose composition is defined component-wise. It is simple to check that this definition of the product of categories is an abstract product in the category $\mathbf{Cat}$.

Example 4.2.27. There is a nice rephrasing of the definition of product and coproduct in terms of representable functors. In particular, we claim that products of $A, B \in \mathcal{C}$ are in bijective correspondance with objects $A \times B \in \mathcal{C}$ paired with natural isomorphisms

$$\eta : \mathrm{Hom}(-, A \times B) \xrightarrow{\sim} \mathrm{Hom}(-, A) \times \mathrm{Hom}(-, B).$$

This can be seen as follows. Suppose η is a natural isomorphism as above. Then, we can define $(\pi_A, \pi_B) = \eta_{A\times B}(\mathrm{id}_{A\times B})$. We claim that $(A \times B, \pi_A, \pi_B)$ is a product in $\mathcal{C}$. Suppose that $C \in \mathcal{C}$, $f_A : C \to A$, $f_B : C \to B$ is another triple. Then, we can define $f = \eta_C^{-1}((f_A, f_B))$. By naturality the following diagram commutes:

$$\begin{tikzcd} \mathrm{Hom}(A \times B, A \times B) \arrow[r, "\eta_{A\times B}"] \arrow[d, "\mathrm{Hom}(f, A\times B)"'] & \mathrm{Hom}(A \times B, A) \times \mathrm{Hom}(A \times B, B) \arrow[d, "\mathrm{Hom}(f,A)\times\mathrm{Hom}(f,B)"] \\ \mathrm{Hom}(C, A \times B) \arrow[r, "\eta_C"] & \mathrm{Hom}(C, A) \times \mathrm{Hom}(C, B) \end{tikzcd}$$

following $\mathrm{id}_{A\times B}$ through this square, we get that $f_A = \pi_A \circ f$ and $f_B = \pi_B \circ f$ as desired. Applying this same procedure in reverse allows one to define a natural transformation η given a product $(A \times B, \pi_A, \pi_B)$. Dually, we find that coproducts of $A, B \in \mathcal{C}$ are in bijective correspondance with objects $A \sqcup B \in \mathcal{C}$ paired with natural isomorphisms

$$\eta : \mathrm{Hom}(A \sqcup B, -) \xrightarrow{\sim} \mathrm{Hom}(A, -) \times \mathrm{Hom}(B, -).$$

WORK: Add a remark which introduces "fully faithful" and "essentially surjecive". Then prove that a functor induces an equivalence of categories if and only if it is fully faithful and essentially surjective.

Proposition 4.2.28. *Let $F : \mathcal{C} \to \mathcal{D}$ be a functor. The functor F induces an equivalence of categories $\mathcal{C} \simeq \mathcal{D}$ if and only if it is fully faithful and essentially surjective.*

4.2.3 Linear categories

WORK: I need to add the definition of *zero object*, so that proposition **??** makes sense.

To understand topological quantum information, we will need our categories to be in some real sense quantum mechanical. Quantum systems are always vector spaces over $\mathbb{C}$. Eventually, the morphisms in our categories will directly correspond to quantum states in certain quantum systems. Thus, we need the hom-spaces in our categories to be vector spaces over $\mathcal{C}$. This leads us to study the abstract properties of *linear categories*.

Definition 4.2.29 ($\mathbb{C}$-linear category)**.** A $\mathbb{C}$-linear category is the following data:

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

such that 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 $A, B, C \in \mathcal{C}$.

Definition 4.2.30 ($\mathbb{C}$-linear functor)**.** A $\mathbb{C}$-linear functor between $\mathbb{C}$-linear categories $\mathcal{C}, \mathcal{D}$ is a functor $F : \mathcal{C} \to \mathcal{D}$ such that $F : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$ is a linear map of vector spaces for all $A, B \in \mathcal{C}$.

Remark 4.2.31. When we refer to a functor between two $\mathbb{C}$-linear categories, we will always assume that that functor is $\mathbb{C}$-linear unless otherwise stated. In general, whenever two categories are equipped with extra structure we will assume that functors between those categories respect that structure. There is no notion of a $\mathbb{C}$-linear natural transformation (or, if there were, it would have to be the same as the notion of usual natural transformation).

Example 4.2.32. The category $\mathbf{Vec}_{\mathbb{C}}$ of vector spaces over the complex numbers is $\mathbb{C}$-linear category, since the space of linear maps $\mathrm{Hom}_{\mathbf{Vec}_{\mathbb{C}}}(V, W)$ between any two vector spaces V, W is itself a vector space. Additionally, the product of two $\mathbb{C}$-linear categories is again a $\mathbb{C}$-linear category. So, the category $\mathbf{Vec}_{\mathbb{C}}^n$ of ordered n-tuples of vector spaces (equivalent to the product of n copies of $\mathbf{Vec}_{\mathbb{C}}^n$) is a $\mathbb{C}$-linear category.

Remark 4.2.33. A noteworthy feature of $\mathbb{C}$-linear categories is the existence of *zero morphisms*. Suppose that $A, B \in \mathcal{C}$ are objects in a $\mathbb{C}$-linear category. There is a distinguished morphism $0 : A \to B$, called the *zero morphism*, corresponding to the zero element of $\mathrm{Hom}(A, B)$ as a vector space. The zero element is uniquely identified by the fact that for all $f : B \to C$ and for all $g : C \to A$,

$$f \circ 0 = 0, \qquad\qquad 0 \circ g = 0.$$

Note that the notation being used is ambiguous, since in the formulas above 0 refers to both the zero morphism $A \to B$ but also to the zero morphisms $A \to C$ and $C \to B$. The reason that the zero morphism satisfies these properties is that $\circ$ is a bilinear map, and bilinear maps evaluate to zero on any pair which has zero as one of its components.

Definition 4.2.34 (Biproduct)**.** Let $A, B \in \mathcal{C}$ be objects in a $\mathbb{C}$-linear category category. A *biproduct* (or *direct sum*) of A and B is the following data:

1. An object $A \oplus B \in \mathcal{C}$;
2. The structure of a product $(A \oplus B, \pi_A, \pi_B)$ on $A \oplus B$;
3. The structure of a coproduct $(A \oplus B, i_A, i_B)$ on $A \oplus B$;

such that:

1. $\pi_A \circ i_A = \mathrm{id}_A$ and $\pi_B \circ i_B = \mathrm{id}_B$;
2. $\pi_A \circ i_B = 0$ and $\pi_B \circ i_A = 0$.

Proposition 4.2.35. *For all vector spaces V, W, the direct sum $A \oplus B$ paired with its projections (π_A, π_B) onto its components and its inclusions $i_V(v) = (v, 0)$, $i_W(v) = (0, v)$ is a biproduct in $\mathbf{Vec}_{\mathbb{C}}$.*

Proof. We have observed in remarks 4.2.2 and 4.2.13 that $A \oplus B$ is individually a product and a coproduct. It is immediate that the structures are compatible in the sense of definition 4.2.34, and thus $A \oplus B$ is a biproduct. □

Example 4.2.36. 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

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

where $\dim(V_i) \cdot (\mathbb{C}_i) = \mathbb{C}_i \oplus \mathbb{C}_i \ldots \oplus \mathbb{C}_i$, $\dim(V_i)$ 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 $\mathbf{Vec}_{\mathbb{C}}^n$. In the language of definition 4.2.37, the objects $\mathcal{C}_i$ are the simple objects of $\mathbf{Vec}_{\mathbb{C}}^n$.

Definition 4.2.37. A *simple object* A in a $\mathcal{C}$-linear category $\mathcal{C}$ is an object which has no direct sum decomposition into smaller objects. That is, $A \ncong B \oplus C$ for any non-zero objects $B, C \in \mathcal{C}$ where $\oplus$ denotes the biproduct in $\mathcal{C}$.

Proposition 4.2.38. *Let $\mathcal{C}$ be a $\mathbb{C}$-linear category. There exists an equivalence of categories $\mathcal{C} \simeq \mathbf{Vec}_{\mathcal{C}}^n$ for some $n \geq 1$ if and only if $\mathcal{C}$ satisfies the following properties:*

1. *$\mathcal{C}$ has finitely many isomorphism classes of simple objects;*
2. *Every object in $\mathcal{C}$ can be decomposed as a direct sum of finitely many simple objects;*
3. *(Schur's lemma) If $A, B \in \mathcal{C}$ are simple objects*

$$
\dim \mathrm{Hom}_{\mathcal{C}}(A, B) = \begin{cases} 1 & A \cong B \\ 0 & \text{otherwise} \end{cases}
$$

WORK: Do I need to require that $\mathcal{C}$ has a zero object, so that 0 is in its essential image?

Proof. Let n be the number of isomorphism classes of simple objects in $\mathcal{C}$. We choose representatives $V_1, V_2 \ldots V_n$ of the isomorphism classes of simple objects in $\mathcal{C}$. We define F on the level of objects by

$$
F\left(\bigoplus_{i=1}^{n} V_i^{n_i}\right) = \bigoplus_{i=1}^{n} \mathbb{C}_i^{n_i},
$$

where $V_i^{n_i} = V_i \oplus V_i \ldots \oplus V_i$ is the n-fold itterated direct sum of V_i. Of course, the direct sum is only defined up to isomorphism so we imagine working over all choices of biproduct on the left hand side, and some arbitrary but specific choice of direct sum on the right hand side. Given a morphism

$$
f \in \mathrm{Hom}_{\mathcal{C}}\left(\bigoplus_{i=1}^{n} V_i^{m_i}, \bigoplus_{j=1}^{n} V_j^{n_j}\right),
$$

we can expand using the natural isomorphism associated with the product/coproduct structure (as in example 4.2.27) to get an associated by

$$f \in \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{n} \bigoplus_{\ell=1}^{m_i} \bigoplus_{k=1}^{n_i} \mathrm{Hom}_{\mathcal{C}}\left(V_i, V_j\right).$$

By Schur's lemma, the cross terms $i \neq j$ cancel, giving us a decomposition $f = \oplus f_i$,

$$f_i \in \bigoplus_{\ell=1}^{m_i} \bigoplus_{k=1}^{n_i} \mathrm{Hom}_{\mathcal{C}}\left(V_i, V_i\right).$$

We can now define the associated morphism

$$F(f) \in \mathrm{Hom}_{\mathbf{Vec}_{\mathbb{C}}^{n}}\left(\bigoplus_{i=1}^{n} \mathbb{C}_i^{m_i}, \bigoplus_{j=1}^{n} \mathbb{C}_j^{n_j}\right)$$

by saying that $F(f)$ acts as the linear map $\mathbb{C}_i^{m_i} \to \mathbb{C}_i^{n_i}$ by the matrix whose coefficients exactly the coefficients of f_i, where we identify $\mathrm{Hom}_{\mathcal{C}}\left(V_i, V_i\right)$ with $\mathbb{C}$ by sending each morphism g to the unique scalar $\lambda \in \mathbb{C}$ for which $g = \lambda \cdot \mathrm{id}_{V_i}$. It is simple to check that F is a well-defined functor.

We observe that F is essentially surjective, because every object in $\mathbf{Vec}_{\mathbb{C}}^{n}$ is a direct sum of some number of copies of $\mathbb{C}_i$ for $1 \leq i \leq n$. It is fully faithful because the correspondance between morphisms and linear maps used in the definition is a bijection. Thus, we conclude the first direction by proposition 4.2.28. The other direction is a simple check. □

WORK: Maybe that a bit of room here to wax poetic about higher linear algebra.

WORK: Here's a lemma I would like to use. Since $\times$ and $\boxtimes$ look too similar, I should use $\boxplus$ to denote the Cartesian product and call it the direct sum. I should then prove this:

Lemma 4.2.39. *Consider the category **2Vec** whose objects are $\mathbb{C}$-linear categories equivalent to $\mathbf{Vec}_{\mathbb{C}}^{n}$ for sme $n \geq 0$, and whose morphisms are $\mathbb{C}$-linear functors. The direct sum $\boxplus$ is a biproduct in **2Vec***

Proof. WORK: do proof □

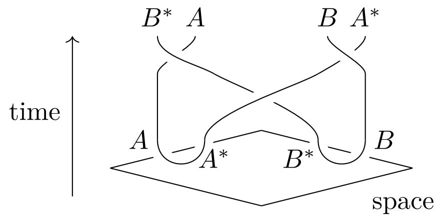
4.3 Monoidal categories

4.3.1 Motivation, definition, and string diagrams

The goal of this section is to introduce the languages of *monoidal categories* and *string diagrams*, which are neccecary for a proper algebraic discussion of anyons and modular tensor categories.

The structures in monoidal category theory and their interpretation in terms of string diagrams will allow us to discuss situations like the one below, where we create and braid quasiparticles:

Example 4.3.1. Suppose that we are braiding quasiparticles in a topological system. In spacetime, the trajectories of the anyons will look something like diagram 4.1.



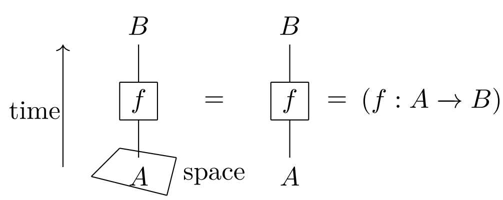
(4.1)

Using the formalism of monoidal categories and the language of string diagrams, we will be able to interpret the above diagram 4.1 as a certain morphism in a category. The exact category in which the morphism should live depends on the underlying topological system. The quasiparticle labels A, B, A^*, B^* represent objects in $\mathcal{C}$. The objects (A, A^*) form a particle/antiparticle pair, and the objects (B, B^*) form a particle/antiparticle pair. The diagram is broadly interpreted 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 braiding operatations (braid_{A^*,B^*}, braid_{A,B^*}, and $\mathrm{braid}_{A^*,B}$) which swap the positions of adjacent quasiparticles. The overall process is the composition of these sub-processes:

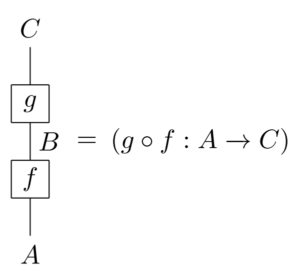
$$(\mathrm{braid}_{A^*,B}) \circ (\mathrm{braid}_{A,B^*}) \circ (\mathrm{braid}_{A^*,B^*}) \circ (\mathrm{create}_{B^*,B}) \circ (\mathrm{create}_{A,A^*}).$$

It is thus clear why categories-with-structure are the right framwork for understanding diagrams like diagram 4.1. The additional structures on $\mathcal{C}$ will give the braiding and creation maps meaning, and the composition structure on $\mathcal{C}$ will tell us how these components fit together to make larger processes.

We now begin to introduce the language of string diagrams. The most basic principle os 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 is expressed cleanly in this langauge as stacking. That is, for all $f : A \to B$, $g : B \to C$, we define



Accordingly, the identity map has a simple implementation:

$$= (\mathrm{id}_A : A \to A)$$

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 4.1 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 4.3.2 (Strict monoidal category)**.** A strict monoidal category is the following data:

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

Such that:

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

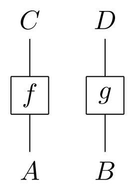
$$A \otimes \mathbf{1} = \mathbf{1} \otimes A = A, \qquad\qquad f \otimes \mathrm{id}_{\mathbf{1}} = \mathrm{id}_{\mathbf{1}} \otimes f = f.$$

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

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

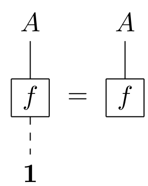
Remark 4.3.3. The object $\mathbf{1} \in \mathcal{C}$ is important. Just like how groups of symmetries always include the "do-nothing" symmetry, strict monoidal categories should always include the unit. In this case, $\mathbf{1} \in \mathcal{C}$ represents the empty particle - no particle at all. In 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 $\mathbf{1} \otimes A = A \otimes \mathbf{1} = A$.

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 $\mathcal{C}$ be a strict monoidal category, let $A, B, C, D \in \mathcal{C}$ be four objects, and let $f : A \to C$, $g : B \to D$ be morphisms. We have



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

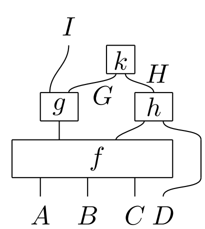
The monoidal unit $\mathbf{1}$ is distinguished in monoidal categories, and hence is represented with a special line. We will either use a dotted line, or no line at all:



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

Remark 4.3.4. 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.

Example 4.3.5. Diagram 4.2 is valid in all strict monoidal categories $\mathcal{C}$, where $A,B,C,D,E,F,G,H \in \mathcal{C}$ are objects, and $f : A \otimes B \otimes C \to E \otimes F$, $g : E \to I \otimes G$, $h : F \otimes D \to H$, and $k : G \otimes H \to \mathbf{1}$ are morphisms:



(4.2)

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

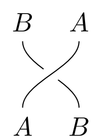
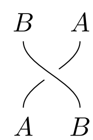
1. A strict monoidal category $\mathcal{C}$;
2. (Braiding) Isomorphisms $\beta_{A,B} : A \otimes B \to B \otimes A$ for all $A, B \in \mathcal{C}$ which form a natural isomorphism between the functors $\mathcal{C} \times \mathcal{C} \to \mathcal{C}$ given by $(A, B) \mapsto A \otimes B$ and $(A, B) \mapsto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

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

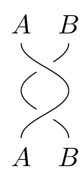
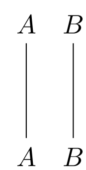
$$
\begin{tikzcd}
A \otimes B \otimes C \arrow[dd, "\beta_{A,B\otimes C}"'] \arrow[dr, "\beta_{A,B}\otimes \mathrm{id}_C"] & \\
& B \otimes A \otimes C \arrow[dl, "\mathrm{id}_B \otimes \beta_{A,C}"] \\
B \otimes C \otimes A &
\end{tikzcd}
,\qquad
\begin{tikzcd}
A \otimes B \otimes C \arrow[dd, "\beta^{-1}_{B\otimes C,A}"'] \arrow[dr, "\beta^{-1}_{B,A}\otimes \mathrm{id}_C"] & \\
& B \otimes A \otimes C \arrow[dl, "\mathrm{id}_B \otimes \beta^{-1}_{C,A}"] \\
B \otimes C \otimes A &
\end{tikzcd}
$$

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 graphically define overcrossing and undercrossing as follows:

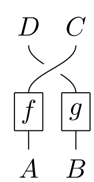
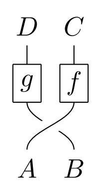

$= \beta_{A,B}$,

$= \beta^{-1}_{B,A}$.

Remark 4.3.7. The fact that overcrossing and undercrossing are related by an inverse encodes the following topological fact:


$= \beta^{-1}_{A,B} \circ \beta_{A,B} = \mathrm{id}_{A\otimes B} =$


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


$=$


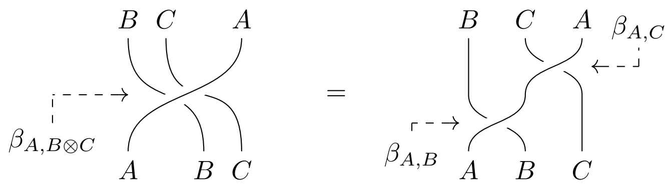
The same formula holds replacing overcrossing with undercrossing on both sides.

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

$$
\begin{tikzcd}
A \otimes B \arrow[r, "f\otimes g"] \arrow[d, "\beta_{A,B}"] & C \otimes D \arrow[d, "\beta_{C,D}"] \\
B \otimes A \arrow[r, "g\otimes f"] & D \otimes C
\end{tikzcd}
$$

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. □

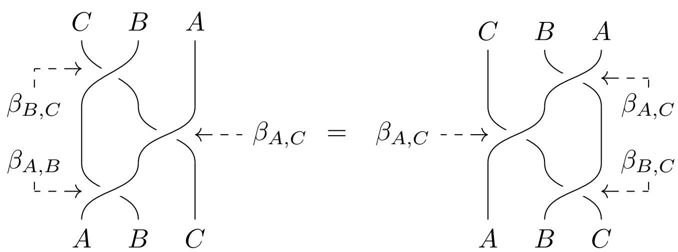
Remark 4.3.9. The first coherence axiom can be stated diagrammatically as follows,



and the second coherence axiom can be stated similarly 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 $(\mathrm{id}_B \otimes \beta_{A,C}) \circ (\beta_{A,B} \otimes \mathrm{id}_C)$.

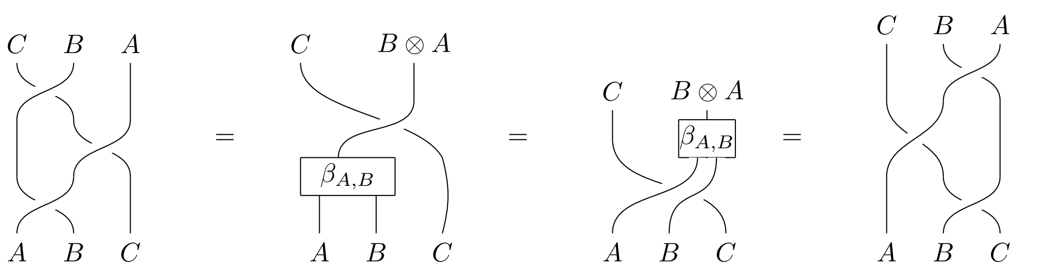
Remark 4.3.10. When discussing the theory of braiding in subsection 1.2.4, we discusses braiding operations. It was asserted that two braiding operations are topologically equivalent if and only if they can be manipulated from one to another via manipulations like the one in equation 4.3. Thus, proposition 4.3.11 proves that any two topologically equivalent braids will correspond to the same morphism in a braided monoidal category.

Proposition 4.3.11 (Yang-Baxter equation)**.** *Let $\mathcal{C}$ be a strict braided monoidal category. Let $A, B, C \in \mathcal{C}$ be objects. We have*



(4.3)

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



□

Corollary 4.3.12. *Let $\mathcal{C}$ be a strict braided monoidal category. Let $A \in \mathcal{C}$ 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. By definition B_n, the only relations we need to verify are $\sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_i\sigma_{i+1}\sigma_i$ for $1 \leq i \leq n-1$. These conditions are satisfied by the map by proposition 4.3.11. $\square$

4.3.3 Examples, equivalences, and MacLane's coherence theorem

Warning 4.3.13. 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.

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 the first category which we would want to give as an example of a monoidal category:

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

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 because the tensor product is not litereally associative. 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.

Remark 4.3.14. 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 $A \otimes (B \otimes) C$. It is for this reason that we need to require 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. In general, when looseing equalities to isomorphisms in category theory it is good to posit the existence of specific isomorphisms instead of only forcing that an isomorphism exists.

Definition 4.3.15 (Monoidal category)**.** A monoidal category is the following data:

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

3. (Unit) A distinguished element $\mathbf{1} \in \mathcal{C}$.
4. (Associator) A natural isomorphism

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

where $- \otimes (- \otimes -)$ denotes the functor $\mathcal{C} \times \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ 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 $\mathcal{C} \to \mathcal{C}$ 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 $\mathcal{C} \to \mathcal{C}$ sending A to $A \otimes \mathbf{1}$.

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

1. (Triangle identity) The diagram

$$\begin{tikzcd}
(A \otimes \mathbf{1}) \otimes B \arrow[rr, "\alpha_{A,1,B}"] \arrow[dr, "\rho_A \otimes \mathrm{id}_B"'] & & A \otimes (\mathbf{1} \otimes B) \arrow[dl, "\mathrm{id}_A \otimes \lambda_B"] \\
& A \otimes B &
\end{tikzcd}$$

commutes for all $A, B \in \mathcal{C}$.
2. (Pentagon identity) The diagram

$$\begin{tikzcd}
& (A \otimes B) \otimes (C \otimes D) & \\
((A \otimes B) \otimes C) \otimes D \arrow[ur, "\alpha_{A \otimes B, C, D}"] \arrow[d, "\alpha_{A,B,C} \otimes \mathrm{id}_D"'] & & A \otimes (B \otimes (C \otimes D)) \arrow[ul, "\alpha_{A,B,C \otimes D}"'] \\
(A \otimes (B \otimes C)) \otimes D \arrow[rr, "\alpha_{A, B \otimes C, D}"'] & & A \otimes ((B \otimes C) \otimes D) \arrow[u, "\mathrm{id}_A \otimes_{B,C,D}"']
\end{tikzcd}$$

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

Example 4.3.16. The following collections of data form monoidal categories

- The category $\mathcal{C} = \mathbf{Set}$, with tensor product $\otimes =$ Cartesian product, monoidal unit $\mathbf{1} = \{*\}$, associator

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

and unitors

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

- The plain category $\mathcal{C} = \mathbf{Vec}_{\mathbb{C}}$, with its standard tensor product, monoidal unit $\mathbf{1} = \mathbb{C}$, associator

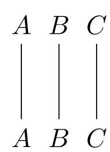
$$\begin{aligned} \alpha_{A,B,C} : A \times (B \times C) &\xrightarrow{\sim} (A \times B) \times C, \\ a \otimes (b \otimes c) &\mapsto (a \otimes b) \otimes c \end{aligned}$$

  and unitors

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

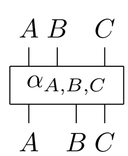
- The category $\mathcal{C} = \mathbf{Set}$ with tensor product $\otimes =$ Disjoint union and $\mathbf{1} = \{\}$, with a standard choice of associators and unitors;
- The category $\mathcal{C} = \mathbf{Vec}_{\mathbb{C}}$ with tensor product $\otimes =$ Direct sum, and $\mathbf{1} = 0$, with a standard choice of assoicators and unitors.

Remark 4.3.17. In expanding our definition from strict monoidal category to monoidal category we have introduced a subtle problem. The diagram



$$= \mathrm{id}_{A \otimes B \otimes C}$$

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



In general, string diagrams for non-strict monoidal categories need α maps thrown in at key points to make a well-defined language. This is quite complicated, and has issues that need to be adressed. Hence, we maintain that our graphical langauge only applies to strict monoidal categories.

Remark 4.3.18. In light of remark 4.3.17, we seem to have made very little progress. 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 fail to describe those examples! This seemingly bad situation is rectified by theorem 4.3.24, 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. Alternatively one can adopt the following simpler policy, with the price of making the usual examples only heuristic:

$$\boxed{\text{We assume monoidal categories are strict whenever it is convenient.}}$$

Example 4.3.19. To illustrate the workflow proposed in 4.3.18 we take a closer look at corollary 4.3.12, where we proved that every strict braided monoidal category $\mathcal{C}$ comes paired with a group homomorphism

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

for all $A \in \mathcal{C}$, $n \geq 1$. 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. It is possible to formalize corollary 4.3.12 for non-strict categories, but it is space-consuming and makes the key insights less clear.

Remark 4.3.20. To state MacLane's coherence theorem, we need a notion of *equivalence* of monoidal categories. Our notion 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 equivalence can preserve information about monoidal structure.

Definition 4.3.21 (Monoidal functor)**.** A monoidal functor between monoidal categories $(\mathcal{C}, \otimes_{\mathcal{C}}, \alpha_{\mathcal{C}}, \lambda_{\mathcal{C}}, \rho_{\mathcal{C}}, \mathbf{1}_{\mathcal{C}})$ and $(\mathcal{D}, \otimes_{\mathcal{D}}, \alpha_{\mathcal{D}}, \lambda_{\mathcal{D}}, \rho_{\mathcal{D}}, 1_{\mathcal{D}})$ is the following data:

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

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

1. (Associativity) The diagram

$$\begin{tikzcd}
(F(A) \otimes_{\mathcal{D}} F(B)) \otimes_{\mathcal{D}} F(C) \arrow[rr, "\alpha_{\mathcal{D};F(A),F(B),F(C)}"] \arrow[d, "\mu_{A,B} \otimes \mathrm{id}_{F(C)}"] & & F(A) \otimes_{\mathcal{D}} (F(B) \otimes_{\mathcal{D}} F(C)) \arrow[d, "\mathrm{id}_{F(A)} \otimes \mu_{B,C}"] \\
F(A \otimes_{\mathcal{C}} B) \otimes_{\mathcal{D}} F(C) \arrow[d, "\mu_{A \otimes_{\mathcal{C}} B, C}"] & & F(A) \otimes_{\mathcal{D}} F(B \otimes_{\mathcal{C}} C) \arrow[d, "\mu_{A, B \otimes_{\mathcal{C}} C}"] \\
F((A \otimes_{\mathcal{C}} B) \otimes_{\mathcal{C}} C) \arrow[rr, "F(\alpha_{\mathcal{C};A,B,C})"] & & F(A \otimes_{\mathcal{C}} (B \otimes_{\mathcal{C}} C))
\end{tikzcd}$$

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

2. (Unitality) The diagrams

$$\begin{tikzcd}
1_{\mathcal{D}} \otimes_{\mathcal{D}} F(A) \arrow[r, "\epsilon \otimes \mathrm{id}_{F(A)}"'] \arrow[d, "\lambda_{\mathcal{C};F(A)}"] & F(1_{\mathcal{C}}) \otimes F(A) \arrow[d, "\mu_{1_{\mathcal{C}},A}"'] \\
F(A) & F(1_{\mathcal{C}} \otimes A) \arrow[l, "F(\lambda_{\mathcal{C};A})"']
\end{tikzcd}$$

and

$$\begin{tikzcd}
F(A) \otimes_{\mathcal{D}} 1_{\mathcal{D}} \arrow[r, "\mathrm{id}_{F(A)} \otimes \epsilon"'] \arrow[d, "\rho_{\mathcal{C};F(A)}"] & F(A) \otimes_{\mathcal{D}} F(1_{\mathcal{C}}) \arrow[d, "\mu_{A,1_{\mathcal{C}}}"'] \\
F(A) & F(1_{\mathcal{C}} \otimes A) \arrow[l, "F(\rho_{\mathcal{C};A})"']
\end{tikzcd}$$

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

Definition 4.3.22 (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 $(\mathcal{C}, \otimes_{\mathcal{C}}, \mathbf{1}_{\mathcal{C}})$ and $(\mathcal{D}, \otimes_{\mathcal{D}}, 1_{\mathcal{D}})$ 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 $A, B \in \mathcal{C}$, the diagram

$$\begin{tikzcd}
F_0(A) \otimes_{\mathcal{D}} F_1(B) \arrow[r, "\eta_A \otimes \eta_B"] \arrow[d, "\mu_{0;A,B}"] & F_1(A) \otimes_{\mathcal{D}} F_1(B) \arrow[d, "\mu_{1;A,B}"] \\
F_0(A \otimes_{\mathcal{C}} B) \arrow[r, "\eta_{A \otimes B}"] & F_1(A \otimes_{\mathcal{C}} B)
\end{tikzcd}$$

commutes.

2. (Compatibility with unit) The diagram

$$\begin{tikzcd}
& 1_{\mathcal{D}} \arrow[dl, "\epsilon_0"'] \arrow[dr, "\epsilon_1"] & \\
F_0(1_{\mathcal{C}}) \arrow[rr, "\eta_{1_{\mathcal{C}}}"] & & F_1(1_{\mathcal{C}})
\end{tikzcd}$$

commutes.

Definition 4.3.23. A *monoidal equivalence* between two monoidal categories $\mathcal{C}, \mathcal{D}$ is a pair of monoidal functors $F : \mathcal{C} \to \mathcal{D}$, $G : \mathcal{D} \to \mathcal{C}$ such that $G \circ F$ is monoidally naturally isomorphic to $\mathrm{id}_{\mathcal{C}}$ and $F \circ G$ is monoidally naturally isomorphic to $\mathrm{id}_{\mathcal{D}}$. We say two categories are *monoidally equivalent* if there is a monoidal equivalence between them.

Theorem 4.3.24 (MacLane's coherence theorem)**.** *Every monoidal category is monoidally equivalent to a strict monoidal category.*

Remark 4.3.25. MacLane's coherence theorem allows us to enjoy a managable string diagram workflow for monoidal categories. However, as we add more structure onto our categories, 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 - if we have a braided monoidal category whose associativity is non-strict, will it be equivalent to a braided monoidal category whose associativity is strict? The answer is yes, by proposition 4.3.30.

Definition 4.3.26 (Braided monoidal category)**.** A braided monoidal category is the following data:

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

$$\begin{tikzcd}
A \otimes (B \otimes C) \arrow[r, "\alpha_{A,B,C}"] \arrow[d, "\mathrm{id}_A \otimes \beta_{B,C}"'] & (A \otimes B) \otimes C \arrow[r, "\beta_{A \otimes B, C}"] & C \otimes (A \otimes B) \arrow[d, "\alpha_{B,C,A}"] \\
A \otimes (C \otimes B) \arrow[r, "\alpha_{A,C,B}"'] & (A \otimes C) \otimes B \arrow[r, "\beta_{A,C} \otimes \mathrm{id}_B"'] & (C \otimes A) \otimes B
\end{tikzcd}$$

and

$$\begin{tikzcd}
(A \otimes B) \otimes C \arrow[r, "\alpha^{-1}_{A,B,C}"] \arrow[d, "\beta_{A,B} \otimes \mathrm{id}_C"'] & A \otimes (B \otimes C) \arrow[r, "\beta_{A, B \otimes C}"] & (B \otimes C) \otimes A \arrow[d, "\alpha^{-1}_{B,C,A}"] \\
(B \otimes A) \otimes C \arrow[r, "\alpha^{-1}_{B,A,C}"'] & B \otimes (A \otimes C) \arrow[r, "\mathrm{id}_B \otimes \beta_{A,C}"'] & B \otimes (C \otimes A)
\end{tikzcd}$$

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

Example 4.3.27. WORK: Now that we have defined braided monoidal category, we can give some example. Namely. it's neccecary that we give $\mathbf{Vec}_{\mathbb{C}}$ as an example.

Definition 4.3.28 (Braided monoidal functor)**.** A braided monoidal functor between braided monoidal categories $(\mathcal{C}, \otimes_{\mathcal{C}}, \beta_{\mathcal{C}})$, $(\mathcal{D}, \otimes_{\mathcal{D}}, \beta_{\mathcal{D}})$ is a monoidal functor $(F, \mu) : \mathcal{C} \to \mathcal{D}$ such that the diagram

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

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

Remark 4.3.29. 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.

Proposition 4.3.30 (Braided MacLane coherence theorem)**.** *Every braided monoidal equivalent is equivalent as a braided monoidal category to a strict braided monoidal category.*

Proof. Let $\mathcal{C}$ be a braided monoidal category. Let $\mathcal{C}'$ be a strict monoidal category equivalent to $\mathcal{C}$ (which exists by theorem 4.3.24), and let $F : \mathcal{C} \to \mathcal{C}'$, $G : \mathcal{C}' \to \mathcal{C}$ be monoidal functors inducing the equivalence. Let $\eta : F \circ G \cong \mathrm{id}_{\mathcal{C}}$ be a monoidal natural isomorphism. We define a natural transformation β' on the A, B component by the followiing composition:

$$\begin{array}{ccccc} A \otimes B & \xrightarrow{\eta^{-1}_{A\otimes B}} & F(G(A \otimes B)) & \xrightarrow{F(\mu^{-1}_{G;A,B})} & F(G(A) \otimes G(B)) \\ & & & & \Big\downarrow F(\beta_{G(A),G(B)}) \\ B \otimes A & \xleftarrow[\eta_{B\otimes A}]{} & F(G(B \otimes A)) & \xleftarrow[F(\mu_{G;B,A})]{} & F(G(B) \otimes G(A)) \end{array}$$

It is a straightforward to show that the axioms of a braided monoidal category on $\mathcal{C}$, the axioms of a monoidal functor on F, G and the axioms of a natural transformation on η imply that β' is the structure of a braiding on $\mathcal{C}'$. Moreover, the monoidal equivalence of categories between $\mathcal{C}$, $\mathcal{C}'$ is a braided monoidal equivalence. ☐

Remark 4.3.31. 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.

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.*

Remark 4.3.32. In the relevant physical systems, every particle has 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 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, and focus instead on the abstract underpinnings of antiparticles (which we call *duals*), pair-creation (which we call *coevaluation*) and fusion (which we all *evaluation*).

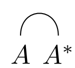
Example 4.3.33. WORK: This section doesn't contain any examples! In particular, there is the fantastic example of $\mathbf{Vec}_{\mathbb{C}}$. This is the canonical example that should be used to motivate the definition. Putting it all the way up here might be the best idea.

Definition 4.3.34 (Right-rigid monoidal category)**.** A right-rigid monoidal category is the following data:

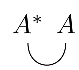
1. A monoidal category $\mathcal{C}$.
2. Objects A^* for all $A \in \mathcal{C}$.
3. Morphisms $\mathrm{ev}_A : A \otimes A^* \to 1$, and $\mathrm{coev}_A : 1 \to A^* \otimes A$ for all $A \in \mathcal{C}$.

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 $A \in \mathcal{C}$.

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

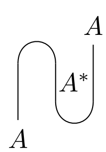


$= \mathrm{ev}_A,$

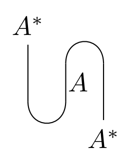


$= \mathrm{coev}_A\,.$

The compatibility conditions are stated graphically as follows:



$= \mathrm{id}_A,$



$= \mathrm{id}_{A^*}$

Definition 4.3.35 (Left-rigid monoidal category)**.** A left-rigid monoidal category is the following data:

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

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 $A \in \mathcal{C}$.

Remark 4.3.36. 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 $\mathcal{C}$. As per usual, there should be some compatibility conditions between these two rigid structures.

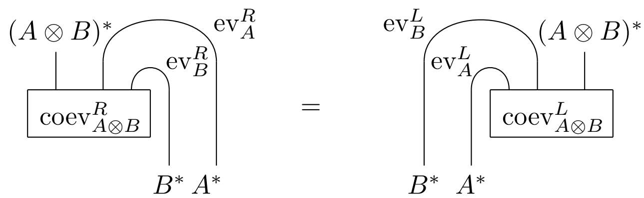
Definition 4.3.37 (Pivotal monoidal category)**.** A pivotal monoidal category is the following data:

1. A monoidal category $\mathcal{C}$;

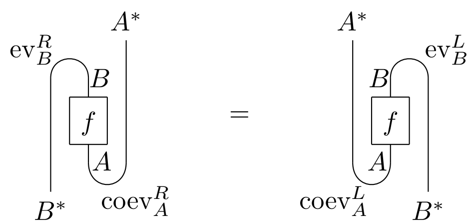
2. A right-rigid structure $(\mathrm{ev}^R, \mathrm{coev}^R)$ on $\mathcal{C}$;
3. A left-rigid structure $(\mathrm{ev}^L, \mathrm{coev}^L)$ on $\mathcal{C}$.

Such that:

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



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

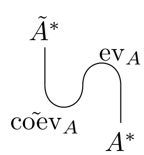


Remark 4.3.38. The first thing to observe is that even though there is a lot of structure involved in the definition of a rigid monoidal category, most of it is in a real sense innessential. Proposition 4.3.39 tells us we could have chosen different duals and the result would have been essentially the same, or in other words, duals are unique up to unique isomorphism.

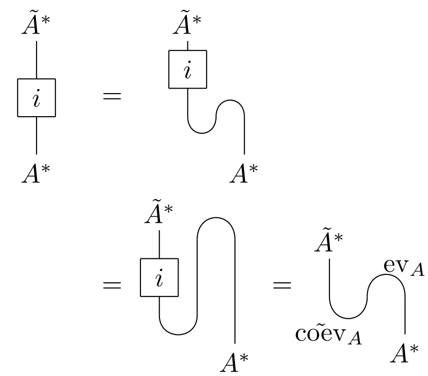
Proposition 4.3.39. *Let $\mathcal{C}$ be right (resp. left) rigid monoidal category. Let $A \in \mathcal{C}$ be an object, and let $(\tilde{A}^*, \tilde{\mathrm{ev}}_A, \tilde{\mathrm{coev}}_A)$ be another triple satisfying the axioms of rigidity. There is a unique morphism $i : A^* \to \tilde{A}^*$ making the diagram*

$$\begin{tikzcd}
 & A^* \otimes A \arrow[dd, "\sim"] \\
1 \arrow[ur, "\mathrm{coev}_A"] \arrow[dr, "\tilde{\mathrm{coev}}_A"'] & \\
 & A \otimes \tilde{A}^*
\end{tikzcd}$$

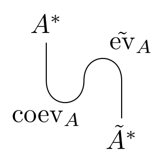
commute (resp. reverse order of tensor factors). This unique morphism is an isomorphism, and it is given by

$i =$ 

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. $\square$

Remark 4.3.40. Seeing as we will be working with rigid and pivotal categories, it behooves us to make sure that we have the correct notion of functors and natural transformations between these categories. Let $F : \mathcal{C} \to \mathcal{D}$ be a functor between pivotal categories. Given an object $A \in \mathcal{C}$, 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 4.3.39, 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. A functor between pivotal categories with this property is known as a *pivotal functor*.

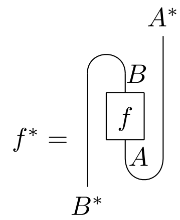
Definition 4.3.41. Define a monoidal category $\overline{\mathcal{C}}$ as follows. The underlying category on $\overline{\mathcal{C}}$ is the opposite category for $\mathcal{C}$. The tensor product is given by $A \overline{\otimes} B = B \otimes A$, and the monoidal unit is $\mathbf{1} \in \mathcal{C}$. WORK: I'm not sure if I like this definition, notation, or location.

Remark 4.3.42. An important feature of rigid categories is that duality is automatically *functorial*, by proposition 4.3.43. This perspective can be used to motivate the axioms of a pivotal category. By proposition 4.3.43 both the right and left rigid structures in a pivotal category induce functors $\mathcal{C} \to \overline{\mathcal{C}}$. The coherence condition is that these two functors should be equal.

Proposition 4.3.43. *Let $\mathcal{C}$ be right (resp. left) rigid monoidal category.*

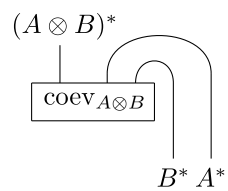
(i) The right (resp.left) rigid structure on $\mathcal{C}$ induces a left (resp. right) rigid structure on $\overline{\mathcal{C}}$;

(ii) Given any morphism $f : A \to B$ in $\mathcal{C}$, 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 $\mathcal{C}$ to $\overline{\mathcal{C}}$ which we denote $(-)^*$.

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



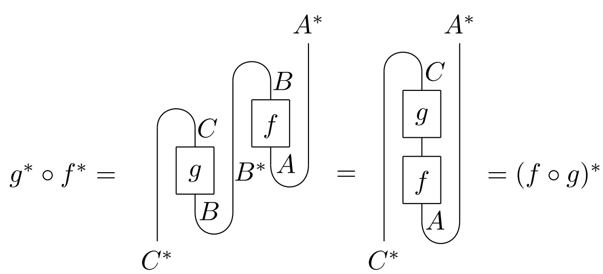
from $B^* \otimes A^*$ to $(A \otimes B)^*$ (resp. same diagram using left rigidity). These maps endows $(-)^*$ with the structure of a monoidal functor.

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

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

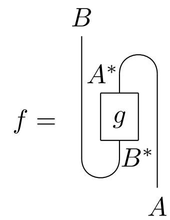
(i) This follows immediately from the definitions;

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



(iii) This is an unenlightening and straightforward computation;

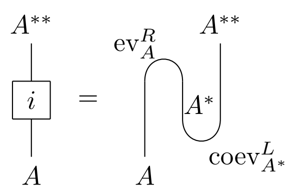
(iv) We first prove that $(-)^*$ is fully faithful. Given any objects $A, B \in \mathcal{C}$ and any morphism $g : B^* \to A^*$, the morphism



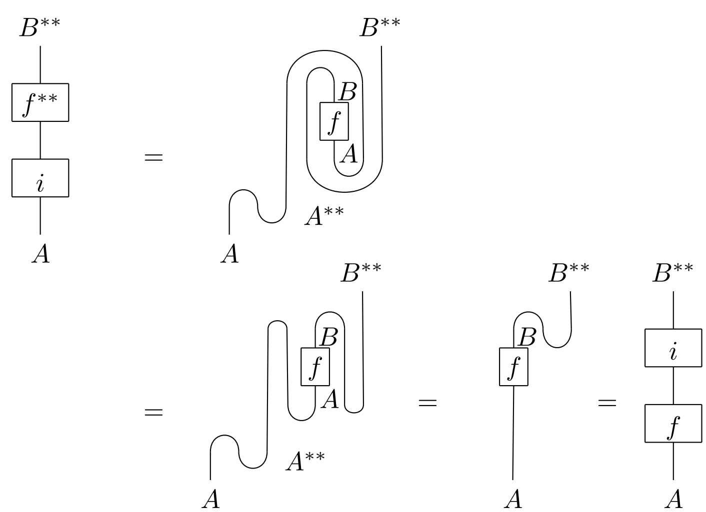
has the property that $f^* = g$. Hence, $(-)^*$ is bijective on hom-spaces as desired.

We now show that $(-)^*$ is an equivalence of categories with $\mathcal{C}$ is pivotal. By part (i), $\overline{\mathcal{C}}$ is a pivotal monoidal category. Hence duality once again induces a monoidal functor, this time $\overline{\mathcal{C}} \to \overline{\overline{\mathcal{C}}}$. Clearly, by our definition of $\overline{\mathcal{C}}$, $\overline{\overline{\mathcal{C}}} = \mathcal{C}$. Hence we have a pair of functors $\mathcal{C} \to \overline{\mathcal{C}}$ and $\overline{\mathcal{C}} \to \mathcal{C}$, 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 $A \in \mathcal{C}$. To show that these morphisms induce a natural transformation, we observe that for all $f : A \to B$

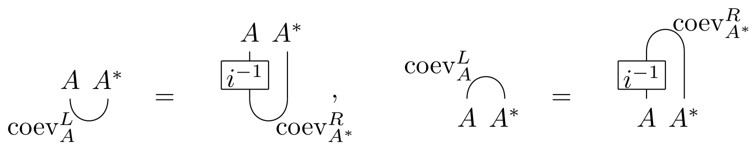


The fact that $\mathcal{C}$ is compatible with the tensor product is a straightforward computation, using the fact that computing the tensor product using right-rigidity and left-rigidity gives the same answer, and compatibility of $\mathcal{C}$ with the unit is immediate.

$\square$

Remark 4.3.44. As a key part of proposition 4.3.43, 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 as rigid categories equipped with isomorphisms between the identity functor and the double dual functor. This is stated precisely in corollary 4.3.45.

Corollary 4.3.45. *Let $\mathcal{C}$ be a right-rigid monoidal category. Let $i : \mathrm{id}_{\mathcal{C}} \xrightarrow{\sim} (-)^{**}$ be a monoidal natural isomorphisms between the identity functor and the double dual functor. The maps*



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

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 4.3.43 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. $\square$

History and further reading:

WORK: an early reference for string diagrams is [**?**]. Maybe I should cite it?
Category theory was first introduced and formalized by Saunders Mac Lane and Samuel Eilenberg in 1945 [**?**]. 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 [**?**]. 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 [**?**, **?**]. The physics in this area has since become and remained extremely categorical in nature [**?**, **?**].

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 [**?**]. 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 [**?**], and a classical but slightly dated reference is [**?**].

Exercises:

4.1. WORK: If $\mathcal{C}$ is a category with products, then the product forms a monoidal structure (with a good $\mathbf{1}$ 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.

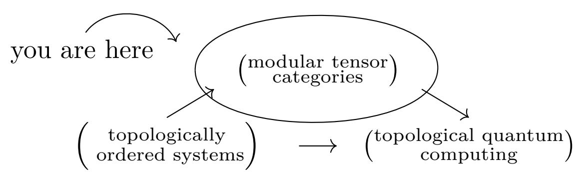
WORK: I'm not consistent about up/down orientation for my string diagrams. I need to go through and fix this.

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 is 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 4. Roughly, we can think of a modular category as being the category with the following data:

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

We have the following general pictuture for our algebraic theory:

Physics-math dictionary 5.1.1. Topological phases of matter are algebraically described by unitary modular categories $\mathcal{C}$ called the *anyon theory* of the phase, and a choice of integer $c_- \in \mathbb{Z}$ called the *chiral central charge* of the phase. [Kit06]

Remark 5.1.2. Throughout these notes, there are some aspects of the general dictionary 5.1.1 that we have not emphasized. For instance, we have not emphasized that the modular categories describing topological phases are supposed to be *unitary* modular categories - we will discuss this later, but by analagy we can say that a unitary modular category is related to a modular category just like a Hilbert space is related to a vector space.

Another aspect we have not emphasized is the *chiral central charge.* This is a real invariant of topological phases which is beyond the description of modular categories. In particular, there are topological phases with no non-trivial anyons (and hence correspond to the trivial modular category) yet are non-trivial as topological phases. These are called *invertible* topological phases. Invertible topological phases are paramaterized by an integer invariant, their chiral central charge. Not every pair $(\mathcal{C}, c_-)$ describes a valid topological phase. In particular, $\mathcal{C}$ determines c_- modulo 8 but there is no other condition. The way that $\mathcal{C}$ determins c_- modulo 8 is known as the Gauss-Milgram formula and is discussed in subsection 5.5.5.

Remark 5.1.3. The major structures of a modular tensor category can be motivated by considering abstractly the possible motions and behaviors of anyons. The most basic thing anyons can do is move anyons around each other - this is known as *braiding.* If the anyons touch each other then they can congeal into a single 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.

Remark 5.1.4. Another potentially useful way of thinking about modular categories comes from analogy with classical physics. We saw in chapter 1 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 G induces a modular category $\mathfrak{D}(G)$, by first constructing the Kitaev quantum double model based on that finite group and then describing its anyons. Many modular categories do not come from the group-theoretical construction.

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 structure, 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. In this 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 putting so much work into defining modular categories..

Example 5.1.5. To highlight how the formalism used to define an object impacts its finitely-generated description, we take an example from group theory. Consider the 3-strand braid group B_3. This group has ininitely many elements and the group operation $B_3 \times B_3 \to B_3$ naively takes 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.

An important step 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 5.6. A large table of these descriptions are found in appendix B. We now give a worked example of how this data is used to compute observable quantities.

Example 5.1.6. WORK: add toric code modular category data

Example 5.1.7. Or, for a more complicated example, we can consider the data for $G = S_3$: WORK: add $G = S_3$ modular category data

5.2 First properties

5.2.1 Definition

In this section we define modular categories, which are the main mathematical subject 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 5.2.1 (Fusion category)**.** A fusion category is the following data:

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

Such that:

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

Remark 5.2.2. 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.

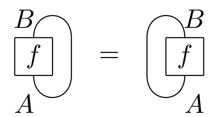
Definition 5.2.3 (Spherical fusion category)**.** A spherical fusion category is the following data:

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

Such that:

1. The left-rigid and right-rigid structures on $\mathcal{C}$ satisfy the axioms of a pivotal structure on $\mathcal{C}$;

2. For every object $A \in \mathcal{C}$ and for every morphism $f : A \to A$, we have



Remark 5.2.4. A spherical fusion category now has a structure for fusion, and a full structure for pair-creation. The 2nd axiom in definition 5.2.3 is known as the *spherical axiom.* We will explain this axiom in more detail later.

Definition 5.2.5 (Pre-modular category)**.** A pre-modular category is the following data:

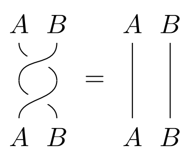
1. A spherical fusion category $\mathcal{C}$;

2. A braided structure on $\mathcal{C}$.

No extra compatibility conditions are required.

Remark 5.2.6. A pre-modular category has all of the structure we require of a modular category: fusion, pair-creation, and braiding. The final axiom it is missing is a non-degeneracy condition. The non-degeneracy condition is subtle in its interpretation, and we will explain it several different ways throughout this chapter.

Definition 5.2.7 (Modular category)**.** A modular category is a pre-modular category satisfying the following condition. Let $A \in \mathcal{C}$ be an object. If



for all $B \in \mathcal{C}$, then $A \cong n \cdot \mathbf{1}$ for some $n \geq 1$.

Remark 5.2.8. Our usage of the term "modular category" is a bit nonstandard. Where we call "modular categories" most authors would call "modular *tensor* categories". I find "modular category" more convient here because it is shorter than "modular tensor category" and I want to be succinct. For many authors, the term "modular category" refers to a potentially non-semsimple modular category, such as in Turaev's original work on modular categories [Tur92].

Example 5.2.9. The category $\mathbf{Vec}_{\mathbb{C}}$ is naturally a modular category. We discusses its $\mathbb{C}$-linear structure in example 4.2.32, we discussed its pivotal structure in subsection 4.3.33, and we discussed its braided monoidal structure in examples 4.3.16, 4.3.27. It satisfies $\mathrm{Hom}_{\mathbf{Vec}_{\mathbb{C}}}(\mathbb{C}, \mathbb{C}) \cong \mathbb{C}$, the right-rigid structure and the $\mathbb{C}$-linear structure turn $\mathbf{Vec}_{\mathbb{C}}$ into a fusion category. As we saw in example 4.3.33, the fusion category structure and the left-rigid structure turn $\mathbf{Vec}_{\mathbb{C}}$ into a spherical fusion category. Clearly $\mathbf{Vec}_{\mathbb{C}}$ satisfies the non-degeneracy axiom, because every object is isomorphic to $n \cdot \mathbf{1}$ for some $n \geq 1$! Thus, $\mathbf{Vec}_{\mathbb{C}}$ is indeed a modular category.

Physics-math dictionary 5.2.10. The category $\mathbf{Vec}_{\mathbb{C}}$ equipped with chiral central charge $c_{-} = 0$ corresponds physically to the *trivial phase.* That is, the phase of matter describing empty space.

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 $\mathcal{C}$ that there is an equivalence $\mathcal{C} \cong \mathbf{Vec}_{\mathbb{C}}^{n}$ as $\mathbb{C}$-linear categories. We saw in proposition [ref] that every object $A \in \mathcal{C}$ is isomorphic to a direct sum of *simple objects*, objects which cannot be written as the direct sum of two nonzero objects. Alternatively, $A \in \mathcal{C}$ is simple if and only if $\mathrm{End}(A) \cong \mathbb{C}$.

Physics-math dictionary 5.2.11. Isomorphism classes of simple objects in $\mathcal{C}$ correspond to anyon types in a topological phase described by the MTC $\mathcal{C}$.

Definition 5.2.12. For all fusion categories $\mathcal{C}$, we define $\mathcal{L}(\mathcal{C})$ (or simple $\mathcal{L}$ when $\mathcal{C}$ is clear from context) to the the set of isomorphism classes of simple objects. By entry 5.2.11 of the physics-math direction, elements of $\mathcal{L}(\mathcal{C})$ correspond bijectively to anyon types in any topological phase described by $\mathcal{C}$.

We now restate the results of proposition 4.2.38 in our current setting for a fusion category $\mathcal{C}$. For every object $X \in \mathcal{C}$, there exists unique nonnegative integers $c_{[A]}$, $[A] \in \mathcal{L}$, such that

$$X \cong \bigoplus_{[A]\in\mathcal{L}} c_{[A]} \cdot A.$$

We assumed in the definition of a fusion category that $\mathrm{End}_{\mathcal{C}}(\mathbf{1}) \cong \mathcal{C}$. Thus, the monoidal unit is a simple object in every fusion category. By our physics-math dictionary, this means that $\mathbf{1}$ corresponds to an anyon type. This anyon $\mathbf{1}$ is the trivial "no-anyon" type, corresponding to a quasiparticle which happens to be the same as the homogenous bulk.

Physics-math dictionary 5.2.13. The monodial unit $\mathbf{1}$ corresponds to the trivial anyon type, which is the same as the homogenous bulk (sometimes called the *vaccuum* anyon type).

Remark 5.2.14. Continuing in our expansion of the physics-math dictionary, we can assert that dual objects (defined using the right-rigid structure on a fusion category) correspond to antiparticles (entry 5.2.15). This is consistent with the fact that anyon types correspond to simple objects, by proposition 5.2.16.

Physics-math dictionary 5.2.15. For every simple object A in a modular category $\mathcal{C}$, the dual object A^* corresponds to the *antiparticle* of A. 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 proposition 5.2.16.

Proposition 5.2.16. *Let $\mathcal{C}$ be a fusion category. If $A \in \mathcal{C}$ is a simple object, then so is A^*.*

Proof. By proposition 4.3.43 duality induces a bijection on hom-spaces. Since composition is bilinear, duality is thus an isomorphism of vector spaces on all hom-spaces. Hence, for all $A \in \mathcal{C}$ there is an isomorphism $\mathrm{Hom}(A, A) \cong \mathrm{Hom}(A^*, A^*)$. So, $\dim \mathrm{Hom}(A, A) = 1$ if and only if $\dim \mathrm{Hom}(A^*, A^*) = 1$, and thus the result follows from Schur's lemma. □

Physics-math dictionary 5.2.17. The tensor product $\otimes$ physically corresponds to joining anyons, forming a composite anyon configuration. That is, the object $A \otimes B$ corresponds to the configuration with one A-type anyon and one B-type anyon.

Remark 5.2.18. By entry 5.2.17 of the physics-math dictionary and proposition **??**, it behooves us to take a moment to interpret the direct sum decomposition

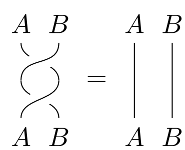
$$A \otimes B \cong \bigoplus_{[C] \in \mathcal{L}} N_C^{A,B} \cdot C, \tag{5.1}$$

where $A, B \in \mathcal{C}$ are objects in a fusion category. We call the non-negative integers $N_C^{A,B}$ the *fusion coefficients* of $\mathcal{C}$. We observe that

$$\dim \operatorname{Hom}(A \otimes B, C) = N_C^{A,B}. \tag{5.2}$$

Morphisms in $\mathcal{C}$ correspond to physical processes. So, equation 5.2 can be interpreted as saying that whenever $N_C^{A,B} > 0$, there is a physical process $A \otimes B \to C$. That is, there is a physical process which goes from the composite system of one A-type anyon and one B-type anyon and ouputs one C-type anyon. Neccecarily, such a process can be interpreted as *fusion* of A and B to C. Moreover, equation 5.2 tells us that the space of possible physical processes which fuse A and B to C (known as *fusion channels* $A \otimes B \to C$) is $N_C^{A,B}$-dimensional.

Remark 5.2.19. We can interpret the modularity axiom in terms of anyons. To begin, we observe the algebraic fact that a pre-modular category is modular if and only if for all *simple* objects $A \in \mathcal{C}$,



for all *simple* objects $B \in \mathcal{C}$ implies $A \cong \mathbf{1}$. This is physically interpreted as saying that if an anyon braids trivially with all other anyons, then it must be the trivial anyon type $\mathbf{1}$. In otherwords, there are no *transparent* anyons. This fact is physically motivated in subsection [ref].

Proposition 5.2.20. *Let $\mathcal{C}$ be a fusion category. For all simple objects $A, B, C, E \in \mathcal{C}$,*

$$\sum_E N_E^{A,B} N_D^{E,C} = \sum_G N_G^{B,C} N_D^{A,G}. \tag{5.3}$$

Proof. We observe on one hand that

$$\begin{aligned}(A \otimes B) \otimes C &\cong \bigoplus_E N_E^{A,B} \cdot E \otimes C \\ &\cong \bigoplus_{E,D} N_E^{A,B} N_D^{E,C} \cdot D\end{aligned}$$

and on the other hand

$$\begin{aligned}A \otimes (B \otimes C) &\cong \bigoplus_G N_G^{B,C} \cdot A \otimes G \\ &\cong \bigoplus_{G,D} N_G^{B,C} N_D^{A,G} \cdot D.\end{aligned}$$

Since $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$, we can compare coefficients to get the result. $\square$

Proposition 5.2.21. *Let $\mathcal{C}$ be a braided fusion category. For all simple objects A, B, C,*

$$N_C^{A,B} = N_C^{B,A}. \tag{5.4}$$

Proof. This follows immediately from the fact that $A \otimes B \cong B \otimes A$ in a braided fusion category. $\square$

5.2.3 States in modular categories and unitarity

It is now worth reflecting on how to interpret states in a topologically ordered system in terms modular categories. Certainly, objects in modular categories do *not* correspod quantum systems. They don't have vector space structure. Objects correspond roughly to anyon configurations, which are classical observables. The hom-spaces are what have vector space structure, by $\mathbb{C}$-linearity. However, they are not yet Hilbert spaces. It is exactly for this reason we need to define *unitary modular categories.* These are modular categories in which hom-spaces have Hilbert space structure.

Definition 5.2.22 (Unitary fusion category)**.** A unitary fusion category is the following data:

1. An fusion category $\mathcal{C}$.
2. (Conjugation) A linear map $\dagger : \mathrm{Hom}(A, B) \to \mathrm{Hom}(B, A)$ for all $A, B \in \mathcal{C}$.

Such that:

1. (Unitarity) Given $f : A \to A$ an endomorphism of $A \in \mathcal{C}$, 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 $f \in \mathrm{Hom}(A, B)$, $A, B \in \mathcal{C}$.
3. $(f \circ g)^\dagger = g^\dagger \circ f^\dagger$ for all $f \in \mathrm{Hom}(B, C)$,$g \in \mathrm{Hom}(A, B)$, $A, B, C \in \mathcal{C}$.
4. $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$ for all $f \in \mathrm{Hom}(A, B)$,$g \in \mathrm{Hom}(C, D)$, $A, B, C, D \in \mathcal{C}$.
5. $(\mathrm{coev}_A)^\dagger \circ (f \otimes \mathrm{id}_{A^*}) \circ \mathrm{coev}_A = \mathrm{tr}(f)$ for all $A \in \mathcal{C}$

Remark 5.2.23. Unitary fusion categories make for a pleasant object of study because by proposition 5.8.1 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.

Remark 5.2.24. In subsection [ref] proposition 5.8.1, we will show that in every 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 $\mathcal{C}$. This left-rigidity endows $\mathcal{C}$ with the structure of a spherical fusion category. Thus, every unitary fusion category is automatically a spherical fusion category.

Definition 5.2.25 (Unitary pre-modular category)**.** A unitary modular category is the following data:

1. A modular category $\mathcal{C}$;
2. (Conjugation) A linear map $\dagger : \mathrm{Hom}(A, B) \to \mathrm{Hom}(B, A)$ for all $A, B \in \mathcal{C}$.

Such that:

1. Forgetting the left-rigid structure and braiding, $(\mathcal{C}, \dagger)$ 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 5.2.26 (Unitary modular category)**.** A unitary modular category is a unitary pre-modular category which satisfies the non-degeneracy axiom of a modular category.

Remark 5.2.27. 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.

Physics-math dictionary 5.2.28. For any phase whose anyons as described by a unitary modular category $\mathcal{C}$.

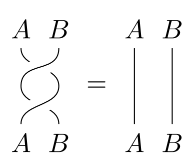
$$\begin{pmatrix} \text{states of topological order } \mathcal{C} \\ \text{on the sphere } S^2 \\ \text{with anyon configuraiton } A_1, A_2 ... A_n \end{pmatrix} = \begin{pmatrix} \text{normalized vectors in the Hilbert space} \\ \mathrm{Hom}_{\mathcal{C}}(\mathbf{1}, A_1 \otimes A_2 ... \otimes A_n) \end{pmatrix} \tag{5.5}$$

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 line segment in the sphere, with corresponding anyon type $A_1, A_2 ... A_n$.

Remark 5.2.29. It is not immediately clear why the physical space in equation 5.5 should be there sphere. As one source of motivation, we can observe the following corollary of equation 5.5:

$$\dim \begin{pmatrix} \text{Hilbert space of topological order } \mathcal{C} \\ \text{on the sphere } S^2 \\ \text{with exactly one anyon of type } A \end{pmatrix} = \dim \mathrm{Hom}(\mathbf{1}, A) = \begin{cases} 1 & A = \mathbf{1} \\ 0 & \text{otherwise.} \end{cases}$$

Hence, we conclude 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 true on physical grounds. Suppose there was a state on the sphere with a single anyon of type A. Now choose any other anyon B. We observe that braiding B around A acts by the phase $+1$, because the loop of B can be contracted around there other side of the sphere, as illustrated in figure 5.1. Diagramatically, this means that for all simple objects $B \in \mathcal{L}$



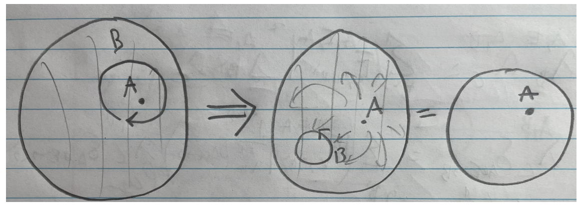


Figure 5.1: Illustration of braiding around a single anyon on the sphere

By modularity (c.f. remark 5.2.19), this implies $A \cong \mathbf{1}$. Thus, the if there is only one anyon on the sphere it must have trivial type. The fact that there is a unique state on the sphere with no anyons is also true on physical grounds, but is more subtle. It is discussed in subsection [ref].

Physics-math dictionary 5.2.30. For any modular category $\mathcal{C}$,:

$$\begin{pmatrix}\text{states of topological order } \mathcal{C} \\ \text{on the infinite flat plane } \mathbb{R}^2 \\ \text{with anyon configuraiton } A_1, A_2 ... A_n\end{pmatrix} = \begin{pmatrix}\text{normalized vectors in the Hilbert space} \\ \mathrm{Hom}_{\mathcal{C}}\left(\bigoplus_{[B]\in\mathcal{L}} B, A_1 \otimes A_2 ... \otimes A_n\right)\end{pmatrix} \tag{5.6}$$

Remark 5.2.31. Replacing $\mathbf{1}$ with $\bigoplus_{[B]\in\mathcal{L}} B$ reflects the differences between the sphere and the infinite flat plane. On a sphere, the only way to have a state with a single isolated anyon is for that anyon to have trivial charge. However, on the plane you can have a state with any single isolated anyon. This is done by creating a particle/antiparticle pair, and then pulling one half of that pair away to infinity, as illustrated in figure 5.2. This is reflected by the fact that equation 5.7 says that for all anyon types A,

$$\dim \begin{pmatrix}\text{Hilbert space of states of topological order } \mathcal{C} \\ \text{on the infinite flat plane } \mathbb{R}^2 \\ \text{with a single anyon of type } A\end{pmatrix} = \dim \mathrm{Hom}\,\Big(\bigoplus_{[B]\in\mathcal{L}} B, A\Big) = 1. \tag{5.7}$$

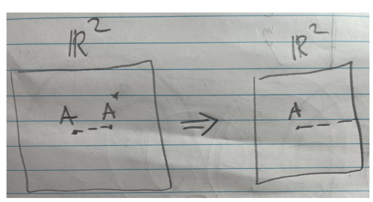


Figure 5.2: Creating a state on the plane with a single isolated anyon

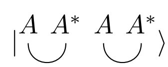
The fact that there is a unique state with a single anyon of type A on the plane $\mathbb{R}^2$ is a more subtle physical argument, discussed in subsection [ref].

Remark 5.2.32. Working on higher-genus surfaces or on surfaces with holes is possible, but it is a bit cumbersome in the approach were are taking. We refer to appendix [ref] for a discussion of the topic.

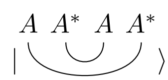
Remark 5.2.33. The anyon configurations in equations 5.5 and 5.7 are always assumed to be linear. The main reason to do this is because it makes the mathematics much simpler. Keeping track of the positions of each of the anyons in two dimensional space adds unnececary complexity. Seeing as every anyon 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 prefered.

Remark 5.2.34. The formula $\mathrm{Hom}_{\mathcal{C}}(\mathbf{1}, A_1 \otimes A_2 ... \otimes A_n)$ encodes the fact that states can be specified by their history. There are multiple states with anyon configuration $A_1 \otimes A_2 ... \otimes A_n$. One way of specifying a state $|\psi\rangle$ is to start with the unique state on the sphere with no anyons, and then specify how $|\psi\rangle$ is constructed from the ground state via some unambigous process. This unambigous process from the state with no anyons to the state with anyons $A_1 ... A_n$ is a morphism in$\mathrm{Hom}_{\mathcal{C}}(\mathbf{1}, A_1 \otimes A_2 ... \otimes A_n)$.

Example 5.2.35. We can describe two states with four the four anyons A, A^*, A, A^* as follows. The first state is obtained by starting with the unique state with no anyons, and creating two independent (A, A^*) particle/antiparticle pairs adjacent to each other:



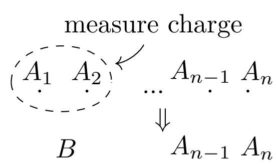
Another state can be constructed by creating a (A, A^*) particle/antiparticle pair, then moving the halves of the pair far apart from each other, and then creating a (A^*, A) particle/antiparticle pair in the space between the halves of the first pair:



These two (unnormalized) states have the same anyon configuration. However, they are distinguished by the fact that they were created by different processes. Translating pair-creation and movement into category theoretic language, we see that these two states correspond to different maps in $\mathrm{Hom}_{\mathcal{C}}(\mathbf{1}, A \otimes A^* \otimes A \otimes A^*)$.

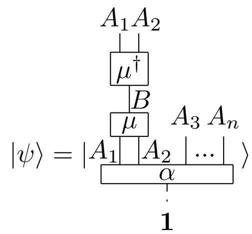
5.2.4 Topological charge measurement

In any reasonable physical theory, one needs to talk about measurements and observables. For the algebraic theory of topological quantum information, the only relevant type of measurement is a *topological charge measurement* [Bon21]. This is the measurement of the overall anyon type (or *topological charge*) of a collection of anyons. When the topological charge of a pair of anyons in a state $|\psi\rangle$ is measured, $|\psi\rangle$ will collapse onto a new state $|\psi'\rangle$ for which that pair of anyons now has a single well-defined charge as shown in equation 5.8. That is, the two anyons will fuse together.



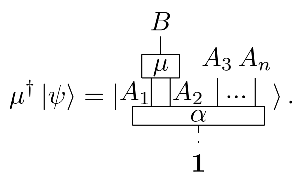
(5.8)

As a first step towards an algebraic understanding of topological charge measurement, suppose that we are presented with a normalized state on the sphere of the following form:



(5.9)

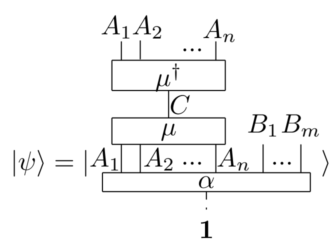
Where $A_1 ... A_n$, B are simple objects, and $\mu : A_1 \otimes A_2 \to B$ is normalized so that $\langle \mu \,|\, \mu \rangle = 1$. If we postcompose $|\psi\rangle$ with the map $\mu \otimes \mathrm{id}_{A_3 \otimes ... \otimes A_n}$, the result will be equal to



(5.10)

This means that μ gives a physical process whereby $|\psi\rangle$ can transform to a state with an anyon of type B where A_1, A_2 used to be. Moreover, if we postcompose $|\psi\rangle$ with $\eta \otimes \mathrm{id}_{A_3 \otimes ... \otimes A_n}$ with any map such that $\eta \circ \mu^\dagger = 0$ so $\eta\,|\psi\rangle$ will be zero (and thus an invalid quantum state). In particular, since there are no maps $B \to C$ for non-isomorphism simple objects B, C, we find that there is no physical process on the first two anyons which can be applied to $|\psi\rangle$ which results in a state with charge $C \ncong B$ where A_1, A_2 used to be. This motivates the following mathematical-physical correspondance:

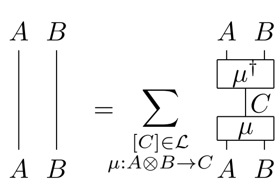
Physics-math dictionary 5.2.36. Given a state $|\psi\rangle$ with anyon content $A_1 ... A_n, B_1 ... B_m$ we say that the anyons $A_1 ... A_n$ have overall topological charge C with fusion channel $\mu : A_1 \otimes A_2 ... \otimes A_n \to C$ if there exists α such that $|\psi\rangle$ can be expressed as follows:



(5.11)

If $|\psi\rangle$ is a superposition of states the form 5.11 for a fixed C over different μ, then we say that the anyons $A_1 ... A_n$ have overal topological charge C but have indefinite fusion channel.

Proposition 5.2.37. *Let $A, B \in \mathcal{C}$ be objects in a modular category. We have that*

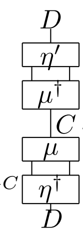


(5.12)

where $[C]$ runs over isomorphism classes of simple objects in $\mathcal{C}$, and μ runs over any orthonomral basis of $\mathrm{Hom}(A \otimes B, C)$.

Proof. Let f denote the morphism on the right hand side of equation 5.12. Choose any $[D] \in \mathcal{L}$, and fusion channels $\eta, \eta' : A \otimes B \to D$ in the same orthonormal basis as in equation 5.12. We have that

$$\eta' \circ f \circ \eta^\dagger = \sum_{\substack{[C]\in\mathcal{L} \\ \mu : A\otimes B \to C}}$$



Seeing as there are no non-zero maps $C \to D$ for $C \ncong D$, the only terms that survive are the ones with $C \cong D$. Moreover, since $\{\mu\}$ is chosen to be an orthonormal basis, the only term which survive are the one with $\mu = \eta = \eta'$. Thus,

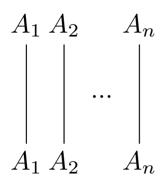
$$\eta' \circ f \circ \eta^\dagger = \begin{cases} \mathrm{id}_D & \eta = \eta' \\ 0 & \eta \neq \eta'. \end{cases}$$

Similarly, the orthonormality of the basis $\{\mu\}$ gives

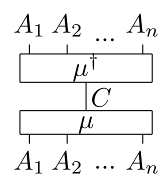
$$\eta' \circ \eta^\dagger = \begin{cases} \mathrm{id}_D & \eta = \eta' \\ 0 & \eta \neq \eta'. \end{cases}$$

Thus, $\eta' \circ f \circ \eta^\dagger = \eta' \circ \mathrm{id}_{A\otimes B} \circ \eta^\dagger$. Since η and η' run over bases of maps $A \otimes B \to D$, we can take linear combinations and sums to find that f and $\mathrm{id}_{A\otimes B}$ are equal when precomposed or postcomposed with any map. Thus, we find that $f = \mathrm{id}_{A\otimes B}$ as desired. □

Corollary 5.2.38. *Let $\mathcal{C}$ be a modular category. For all simple objects $A_1, A_2 ... A_n \in \mathcal{C}$, we have that*



$$= \sum_{\substack{[C]\in\mathcal{L} \\ \mu : A_1\otimes A_2 ... \otimes A_n \to C}}$$



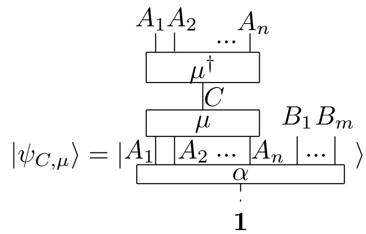
(5.13)

Proof. The proof follows be precomposing and postcomposing with fusion channels, completely analagously to the proof of proposition 5.2.37. □

Remark 5.2.39. Corollary 5.2.38 tells us every state $|\psi\rangle$ with anyon content $A_1 ... A_n$, $B_1 ... B_m$ can be made into a superposition of states with defininte overall charge and fusion channel of $A_1 ... A_n$. The general principles of quantum mechanics tell us how to measure

Physics-math dictionary 5.2.40. Let $|\psi\rangle = |\alpha\rangle$ be a normalized state, where $\alpha : \mathbf{1} \to A_1 ... \otimes A_n \otimes B_1 ... \otimes B_m$. For all normalized $\mu^\dagger : A_1 \otimes A_2 ... \otimes A_n \to C$, define the state

$$|\psi_{C,\mu}\rangle =$$



and

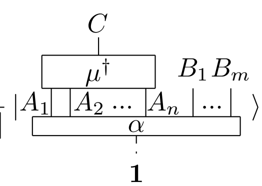
$$|\psi_C\rangle = \sum_{\mu: A_1 \ldots \otimes A_n \to C} |\psi_{C,\mu}\rangle$$

By proposition 5.2.38, we have that

$$|\psi\rangle = \sum_C |\psi_C\rangle = \sum_{C,\mu} |\psi_{C,\mu}\rangle .$$

A *topological charge measurement* on the anyons $A_1 \ldots A_n$ with respect to the orthonormal basis $\{\mu\}$ of $\bigoplus_C \mathrm{Hom}(C, A_1 \otimes \ldots A_n)$ collapses $|\psi\rangle$ onto the state $\frac{1}{\| |\psi_{C,\mu}\rangle \|} |\psi_{C,\mu}\rangle$ with probability $\| |\psi_{C,\mu}\rangle \|^2$, and the corresponding observable is (C, μ). Alternatively, we can think of the state resulting from the measurement as being

$$\frac{\mu^\dagger \circ |\psi_{C,\mu}\rangle}{\| |\psi_{C,\mu}\rangle \|} = \frac{1}{\| |\psi_{C,\mu}\rangle \|}$$



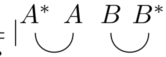
A topological charge measurement of the anyons $A_1 \ldots A_n$ without respect to any basis of $\bigoplus_C \mathrm{Hom}(C, A_1 \otimes \ldots A_n)$ collapses $|\psi\rangle$ onto the state $\frac{1}{\| |\psi_C\rangle \|} |\psi_C\rangle$ with probability $\| |\psi_C\rangle \|^2$.

Definition 5.2.41. Let $\mathcal{C}$ be a modular category. We define the *quantum dimension* of a simple object $A \in \mathcal{C}$ to be $d_A = \mathrm{tr}(\mathrm{id}_A)$.

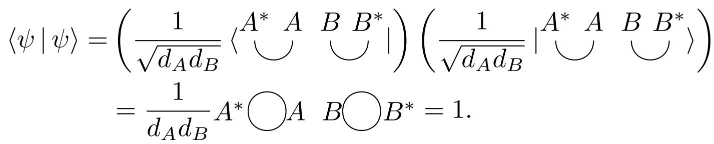
Remark 5.2.42. We will discuss quantum dimensions in more detail in subsection [ref]. For now, it suffices to recall from proposition [ref] that quantum dimensions are positive (in particular, nonzero) for unitary modular categories.

Example 5.2.43. We give a basic and fundamental example of topological charge measurement. Suppose that we create adjacent particle/antiparticle pairs, $(A^* \otimes A)$ and $(B \otimes B^*)$. What is the probability that we measure the charge C when the middle anyons A, B are fused? When we create the pairs of anyons (A^*, A), $(B, B*)$, the state is represented algebraically as

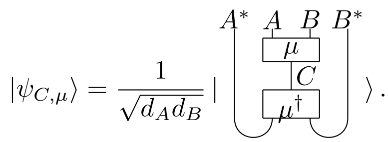
$$|\psi\rangle = \frac{1}{\sqrt{d_A d_B}}$$



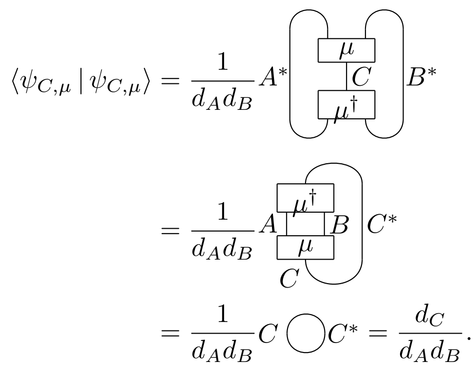
The normalization is correct, because



Now, choosing some an orthonormal basis $\{\mu\}$ of $C \to A \otimes B$ for all C, we can define



We compute



Thus, when the topological charge measurement is performed with respect to the basis $\{\mu\}$, the probability of the result being (C, μ) is $d_C/(d_A d_B)$. Since for any given C there are $N_C^{A,B}$ different choices of μ, the probability of measuring C when the topological charge measurement is performed without a choice of basis is

$$\text{(probability of measuring } C \text{ when fusing } A, B) = \frac{d_C}{d_A d_B} N_C^{A,B}. \tag{5.14}$$

Remark 5.2.44. As a sanity check, we can remark that (proposition [ref])

$$\sum_C \frac{d_C}{d_A d_B} N_C^{A,B} = 1.$$

Thus, the probabilities from equation 5.14 really do form a probability distribution.

Remark 5.2.45. When we measure fusion channel, we need a measurement apparatus with a distinguished choice of fusion basis.

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.

5.3.1 Duality

Duality is baked into our definition of modular categories as a fundamental part of the structure. In this subsection we will explore the basic properties of duality in modular categories.

Proposition 5.3.1. *Let $\mathcal{C}$ be a fusion category and let $A, B, C \in \mathcal{C}$ be simple objects. We have the following:*

(i) (Anti-involution) $N_C^{A,B} = N_{C^*}^{B^*,A^*}$*;*

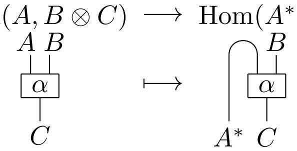
(ii) (Frobenius reciprocity) $N_C^{A,B} = N_B^{A^*,C} = N_A^{C,B^*}$.

Proof. Part (i) follows from the fact that the duality functor is fully faithful and monoidal from propositon 4.3.43, so

$$N_C^{A,B} = \dim \mathrm{Hom}(C, A \otimes B) = \dim \mathrm{Hom}(A^* \otimes B^*, C^*) = N_{C^*}^{B^*,A^*}.$$

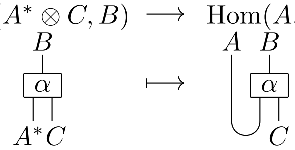
Part (ii) follows from the following computation. Consider the map

$$i : \mathrm{Hom}(A, B \otimes C) \longrightarrow \mathrm{Hom}(A^* \otimes C, B)$$



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. □

Corollary 5.3.2. *Let $\mathcal{C}$ be a fusion category. Let $A, B \in \mathcal{C}$ 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:

$$N_{\mathbf{1}}^{A,B} = N_A^{A^*,\mathbf{1}} = \dim(\mathrm{Hom}(A, A^*)) = \begin{cases} 1 & B \cong A^* \\ 0 & \text{otherwise.} \end{cases}$$

□

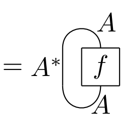
Corollary 5.3.3. *If $\mathcal{C}$ is a fusion category, then $A \cong A^{**}$ for all $A \in \mathcal{C}$.*

Proof. Since $N_{\mathbf{1}}^{A^*,A^{**}} > 0$, we conclude that $A^{**} \cong A$ by the $(iii) \implies (i)$ implication in proposition 5.3.1. ☐

Remark 5.3.4. Despite corollary 5.3.3, we *cannot* conclude that every fusion category admits a pivotal structure. The isomorphisms $A \cong A^{**}$ 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 fusion category admits a spherical structure [ENO05].

5.3.2 Trace

The first structure to define in the theory of modular categories is the *trace*. Let $\mathcal{C}$ be a spherical fusion category. Given any object $A \in \mathcal{C}$ and any endomorphism $f : A \to A$, we define the *trace of* f by the following formula:

$\mathrm{tr}(f) =$ 

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 $g = \lambda \cdot \mathrm{id}_{\mathbf{1}}$.

Remark 5.3.5. The trace is used mainly as a tool for linearization. Morphisms and objects are hard to describe, but the trace is a complex number.

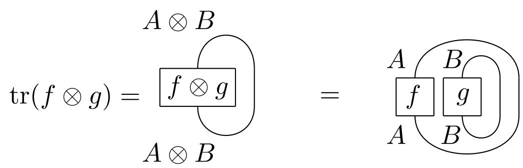
Proposition 5.3.6. *Let $\mathcal{C}$ be a spherical fusion category. For all $A, B \in \mathcal{C}$, $f \in \mathrm{End}(A)$ the following claims are all true:*

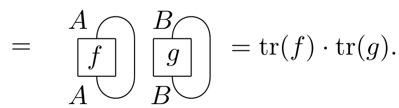
1. $\mathrm{tr} : \mathrm{End}(A) \to \mathbb{C}$ *is a linear map of vector spaces,*
2. $\mathrm{tr}(f^*) = \mathrm{tr}(f)$,
3. $\mathrm{tr}(f \oplus g) = \mathrm{tr}(f) + \mathrm{tr}(g)$ *for all* $g \in \mathrm{End}(B)$,
4. $\mathrm{tr}(f \otimes g) = \mathrm{tr}(f) \cdot \mathrm{tr}(g)$ *for all* $g \in \mathrm{End}(B)$,
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 $\mathcal{C}, \mathcal{D}$ be spherical categories with traces $\mathrm{tr}_{\mathcal{C}}, \mathrm{tr}_{\mathcal{D}}$ respectively. Let $F : \mathcal{C} \to \mathcal{D}$ be a pivotal functor. We have that* $\mathrm{tr}_{\mathcal{C}}(f) = \mathrm{tr}_{\mathcal{D}}(F(f))$*;*

Proof. We prove the claims one by one.

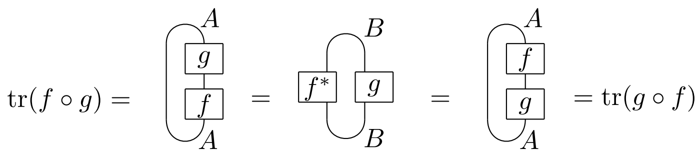
1. This follows immediately from the bilinearity of composition.
2. This is a straightforward computation.
3. This is a special case of the proof strategy used in corollary 5.3.7.

4. We compute as follows:

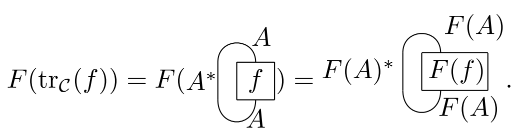




5. We compute as follows:



6. Treating the trace as a morphism $\mathbf{1}_{\mathcal{C}} \to \mathbf{1}_{\mathcal{C}}$, we find



   Here, we used that F sends evaluation/coevaluation maps to evaluation/coevaluation maps, with compatible isomorphisms $A \cong A^*$ between the left/right rigid structures.

This completes the proof. ☐

Corollary 5.3.7. *Let $f : A \to A$ be an endomorphism in a fusion category $\mathcal{C}$. 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 $A_i \not\cong A_j$ 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

$$\mathrm{tr}_{\mathcal{C}}(f) = \mathrm{tr}_{\mathbf{Vec}}(M).$$

Proof. Suppose that $A = A_0 \oplus A_1$ is the direct sum of two objects, not neccecarily simple. By proposition 4.3.43 we have a canonical decomposition

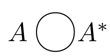
$$(A_0 \oplus A_1) \otimes (A_0 \oplus A_1)^* \cong (A_0 \otimes A_0^*) \oplus (A_0 \otimes A_1^*) \oplus (A_1 \otimes A_0^*) \oplus (A_1 \otimes A_1^*).$$

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. $\square$

5.3.3 Quantum dimension and Frobenius-Perron dimension

Our next tool to discuss is the *quantum dimension*. We have already seen quantum dimensions appear in subsection 5.2.4. We recall that given any spherical fusion category $\mathcal{C}$ and any simple object $A \in \mathcal{C}$, we the quantum dimension of A by the 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 5.3.8. *For every spherical fusion category $\mathcal{C}$ and any objects $A, B \in \mathcal{C}$, we have the following formulas:*

(i) *If $A \cong B$, then $d_A = d_B$;*

(ii) $d_{A^*} = d_A$;

(iii) $d_A \neq 0$;

(iv) $d_A \in \mathbb{R}$.

Proof.

(i) Let $f : A \cong B$ be an isomorphism. Using proposition 5.3.6 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 5.3.6.

(iii) From proposition 5.3.2, we know that $A \otimes A^* \cong \mathbf{1} \oplus X$ for some $X \in \mathcal{C}$ 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.

(iv) WORK: There is reference to this fact in the MathOverflow question ‘Modular Tensor Categories: Reasoning behind the axioms”

□

Definition 5.3.9. For every simple object $A \in \mathcal{C}$ in a fusion category, we define the *fusion matrix* N^A corresponding to A to be the matrix whose rows and collumns are labeled by $\mathcal{L}$, and whose (B, C) entry is $N_C^{A,B}$. As a linear operator, this means that N^A acts as follows:

$$\begin{aligned} N^A : \mathbb{C}[\mathcal{L}] &\to \mathbb{C}[\mathcal{L}]. \\ |[B]\rangle &\mapsto \sum_{[C]\in\mathcal{L}} N_C^{A,B} \, |[C]\rangle \end{aligned}$$

Proposition 5.3.10. *Let $\mathcal{C}$ be a spherical fusion category.*

(i) Let $A, B \in \mathcal{C}$ be simple objects. We have that

$$d_A d_B = \sum_{[C]\in\mathcal{L}} N_C^{A,B} d_C.$$

(ii) Define $\mathbf{d} = \sum_{[B]\in\mathcal{L}} d_B \, |[B]\rangle \in \mathbb{C}[\mathcal{L}]$. We have that

$$N^A \mathbf{d} = d_A \mathbf{d}$$

for all simple objects A.

Proof. Taking the trace of the identity of both sides of the isomorphism

$$A \otimes B \cong \bigoplus_{[C]\in\mathcal{L}} N_C^{A,B} \cdot C,$$

we find that

$$\mathrm{tr}(\mathrm{id}_{A\otimes B}) = \mathrm{tr}(\mathrm{id}_{\bigoplus_{[C]\in\mathcal{L}} N_C^{A,B} \cdot C}).$$

Expanding using the rules in proposition 5.3.2 gives part (i). Part (ii) follows from expanding the definition of the linear operator and applying part (i). □

Definition 5.3.11. For every spherical fusion category $\mathcal{C}$, we define the *global quantum dimension* $\mathcal{D} = \mathcal{D}_{\mathcal{C}}$ of $\mathcal{C}$ by

$$\mathcal{D}^2 = \sum_{[A]\in\mathcal{L}} d_A^2. \tag{5.15}$$

Since $d_A \in \mathbb{R}$ by proposition 5.3.8, $\mathcal{D}^2 \geq 0$, so taking $\mathcal{D}$ to be the positive square root of the right hand side in equation 5.15 gives an unambiguous definition of $\mathcal{D}$.

Proposition 5.3.12. *Let $\mathcal{C}$ be a spherical fusion category. For all $C \in \mathcal{C}$, we have that*

$$d_C \mathcal{D}^2 = \sum_{[A],[B]\in\mathcal{L}} d_A d_B N_C^{A,B}.$$

Proof. From proposition 5.3.10, we have that

$$\sum_{A,B\in\mathcal{L}} d_A d_B N_C^{A,B} = \sum_{[A],[B],[D]\in\mathcal{L}} d_D N_D^{A,B} N_C^{A,B}.$$

Now, we observe that for all $A, C \in \mathcal{L}$,

$$\begin{aligned} A \otimes (C \otimes A^*) &\cong \sum_{[B]\in\mathcal{L}} N_B^{C,A^*} A \otimes B \\ &\cong \sum_{[B],[D]\in\mathcal{L}} N_B^{C,A^*} N_D^{A,B} D. \end{aligned}$$

Taking the trace of $\mathrm{id}_{A\otimes C\otimes A^*}$, we thus find that

$$d_A d_C d_{A^*} = \sum_{[B],[D]} N_B^{C,A^*} N_D^{A,B} d_D.$$

Now, proposition 5.3.8 tells us $d_{A^*} = d_A$, and proposition 5.3.1 tells us that $N_B^{C,A^*} = N_C^{A,B}$. Thus, we find that

$$\sum_{[A],[B],[D]\in\mathcal{L}} d_D N_D^{A,B} N_C^{A,B} = \sum_A d_A^2 d_C = d_C \mathcal{D}^2$$

as desired. □

Theorem 5.3.13 (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: $|\mu| \le \lambda(B)$. 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 $\lambda(B)$.

Definition 5.3.14. We call the largest positive real eigenvalue of a matrix its *Frobenius-Perron eigenvalue.*

Corollary 5.3.15. *Let $\mathcal{C}$ be a unitarizable spherical fusion category. Let $A \in \mathcal{C}$ be a simple object. The quantum dimension d_A is equal to the Frobenius-Perron eigenvalue of N^A.*

Proof. Since $\mathcal{C}$ 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. □

Definition 5.3.16. Let $A \in \mathcal{C}$ be a simple object in a spherical fusion category. We define the *Frobenius-Perron dimension* of A (denoted $\mathrm{FPdim}(A)$) by the formula

$$\mathrm{FPdim}(A) = (\text{Frobenius-Perron eigenvalue of } N^A).$$

Remark 5.3.17. In light of corollary 5.3.15, $\mathrm{FPdim}(A) = d_A$ whenever $\mathcal{C}$ is unitarizable. However, in this chapter we will mostly work with spherical fusion categories with no conditions on unitarizability. Thus, the definition of $\mathrm{FPdim}(A)$ is not redundant and is at times useful. An additional observation is that the definition of quantum dimension strongly uses the spherical structure on $\mathcal{C}$. 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.

Remark 5.3.18. Proposition 5.3.10 tells us that d_A is an eigenvalue of N^A. This gives a restriction on d_A. For instance, d_A is always an algebraic number since it is the root of the characteristic polynomial of N^A. Frobenius-Perron dimensions are much more strongly restricted, by the general theory of matrices with nonnegative integer coefficients. In particular, Theorem 1.1.1 of [GdLHJ12] says that that Frobenius-Perron eigenvalue of a matrix with nonnegative integer entries must be either greater or equal to 2, or it will be equal to $2\cos(\pi/q)$ for some integer $q \geq 2$. Thus, we get that

$$\mathrm{FPdim}(A) \geq 2 \qquad \text{or} \qquad \mathrm{FPdim}(A) = 2\cos(\pi/q),\ q \geq 3.$$

Writing out the first few values of $2\cos(\pi/q)$, we find the following possible values for $\mathrm{FPdim}(A)$:

$$\mathrm{FPdim}(A) = 1, \sqrt{2}, \phi, \sqrt{3}, ...$$

where $\phi = (1+\sqrt{5})/2$ is the golden ratio.

Proposition 5.3.19. *Let $\mathcal{C}$ be a fusion category, and let $A \in \mathcal{C}$ 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)

$$\mathrm{FPdim}(A) = \lim_{n\to\infty} (\#\ \textit{of simple objects in the direct sum decomposition of}\ A^{\otimes n})^{1/n}.$$

Proof. (i) We observe that if in $\mathbb{C}[\mathcal{L}]$

$$\left(N^A\right)^n |\mathbf{1}\rangle = \sum_{[B]\in\mathcal{L}} n_B\, |[B]\rangle\,,$$

then $A^{\otimes n} \cong \bigoplus_{[B]\in\mathcal{L}} n_B B$. So,

$$\dim(\mathrm{Hom}(A^{\otimes n}, A^{\otimes n})) = \sum_{[B]\in\mathcal{L}} n_B^2 = \left\|\left(N^A\right)^n |\mathbf{1}\rangle\right\|^2.$$

We can now decompose $|\mathbf{1}\rangle = \sum_i \mathbf{v}_i$ where $\mathbf{v}_i$ is in the λ_i generalized eigenspace of N^A. We observe that element $\mathbf{v}_i$ with $\lambda_i = \mathrm{FPdim}(A)$ is non-zero, since

$$\langle \mathbf{1}| \sum_{[B]\in\mathcal{L}} \mathrm{FPdim}(B)\, |[B]\rangle = 1 \neq 0.$$

Now,

$$\left\| \left(N^A\right)^n |\mathbf{1}\rangle \right\|^2 = \sum_i \left\| \left(N^A\right)^n \mathbf{v}_i \right\|^2 .$$

This sum is dominated by the terms with $|\lambda_i| = \mathrm{FPdim}(A)$, which grow like $\mathrm{FPdim}(A)^{2n}$. Thus,

$$\lim_{n\to\infty} \left(\left\| \left(N^A\right)^n |\mathbf{1}\rangle \right\|^2 \right)^{1/2n} = \mathrm{FPdim}(A)$$

as desired.

(ii) WORK: This one is more subtle. There's some arguing I have to do. By hand, it seems like it uses an approximation theorem of Dirichlet. Perhaps there is a good reference for the general linear algebra result?

(iii) We observe that

$$(\#\text{ of simple objects in the direct sum decomposition of } A^{\otimes n}) = \sum_{[B]\in\mathcal{L}} \langle [B]| \left(N^A\right)^n |\mathbf{1}\rangle .$$

Up to constant factors, this grows like $\sum_{[B]\in\mathcal{L}} \mathrm{FPdim}(B) \langle [B]| \left(N^A\right)^n |\mathbf{1}\rangle$. This term is exactly

$$\langle \mathbf{w}| \left(N^A\right)^n |\mathbf{1}\rangle$$

where $\mathbf{w} = \sum_{[B]\in\mathcal{L}} \mathrm{FPdim}(B)\, |[B]\rangle$. This term is an eigenvector with Frobenius-Perron eigenvalue. Thus, its inner product with $\left(N^A\right)^n |\mathbf{1}\rangle$ grows like $\mathrm{FPdim}(A)^n$ as desired.

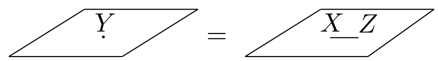
□

Remark 5.3.20. Proposition 5.3.19 gives 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]. 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 5.3.19, $\mathrm{FPdim}(A)^n$ 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.

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.

Example 5.3.21. Consider the Y-type anyon on the toric code. It consists of the fusion of an X-type anyon and a Z-type anyon, as shown below:



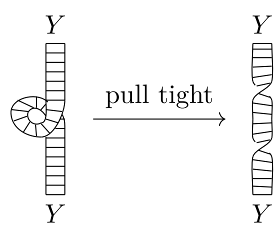
(5.16)

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

(5.17)

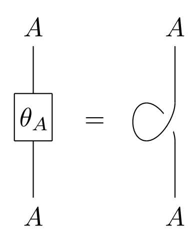
This is the twist.

Remark 5.3.22. 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. We observe that the twist can be constructed in an alternative form more amenable to our usual string diagrams:



(5.18)

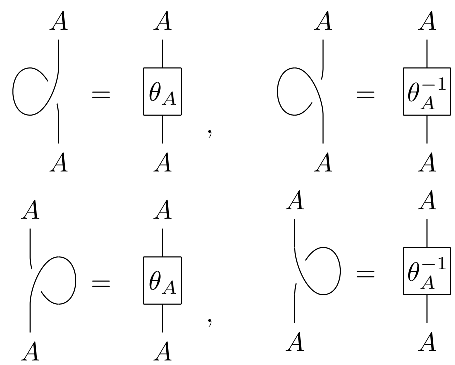
Definition 5.3.23. Let $\mathcal{C}$ be a pre-modular fusion category, we define the *twist* θ_A of an object $A \in \mathcal{C}$ to be



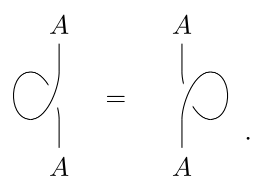
Remark 5.3.24. For every simple object $A \in \mathcal{C}$, the map $\theta_A \in \mathrm{End}(A)$ can be identified with the unique complex number λ such that $\theta_A = \lambda \cdot \mathrm{id}_A$. Equivilantly, we can identify θ_A with the complex number $\lambda = \mathrm{tr}(\theta_A)/d_A$ which gives the graphical formula

$$\theta_A = \frac{1}{d_A}$$ 

Lemma 5.3.25. *Let $\mathcal{C}$ be a pre-modular fusion category. We have that*



Proof. To begin we show that



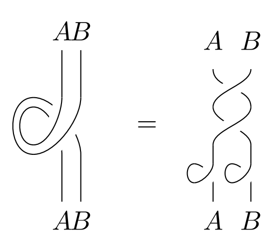
When A is simple, this follows from the spherical axiom. Taking the trace of both sides gives the same formula for θ_A as a figure-eight. Additionally, pushing through duals it is clear that both sides in the above proposed equality are natural isomorphisms. Natural isomorphisms are determined by their 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. □

Proposition 5.3.26. *Let $\mathcal{C}$ be a pre-modular fusion category. The twists θ induce a monoidal natural isomorphism $\mathrm{id}_{\mathcal{C}} \xrightarrow{\sim} \mathrm{id}_{\mathcal{C}}$. Additionally, θ satisfies the identity*

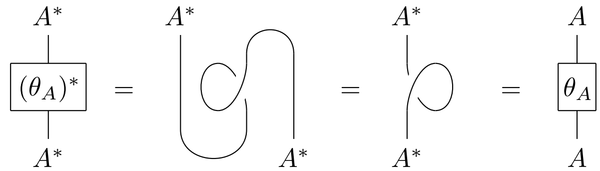
$$\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$$

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

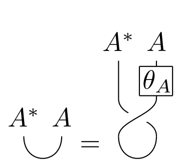


Finally, $\theta_{A^*} = (\theta_A)^*$ comes from the string-diagram manipulation and proposition [ref]:

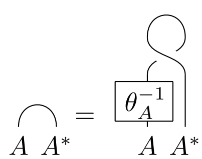


as desired. ☐

Remark 5.3.27. 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 an efficient way of encoding the spherical structure on $\mathcal{C}$. 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



and

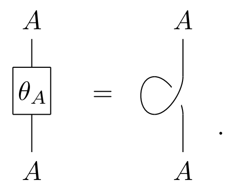


In this way, giving a spherical structure on a right-rigid monoidal category is the *same* as giving a twist structure, as codified in proposition 5.3.28.

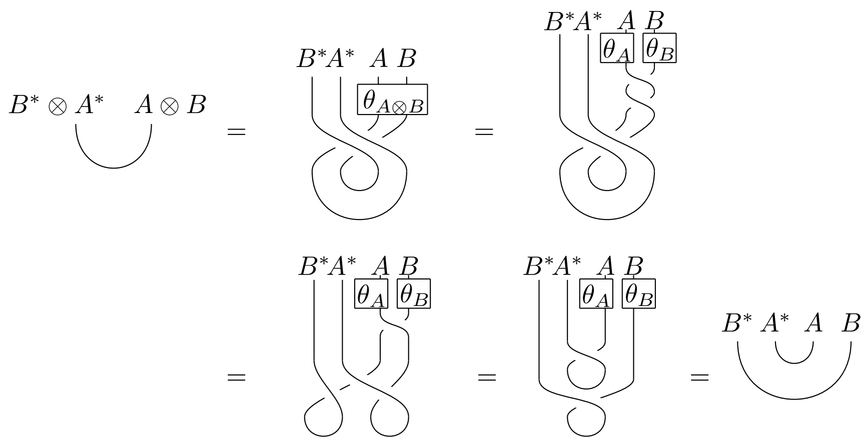
Proposition 5.3.28 (Deligne's twisting lemma, [Yet92])**.** *Let $\mathcal{C}$ be a right-rigid braided monoidal category. Every pivotal structure on $\mathcal{C}$ naturally gives a twist natural transformation $\theta : \mathrm{id}_{\mathcal{C}} \to \mathrm{id}_{\mathcal{C}}$. This assignment induces a canonical bijection between the set of pivotal structures on $\mathcal{C}$ and the set of natural isomorphism $\theta : \mathrm{id}_{\mathcal{C}} \to \mathrm{id}_{\mathcal{C}}$ satisfying $\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$ for all $A, B \in \mathcal{C}$.*

Moreover, restricting the assignment to the space of spherical structures on $\mathcal{C}$ induces a canonical bijection between the set of spherical structures on $\mathcal{C}$ and the set of isomorphisms $\theta : \mathrm{id}_{\mathcal{C}} \to \mathrm{id}_{\mathcal{C}}$ satisfying $\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$ for all $A, B \in \mathcal{C}$ and $\theta_{A^*} = (\theta_A)^*$.

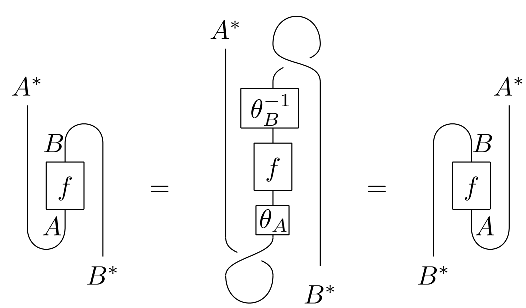
Proof. We already showed in proposition [ref] that every spherical category gives a twist natural transformation satisfying the desired axioms. Restriciting the proof to only a possibly non-spherical pivotal category still gives a twist natural transformation satisfying $\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$ for all $A, B \in \mathcal{C}$. 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



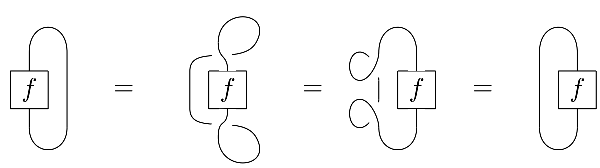
To begin, we assume that $\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$ and we seek to prove that the corresponding ev^L, coev^L maps induce a pivotal structure. We first axiom of pivotality follows from use of the axiom $\theta_{A\otimes B} = \beta_{B,A} \circ \beta_{A,B} \circ (\theta_A \otimes \theta_B)$:



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. $\square$

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.

Remark 5.3.29. Functors which do not induce equivalences of categories are also physically relevant. In certain contexts, a functor $F : \mathcal{C} \to \mathcal{D}$ is used to model a *phase transition* from $\mathcal{C}$ to $\mathcal{D}$. We will see a lot more functors and natural transformations between modular categories throughout the book, especially in chapter [ref].

We now dicuss the correct notion of functor nad natural transfrormation between our different levels and categorical structure:

- 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 functor. There is no compatibility condition required between the $\mathbb{C}$-linear structure and the pivotal 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 structure, or braided monoidal structure. We call these *pre-modular functors*. 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.

5.3.6 Deligne tensor product

WORK: There's another structure I would like to include - time reversal. Given a modular category $\mathcal{C}$, define $\overline{\mathcal{C}}$. Say that this corresponds to time reversal. I'm not sure if there's anything much to say. Somehow it feels natural for me to put this with the Deligne tensor product, but I think that's because I know about quantum double MTC... maybe there's a better place somewhere else.

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* [Del02]. Given any fusion categories $\mathcal{C}$, $\mathcal{D}$, their Deligne tensor product $\mathcal{C} \boxtimes \mathcal{D}$ 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.

Definition 5.3.30. Let $\mathcal{C}, \mathcal{D}$ 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 $\mathcal{C}$ and $\mathcal{D}$ to be be the following data:

1. A $\mathbb{C}$-linear category $\mathcal{C} \boxtimes \mathcal{D}$;
2. A $\mathbb{C}$-linear functor $\mathcal{C} \times \mathcal{D} \to \mathcal{C} \boxtimes \mathcal{D}$.

Such that:

1. Every object $X \in \mathcal{C} \boxtimes \mathcal{D}$ has a direct sum decomposition

$$X \cong \bigoplus_{i=1}^{n} A_i \boxtimes B_i$$

for some $n \geq 1$, $A_i \in \mathcal{C}$, $B_i \in \mathcal{D}$.

2. There is an equality of vector spaces

$$\mathrm{Hom}_{\mathcal{C}\boxtimes\mathcal{D}}(A \boxtimes B, A' \boxtimes B') = \mathrm{Hom}_{\mathcal{C}}(A, A') \otimes \mathrm{Hom}_{\mathcal{D}}(B, B').$$

3. Given any $A, A', A'' \in \mathcal{C}$, $B, B', B'' \in \mathcal{D}$, $f : A \to A'$, $f' : A' \to A''$, $g : B \to B'$, $g' : B' \to B''$, the diagram

$$\begin{tikzcd} A \boxtimes B \arrow[r, "f\boxtimes g"] \arrow[rr, bend right, "(f'\circ f)\boxtimes(g'\circ f)"'] & A' \boxtimes B' \arrow[r, "f'\boxtimes g'"] & A'' \boxtimes B'' \end{tikzcd}$$

commutes.

Proposition 5.3.31. *Let $\mathcal{C}, \mathcal{D}$ 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 $\mathcal{C} \boxtimes \mathcal{D}$ for $\mathcal{C}$ and $\mathcal{D}$. Moreover, given any other deligne tensor product $\mathcal{C} \boxtimes' \mathcal{D}$ of $\mathcal{C}$ and $\mathcal{D}$ there exists a unique functor $F : \mathcal{C} \boxtimes \mathcal{D} \to \mathcal{C} \boxtimes' \mathcal{D}$ making the diagram*

$$\begin{tikzcd} \mathcal{C} \times \mathcal{D} \arrow[r] \arrow[dr] & \mathcal{C} \boxtimes \mathcal{D} \arrow[d, "F"] \\ & \mathcal{C} \boxtimes' \mathcal{D} \end{tikzcd}$$

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 $\mathcal{C} \to \mathcal{C}'$ induces an equivalence of categories $\mathcal{C} \boxtimes \mathcal{D} \to \mathcal{C}' \boxtimes \mathcal{D}$. Hence, since $\mathcal{D}$ and $\mathcal{D}$ 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]. $\square$

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 5.3.32. *The following claims are all true.*

(i) Let $\mathcal{C}$, $\mathcal{D}$ be fusion categories. On the level of objects, define a monoidal structure $\mathcal{C} \boxtimes \mathcal{D}$ 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 $\mathbf{1}_{\mathcal{C}\boxtimes\mathcal{D}} = \mathbf{1}_{\mathcal{C}} \boxtimes \mathbf{1}_{\mathcal{D}}$, and a natural choice of associator and unitors, this induces the structure of a monoidal category on $\mathcal{C}$.

Define a right-rigid structure on $\mathcal{C} \boxtimes \mathcal{D}$ 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 $\mathcal{C} \boxtimes \mathcal{D}$.

The above definitions induce the structure of a fusion category on $\mathcal{C} \boxtimes \mathcal{D}$.

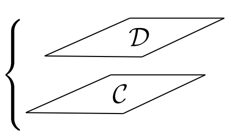
(ii) Let $\mathcal{C}, \mathcal{D}$ be spherical fusion categories. The evaluation and coevaluation maps $\mathrm{ev}^L_{A\boxtimes B} = \mathrm{ev}^L_A \boxtimes \mathrm{ev}^L_B$ and $\mathrm{coev}^L_{A\boxtimes B} = \mathrm{coev}^L_A \boxtimes \mathrm{coev}^L_B$ induce a left-rigid structure on $\mathcal{C}\boxtimes\mathcal{D}$. Along with the canonial structure of a fusion category on $\mathcal{C} \boxtimes \mathcal{D}$, this induces the structure of a spherical fusion category on $\mathcal{C} \boxtimes \mathcal{D}$.

(iii) Let $\mathcal{C}, \mathcal{D}$ be pre-modular categories. The braiding map $\beta_{\mathcal{C}\boxtimes\mathcal{D}} = \beta_{\mathcal{C}} \boxtimes \beta_{\mathcal{D}}$ induces the structure of a pre-modular category on $\mathcal{C} \boxtimes \mathcal{D}$. The product $\mathcal{C} \boxtimes \mathcal{D}$ is modular if and only if $\mathcal{C}, \mathcal{D}$ are both modular.

Proof. Given any of the above structures, all of the axioms on $\mathcal{C}\boxtimes\mathcal{D}$ immediately follow from their respective axioms on $\mathcal{C}$ and $\mathcal{D}$. Hence, the proof is an exercise is recalling definitons which we omit. □

Physics-math dictionary 5.3.33. Physically, the Deligne tensor product corresponds to *stacking*. Consider two sheets of material. Assume that the bottom one has topological order described by modular category $\mathcal{C}$ and chiral central charge $c_-^{\mathcal{C}}$, and that the top one has topological order described by the modular category $\mathcal{C}$ and chiral central charge $c_-^{\mathcal{D}}$. Consider a composite system obtained from stacking the two sheet, as shown in diagram 5.19. The modular category describing the stacked system is $\mathcal{C} \boxtimes \mathcal{D}$, and the chiral central charge is $c_-^{\mathcal{C}} + c_-^{\mathcal{D}}$.

$\mathcal{C} \boxtimes \mathcal{D}$



(5.19)

Example 5.3.34. For any fusion category $\mathcal{C}$, we have that

$$\mathbf{Vec}_{\mathbb{C}} \boxtimes \mathcal{C} \simeq \mathcal{C} \boxtimes \mathbf{Vec}_{\mathbb{C}} \simeq \mathcal{C}.$$

Physically, this corresponds to the fact that stacking a sheet of material with the copy of the trivial phase (empty space) does not change the phase of that material.

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*, which we define as plain categories below:

Definition 5.4.1. We define a category $\mathfrak{D}(G)$, the category of *G-graded G-representations*, as follows. It's objects are pairs (V, ρ), where $V = \bigoplus_{g \in G} V_g$ is a $\mathbb{C}$ vector space with a distinguished choice of direct sum decomposition into terms indexed by G, and

$$\rho : G \to \mathrm{Aut}(V)$$

is a group homomorphism such that

$$\rho(g)(V_h) \subseteq V_{ghg^{-1}}.$$

Morphisms in $\mathfrak{D}(G)$ from (V, ρ_V) to (W, ρ_W) are linear maps $f : V \to W$ such that $f(V_g) \subseteq W_g$ and the diagram

$$\begin{tikzcd} V \arrow[r, "\rho_V(g)"] \arrow[d, dashed, "f"] & V \arrow[d, dashed, "f"] \\ W \arrow[r, "\rho_W(g)"] & W \end{tikzcd}$$

commutes for all $g \in G$.

Remark 5.4.2. The conclusion of subsection 3.4.4 was that G-graded G-representations are the correct objects to characterize anyons in discrete gauge theory based on the finite group G. This physically motivates most of the developments made in this section.

In addition to proving that the category of G-graded G-representations, we will define two other auxiliary categories which we will track through the process:

Definition 5.4.3. We define a category $\mathbf{Vec}_G$, the category of *G-graded vector spaces*, as follows. It's objects are $\mathbb{C}$ vector spaces $V = \bigoplus_{g \in G} V_g$, with a distinguished choice of direct sum decomposition into terms indexed by G. Morphisms in $\mathbf{Vec}_G$ from V to W are linear maps $f : V \to W$ such that $f(V_g) \subset W_g$.

Definition 5.4.4. We define a category $\mathbf{Rep}(G)$, the category of *G-representations*, as follows. It's objects are pairs (V, ρ) where V is a $\mathbb{C}$ vector space and $\rho : G \to \mathrm{Aut}(V)$ is a group homorphism. Morphisms in $\mathbf{Rep}(G)$ from (V, ρ_V) to (W, ρ_W) are linear maps $f : V \to W$ such that $\rho_W(g) \circ f = f \circ \rho_V(g)$ for all $g \in G$.

Currently, we have only defiened $\mathfrak{D}(G)$, $\mathbf{Vec}_G$, and $\mathbf{Rep}(G)$ as plain categories. It is one of the main projectes of the section to endow these categories with additional structure. We will endow $\mathfrak{D}(G)$ with the structure of a modular category (theorem [ref]). We will endow $\mathbf{Vec}_G$ and $\mathbf{Rep}(G)$ with the structure of spherical fusion categories (propositions [ref] and [ref]). We will show that $\mathbf{Rep}(G)$ always admits a braiding, but this braiding is not non-degenerate (in fact, it is in a sense maximally degenerate, which we call *symmetric*). We show that $\mathbf{Vec}_G$ admits a symmetric braiding whenever G is abelian, and admits no braiding whenver G is nonabelian.

The categories $\mathbf{Vec}_G$, $\mathbf{Rep}(G)$ are all related in various ways. For instance, we have forgetful functors

$$\mathfrak{D}(G) \to \mathbf{Vec}_G$$
$$\mathfrak{D}(G) \to \mathbf{Rep}(G)$$

which send a G-graded G-representation to their underlying G-graded vector space or G-representation. Additionally, there is a functor

$$\mathbf{Rep}(G) \to \mathfrak{D}(G)$$

which sends a representation (V, ρ) to the same representation, with the G-grading on V that puts all of V into the 1-graded component, where 1 is the identity elemenet of G. We will see that all of these functors can be upgraded to functors of spherical categories (that is, $\mathbb{C}$-linear pivotal functors). Moreover, the functor $\mathbf{Rep}(G) \to \mathfrak{D}(G)$ can be upgraded to a functor of pre-modular categories.

Remark 5.4.5. In chapter [ref], all of the functors defined above will be given physical interpretations. Namely, the forgetful functors $\mathfrak{D}(G) \to \mathbf{Vec}_G$ and $\mathfrak{D}(G) \to \mathbf{Rep}(G)$ are interpreted as bulk-to-boundary condensation maps and the functor $\mathbf{Rep}(G) \to \mathfrak{D}(G)$ is interpreted as internal G-symmetry of $\mathfrak{D}(G)$.

In our study of G-graded G-representations, we will repeatedly make use of the following result:

Proposition 5.4.6. *Simple objects in $\mathfrak{D}(G)$ are in bijection with pairs (C, χ) where $C \subseteq G$ is a conjugacy class and χ is a simple representation of the centralizer of C. WORK: I don't know if this should go here, of if it is going to be in the TQO section. This proposition is not well-stated yet, becauase there is no such thing as "centralizer of a conjugacy class". The centralizer depends on which element in the conjugacy class you choose. It is only well-defined up to conjugacy. Of course, conjugacy groups are isomorphic so in a sense this is not a problem.*

5.4.2 $\mathbb{C}$-linear structures

In this subsection, we will define $\mathbb{C}$-linear structures on $\mathbf{Vec}_G$, $\mathbf{Rep}(G)$, and $\mathfrak{D}(G)$ for all finite groups G, and show that they are all equivalent to $\mathbf{Vec}_{\mathbb{C}}^n$ for various values of n. The definitions of the structures are simple. In particular, all three categories $\mathbf{Vec}_G$, $\mathbf{Rep}(G)$, and $\mathfrak{D}(G)$ have forgetful functors onto $\mathbf{Vec}_{\mathbb{C}}$ assigning to every G-graded vector space/G-representation/G-graded G-repesentation its underlying vector space. The hom-sets in $\mathbf{Vec}_G$, $\mathbf{Rep}(G)$, $\mathfrak{D}(G)$ are all linear subspaces of the hom-sets of their underlying vector spaces, and thus inherit a subspace $\mathbb{C}$-linear structure. This defines a $\mathbb{C}$-linear structure on $\mathbf{Vec}_G$, $\mathbf{Rep}(G)$, $\mathfrak{D}(G)$.

Proposition 5.4.7. *For all finite groups G, there is an equivalence of categories $\mathbf{Vec}_G \cong \mathbf{Vec}_{\mathbb{C}}^{|G|}$.*

Proof. We can define a functor $F : \mathbf{Vec}_G \to \mathbf{Vec}_{\mathbb{C}}^{|G|}$ which sends a G-graded vector space V to the arrangement of $|G|$ of vector spaces $\{V_g\}_{g \in G}$. Morphisms in $\mathbf{Vec}_G$ are exactly the same thing as a morphism in $\mathbf{Vec}_{\mathbb{C}}^{|G|}$, so F is bijective on hom-spaces. Thus, by proposition [ref], it induces an equivalence of categories. $\square$

Proposition 5.4.8. *Let G be a finite group. Let $(V,\rho) \in \mathbf{Rep}(G)$ be a representation of G. There exists an inner product $\langle - \,|\, - \rangle$ on V such that ρ acts by unitary transformations*

Proof. Choose any inner product $\langle - \,|\, - \rangle$ on V. Define a new inner product by

$$\langle v \,|\, w \rangle' = \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)(v) \,|\, \rho(g)(w) \rangle .$$

It is simple to check that $\langle - \,|\, - \rangle'$ satisfies all of the axioms of an inner product. Additionally, we find that for all $h \in G$,

$$\begin{aligned} \langle \rho(h)v \,|\, \rho(h)w \rangle' &= \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)\rho(h)(v) \,|\, \rho(g)\rho(h)(w) \rangle \\ &= \frac{1}{|G|} \sum_{g \in G} \langle \rho(gh)(v) \,|\, \rho(gh)(w) \rangle \\ &= \langle v \,|\, w \rangle . \end{aligned}$$

Thus, $\rho(h)$ is unitary as desired.

□

Proposition 5.4.9 (Schur's lemma)**.** *Let G be a finite group. Let $V, W \in \mathbf{Rep}(G)$ be simple representations. We have that*

$$\dim \mathrm{Hom}_{\mathbf{Rep}(G)}(V, W) = \begin{cases} 1 & V \cong W \\ 0 & V \ncong W. \end{cases}$$

Proof. Choose inner products on V,W so that ρ_V, ρ_W act by unitary transformations. Let $f : V \to W$ be a morphism of representations. We find that $\ker(f) \subseteq V$ is a subspace of V which is invariant under the G action. Moreover, the orthogonal complement $\ker(f)^\perp$ is also invariant under the G action since ρ_V acts by unitaries. Thus, we have that

$$V = \ker(f) \oplus \ker(f)^\perp$$

is a decomposition of V into a direct sum of representations. Since V is simple, we must have $\ker(f) = 0$ (in which case f is injective) or $\ker(f)^\perp = 0$ (in which case $f = 0$). Similarly, the image $\mathrm{ims}(f) \subseteq W$ is invariant under the G-action, so the decomposition

$$W = \mathrm{ims}(f) \oplus \mathrm{ims}(f)^\perp$$

proves either $\mathrm{ims}(f) = 0$ (in which case $f = 0$) or $\mathrm{ims}(f)^\perp = 0$ (in which case f is surjective). Thus, f is either 0 or an isomorphism.

We now show that if $V = W$ then the space of maps $V \to V$ is one dimensional. Let $f : V \to V$ be a morphism of represenations. Since $\mathbb{C}$ is algebraically closed, we can choose an eigenvector λ of f, so that $f - \lambda \cdot \mathrm{id}_V$ is not invertible. However, every non-invertible morphism of representations must be 0 by the above argument. Thus, $f - \lambda \cdot \mathrm{id}_V = 0$ so $f = \lambda \cdot \mathrm{id}_V$. Thus, the space of maps $V \to V$ is spanned by id_V so is one-dimensional as desired. □

Proposition 5.4.10 (Mashke's theorem)**.** *Let G be a finite group. Every representation in* $\mathbf{Rep}(G)$ *is the direct sum of finitely many simple representations*

Proof. We argue by induction on the dimension of the representation as a vector space, $\dim V = n$. Suppose that V is a representation of dimension n. It is simple, we are done. If it is not simple, then we can write $V \cong V_0 \oplus V_1$ with $V_0, V_1 \neq 1$. Since $\dim(V_0), \dim(V_1) < n$, they are the direct sum of finitely many simple representations by the induction hypothesis. Thus, V is the direct sum of finitely many simple representations as desired. □

Example 5.4.11. The vector space $\mathbb{C}[G]$ spanned by elements of G is naturally equipped with the structure of a G-representation. Namely, there is a map

$$\begin{aligned} \rho : G &\to \mathrm{Aut}(\mathbb{C}[G]). \\ g &\mapsto (|h\rangle \mapsto |gh\rangle) \end{aligned}$$

This is called the *regular representation* of G.

Lemma 5.4.12. *Let G be a finite group. There is an isomorphism of representations*

$$\mathbb{C}[G] \cong \bigoplus_{[V] \in \mathcal{L}(\mathbf{Rep}(G))} (\dim V) \cdot V \tag{5.20}$$

where $\dim V$ *denotes the dimension V as a vector space.*

Proof. By Mashke's theorem we find that

$$\mathbb{C}[G] \cong \bigoplus_{[V] \in \mathcal{L}} n_V \cdot V$$

for some $n_V \geq 0$, only finitely many of which are nonzero, and by Schur's lemma we can compute

$$n_V = \dim \mathrm{Hom}_{\mathbf{Rep}(G)}(\mathbb{C}[G], V).$$

Now, given any $v \in V$, we can define a map

$$\begin{aligned} \pi_{V,v} : \mathbb{C}[G] &\to V. \\ |g\rangle &\mapsto \rho_V(g)(v) \end{aligned}$$

Clearly, $\pi_{V,v}$ is the unique map $\mathbb{C}[G] \to V$ satisfying $\pi_{V,v}(|1\rangle) = v$. Thus, we find a bijection between maps of representations $\mathbb{C}[G] \to V$ and vectors $v \in V$. Thus, we conclude that $n_V = \dim V$ as desired.

□

Corollary 5.4.13. *For all finite groups G, there is an equivalence of categories $\mathbf{Rep}(G) \simeq \mathbf{Vec}_{\mathbb{C}}^n$ for some $n \geq 1$.*

Proof. We show that $\mathbf{Rep}(G)$ satisfies all of the criteria of proposition 4.2.38. First, we show that $\mathbf{Rep}(G)$ has finitely many isomorphism classes of simple objects. Taking the dimension of both sides of equation 5.20, we find that

$$\sum_{[V] \in \mathcal{L}(\mathbf{Rep}(G))} (\dim V)^2 = |G|.$$

In particular, since $\dim V \geq 1$, we conclude that $\mathcal{L}(\mathbf{Rep}(G))$ is finite. The fact that every object in $\mathbf{Rep}(G)$ decomposes as a direct sum of finitely many simple objects is Mashke's theorem (proposition 5.4.10). The Schur's lemma axiom is satisfied by the Schur's lemma for representations (proposition 5.4.9). □

Proposition 5.4.14. *For all finite groups G, there is an equivalence of categories $\mathfrak{D}(G) \simeq \mathbf{Vec}_{\mathbb{C}}^n$ for some $n \geq 1$.*

Proof. The proof of Schur's lemma and Mashke's theorem carry over essentially verbatim to the case of $\mathfrak{D}(G)$, so we do not repeat them. Thus, applying proposition 4.2.38, it remains to prove that $\mathfrak{D}(G)$ has finitely many isomorphism classes of simple objects. By proposition 5.4.6, simple objects in $\mathfrak{D}(G)$ correspond to pairs (C, χ) where $C \subseteq G$ is a conjugacy clas and χ is an irridicible representation of the centralizer of C. Since G is finite, it has finitely many conjugacy classes. By proposition 5.4.13, the centralizers of each of those conjugacy classes have finitely many irridicible representations. Hence, we conclude the result. □

5.4.3 Spherical fusion structures

We now work on the spherical fusion structures of $\mathbf{Vec}_G$, $\mathbf{Rep}(G)$, and $\mathfrak{D}(G)$.

Definition 5.4.15. The monoidal structures are defined as follows. We define a tensor product on $\mathbf{Vec}_G$ by

$$\begin{aligned} \otimes : \mathbf{Vec}_G \otimes \mathbf{Vec}_G &\to \mathbf{Vec}_G, \\ V \otimes W &\mapsto \bigoplus_{g \in G} (V \otimes W)_g \end{aligned}$$

where the g-graded component $(V \otimes W)_g$ is defined to be

$$(V \otimes W)_g = \bigoplus_{\substack{h,k \in G \\ hk = g}} V_h \otimes W_k.$$

We define a tensor product on $\mathbf{Rep}(G)$ by

$$\begin{aligned} \otimes : \mathbf{Rep}(G) \otimes \mathbf{Rep}(G) &\to \mathbf{Rep}(G), \\ (V, \rho_V) \otimes (W, \rho_W) &\mapsto (V \otimes W, \rho_V \otimes \rho_W) \end{aligned}$$

where for all $g \in G$,

$$(\rho_V \otimes \rho_W)(g)(v \otimes w) = \rho_V(g)(v) \otimes \rho_W(g)(w).$$

We define a tensor product on $\mathfrak{D}(G)$ by endowing $V \otimes W$ with the tensor-product graded structure of its underlying graded vector spaces, with the with representation structure of its underlying representations.

Proposition 5.4.16. *Endowed with their natural tensor products $\mathbf{Vec}_G$, $\mathbf{Rep}(G)$, and $\mathfrak{D}(G)$ are all monoidal categories*

Proof. In all three cases, the underlying vector space of the tensor product is the tensor product of the underlying vector spaces. This means that all three categories inherit unit and associativity maps from $\mathbf{Vec}_{\mathbb{C}}$, which automatically satisfy the correct coherence relations. What one needs to prove is that these unit/associativity maps repsect the structure of $\mathbf{Vec}_G$, $\mathbf{Rep}(G)$, and $\mathfrak{D}(G)$ respectively. For $\mathbf{Vec}_G$, we obseve that

$$\begin{aligned}(V \otimes (V' \otimes V''))_g &= \bigoplus_{hk=g} V_h \otimes (V' \otimes V'')_k \\ &= \bigoplus_{hk=g} V_h \otimes \big(\bigoplus_{h'h''=k} V'_{h'} \otimes V''_{h''} \big) \\ &\cong \bigoplus_{hh'h''=g} V_h \otimes V'_{h'} V''_{h''}.\end{aligned}$$

Clealy, repeating this process on $((V \otimes V') \otimes V'')_g$ would have given the same answer with the other parenthesization, and so the associativity map is indeed a graded map. Since $\mathbb{C}_1$ does not change gradings, it serves as a monoidal unit.

We now move on to $\mathbf{Rep}(G)$. It is clear in this case that the associativity maps are morphisms of representations, and the trivial representation $G \to \mathrm{Aut}(\mathbb{C})$ where every group element acts by the identity is the monoidal unit. As for $\mathfrak{D}(G)$, all that remains to check is that the tensor product of representations is compatible with the tensor product grading. This follows from the following computation:

$$\begin{aligned}(\rho_V \otimes \rho_W)(g)((V \otimes W)_h) &= \bigoplus_{kk'=h} \rho_V(g)(V_k) \otimes \rho_W(g)(W_{k'}) \\ &\subseteq \bigoplus_{kk'=h} V_{gkg^{-1}} \otimes W_{gk'g^{-1}}.\end{aligned}$$

Seeing as $(gkg^{-1})(gk'g^{-1}) = gkk'g^{-1} = ghg^{-1}$, each term in the direct sum is contained in ghg^{-1}. Thus, we get

$$(\rho_V \otimes \rho_W)(g)((V \otimes W)_h) \subseteq (V \otimes W)_{ghg^{-1}}$$

so the tensor product and grading are compatible, as desired. ☐

Definition 5.4.17. The right and left rigid structures are defined as follows. On $\mathbf{Vec}_G$, $\mathbf{Rep}(G)$, $\mathfrak{D}(G)$, the underlying vector space of the dual will be equal to the dual of the underlying vector space. The left and right evaluation and coevaluation maps are inherited from the evaluation and coevaluation maps on $\mathbf{Vec}_{\mathbb{C}}$. On $\mathbf{Vec}_G$, we define the dual as follows:

$$V^* = \bigoplus_{g \in G} V^*_{g^{-1}}.$$

On $\mathbf{Rep}(G)$ we define the dual as $(V, \rho)^* = (V^*, \rho^*)$, where

$$\rho^*(g)(\varphi) = \varphi \circ \rho\big(g^{-1}\big).$$

On $\mathfrak{D}(G)$ we inherit a structure of a G-graded G-representation on the dual V^* by endowing with the dual structures defined on $\mathbf{Vec}_G$, $\mathbf{Rep}(G)$ seperately.

Proposition 5.4.18. *Endowed with their natural right and left rigid structures,* $\mathbf{Vec}_G$*,* $\mathbf{Rep}(G)$*, and* $\mathfrak{D}(G)$ *are all pivotal categories.*

Proof. It suffices to show that the evaluation and coevaluation maps respect the structures on each of the categories. For $\mathbf{Vec}_G$, the evaluation and coevaluatin maps will act by components as evaluation and coevaluation maps $V_g \otimes V_g^* \to \mathbb{C}_1$, $\mathbb{C}_1 \to V_g^* \otimes V_g$, and the same with the orders of the duals swapped. In all cases V_g is in the g-graded component and V_g^* is in the g^{-1}-graded component. Thus, $V_g \otimes V_g^*$ and $V_g^* \otimes V_g$ are both in the 1-graded component, so the evaluation and coevaluation maps respect grading.

We now move on to $\mathbf{Rep}(G)$. To check that the dual representation is a representation is a representation, we compute for all $\varphi \in V^*$

$$\begin{aligned}\rho^*(g)(\rho^*(h)(\varphi)) &= \varphi \circ \rho(h^{-1}) \circ \rho(g^{-1}) \\ &= \varphi \circ \rho((gh)^{-1}) = \rho^*(gh)(\varphi).\end{aligned}$$

To check that the evaluation map is a morphism of representations, we compute for all $v \otimes \varphi \in V \otimes V^*$

$$\begin{aligned}\mathrm{ev}_V((\rho \otimes \rho^*)(g)(v \otimes \varphi)) &= \mathrm{ev}_V(\rho(g)(v) \otimes (\varphi \circ \rho(g^{-1}))) \\ &= (\varphi \circ \rho(g^-1) \circ \rho(g))(v) = \varphi(v).\end{aligned}$$

The proof that ρ respect the coevaluation map is similar, so we conclude that $\mathbf{Rep}(G)$ is a pivotal category. Seeing as the pivotal on $\mathfrak{D}(G)$ is the composite of the pivotal structure on $\mathbf{Vec}_G$ and $\mathbf{Rep}(G)$, it remains to show that that the dual grading is compatible with the dual representation. By definition V_h^* consists of functions on V which act by 0 on all vectors $v \notin V_h$. We compute

$$\rho^*(g)(\varphi)(v) = \varphi(\rho(g^{-1})v),$$

which is 0 whenever $\rho(g^{-1})v \notin V_h$, or equivalently, whenever $v \notin V_{ghg^{-1}}$. Thus, $\rho^*(g)(\varphi)$ is in $V_{ghg^{-1}}^*$. This means that ρ^* respects the grading, so our proof is complete. $\square$

Corollary 5.4.19. *The categories* $\mathbf{Vec}_G$*,* $\mathbf{Rep}(G)$ *and* $\mathfrak{D}(G)$ *are all spherical fusion categories.*

Proof. We have already seen that the pivotal structure on $\mathbf{Vec}_{\mathbb{C}}$ is spherical, so the pivotal structures on $\mathbf{Vec}_G$, $\mathbf{Rep}(G)$, and $\mathfrak{D}(G)$ are spherical as well. Thus, the result follows immediately form combining our results on $\mathbb{C}$-linear structures from subsection 5.4.2 and proposition 5.4.18, and checking some simple axioms (such as, the compatibility of the tensor product and the $\mathbb{C}$-linear structure). $\square$

5.4.4 Braiding and modularity

We can now define our braided structures.

Definition 5.4.20. We define a braided structure on $\mathbf{Rep}(G)$ as follows. Given any (V, ρ_V), (W, ρ_W), we define

$$\beta_{V,W} : V \otimes W \to W \otimes V$$
$$(v,w) \mapsto (w,v)$$

We define a braided structure on $\mathfrak{D}(G)$ as follows. Decomposing $V \otimes G = \bigoplus_{g \in G} V_g \otimes W$, we define β on each component as

$$\begin{aligned} \beta_{V,W} : V_g \otimes W &\to W \otimes V_g, \\ (v,w) &\mapsto (\rho_W(g)(w), v) \end{aligned}$$

and we define $\beta_{V,W} : V \otimes W \to W \otimes V$ by summing these maps.

Proposition 5.4.21. *Endowed with their natural braiding maps, both* $\mathbf{Rep}(G)$ *and* $\mathfrak{D}(G)$ *are braided monoidal categories. In fact, they are pre-modular categories.*

Proof. This is clear for $\mathbf{Rep}(G)$, since its braiding is inherited from $\mathbf{Vec}_{\mathbb{C}}$ and $\mathbf{Vec}_{\mathbb{C}}$ is a braided monoidal category. All that one needs to check is that the braiding maps are morphisms of representations, but this is immediate. Thus, we can focus on $\mathfrak{D}(G)$. For simplicity, we will supress associativity maps and prove that $\mathfrak{D}(G)$ satisfies the axioms as stated for strict braided monoidal categories. Choose some elements $V, V', V'' \in \mathfrak{D}(G)$. Suppose that $v \in V_g$, $v' \in V'_{g'}$, and $v'' \in V''_{g''}$. For the first coherence axiom, we compute

$$\begin{aligned} (\mathrm{id}_{V'} \otimes \beta_{V,V''})(\beta_{V,V'} \otimes \mathrm{id}_{V''})(v \otimes v' \otimes v'') &= (\mathrm{id}_{V'} \otimes \beta_{V,V''})(\rho_{V'}(g)v' \otimes v \otimes v'') \\ &= (\rho_{V'}(g)v' \otimes \rho_{V''}(g)v'' \otimes v) \\ &= \beta_{V,V' \otimes V''}(v \otimes v' \otimes v''). \end{aligned}$$

For the second coherence axiom, we compute

$$\begin{aligned} (\mathrm{id}_{V'} \otimes \beta^{-1}_{V'',V})(\beta^{-1}_{V',V} \otimes \mathrm{id}_{V''})(v \otimes v' \otimes v'') &= (\mathrm{id}_{V'} \otimes \beta^{-1}_{V'',V})(v' \otimes \rho_V(g'^{-1})v \otimes v'') \\ &= (v' \otimes v'' \otimes \rho_V(g''^{-1})\rho_V(g'^{-1})v) \\ &= \beta^{-1}_{V' \otimes V'',V}(v \otimes v' \otimes v''). \end{aligned}$$

where in the last step we used that

$$\rho_V(g''^{-1})\rho_V(g'^{-1}) = \rho_V((g'g'')^{-1}).$$

Thus, $\mathfrak{D}(G)$ forms a braided monoidal category so our proof is complete. □

Definition 5.4.22. We call a braided monoidal category $\mathcal{C}$ a *symmetric* monoidal category if $\beta_{B,A} \circ \beta_{A,B} = \mathrm{id}_{A \otimes B}$ for all $A, B \in \mathcal{C}$.

Remark 5.4.23. In a sense, symmetric monoidal categories are the opposite of modular categories. In a modular category, $\beta_{B,A} \circ \beta_{A,B} = \mathrm{id}_{A \otimes B}$ for all $B \in \mathcal{C}$ implies $A \cong n \cdot \mathbf{1}$ for some $n \geq 1$. In a symmetric category $\beta_{B,A} \circ \beta_{A,B} = \mathrm{id}_{A \otimes B}$ is true for all $A, B \in \mathcal{C}$. The only way for a pre-modular category to be both symmetric and modular is to have every object be isomorphic to $\mathbf{1}$. That is, the only symmetric modular category is $\mathbf{Vec}_{\mathbb{C}}$

Example 5.4.24. For all finite groups G, $\mathbf{Rep}(G)$ is a symmetric monoidal category. In light of remark 5.4.23, we observe thus that $\mathbf{Rep}(G)$ is modular if and only if $G = 1$ is the trivial group.

Example 5.4.25. The category $\mathbf{Vec}_G$ typically does not admit a braiding. In particular, we have that $\mathbb{C}_g \otimes \mathbb{C}_h \cong \mathbb{C}_{gh}$ and $\mathbb{C}_h \otimes \mathbb{C}_g \cong \mathbb{C}_{hg}$. A prerequisite for being braided is to have non-natural isomorphisms $A \otimes B \cong B \otimes A$ for all A, B. Thus, for $\mathbf{Vec}_G$ to admit a braiding, we would need $\mathbb{C}_{gh} \cong \mathbb{C}_{hg}$ for all $g, h \in G$. That is, we would need G to be abelian. In this case, the map $\beta_{V,W} : V \otimes W \to W \otimes V$ which sends $v \otimes w$ to $w \otimes v$ can be readily shown to be a symmetric braiding on $\mathbf{Vec}_G$, along the same lines as the proof of proposition 5.4.21.

Theorem 5.4.26. *For all finite groups G, $\mathfrak{D}(G)$ is a modular category.*

Proof. Suppose that $V \in \mathfrak{D}(G)$ is an element such that $\beta_{W,V} \circ \beta_{V,W} = \mathrm{id}_{V \otimes W}$ for all $W \in \mathfrak{D}(G)$. We first take $W = \mathbb{C}[G]_1$ to be the regular representation of G, with the entire vector space put into the 1-graded component. Then, for all $v \in V_g$ we find that

$$\begin{gathered} V_g \otimes W \xrightarrow{\beta} W \otimes V_g \xrightarrow{\beta} V_g \otimes W. \\ v \otimes |1\rangle \mapsto |g\rangle \otimes v \mapsto v \otimes |g\rangle \end{gathered}$$

So, $V_g = 0$ for all $g \neq 1$. That is, V is entirely supported in its 1-graded component. Now, we let $W = \mathbb{C}[G]$ as a vector space, where W_g is spanned by $|g\rangle$, and $\rho_W(g)(|h\rangle) = |ghg^{-1}\rangle$. We observe for all $g \in G$

$$\begin{gathered} V \otimes W \xrightarrow{\beta} W \otimes V \xrightarrow{\beta} V \otimes W. \\ v \otimes |g\rangle \mapsto |g\rangle \otimes v \mapsto \rho(g)(v) \otimes |g\rangle \end{gathered}$$

Thus, $\rho(g)(v) = v$ for all $v \in V$, $g \in G$. That is, the action of ρ is trivial. Since V lives entirely in the 1-graded component and has trivial action, we thus find that V is a direct sum of the trivial vector space in the 1-graded component some number of times. Since V was chosen arbitrarily among elements with $\beta_{W,V} \circ \beta_{V,W} = \mathrm{id}_{V \otimes W}$ for all $W \in \mathfrak{D}(G)$, we conclude the result. □

Proposition 5.4.27. *The forgetful functors $\mathfrak{D}(G) \to$ $\mathbf{Vec}_G$ and $\mathfrak{D}(G) \to \mathbf{Rep}(G)$ are functors of spherical fusion categories. The natural functor $\mathbf{Rep}(G) \to \mathfrak{D}(G)$ is a functor of pre-modular categories.*

Proof. Every structure of $\mathfrak{D}(G)$ as a spherical fusion category was defined so that if you forget the grading it is the same structure as in $\mathbf{Rep}(G)$ and if you forget the representation it is the same structure as in $\mathbf{Vec}_G$. Thus, it is immediate that the forgetful functors are functors of spherical fusion categories. It thus remains to show that the natural functor $\mathbf{Rep}(G) \to \mathfrak{D}(G)$ respects braiding. This comes from the fact that the braiding in $\mathfrak{D}(G)$ is the same as the braiding of $\mathbf{Rep}(G)$ in the 1-graded component, and the image of $\mathbf{Rep}(G)$ consists of objects which are supported entirely in their 1-graded components. □

Proposition 5.4.28. *For all finite groups G, H, we have that*

$$\mathbf{Vec}_G \boxtimes \mathbf{Vec}_H \simeq \mathbf{Vec}_{G\times H}$$
$$\mathbf{Rep}(G) \boxtimes \mathbf{Rep}(H) \simeq \mathbf{Rep}(G\times H)$$
$$\mathfrak{D}(G) \boxtimes \mathfrak{D}(H) \simeq \mathfrak{D}(G\times H)$$

where the first equivalence is an equivalence of spherical fusion categories, and the last two are equivalences of pre-modular categories.

Proof. We suffice ourselves to defining the relevant functors which induce the equivalences of categories. Verifying that these functors respect the appropriate structures is tedious but straightforward, and they are all manifestly fully faithful and essentially surjective so they induce equivalences of categories by proposition [ref]. The first functor is

$$\mathbf{Vec}_G \boxtimes \mathbf{Vec}_H \to \mathbf{Vec}_{G\times H} V \boxtimes W \qquad \mapsto \bigoplus_{(g,h)\in G\times H} V_g \otimes W_h.$$

The next is

$$\mathbf{Rep}_G \boxtimes \mathbf{Rep}_H \to \mathbf{Rep}_{G\times H}(V,\rho_V)\otimes(W,\rho_W) \qquad \mapsto (V\otimes W, \rho_V\otimes\rho_W)$$

where

$$(\rho_V\otimes\rho_W)(g,h)(v\otimes w) = \rho_V(g)(v)\otimes\rho_W(h)(w).$$

The functor $\mathfrak{D}(G)\boxtimes\mathfrak{D}(H)\to\mathfrak{D}(G\times H)$ is defined on the level of graded vector spaces by forgeting the representation structure and using the first functor we defined, and it is defined on the level of representations by forgetful the graded structure and using the second functor we defined. ☐

Example 5.4.29. WORK: Work through the toric code. What I should include here is quite dependent on what is covered in the TQO chapter. Additionally, it would be nice to have a second example with the $G = S_3$ model.

5.5 The modular representation

5.5.1 Definition

In this chapter we will discuss the *modular representations* of modular categories. Let $\mathcal{C}$ be a modular category. Let $\mathcal{L}$ be the set of isomorphism classes of simple objects of $\mathcal{C}$. We will define a group homomorphism

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

assocociated to $\mathcal{C}$, 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, $\rho_{\mathcal{C}}$ is known as the *modular representation* of $\mathcal{C}$. It is from the existence of this representation that modular categories get their name. The goal of this chapter is to introduce $\rho_{\mathcal{C}}$, show it is well defined, and then prove a series of theorems related to $\rho_{\mathcal{C}}$.

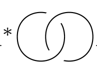
Remark 5.5.1. We recall the basic group theory of $\mathrm{SL}_2(\mathbb{Z})$. It is generated by the matrices

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

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 [ref]:

$$\mathrm{SL}_2(\mathbb{Z}) = \left\langle s, t \,\middle|\, s^4 = 1, \ (st)^3 = s^2 \right\rangle. \tag{5.21}$$

In light of remark 5.5.1, to define a homomorphism $\rho_{\mathcal{C}} : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Aut}(\mathbb{C}[\mathcal{L}])$ it suffices to choose automorphisms $\rho_{\mathcal{C}}(s)$, $\rho_{\mathcal{C}}(t)$ of $\mathbb{C}[\mathcal{L}]$, and show that they satisfy the relations $\rho_{\mathcal{C}}(s)^4 = 1$ and $(\rho_{\mathcal{C}}(s)\rho_{\mathcal{C}}(t))^3 = \rho_{\mathcal{C}}(s)^2$. 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 $S_{[A],[B]} = S_{A,B}$ defined by

$S_{A,B}=$ A^*  B^*

We 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 $[A] \in \mathcal{L}$. We call these the *S-matrix* and *T-matrix* of $\mathcal{C}$ respectively. 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*,

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

We can now state the main theorem of this chapter:

Theorem 5.5.2. *Let $\mathcal{C}$ be a modular category. The values $p_{\mathcal{C}}^{+}$ and $p_{\mathcal{C}}^{-}$ are nonzero, and the map*

$$\begin{aligned} \rho_{\mathcal{C}} : \mathrm{SL}_2(\mathbb{Z}) &\to \mathrm{Aut}(\mathbb{C}[\mathcal{L}]) \\ s &\mapsto \frac{1}{\mathcal{D}} \cdot S \\ t &\mapsto \left(p_{\mathcal{C}}^{-}/p_{\mathcal{C}}^{+}\right)^{1/6} \cdot T \end{aligned}$$

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.

Example 5.5.3. WORK: Write out modular data for toric code.

Example 5.5.4. WORK: Write out modular data for $G = S_3$.

5.5.2 Torus perspective

WORK: I should wait until I'm done with the TQO chapter to write this section.

It's good to reflect physically on why modular categories 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 $\mathcal{C}$ (paired with a chiral central charge c_-) is supposed to describe a topologically ordered phase. Up to now we have only considered what happens when this topological order is applied to an infnitely large flat sheet or sphere. 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 $\mathcal{C}$ 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 $\mathcal{C}$.

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

$$\rho_{\mathcal{C}}^{T^2} : \mathrm{MCG}(T^2) \to \mathrm{Aut}\left(V_{\text{g.s.}}^{T^2}\right).$$

This homomorphism connects back to our modular representation as follows:

- **Claim 1:** $\mathrm{MCG}(T^2) \cong \mathrm{SL}_2(\mathbb{Z})$;
- **Claim 2:** $V_{\text{g.s.}}^{T^2} \cong \mathbb{C}[\mathcal{L}]$;
- **Claim 3:** $\rho_{\mathcal{C}}^{T^2} \cong \rho_{\mathcal{C}}$, passing through the identifications in claims 1 and 2.

In general, we see that associated to every modular category $\mathcal{C}$ 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 $\mathcal{C}$ on Σ_g we get a map

$$\rho_{\mathcal{C}}^{\Sigma_g} : \mathrm{MCG}(\Sigma_g) \to \mathrm{Aut}(V_{\text{g.s.}}^{\Sigma_g}).$$

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: $V_{\text{g.s.}}^{T^2} \cong \mathbb{C}[\mathcal{L}]$.

WORK: explain this. Cut into cylinder, label by charge on boundary

Claim 3: $\rho_{\mathcal{C}}^{T^2} \cong \rho_{\mathcal{C}}$.

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.

WORK: I wrote a little extra about this for the Kapustin final, might be useful

To demonstrate the TQFT perspective in action, we focus on the case of the genus one surface - the torus. As part of the data of every TQFT $(V_g, \rho_g, Z_{g,g'})$ there is a map

$$\rho_1 : \mathrm{MCG}(\Sigma_1) \to \mathrm{Aut}(V_1).$$

We seek to understand this map in full detail, and as such gain some level of enlightenment about the behavior of topological order on the torus. On physical groups, the space V_1 is easy to describe. We argued before it should be $\mathbb{C}[\mathcal{L}]$. The mapping class group $\mathrm{MCG}(\Sigma_1) = \mathrm{MCG}(T^2)$ is also straightforward to describe. We state a classical theorem about $\mathrm{MCG}(T^2)$ below:

Theorem 5.5.5 ([FM11], Theorem 2.5)**.** *There is an isomorphism* $\mathrm{MCG}(T^2) \cong \mathrm{SL}_2(\mathbb{Z})$*, which sends the element of* $\mathrm{MCG}(T^2)$ *represented by* $\pi/2$*-rotation to* s*,*

WORK: add picture

and which sends the element of $\mathrm{MCG}(T^2)$ *represented by a Dehn twist around a handle of the torus to* t*.*

Remark 5.5.6. For simplicity of notation, we will from now on identify $\mathrm{MCG}(T^2)$ with $\mathrm{SL}_2(\mathbb{Z})$, using the letters s, t to represent both the elements of $\mathrm{SL}_2(\mathbb{Z})$ and their corresponding preimage in $\mathrm{MCG}(T^2)$.

A more elementary way of stating this theorem is that every self-homeomorphism of the torus can be deformed to a composition of Dehn twists and rotations, and that the rotation and Dehn twist satisfy the $\mathrm{SL}_2(\mathbb{Z})$ relations $s^4 = 1$ and $(st)^3 = s^2$.

The Dehn twist is described as follows. WORK: describe Dehn twist in terms of theta-symbols θ_A.

The rotation is described as follows.WORK: describe the rotation in terms of the S-matrix.

Now that we have described $\mathrm{MCG}(T^2) = \mathrm{SL}_2(\mathbb{Z})$ and $V_1 = \mathbb{C}[\mathcal{L}]$, we are tasked with understanding $\rho_1 : \mathrm{SL}_2(\mathbb{Z}) \to \mathbb{C}[\mathcal{L}]$. That is, we must describe the maps $\rho_1(s), \rho_1(t) \in \mathrm{Aut}(\mathbb{C}[\mathcal{L}])$.

]

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 $\mathcal{C}$, the S-matrix S is invertible if and only if $\mathcal{C}$ 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 [Bru00] that the invertability of the S-matrix is equivalent to $\mathcal{C}$ having the non-degenerate braiding property. In this way our definition of modular category is historically incorrect, 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 $\mathcal{C}$. This algebra will be of use for us in proving other theorems in the future, in particular the Verlinde formula (theorem 5.5.11).

Definition 5.5.7. We define the Verlinde algebra $K_{\mathbb{C}}(\mathcal{C})$ of $\mathcal{C}$ as follows:

$$K_{\mathbb{C}}(\mathcal{C}) = \left\{ \mathbb{C}[\mathcal{L}] \text{ with algebra structure } |[A]\rangle \cdot |[B]\rangle = \sum_{[C]\in\mathcal{L}} N_C^{A,B} \, |[C]\rangle \right\}.$$

We additionally define the function algebra

$$\mathbb{C}[\mathcal{L}]^{\text{func}} = \left\{ \mathbb{C}[\mathcal{L}] \text{ with algebra structure } \left(\sum_{[A]\in\mathcal{L}} c_A \, |[A]\rangle\right) \cdot \left(\sum_{[A]\in\mathcal{L}} c'_A \, |[A]\rangle\right) = \sum_{[A]\in\mathcal{L}} c_A c'_A \, |[A]\rangle \right\}.$$

Recall that an *algebra* over $\mathbb{C}$ is 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.

Lemma 5.5.8. *Both $K_{\mathbb{C}}(\mathcal{C})$ and $\mathbb{C}[\mathcal{L}]^{func}$ are commutative algebras.*

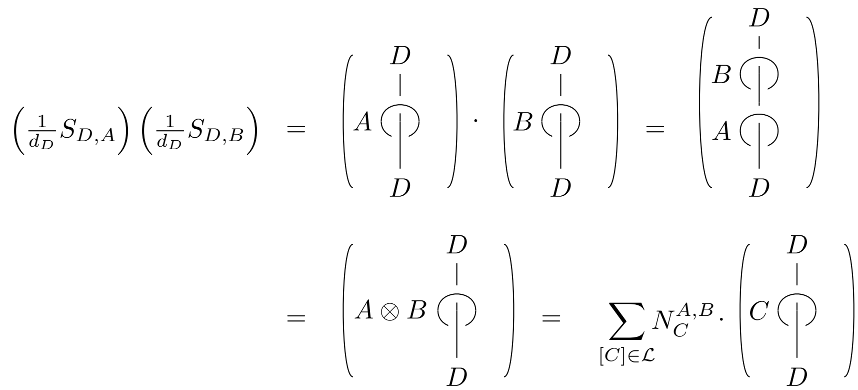
Proof. The fact that $K_{\mathbb{C}}(\mathcal{C})$ is associative follows from the associativity of the tensor product. Its unit is $|[\mathbf{1}]\rangle$. It is commutative because $\mathcal{C}$ is braided. The fact that $\mathbb{C}[\mathcal{L}]^{\text{func}}$ is a commutative algebra is a standard exercise in algebra. Its unit is $\sum_{[A]\in\mathcal{L}} |[A]\rangle$. $\square$

Proposition 5.5.9. *The map*

$$\begin{aligned} \mathcal{S} : K_{\mathbb{C}}(\mathcal{C}) &\to \mathbb{C}[\mathcal{L}]^{func} \\ |[A]\rangle &\mapsto \sum_{[B]\in\mathcal{L}} \frac{1}{d_B} S_{B,A} \, |[B]\rangle \end{aligned}$$

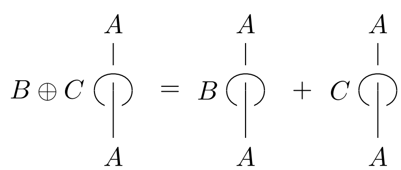
is a morphism of algebras.

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.



$$= \sum_{[C]\in\mathcal{L}} N_C^{A,B} \left(\tfrac{1}{d_D} S_{D,C}\right).$$

Note our key use of the fact that



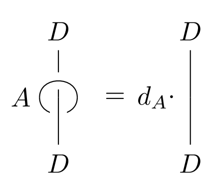
which follows from the facts that $\mathrm{id}_{B\oplus C}$ can be decomposed as projection onto B plus projection onto C, and composition is bilinear. We now conclude that

$$\begin{aligned}
\mathcal{S}(|[A]\rangle)\cdot\mathcal{S}(|[B]\rangle) &= \sum_{[D]\in\mathcal{L}} \left(\frac{1}{d_D}S_{D,A}\right)\left(\frac{1}{d_D}S_{D,B}\right)|[D]\rangle \\
&= \sum_{[D]\in\mathcal{L}} \left(\sum_{[C]\in\mathcal{L}} N_C^{A,B}\left(\frac{1}{d_D}S_{D,C}\right)\right)|[D]\rangle \\
&= \mathcal{S}(|[A]\rangle\cdot|[B]\rangle)
\end{aligned}$$

as desired. ∎

Theorem 5.5.10 (Bruguieres's modularity theorem)**.** *Let $\mathcal{C}$ be a pre-modular category. The braiding on $\mathcal{C}$ satisfies the non-degenerate braiding axiom if and only if the S-matrix is invertible.*

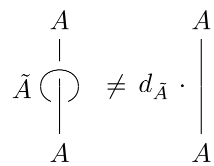
Proof. We observe that $\mathcal{C}$ has a degenerate braiding if and only if there exists some $A \ncong \mathbf{1}$ such that



for all $D \in \mathcal{D}$. 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 $\mathcal{C}$ 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 $\mathcal{C}$ 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

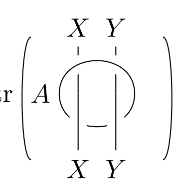
$$\prod_{\substack{[A]\in\mathcal{L}\\ A\ncong\mathbf{1}}} \left(\mathcal{S}(|[\tilde{A}]\rangle) - \frac{S_{A,\tilde{A}}}{d_A}\mathcal{S}(|[\mathbf{1}]\rangle) \right)$$

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.

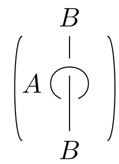
Part 2: $\mathcal{S}$ is surjective. Let $\omega = \sum_{[A]\in\mathcal{L}} \omega_A |[A]\rangle \in K_{\mathbb{C}}(\mathcal{C})$ be a vector such that $\mathcal{S}(\omega) = |[\mathbf{1}]\rangle$, which exists by part 1 of the proof. We now compute the quantity

$$h_{X,Y} \;=\; \sum_{[A]\in\mathcal{L}} \omega_A \cdot \;\; \mathrm{tr}$$

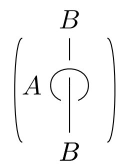


two ways, for all simple objects $X, Y \in \mathcal{C}$. The first way folllows by expanding $X \otimes Y$ as a direct sum and using the fact that $\mathcal{S}(\omega) = |[\mathbf{1}]\rangle$:

$$h_{X,Y} = \sum_{[A]\in\mathcal{L}} \sum_{[B]\in\mathcal{L}} \omega_A N_B^{X,Y} d_B \cdot$$

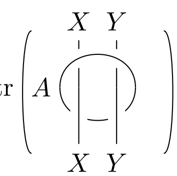


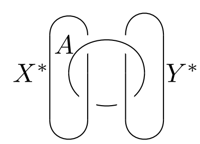
$$= \sum_{[B]\in\mathcal{L}} N_B^{X,Y} d_B \sum_{[A]\in\mathcal{L}} \omega_A \cdot$$

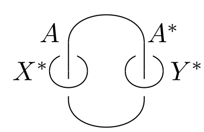


$$= N_{\mathbf{1}}^{X,Y} d_1 = \begin{cases} 1, & X \cong Y^* \\ 0, & \text{otherwise.} \end{cases}$$

In our second way of computing $h_{X,Y}$, we relate the string diagram trace to S-matrix values:

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 $X \in \mathcal{C}$. 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.

□

We can also use proposition 5.5.9 to 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].

Theorem 5.5.11 (Verlinde formula)**.** *Let $\mathcal{C}$ be a modular category.*

(i) For all simple objects $A, B, C \in \mathcal{C}$,

$$N_C^{A,B} = \sum_{[E] \in \mathcal{L}} \frac{S_{A,E} S_{B,E} \left(S^{-1}\right)_{C,E}}{d_E}$$

where $(S^{-1})_{C,E}$ denotes the (C, E)-coefficeint of the inverse of the S matrix.

(ii) For all simple objects $A \in \mathcal{C}$, 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 $K_{\mathbb{C}}(\mathcal{C})$. 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

$$\begin{aligned}
(\mathcal{S} N^A \mathcal{S}^{-1}) \, |[B]\rangle &= \mathcal{S} \left(|[A]\rangle \cdot_{K_{\mathbb{C}}(\mathcal{C})} \mathcal{S}^{-1}(|[B]\rangle) \right) \\
&= \mathcal{S}(|A\rangle) \cdot_{\mathbb{C}[\mathcal{L}]^{\text{func}}} |[B]\rangle \\
&= \frac{S_{A,B}}{d_B} \, |[B]\rangle \, .
\end{aligned}$$

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.

□

5.5.4 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 5.5.2. 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 5.5.2. We begin with the most fundamental relationship between S-matrix and T-matrix entries:

Lemma 5.5.12. *Let $\mathcal{C}$ be a pre-modular category. For all simple objects $A, B \in \mathcal{C}$,*

$$S_{A,B} = \theta_A^{-1}\theta_B^{-1} \sum_{[C]\in\mathcal{L}} N_C^{A,B}\theta_C d_C$$

and

$$S_{A^*,B} = \theta_A\theta_B \sum_{[C]\in\mathcal{L}} N_C^{A,B}\theta_C^{-1} d_C.$$

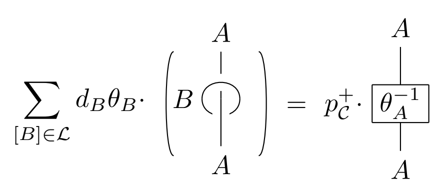
Proof. By proposition 5.3.26, we have $\beta_{B,A}\circ\beta_{A,B} = (\theta_A^{-1}\otimes\theta_B^{-1})\circ\theta_{A\otimes B}$. Taking the trace of this formula we get

$$S_{A,B} = \theta_A^{-1}\theta_B^{-1}\operatorname{tr}(\theta_{A\otimes B}).$$

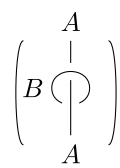
Now, since θ is a natural transformation it splits over direct sums. Traces split over direct sums as well by proposition 5.3.6 and hence $\operatorname{tr}(\theta_{A\otimes B}) = \sum_{[C]\in\mathcal{L}} N_C^{A,B}\theta_C d_C$. This concludes the proof of the first formula.

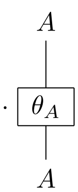
For the second formula, we observe that replacing overcrossings with undercrossings in the definition of $S_{A,B}$ has the effect of taking the dual of one of elements, replacing it with $S_{A^*,B}$. Hence $\operatorname{tr}(\beta_{A,B}^{-1}\circ\beta_{B,A}^{-1}) = S_{A^*,B}$. Thus, taking the trace 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. □

Lemma 5.5.13. *Let $\mathcal{C}$ be a pre-modular category. Let $A \in \mathcal{C}$ be a (possibly non-simple) object. We have that*



and

$$\sum_{[B]\in\mathcal{L}} d_B\theta_B^{-1}\cdot$$


$$= p_{\mathcal{C}}^{-}\cdot$$


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 5.5.12 and the fact that $\sum_{[C]\in\mathcal{L}} N_C^{A,B} d_B = d_A d_C$ from proposition 5.3.10:

$$\begin{aligned}
\sum_{[B]\in\mathcal{L}} d_B\theta_B S_{A,B} &= \sum_{[B]\in\mathcal{L}} d_B\theta_B\left(\theta_A^{-1}\theta_B^{-1}\sum_{[C]\in\mathcal{L}} N_C^{A,B}\theta_C d_C\right)\\
&= \theta_A^{-1}\sum_{[C]\in\mathcal{L}}\theta_C d_C\left(\sum_{[B]\in\mathcal{L}} N_C^{A,B} d_B\right)\\
&= \theta_A^{-1} d_A\sum_{[C]\in\mathcal{L}}\theta_C d_C^2 = p_{\mathcal{C}}^{+}\theta_A^{-1} d_A.
\end{aligned}$$

This result is exact the trace of the right hand sides of the lemma. Hence, the proof is complete. □

Theorem 5.5.14. *Let $\mathcal{C}$ 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* $\check{C}^2 = 1$*;*

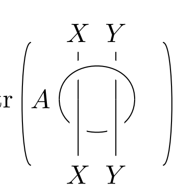
(ii) $(ST)^3 = p_{\mathcal{C}}^{+}S^2$*;*

(iii) $(ST^{-1})^3 = p_{\mathcal{C}}^{-}S^2\check{C}$.

If $\mathcal{C}$ is modular, then

(iv) $S^2 = p_{\mathcal{C}}^{+}p_{\mathcal{C}}^{-}\check{C}$.

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 $\mathcal{C}$ is modular by theorem 5.5.10. Hence, it suffices to prove part (ii). The proof comes from computing in two different ways the quantity

$$h_{X,Y} = \sum_{[A]\in\mathcal{L}} d_A\theta_A\cdot\ \mathrm{tr}$$


In the first way of computing $h_{X,Y}$, we use lemma 5.5.12. We find the following:

$$h_{X,Y} \;=\; p_{\mathcal{C}}^{+} \cdot \ \operatorname{tr}\left(\begin{array}{c} X \quad Y \\ | \quad\ | \\ \boxed{\theta^{-1}_{X\otimes Y}} \\ | \quad\ | \\ X \quad Y \end{array} \right) \;=\; p_{\mathcal{C}}^{+} \theta_X \theta_Y S_{X^*,Y}$$

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 5.5.10. 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 $\sum_{[A]\in\mathcal{L}} \theta_A S_{X,A} S_{Y,A} = p_{\mathcal{C}}^{+} \theta_X \theta_Y S_{X^*,Y}$. Thinking of these quantites as the $([X],[Y])$ entries in operators $\mathbb{C}[\mathcal{L}] \to \mathbb{C}[\mathcal{L}]$, we get the equation

$$STS = p_{\mathcal{C}}^{+} TST\check{C}.$$

WORK: This formula is WRONG. It should be

$$STS = p_{\mathcal{C}}^{+} T^{-1} S T^{-1}.$$

From this we get

$$(ST)^3 = p_{\mathcal{C}}^{+} S^2$$

as desired. I'm not sure where I went wrong, but something is off in here. □

Corollary 5.5.15. *Let $\mathcal{C}$ be a modular category. The quantities $p_{\mathcal{C}}^{+}$ and $p_{\mathcal{C}}^{-}$ are nonzero, and*

$$p_{\mathcal{C}}^{+} p_{\mathcal{C}}^{-} = \mathcal{D}^2.$$

Proof. The values $p_{\mathcal{C}}^{+}$ and $p_{\mathcal{C}}^{-}$ must be nonzero because S is invertible and $S^2 = p_{\mathcal{C}}^{+} p_{\mathcal{C}}^{-} \check{C}$. The formula $S^2 = p_{\mathcal{C}}^{+} p_{\mathcal{C}}^{-} \check{C}$, when expanded, says that

$$\sum_{[C]\in\mathcal{L}} S_{C,A} S_{C,B} = \begin{cases} p_{\mathcal{C}}^{+} p_{\mathcal{C}}^{-} & A \cong B^* \\ 0 & \text{otherwise.} \end{cases}$$

Applying this formula to $A = B = \mathbf{1}$, we find

$$\sum_{[C]\in\mathcal{L}} S_{C,\mathbf{1}} S_{C,\mathbf{1}} = \sum_{[C]\in\mathcal{L}} d_C^2 = p_{\mathcal{C}}^{+} p_{\mathcal{C}}^{-}$$

as desired. □

Remark 5.5.16. Normalizing the representation appropriately, we can conclude theorem 5.5.2 from theorem 5.5.14 and corollary 5.5.15.

5.5.5 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 $z \in \mathcal{C}$ is called a root of unity if $z^n = 1$ for some integer $n \geq 1$.

Additionally, these techniques will allow us to analyze Gauss sums in more detail. By Vafa's theorem, $p^-_{\mathcal{C}} = \overline{p^+_{\mathcal{C}}}$. By corollary 5.5.15, thus, $|p^+_{\mathcal{C}}| = |p^-_{\mathcal{C}}| = \mathcal{D}$. We will even prove that the quantity $p^-_{\mathcal{C}}/p^+_{\mathcal{C}}$ is a root of unity, so $p^+_{\mathcal{C}}/\mathcal{D}$ and $p^-_{\mathcal{C}}/\mathcal{D}$ are both roots of unity as well. These roots of unity are related to the chiral central charge c_- of the theory by the following equation, known as the Gauss-Milgram formula ([**?**]):

$$\frac{1}{\mathcal{D}}p^+_{\mathcal{C}} = \frac{1}{\mathcal{D}}\sum_{[A]\in\mathcal{L}} \theta_A d_A^2 = e^{\frac{2\pi i c_-}{8}}. \tag{5.22}$$

Remark 5.5.17. We had already remarked in remark 5.1.2 that the modular category determines the chiral central charge modulo 8. Equation 5.22 is the mechanism by which the modular category restricts the chiral central charge. There exists a topological phase with chiral central chage 8 but without any anyons, known as Kitaev's $E8$ phase [**?**]. By stacking with copies of the $E8$ phase, one can take a phase with anyon content $\mathcal{C}$ and chiral central charge c_- and obtain a phase with the same anyon content any chiral central charge c'_- equivalent to c_- modulo 8.

We begin with a key topological lemma which will underscore our proof:

Lemma 5.5.18 (Lantern identity)**.** *Let $\mathcal{C}$ be a pre-modular category. Let $A, B, C \in \mathcal{C}$ be objects. As maps $A \otimes B \otimes C \to A \otimes B \otimes C$, we have the identity*

$$\theta_{A\otimes B} \circ (\mathrm{id}_A \circ \beta^{-1}_{B,C}) \circ \theta_{A\otimes C} \circ (\mathrm{id}_A \circ \beta_{B,C}) \circ \theta_{B\otimes C} = \theta_{A\otimes B\otimes C} \circ (\theta_A \otimes \theta_B \otimes \theta_C).$$

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 will need another more linear-algebraic lemma for the proof:

Lemma 5.5.19. *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 $\sum_{b=1}^n M_{b,a} < 0$ for all $1 \leq a \leq n$. Then, M is invertible.*

Proof. Let $v = \sum_{a=1}^n c_i |a\rangle$ be a vector. Choose some value $1 \leq a \leq n$ such that $|c_a| \geq |c_b|$ for all $1 \leq b \leq n$. The coefficient of $|a\rangle$ in Mv is $\sum_{b=1}^n c_b M_{b,a}$. We observe

$$\Big|\sum_{\substack{b=1\\b\neq a}}^{n} c_b M_{b,a}\Big| \leq |c_a| \sum_{b\neq a}^{n} M_{b,a} \leq |c_a| M_{a,a}.$$

Thus, $\sum_{b=1}^{n} c_b M_{b,a} \neq 0$, so Mv is nonzero, and hence is invertible since v was chosen arbitrarily. $\square$

Theorem 5.5.20 (Vafa, [Vaf88])**.** *Let $\mathcal{C}$ be a pre-modular category. The values θ_A are roots of unity for all simple object $A \in \mathcal{C}$.*

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 5.5.18) on the stands A, A^*, A,

$$\theta_{A\otimes A^*} \circ (\mathrm{id}_A \circ \beta^{-1}_{A^*,A}) \circ \theta_{A\otimes A} \circ (\mathrm{id}_A \otimes \beta_{A^*,A}) \circ \theta_{A^*\otimes A} = \theta_{A\otimes A^*\otimes A} \circ (\theta_A \otimes \theta_{A^*} \otimes \theta_A).$$

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 5.5.19, 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. ☐

Corollary 5.5.21. *Let $\mathcal{C}$ 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 $A, B \in \mathcal{C}$

Proof. Choose $n \geq 1$ so that $\theta_C^n = 1$ for all simple objects $C \in \mathcal{C}$, 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 5.5.22. *Let $\mathcal{C}$ be a modular category. The quantity $p_{\mathcal{C}}^-/p_{\mathcal{C}}^+$ is a root of unity.*

Proof. We take determinants. From $S^2 = p_{\mathcal{C}}^+ p_{\mathcal{C}}^- \check{C}$ we find that $\det(S)^2 = \pm p_{\mathcal{C}}^+ p_{\mathcal{C}}^-$, since $\det \check{C} = \pm 1$. From the formula $(ST)^3 = p_{\mathcal{C}}^+ S^2$ we find that

$$\left(p_{\mathcal{C}}^+/\det(S)\right)^2 = \det(T)^6$$

so $p_{\mathcal{C}}^+/p_{\mathcal{C}}^- = \pm \det(T)^6$. By Vafa's theorem $\det(T)$ is a root of unity. Hence, we conclude that $p_{\mathcal{C}}^+/p_{\mathcal{C}}^-$ is a root of unity as desired. ☐

We now move on to proving that the S matrix is unitary. The main technical ingredient is as follows:

Proposition 5.5.23. *Let $\mathcal{C}$ be a modular category. For all simple objects $A, B \in \mathcal{C}$ 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 5.5.24 (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 5.5.20 and corollary 5.5.22 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 5.5.23 $(\frac{1}{\mathcal{D}}S) \cdot \check{C} = (\frac{1}{\mathcal{D}}S)^\dagger$ 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. A good mathematical reference is [DHW13].

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 $\mathcal{C}$ a quantum double if it is of the form $\mathcal{Z}(\mathcal{C}_0)$ for some spherical fusion category $\mathcal{C}_0$. 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 $\mathcal{Z}(\mathcal{C})$ is thus

$$\mathcal{Z}(\mathcal{C}) = \{A \in \mathcal{C} | A \otimes B \cong B \otimes A \ \forall B \in \mathcal{C}\}.$$

This is almost correct, but not quite. The issue is that $\mathcal{Z}(\mathcal{C})$ is not quite a braided monoidal category yet. Even though $A \otimes B \cong B \otimes A$ for all $A, B \in \mathcal{Z}(\mathcal{C})$, 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 5.7.1. *The Drinfeld center $\mathcal{Z}(\mathcal{C})$ of a monoidal category $\mathcal{C}$ is a braided monoidal category defined as follows:*

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

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

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

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

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

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

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

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

Proof. Since morphisms in $\mathcal{Z}(\mathcal{C})$ are a subspace of morphisms in $\mathcal{C}$, commutative diagrams don't change when going from $\mathcal{C}$ to $\mathcal{Z}(\mathcal{C})$. Hence, the triangle and pentagon axioms for $\mathcal{Z}(\mathcal{C})$ follow immediately from the triangle and pentagon axioms on $\mathcal{C}$. One thing to be checked is that evaluation/co-evaluaiton satisfy the compatibility condition required to a morphism in $\mathcal{Z}(\mathcal{C})$, 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. The standard proof people use is completeley steeped in the language of module categories. The original proof uses the tube algebra, and is "elementary" in the sense that you don't need tube algebras but it is heineous, and I would very much like to avoid it. I'll figure out what to write hence once I've done the module category section and I've digested the proof. Maybe there's a way to de-module-ify it, but maybe not. Maybe I don't want to do that if it'll lose its essence.

5.7.3 Discrete gauge theory as a quantum double and Morita equivalence

We saw in chapter [ref] that $\mathbf{Vec}_G$ anad $\mathbf{Rep}(G)$ are both naturally spherical fusion categories. Thus, Muger's theorem tells us that $\mathcal{Z}(\mathbf{Vec}_G)$ and $\mathcal{Z}(\mathbf{Rep}(G))$ are both modular categories. Hence, given a finite group G we have three different modular categories we can associate to it: $\mathfrak{D}(G)$, $\mathcal{Z}(\mathbf{Vec}_G)$, $\mathcal{Z}(\mathbf{Rep}(G))$. The amazing fact is that these are all the same category:

Proposition 5.7.2. *Let G be a finite group. There are equivalences of modular categories $\mathfrak{D}(G) \cong \mathcal{Z}(\mathbf{Vec}_G) \cong \mathcal{Z}(\mathbf{Rep}(G))$.*

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 $\mathcal{C}$, we can forget the braiding on $\mathcal{C}$ and only remember its structure as a spherical fusion category. Hence, Muger's theorem tells us that $\mathcal{Z}(\mathcal{C})$ is canonically a modular category. It is a fantastic fact that in this case $\mathcal{Z}(\mathcal{C})$ can be explicitely computed in terms of $\mathcal{C}$. We describe this computation now.

WORK: Define the time-reversal conjugate $\overline{\mathcal{C}}$. Setup the map $\mathcal{C} \boxtimes \overline{\mathcal{C}} \to \mathcal{Z}(\mathcal{C})$

Proposition 5.7.3. *Let $\mathcal{C}$ be a pre-modular category. The canonical map $\mathcal{C} \boxtimes \overline{\mathcal{C}} \to \mathcal{Z}(\mathcal{C})$ is an equivalence of categories if and only if $\mathcal{C}$ is modular.*

Proof. WORK: proof □

This theorem is fantastic because it not only computes $\mathcal{Z}(\mathcal{C})$ for every modular category $\mathcal{C}$, but also it gives an equivalent definition of modularity. This gives us our third definition of modularity. Namely a pre-modular category $\mathcal{C}$ 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 unitarizability

WORK: An early reference about unitary MTCs is [KJ96]. I should read this.

WORK: Include this somewhere:

Proposition 5.8.1. *Let $\mathcal{C}$ 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 $\mathcal{C}$. This left-rigidity endows $\mathcal{C}$ with the structure of a spherical fusion category.*

As we've mentioned beofre, the algebraic theory of topological order is not modular category theory but *unitary* modular category theory because hom-spaces need Hilbert space structure to define valid quantum systems. We define unitary fusion categories and unitary modular categories in section [ref].

We've mostly ignored unitary fusion categories for the following reasons: their additional structure is a large semantic burden, and is in a way inessential. We mean this in the following sense:

1. Given a spherical fusion category, $\mathcal{C}$ every unitary structure on $\mathcal{C}$ is equivalent. That is, all the unitary fusion categories obtained by enriching $\mathcal{C}$ with unitary structure are equivalent to one another as unitary fusion categories;

2. All braidings on unitary fusion categories are automattically unitary so there is no subtelty in passing to unitary modular categories;
3. A spherical fusion category admits a unitary structure if and only if its quantum dimensions are all positive.

Still, it is worthwhile to study unitary fusion categories. They are the correct algebraic structure to describe topological order, so understanding *why* points (1-3) above are true gives insight into unitarity in practice. There is also a characterization of unitary fusion categories in the skeletized perspective which is of much utility in practice. Namely, a fusion category admits a unitary structure if and only if its F-matrices and R-matrices can all be made unitary. We discuss this more and offer a proof in section [ref].

We now prove the first main result of the section:

Proposition 5.8.2. *Let $\mathcal{C}$ be a spherical fusion category. There is a compatible unitary structure on $\mathcal{C}$ if and only if the quanutum dimensions d_A are positive for all simple objects $A \in \mathcal{C}$.*

Proof. Suppose first that $\mathcal{C}$ admits a unitary structure. Then, for all simple objects $A \in \mathcal{C}$,

$$d_A = \mathrm{tr}(\mathrm{id}_A) = \langle \mathrm{id}_A \,|\, \mathrm{id}_A \rangle > 0$$

because the inner product is positive definite. Conversely, suppose that all of the quantum dimensions of $\mathcal{C}$ are positive. We will suppose for simplicity that $\mathcal{C}$ is skeletal, which is possible by proposition [ref]. Suppose that $f : A \to B$ is a morphism between objects $A, B \in \mathcal{C}$. We know that there are direct sum decompositions $A = \bigoplus_i A_i$ and $B = \bigoplus_j B_j$. Writing f as an element of $\bigoplus_{i,j} \mathrm{Hom}(A_i, B_j)$, we find that f acts by some scalar $f_{i,j}$ on each homspace $\mathrm{Hom}(A_i, B_j)$, where $f_{i,j} = 0$ if $A \ncong B$. We define $f^\dagger : B \to A$ to be the map whose $\mathrm{Hom}(B_j, A_i)$ is $f^\dagger_{j,i} = \overline{f_{i,j}}$.

We now prove that this defines a unitary structure on $\mathcal{C}$. Given any two morphism $f : A \to B$, we compute

$$\langle f \,|\, f \rangle = \mathrm{tr}(f^\dagger \circ f) = \sum_{i,j} |f_{i,j}|^2 d_{A_i}.$$

Clearly, $\langle f \,|\, f \rangle = 0$ if and only if $f = 0$ because all of the quantum dimensions d_{A_i} are positive real numbers. Hence, $\langle \cdot \,|\, \cdot \rangle$ is positive definition.

It is clear that $(f^\dagger)^\dagger = f$, $(f \circ g)^\dagger = g^\dagger \circ f^\dagger$, and $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$ for appropriate choices of f, g. It remains to show that $\left(\mathrm{ev}_A^R\right)^\dagger = \mathrm{coev}_A^L$ and $\left(\mathrm{coev}_A^R\right)^\dagger = \mathrm{ev}_A^L$.

WORK: I don't know how to do this part of the proof. It's something to come back to. ☐

5.8.2 Unitary braidings

WORK: Show that every braiding is automatically unitary. This is the content of [Gal14].

5.8.3 Uniqueness of unitary structure

WORK: Show that unitary structures are unique. This is the content of [Reu23].

5.8.4 Skeletonization of unitarity

WORK: Show that a fusion category admits a unitary structure if and only if its F and R symbols can be made unitary in some basis. There are good references for this in the papers cited above.

5.9 Number theory in modular categories

5.9.1 Techniques and first results

WORK: A good general reference about this stuff is [GS19]. To-read, for sure. There is also interesting work in [MS12] which gives some counterexamples. Another reference is [DHW13].

5.9.2 Galois conjugation

WORK: An early reference is [CG93]. Some other papers not to ignore in this area are [PSYZ23, BR22].

5.9.3 Ocneanu rigidity

5.9.4 Rank-finiteness theorem

WORK: Of course there is the original paper on the topic. However, there is also the generaliation for G-crossed MTCs and fermionic MTCs - [JMNR21]. Should I bring this up now or later?

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: I would quite like to show that fusion categories (or at least modular categories) have finitely automorphisms of the identity functor. The proof I know follows from generalities about the universal grading group - [GN08]. I wonder if this proof can be done completely without the use of grading. Then, the fact that the universal grading group can be interpreted in terms of grading can be put as an exercise in the "further structure" section!

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: One of the pivotal axioms automatically holds in fusion categories. Namely, the one with the twists going the two different ways. The proof is very standard - reduce to the case A, B are both simple, reduce to case $A = B$, $f = \lambda \cdot \mathrm{id}_A$ and hence commutes with everything. This would be a nice exercise.

5.4. WORK: there's a notion of prime factorization of MTCs. If $\mathcal{C}$ is an MTC, then it can be decomposed as a tensor product

$$\mathcal{C} = \mathcal{C}_1 \boxtimes \mathcal{C}_2 ... \boxtimes \mathcal{C}_n,$$

where $\mathcal{C}_i \neq 0$ all have no proper non-degenerate braided fusion subcategories other than $\mathbf{Vec}_{\mathbb{C}}$. We call suchMTCs *prime MTCs*. Suppose that $\mathcal{C}$ has NO abelian anyons. Then, the decomposition is unique. However, if $\mathcal{C}$ has abelian anyons then the decomposition can fail to be unique. In particular, the color code is equivalent to both bilayer toric code and bilayer 3-fermion (c.f. [KPEB18]). The factorization results I asserted come from the (largely ignored?) paper by Muger: [Müg02]. This could make for a very nice exericse. First, prove Muger's double centralizer theorem. Then, prove the factorization into prime MTCs. Then, if $\mathcal{C}$ has no abelian anyon anyons, prove that the decomposition is unique. Then, prove that bilayer toric code is equivalent to bilayer 3-fermion (or maybe just leave that as a comment)!

6 Further structure

6.1 Overview

6.1.1 Introduction

We've seen this general picture throughout the book:

[WORK: add triangle.]

In this chapter we will talk about aspects of the algebraic theory of topological quantum information *beyond* this basic model. In particular, we will talk about physical phenomina beyond plain topological order. These phenomina are not just a phisical or mathematical curiosity. They are central to almost all proposals for topological quantum computation, including the majority of the proposals we will present in chapter [ref].

We will show by example how easy it is to start running into phenomina beyond plain topological order. Suppose we want to make a topological quantum computer on some chip in the lab. Realistically, this chip is going to be *flat*. It's difficult and unpractical to make chips bend into spheres or tori for all sorts of reasons. The chip is also going to be finite. Hence, the chip is going to have *boundary*. This boundary and the way it is manipulated have serious and subtle impacts on the computation being performed. It cannot be ignored. Up to now, we have given no indication about how boundaries are to be dealt with.

[WORK: add picture of chip with boundary.]

These boundaries are not described by modular categories - we need additional algebraic structures to define them. In general, whenever we have any phenominon beyond plain topological order we will need to introduce new algebraic structures.

In this chapter, we will discuss three different classes of important physical phenomina:

1. **Boundaries and domain walls**. In this section, we will talk about how topological phases can interact with one another. If you have one topological phase next to another, they can be physically seperated by a *domain wall*:

   [WORK: add picture of domain wall.]

   If tuned correctly, this domain wall can be chosen so that the composite system keeps its topological gap. That is, we can make a composite topological system with two different sub-phases! The theory of domain walls includes the theory of boundaries as a special case, because a boundary can be viewed as a domain wall between a topological phase and empty space (which is itself a trivial topological phase).

2. **Symmetry enriched topological order**. [WORK: describe SETs]

3. **Fermionic topological order**. [WORK: describe fermionic TO.]

One of the fantastic features of the above structures is that they are all mathematically based on the same ideas: *module categories* and *graded categories*. The basic theory of module categories and graded categories will take us very far. Hence even though physically we will be stopping-and-starting every section with new phenomina, mathematically we will see a very smooth narrative.

[WORK: Another thing to mention is that there are all sorts of ways of extending topological order, many of which have a nice algebraic extension in terms of extending the category theoretic language. Here's a little running list below:

- Intrinsically mixed-state topological order, which corresponds to pre-modular categories [**?**, **?**];
- In the non-semisimple case there is the theory of relative modular categories. This theory is much less physical; its importance lies in the ability of its associated link invariants to prove results in topology [**?**, **?**, **?**];
-

]

6.2 Boundaries and domain walls

6.2.1 Physical picture

In this section we will talk about boundaries and domain walls in topological systems. To begin, we'll talk about boundaries in topological phases. We have the following general picture:

[WORK: topologically ordered system with boundary. DON'T use the categorical "$\mathcal{C}$". Use the words "topologically ordered system". Keep with this convention for the whole section. I'm not assuming that the reader knows any category theory.]

This topologically ordered system with boundary will be described by some Hamiltonian. Within the bulk of the system the Hamiltonian would be the same as if the topological system had no boundary. On the boundary, however, it will neccecarily be different. A-priori, we could chose our boundary terms in the Hamiltonian to behave arbitrarily. This will cause a problem, however. It can close the topological gap!

The main point of a topologically ordered system is that it has an energy gap in its spectrum between its lowest energy eigenstate and its next lowest energy eigenstate:

[WORK: add picture of gap.]

Adding the wrong terms on the boundary could close the gap. Namely, the size of the gap could tend to zero as the system size tends to infinity. To preserve the gap, the boundary terms in the Hamiltonian need to have a very special form. This special form implies a quite rigid structure on the space of gapped boundaries.

[WORK: Talk about how gapped boundaries can be equivalent to one another, they can be stable or unstable. When we say boundary theory, we mean *stable gapped boundary* theory. State that there are finitely many equivalence classes of boundary theories for a given topological order.

I don't really know how this equivalence works and how stability works. This is something to learn.]

Within a boundary there can be *boundary defects*. These are points in which the boundary theory changes from one theory to another, as shown below:

[WORK: add basic picture of a boundary defect.]

Just like with boundaries, it is important that the terms of the Hamiltonian around the boundary defect are chosen so that the topological gap is maintained. There can be stable and unstable boundary defects. There is a natural equivalence relation on the space of stable boundary defects, under which there are finitely many equivalence classes.

One important feature of boundary defects is that they can be *fused*. This happens when two defects are brought very close to one another, as shown below:

[WORK: add a picture for the fusion of boundary defects.]

This fusion can be nondeterministic. That is, repeating the fusion of two boundary defects can yield different results. In this sense boundaries can host non-abelian defects. Importantly, we will find that abelian bulk theories can host non-abelian boundary defects! This is the heart of our proposal for quantum computing with $\mathfrak{D}(\mathbb{Z}_2)$ topological order. Instead of working with the abelian anyons, we work with the nonabelian boundary defects!

More generally, in this section we will also discuss *domain walls*. Domain walls are boundaries between two different phases. That is, a domain wall is a one-dimensional line seperating two-dimensional topologically ordered systems, as shown below:

[WORK: add picture.]

Domain walls include boundaries as a special case. Empty space can be viewed as a topologically ordered system. Namely, it is the topologically ordered space with a unique ground state - emptyness! This is the trival topological theory. A domain wall can be chosen between any topological theory and the empty theory. This is a boundary!

Of course, domain walls should be chosen to maintain the topological gap. There is a notion of stable and unstable domain walls. There is a notion of equivalnece of stable domain walls. There are finitely many equivalence classes of stable domain walls between any two phases.

Within a domain wall there can be a boundary defect, just like before, which can fuse:

[WORK: add picture of boundary defect in domain wall, alongside a picture for fusion of defects.]

Domain walls also have the added structure of a notion of fusion. Given three topological phases and successive domain walls between them, bringing the domain walls will result in a new domain wall:

[WORK: fusion of domain walls.]

It is important to observe that just like how every boundary can be interpreted as a domain wall, we can interpret every domain wall in terms of a boundary. This goes as follows. Given a domain wall between two phases, we can *fold* the domain wall to get a boundary of the resulting bilayer theory:

[WORK: add folding picture.]

This establishes a bijection,

$$\begin{pmatrix}\text{domain walls between}\\ \text{phase 1 and phase 2}\end{pmatrix} \xrightarrow{\sim} \begin{pmatrix}\text{boundaries of the bilayer phase}\\ \text{obtained by stacking phase 1}\\ \text{and a flipped copy of phase 2}\end{pmatrix}.$$

This bijection is known as the *folding trick*.[WORK: Should I attribute it to Wen? People at the conference at the Perimeter institute were doing that. Kitaev and Kong are an early reference for the trick.]

In this section, we will be discussing the theory of domain walls, boundary defects, and their fusion.

6.2.2 Boundaries and domain walls in the toric code

.[WORK: Do boundaries and domain walls in the toric code. The original reference is [**?**]. There's also a good discussion in "Topological quantum". I suppose I'll stay away from the surface code literature because they all do it for Bravyi's $\pi/4$ twisted version.]

6.2.3 The algebraic theory of gapped boundaries

In this subsection, we will take all of the principles discussed in section [ref] and interpret them in terms of category theory. This will give us an algebraic theory of gapped boundaries.

[WORK: Motivate why gapped boundaries correspond to Lagrangian algebras. As you approach a gapped boundary, every anyon is *confied* (become a boundary excitation) or *condensed* (dissapear at the boundary). A nice talk about this perspective is [**?**].

I still don't quite get how you get from this to Lagrangian algebras. What does the multiplication map mean, physically? Why does it need to be commutative? Why does it need to be seperable? Why does it need to be connected? What's with the condition on dimensions?

Also, there's this quote by Burnell which is very mysterious to me:

"In a conventional ordering transition, the order parameter results from condensing a bosonic excitation– for example, the ordering of a magnet can be viewed as the Bose condensation of spinons."

What does it mean?

What do boundary defects correspond to? If the boundary defects go from one boundary type to the same boundary type then the answer is that it is the idempotent completion of the quotient of the original category by the algebra object. This quotient procedure is supposed to describe condensation of anyons at the domain wall. What is the general definition of boundary defect? I can't find it in Cong-Cheng-Wang.

I'll talk to Zhenghan and he will explain everything to me.]

[WORK:

- A discussion of anyon condensation at boundaries as a physical mechanism for gapped boundaries - smoothly get to Lagrangian algebras without needing to go through module categories or the Levin-Wen model!
- Prove that every module category is equivalent to the category of modules over some algebra (this is is Ostrik's original paper);
- Classification of irriducible module categories in terms of Lagrangian algebras - this is proposition 4.8 of [**?**].
- Characterization of Lagrangian algebras in terms of algebras with nice properties - this is due to Cong-Cheng-Wang;
- Proof that an MTC is doubled iff it contains a Lagrangian algebra
- Characterization of Lagrangian algebras in $\mathcal{Z}(\mathbf{Vec}_G)$;

]

[WORK:

There's the very important issue of what the ground state degeneracy of systems with boundaries and boundary defects is. What is a basis for these states? How does braiding act on them? All that stuff. This is done well in Cong-Cheng-Wang.

Another part of this is giving a treatment of topological charge measurement. What are observables? What are the associated probabilities?]

6.2.4 Lagrangian algebras and algebra objects

.[WORK: Give a nice mathematical treatment of Lagrangian algebras and algebra objects.]

6.2.5 Module categories and boundaries in the Levin-Wen model

[WORK: This subsection needs to be totally re-done. This is now an *alternate* perspective on gapped boundaries. I'm including it because the theory of module categories is neccecary for the next section. I'm also including it because its nice to have multiple perspectives on this sort of stuff. I'm also including it because the theory of modules is very powerful. This might be the only reasonable way to get at Muger's theorem and Lagrange's theorem for fusion categories.]

In this subsection, we will take all of the principles discussed in section [ref] and interpret them in terms of category theory.

To begin, we re-iteratre that not every topological phase admits a gapped boundary. In fact, we have the following physical principle [**?**]:

$$\begin{pmatrix}\text{the topological order described}\\ \text{by the modular category } \mathcal{B}\\ \text{admits a gapped boundary}\end{pmatrix} \iff \begin{pmatrix}\text{there is an equivalence of categories}\\ \mathcal{B} \cong \mathcal{Z}(\mathcal{C}) \text{ for some}\\ \text{spherical fusion category } \mathcal{C}\end{pmatrix}.$$

For this reason, we will restrict our attention to *doubled* topological order for the rest of the section. That is, modular categories $\mathcal{B}$ which are equivalent to $\mathcal{Z}(\mathcal{C})$ for some spherical fusion category $\mathcal{C}$. We will simplify notion for doubled topological order. We will write

[WORK: bulk theory with letter $\mathcal{C}$ in it = topological ordered described by $\mathcal{Z}(\mathcal{C})$.]

This now leads us to the big question: what, algebraically, are boundaries theories in the $\mathcal{Z}(\mathcal{C})$ topological order?

[WORK: The answer is $\mathcal{C}$-module categories. I am suspecting that to motivate this answer one needs to take some physical principles from the string-nets developped in the Levin-Wen model. I haven't written the Levin-Wen section yet, so this can wait until that.]

More generally, a domain wall between the phases described by $\mathcal{Z}(\mathcal{C})$ and $\mathcal{Z}(\mathcal{D})$ will be a $(\mathcal{C}, \mathcal{D})$-bimodle category. [WORK: motivate this as well].

We rigorously define the above intuitive notions as follows.

Definition 6.2.1 (Left module category)**.** A *left module category* over a fusion category $\mathcal{C}$ is the following data:

1. A $\mathbb{C}$-linear category $\mathcal{M}$;
2. (Action) A functor $\otimes : \mathcal{C} \times \mathcal{M} \to \mathcal{M}$;
3. (Left associator) A natural isomorphism $m : ((-) \otimes (-)) \otimes (-) \xrightarrow{\sim} (-) \otimes ((-) \otimes (-))$ of functors $\mathcal{C} \times \mathcal{C} \times \mathcal{M} \to \mathcal{M}$;
4. (Unit) A natural isomorphism $\lambda_m : \mathbf{1} \otimes (-) \to (-)$ of functors $\mathcal{M} \to \mathcal{M}$.

Such that:

1. There is an equivalence $\mathcal{C} \cong \mathbf{Vec}_{\mathbb{C}}^n$ as $\mathbb{C}$-linear categories for some integer $n \geq 1$.
2. The functor $\otimes$ is $\mathbb{C}$-linear.
3. For all $A, B, C \in \mathcal{C}$ and $M \in \mathcal{M}$ the diagram

$$\begin{tikzcd}
 & ((A \otimes B) \otimes C) \otimes M \arrow[dl, "\alpha_{A,B,C} \otimes \mathrm{id}_M"'] \arrow[dr, "m_{A \otimes B, C, M}"] & \\
(A \otimes (B \otimes C)) \otimes M \arrow[d, "m_{A, B \otimes C, M}"] & & (A \otimes B) \otimes (C \otimes M) \arrow[d, "m_{A,B,C \otimes M}"'] \\
A \otimes ((B \otimes C) \otimes M) \arrow[rr, "\mathrm{id}_A \otimes m_{B,C,M}"] & & A \otimes (B \otimes (C \otimes M))
\end{tikzcd}$$

commutes.

4. For all $A \in \mathcal{C}$ and $M \in \mathcal{M}$, the diagram

$$\begin{tikzcd}
(A \otimes \mathbf{1}) \otimes M \arrow[r, "m_{A,\mathbf{1},M}"] \arrow[d, "\rho_A"] & A \otimes (\mathbf{1} \otimes M) \arrow[dl, "id_A \otimes \lambda_m"] \\
A \otimes M &
\end{tikzcd}$$

commutes.

□

The definition of a *right* module category is completely symmetric, with no surprises. The definition of a bimodule category comes from putting these definitions together:

Definition 6.2.2 (Bimodule category)**.** A $(\mathcal{C}, \mathcal{D})$-*bimodule category* $\mathcal{M}$ over fusion categories $\mathcal{C}, \mathcal{D}$ is the following data:

1. The structure of a right $\mathcal{C}$-module on $\mathcal{M}$;
2. The structure of a left $\mathcal{D}$-module on $\mathcal{M}$;
3. (Middle associator) A natural isomorphism $b : ((-) \otimes (-)) \otimes (-) \xrightarrow{\sim} (-) \otimes ((-) \otimes (-))$ of functors $\mathcal{C} \times \mathcal{M} \times \mathcal{D} \to \mathcal{M}$;

Such that:

1. For all $A, B \in \mathcal{C}$, $M \in {}_{\mathcal{C}}\mathcal{M}_{\mathcal{D}}$, $A', B \in \mathcal{D}$, the diagrams

$$\begin{tikzcd}
 & ((A \otimes B) \otimes M) \otimes C \arrow[dl, "m^L_{A,B,M}"'] \arrow[dr, "b_{A \otimes B, M, C}"] & \\
(A \otimes (B \otimes M)) \otimes C \arrow[d, "b_{A, B \otimes M, C}"] & & (A \otimes B) \otimes (M \otimes C) \arrow[d, "m^L_{A,B,M \otimes C}"'] \\
A \otimes ((B \otimes M) \otimes C) \arrow[rr, "\mathrm{id}_A \otimes b_{B,M,C}"] & & A \otimes (B \otimes (M \otimes C))
\end{tikzcd}$$

and

$$\begin{tikzcd}
 & ((A \otimes M) \otimes B) \otimes C \arrow[dl, "b_{A,M,B} \otimes \mathrm{id}_C"'] \arrow[dr, "m^R_{A \otimes M,B,C}"] & \\
(A \otimes (M \otimes B)) \otimes C \arrow[d, "b_{A,M \otimes B,C}"'] & & (A \otimes M) \otimes (B \otimes C) \arrow[d, "b_{A,M,B \otimes C}"] \\
A \otimes ((M \otimes B) \otimes C) \arrow[rr, "\mathrm{id}_A \otimes m^R_{M,B,C}"] & & A \otimes (M \otimes (B \otimes C))
\end{tikzcd}$$

commute.

□

Given two fusion categories $\mathcal{C}, \mathcal{D}$ and a $(\mathcal{C}, \mathcal{D})$-bimodule categories $\mathcal{M}$, we define $\mathcal{M}$ to be a *simple* module if for all simple objects $N, M \in \mathcal{M}$ there exists some $A \in \mathcal{C}$ such that $\mathrm{Hom}(N, A \otimes M) \neq 0$. This condition of irriducibility corresponds exactly the condition of stability of boundaries. Hence, we arrive at the following correspondance:

[WORK: boundary theories correspond to simple module categories;]

[WORK: domain walls correspond to simple bimodule categories.]

We now turn our attention towards boundary defects.

[WORK: motivate why boundary defects are bimodule functors. I think this one can be easily seen by passing boundary excitations through the defect and thus noticing that the defect must act like a functor.]

Formally, we get the following definition:

Definition 6.2.3 (Left module functor)**.** A *left module functor* between left $\mathcal{C}$-module categories $\mathcal{M}$, $\mathcal{N}$ is the following data:

1. A functor $F : \mathcal{M} \to \mathcal{N}$;
2. A natural isomorphism $s : F((-) \otimes (-)) \xrightarrow{\sim} (-) \otimes (-)$ of functors $\mathcal{C} \times \mathcal{M} \to \mathcal{N}$.

Such that:

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

$$\begin{tikzcd}
 & F((A \otimes B) \otimes M) \arrow[dl, "F(m^{\mathcal{M}}_{A,B,M})"'] \arrow[dr, "s_{A \otimes B,M}"] & \\
F(A \otimes (B \otimes M)) \arrow[d, "s_{A,B \otimes M}"'] & & (A \otimes B) \otimes F(M) \arrow[d, "m^{\mathcal{N}}_{A,B,F(M)}"] \\
A \otimes F(B \otimes M) \arrow[rr, "\mathrm{id}_A \otimes s_{B,M}"] & & A \otimes (B \otimes F(M))
\end{tikzcd}$$

commutes.

2. For all $M \in \mathcal{M}$ the diagram

$$\begin{tikzcd}
F(\mathbf{1} \otimes M) \arrow[r, "s_{\mathbf{1},M}"] \arrow[dr, "F(\lambda^{\mathcal{M}}_{m,M})"'] & \mathbf{1} \otimes F(M) \arrow[d, "\lambda^{\mathcal{N}}_{m,F(M)}"] \\
 & F(M)
\end{tikzcd}$$

commutes.

$\square$

A right module functor is defined in complete analogy to left module functor. A $(\mathcal{C}, \mathcal{D})$-bimodule functor is defined to be a functor which is simulaneously equipped with the structure of a left and right module functor. We denote by $\mathrm{Fun}_{\mathcal{C}}(\mathcal{M}, \mathcal{N})$, the space of $\mathcal{C}$-modue functors from $\mathcal{M}$ to $\mathcal{N}$, and we denote by $\mathrm{Fun}_{\mathcal{C}|\mathcal{D}}(\mathcal{M}, \mathcal{N})$ the space bimodule functors.

To turn these spaces of module functors into categories, we will need to define an appropriate notion of natural transformation

Definition 6.2.4 (Natural transformation of left module functors)**.** A *natural transformation of left module functions* between left $\mathcal{C}$-module functors $F, G : \mathcal{M} \to \mathcal{N}$ is a natural transformation $\eta : F \to G$ such that for all $A \in \mathcal{C}$, $M \in \mathcal{M}$

$$\begin{tikzcd} F(A \otimes M) \arrow[r, "\eta_{A \otimes M}"] \arrow[d, dashed, "s^F_{A,M}"] & G(A \otimes M) \arrow[d, dashed, "s^G_{A,M}"] \\ A \otimes F(M) \arrow[r, "\mathrm{id}_A \otimes \eta_M"] & A \otimes G(M) \end{tikzcd}$$

$\square$

Just like in our general theory, we define an object in a functor category to be irriducible if it cannot be expressed as the biproduct of two nonzero elements. We arrive at the following correspondance:

[WORK: boundary defects correspond to simple bimodule functors.]

The fusion of boundary defects is clear. Given two boundary defects $F : \mathcal{M} \to \mathcal{M}'$ and $G : \mathcal{M}' \to \mathcal{M}''$ the composition $(G \circ F) : \mathcal{M} \to \mathcal{M}''$ gives another boundary defect. This is the correct physical choice becase [WORK: depends on the physical motivation I gave for defects corresponding to functors].

The fusion of domain walls is a bit more sublte. It requires the notion of relative tensor product:

Definition 6.2.5 (Relative Deligne tensor product)**.** [WORK: give definition]

Physically, we can define fusion of domain walls $\mathcal{M}$ and $\mathcal{N}$ to be the relative Deligne tensor product $\mathcal{M} \boxtimes_{\mathscr{K}} \mathcal{N}$, where $\mathcal{M}$ is a $(\mathcal{C}\, \mathscr{K})$-bimodule and $\mathcal{N}$ is a $(\mathscr{K}, \mathcal{D})$-bimodule. This is the correct definition because [WORK: give physical motivation].

All together, this gives us the following physics-math dictionary:

[WORK: add dictionary.]

As we have just seen, the algebraic theory of of topological boundaries and domain walls is modules and bimodules. So, mathematically, we now take the time to set up the theory of modules and bimodules over fusion categories.

The first thing we are going to do is reinterpret bimodules in terms of modules. This will allow us to state all of our results in this section in terms of modules without loss of generality, because dealing with bimodules adds unnececary notational difficulty. This is done via the folding trick. As mentioned before, we have a correspondance as follows:

[WORK: add folding trick. The flat plane should have the label $(\mathcal{C}, \mathcal{D})$-bimodules and the folded plane shuld have the label $(\mathcal{C} \boxtimes \overline{\mathcal{D}})$-modules.]

This is codifed mathematically in the following proposition:

Proposition 6.2.6 (Folding trick)**.** *Let $\mathcal{C}, \mathcal{D}$ be fusion categories. Given a $(\mathcal{C}, \mathcal{D})$-bimodule $\mathcal{M}$, define a left $(\mathcal{C} \boxtimes \overline{\mathcal{D}})$-module structure on $\mathcal{M}$ via the formula*

$$(A \boxtimes \overline{B}) \otimes M = (A \otimes M) \otimes B$$

for any $A \in \mathcal{C}$, $B \in \mathcal{D}$, $M \in \mathcal{M}$. This is a well-defined left $(\mathcal{C} \boxtimes \overline{\mathcal{D}})$-module structure. This assignment induces a bijection between the set of $(\mathcal{C}, \mathcal{D})$-bimodules and the set of left $(\mathcal{C} \boxtimes \overline{\mathcal{D}})$-modules.

Proof. This is a straightforward and unenlightening exercise. $\square$

Next, we take a closer look at simple modules. That is, module categories with no proper nontrivial submodule categories. Given two categories $\mathcal{M}$ and $\mathcal{N}$, we can define their Cartesian product $\mathcal{M} \times \mathcal{N}$, whose objects are pairs (A, B), $A \in \mathcal{M}$, $B \in \mathcal{N}$. To avoid confusion with the Deligne tensor product, we will use the notation $\boxplus$ to denote the Cartesian product in this context, and refer to it as the direct sum. This is consistent with our genereal principles of higher linear algebra (see section [ref]). If $\mathcal{M}$ and $\mathcal{N}$ are left $\mathcal{C}$-module categories, then $\mathcal{M} \boxplus \mathcal{N}$ can be equipped with the structure of a left $\mathcal{C}$-module via the action

$$A \otimes (M \boxplus N) = (A \otimes M) \boxplus (A \otimes N).$$

We seek to prove that every module is the direct sum of simple modules. This follows after a lemma.

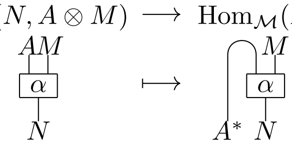
Lemma 6.2.7. *Let $\mathcal{C}$ be a fusion category. Let $\mathcal{M}$ be a left $\mathcal{C}$-module. For all $A \in \mathcal{C}$ and $N, M \in \mathcal{M}$, we have that*

$$\mathrm{Hom}_{\mathcal{M}}(N, A \otimes M) \cong \mathrm{Hom}_{\mathcal{M}}(A^* \otimes N, M)$$

as $\mathbb{C}$-vector spaces.

Proof. The proof is exactly the same as of proposition [ref]. We opt for a proof using the graphical language of morphisms instead of the algebraic approach, because it is more lucid. We have not formally introduced the graphical language for module categories, but it is completely analogous to the graphical language for fusion categories. We define the map

$$\mathrm{Hom}_{\mathcal{M}}(N, A \otimes M) \longrightarrow \mathrm{Hom}_{\mathcal{M}}(A^* \otimes N, M)$$



Twisting the A^* the other way serves as an inverse, completing the proof. $\square$

Proposition 6.2.8. *Let $\mathcal{C}$ be a fusion category. Every left $\mathcal{C}$-module category is equivalent to a direct sum of simple $\mathcal{C}$-module categories.*

Remark 6.2.9. The usual way of summarizing this proposition is by saying that the space of left $\mathcal{C}$-modules is *semsimple.*

Proof. Let $\mathcal{M}$ be a left $\mathcal{C}$-module. Denote by $\mathcal{L}_{\mathcal{M}}$ the set of isomorphism classes of simple objects in $\mathcal{M}$. We define a equivalence relation $\sim$ on $\mathcal{L}_{\mathcal{M}}$ by saying that $[N] \sim [M]$ if there exists some $A \in \mathcal{C}$ such that $\mathrm{Hom}(N, A \otimes M) \neq 0$. This relation is reflexive since $\mathrm{Hom}(M, \mathbf{1} \otimes M) \neq 0$, it is transitive since if $\mathrm{Hom}(M, A \otimes M') \neq 0$ and $\mathrm{Hom}(M', B \otimes M'') \neq 0$, then $\mathrm{Hom}(M, A \otimes B \otimes M'') \neq 0$ by composing morphisms. Seeing as $\mathcal{M} \cong \mathbf{Vec}_{\mathbb{C}}^{n}$ for some $n \geq 1$ as a category, we have that $\mathrm{Hom}(N, M) \cong \mathrm{Hom}(M, N)$ as vector spaces for all $N, M \in \mathcal{M}$. Hence, the equivalence relation is symmetric by lemma [ref].

For all $i \in \mathcal{L}_M / \sim$, we define a full subcategory of $\mathcal{M}$ via

$$\mathcal{M}_i = \left\{ M \in \mathcal{M} | \, M \cong \bigoplus_{[N] \in i} n_N \cdot N, \text{ for some integers } n_A \geq 0 \right\}.$$

Now, our equivalence relation gaurantees that $\mathcal{M}_i$ is closed under the action of $\mathcal{C}$ for all $i \in \mathcal{L}_{\mathcal{M}} / \sim$. That is, it forms a left $\mathcal{C}$-submodule of $\mathcal{M}$. We claim that the map

$$\begin{aligned} \boxplus_{i \in \mathcal{L}_{\mathcal{M}}/\sim} \mathcal{M}_i &\to \mathcal{M} \\ (M_i)_{i \in \mathcal{L}_{\mathcal{M}}/\sim} &\mapsto \bigoplus_{i \in \mathcal{L}_{\mathcal{M}}/\sim} M_i \end{aligned}$$

is an equivalence of categories. It is faithful by the general properties of the direct sum. It is full because $\mathrm{Hom}(M_i, M_j) = 0$ for all $i \neq j$ since M_i, M_j are the direct sums of disjoint sets of simple objects, and hence every morphisms can be broken into its i-components for each $i \in \mathcal{L}_{\mathcal{M}} / \sim$. It is essentially surjective because every simple objects appears in the category $\mathcal{M}_i$ for some $i \in \mathcal{L}_{\mathcal{M}} / \sim$. Hence, it is an equivalence of categories by proposition [ref] so our proof is complete. □

With propositions [ref] and [ref] in hand, we can set up more directly the theory of fusion of domain walls. Let $\mathcal{C}$, $\mathscr{K}$, $\mathcal{D}$ be fusion categories. Let $\mathcal{M}$ be a $(\mathcal{C}, \mathscr{K})$-bimodule and let $\mathcal{N}$ be a $(\mathscr{K}, \mathcal{D})$ bimodule. We have an equivalence

$$\mathcal{N} \boxtimes \mathcal{M} \cong \boxplus_{[\mathcal{M}']} n_{\mathcal{M}'}^{\mathcal{N}, \mathcal{M}} \cdot \mathcal{M}',$$

where $[\mathcal{M}']$ runs over the set of equivalence classes of simple $(\mathcal{C}, \mathcal{D})$-bimodules. This is completely analogus to the algebraic theory of fusion of anyons introduced in section [ref]. One of the major differenes is that we are now up a categorical level. Instead of fusing objects in a category, we are fusing the categories themselves.

We now turn our attention towards functors between module categories. When the source and target of our functors are the same, we have the following main result:

Proposition 6.2.10. *Let $\mathcal{C}$ be a fusion category. Let $\mathcal{M}$ be a left $\mathcal{C}$-module. Define*

$$\mathcal{C}_{\mathcal{M}}^{\vee} = \mathrm{Fun}_{\mathcal{C}}(\mathcal{M}, \mathcal{M}).$$

We call $\mathcal{C}_{\mathcal{M}}^{\vee}$ the dual of $\mathcal{C}$ with respect to $\mathcal{M}$. We define a monoidal structure on $\mathcal{C}_{\mathcal{M}}^{\vee}$ via the formula

$$F \otimes G = G \circ F.$$

Along with a natural choice of rigid structure, $\mathcal{C}^\vee_\mathcal{M}$ has the structure of a fusion category.

If $\mathcal{C}$ is a spherical fusion category, then $\mathcal{C}^\vee_\mathcal{M}$ is naturally equipped with the structure of a spherical fusion category.

Proof. .[WORK: do proof. This is going to use some stuff from "on fusion categories". Might need the same results for the next proposition as well.

I'm in trouble the proof uses Yetter cohomology and other scary-looking tools. Is there a simpler proof? The hard part is showing that if $\mathcal{N}, \mathcal{M}$ are module categories the space of module functors is equivalent to $\mathbf{Vec}_\mathbb{C}^n$ for some $n \geq 0$. In particular, we need to show that there are finitely many isomorphism classes of simple module functors. How do I do it?! It's a sort of generalized Ocneanu rigidity.] ☐

When the source and target are different, we have the follwing result:

Proposition 6.2.11. *Let $\mathcal{C}$ be a fusion category. Let $\mathcal{N}$, $\mathcal{M}$ be left $\mathcal{C}$-modules. The category* $\mathrm{Fun}_\mathcal{C}(\mathcal{N}, \mathcal{M})$ *is naturally equipped with the structure of a left $\mathcal{C}^\vee_\mathcal{N}$-module and a right $\mathcal{C}^\vee_\mathcal{M}$-module.*

Proof. .[WORK: do proof. Again, the finiteness part is hard.] ☐

Now, we verify the finiteness result that we claimed in section [ref]:

Proposition 6.2.12. *Let $\mathcal{C}$ be a fusion category. There are finitely many equivalence classes of simple left $\mathcal{C}$-modules.*

Proof. .[WORK: do proof. In "On fusion categories" they say that this follows from the finiteness condition on functors, along with a decategorified version of the same result which follows from counting.] ☐

The following result serves as the centerpiece of our study of module categories:

Theorem 6.2.13. *Let $\mathcal{C}$ be a fusion category. Let $\mathcal{M}$ be a left $\mathcal{C}$ module. The map*

$$\begin{aligned} \mathrm{can} : \mathcal{C} &\xrightarrow{\sim} (\mathcal{C}^\vee_\mathcal{M})^\vee_\mathcal{M} \\ A &\mapsto (M \mapsto A \otimes M) \end{aligned}$$

is an equivalence of categories. The $\mathcal{C}^\vee_\mathcal{M}$-module functor structure on can_A *is defined for all $A \in \mathcal{C}$, $M \in \mathcal{M}$, $F \in \mathcal{C}^\vee_\mathcal{M}$ by*

$$s^{\mathrm{can}_A}_{F,M} : \mathrm{can}_A(F \otimes M) = A \otimes F(M) \xrightarrow{s^{-1}_{A,M}} F(A \otimes M) = F \otimes \mathrm{can}_A(M).$$

If $\mathcal{C}$ is a spherical fusion category, can *is an equivalence of spherical fusion categories.*

Remark 6.2.14. This result is an analogue of the *double centralizer theorem* from classical representation theory.

Proof. .[WORK: do proof. The proof in EGNO uses algebras an algebra structures. It would be nice to get around this.] ☐

As a corollary, we get the following:

Corollary 6.2.15. *Let $\mathcal{C}$ be a fusion category and let $\mathcal{M}$ be a left $\mathcal{C}$-module. The module $\mathcal{M}$ is simple as a right $\mathcal{C}^\vee_\mathcal{M}$-module.*

Proof. .[WORK: do proof] □

Of course, the above discussion gaurantees a proper theory of fusion of boundary defects. Suppose that $\mathcal{C}, \mathcal{D}$ are fusion categories, and $\mathcal{M}$, $\mathcal{M}'$, $\mathcal{M}''$ are simple $(\mathcal{C}, \mathcal{D})$-bimodules. Suppose that $F : \mathcal{M} \to \mathcal{M}'$ and $G : \mathcal{M}' \to \mathcal{M}''$ are simple $(\mathcal{C}, \mathcal{D})$ bimodule functors. Since $\mathrm{Fun}_{\mathcal{C}|\mathcal{D}}(\mathcal{M}, \mathcal{M}'')$ is equivalent to $\mathbf{Vec}_{\mathbb{C}}^n$ for some ≥ 0 as a $\mathbb{C}$-linear category, we have a decomposition

$$G \circ F \cong \bigoplus_{[H]} n_H^{F,G} \cdot H$$

in $\mathrm{Fun}_{\mathcal{C},\mathcal{D}}(\mathcal{M}, \mathcal{M}'')$ where $[H]$ runs over isomorphism classes of simple functors in $\mathrm{Fun}_{\mathcal{C}|\mathcal{D}}(\mathcal{M}, \mathcal{M}'')$. Again, this is completely analagous to the fusion of anyons.

6.2.6 The Drinfeld center via bimodules

[WORK: The paper [**?**] has some interesting additional insights. Maybe if I took the time to understand it it would be relevant as a comment?]

So far we have been setting up a powerful theory of domain walls to study doubled topological order.

We already know one thing about doubled topological order - its anyons are described by the Drinfeld center $\mathcal{Z}(\mathcal{C})$ of the input spherical fusion category $\mathcal{C}$. These anyonic bulk excitations can interact with the boundaries, and produce non-trivial effects. This means that the category $\mathcal{Z}(\mathcal{C})$ neccecarily has deep connections to the theory of boundaries, and thus mathematically will have a module-theoretic interpretation. This will also help answer the question of why the Drinfeld center $\mathcal{Z}(\mathcal{C})$ is the category which describes anyons in the Levin-Wen model.

To start, consider an anyon in the bulk. This anyon is a stable localized excitation. Above it and below it the theory is in its ground state. Hence, we can think of this anyon as an interface between the trivial boundary and itself! This is seen visually below:

[WORK: add picture of anyon as interface between trivial boundary and itself.]

Thus, from our general description of boundary defects, we should conclude the following:

$$(\text{anyon types}) = \begin{pmatrix} \text{boundary defects} \\ \text{between trivial theory and itself} \end{pmatrix} = \begin{pmatrix} \text{simple objects in} \\ \mathrm{Fun}_{\mathcal{C}|\mathcal{C}}(\mathcal{C},\mathcal{C}) \end{pmatrix}.$$

However, we know from our first discussion of the Levin-Wen model that anyon types should correspond to simple objects in $\mathcal{Z}(\mathcal{C})$. Hence, we conclude that simple objects in $\mathcal{Z}(\mathcal{C})$ should correspond to simple objects in $\mathrm{Fun}_{\mathcal{C}|\mathcal{C}}(\mathcal{C}, \mathcal{C})$. Of course, this equivalence should repsect fusion, duality, braiding, and all the other algebraic structures of anyons. Thus, if our boundary theory is correct, it predicts an equivalence of categories $\mathcal{Z}(\mathcal{C}) \cong \mathrm{Fun}_{\mathcal{C}|\mathcal{C}}(\mathcal{C}, \mathcal{C})$. This mathematical prediction is accurate, by the following proposition:

Proposition 6.2.16. *Let $\mathcal{C}$ be a fusion category. The map*

$$\mathrm{Fun}_{\mathcal{C}|\mathcal{C}}(\mathcal{C}, \mathcal{C}) \xrightarrow{\sim} \mathcal{Z}(\mathcal{C})$$
$$F \mapsto \big(F(1), \beta_{F(1),-}\big)$$

is an equivalence of categories, where $\beta_{F(1),-}$ is defined by the composition

$$\beta_{F(1),-} : F(\mathbf{1}) \otimes B \xrightarrow{s^R_{\mathbf{1},B}} F(\mathbf{1} \otimes B) = F(B) = F(B \otimes \mathbf{1}) \xrightarrow{(s^L_{B,\mathbf{1}})^{-1}} B \otimes F(\mathbf{1})$$

and s^L, s^R are the compatibility maps implicit in the left/right module functor structure of F.

If $\mathcal{C}$ is a spherical category, then the map $\mathrm{Fun}_{\mathcal{C}|\mathcal{C}}(\mathcal{C}, \mathcal{C}) \xrightarrow{\sim} \mathcal{Z}(\mathcal{C})$ *induces an equivalence as pre-modular categories.*

Proof. . [WORK: do proof] □

This equivalence of categories gives the proper interpretation for $\mathcal{Z}(\mathcal{C})$ in the theory of boundaries. If we wanted we could have taken it as a *defn* of $\mathcal{Z}(\mathcal{C})$. We now examine how anyons interact with boundaries to get more module-theoretic properties of the Drinfeld center.

Suppose $\mathcal{C}$, $\mathcal{D}$ are spherical fusion categories, and ${}_{\mathcal{C}}\mathcal{M}_{\mathcal{D}}$ is a bimodule. If a $A \in \mathcal{C}$ is a simple object describing an anyon, we can imagine trying to push A from $\mathcal{C}$ to $\mathcal{D}$ through the boundary theory ${}_{\mathcal{C}}\mathcal{M}_{\mathcal{D}}$:

[WORK: add picture: first its on one side, then a bubble starts to form, then the bubble detaches. It leaves behind a dotted line with label ${}_{\mathcal{D}}\mathcal{M}^{op}_{\mathcal{C}} \boxtimes_{\mathcal{C}} {}_{\mathcal{C}}\mathcal{M}_{\mathcal{D}}$]

Suppose that the domain wall is *invertible*. This means that ${}_{\mathcal{D}}\mathcal{M}^{op}_{\mathcal{C}} \boxtimes_{\mathcal{C}} {}_{\mathcal{C}}\mathcal{M}_{\mathcal{D}} \cong \mathcal{D}$. Thus, the anyon can pass directly through the boundary, and the boundary can re-close without leaving a trace of the fact that the anyon went through.

This gives an assignment of anyons in the $\mathcal{Z}(\mathcal{C})$ to anyons in the $\mathcal{Z}(\mathcal{D})$ phase. This assignement is reversible, because anyons in the $\mathcal{Z}(\mathcal{D})$ phase can pass through the domain wall in the other direction. Thus, our boundary theory predicts that every invertible bimodule ${}_{\mathcal{C}}\mathcal{M}_{\mathcal{D}}$ will induce an equivalence of categories $F_{\mathcal{M}} : \mathcal{Z}(\mathcal{C}) \xrightarrow{\sim} \mathcal{Z}(\mathcal{D})$. We verify this prediction with a theorem. Before we can prove it, we need a lemma.

Lemma 6.2.17. *Let $\mathcal{C}$ be a fusion category. The forgetful functor*

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

is surjective onto the objects of $\mathcal{C}$.

Proof. .[WORK: this proof is steeped in the theory of module categories.] □

Theorem 6.2.18. *Let $\mathcal{C}$, $\mathcal{D}$ be spherical fusion categories. There is a bijection*

$$\begin{pmatrix} \textit{invertible } (\mathcal{C},\mathcal{D})\textit{-bimodule} \\ \textit{categories } \mathcal{M} \end{pmatrix} \overset{\sim}{\longleftrightarrow} \begin{pmatrix} \textit{equivalences of pre-modular} \\ \textit{categories } \mathcal{Z}(\mathcal{C}) \xrightarrow{\sim} \mathcal{Z}(\mathcal{D}) \end{pmatrix},$$

defined by sending a $(\mathcal{C},\mathcal{D})$-bimodule category $\mathcal{M}$ to the functor $F_{\mathcal{M}} : \mathcal{Z}(\mathcal{C}) \to \mathcal{Z}(\mathcal{D})$ defined by

$$\begin{aligned} F_{\mathcal{M}} : \mathcal{Z}(\mathcal{C}) \cong \mathrm{Fun}_{\mathcal{C}|\mathcal{C}}(\mathcal{C}, \mathcal{C}) &\to \mathrm{Fun}_{\mathcal{D}|\mathcal{D}}(\mathcal{D}, \mathcal{D}) \cong \mathcal{Z}(\mathcal{D}). \\ G &\mapsto \left(\mathcal{D} \to \mathcal{M}^{op} \boxtimes_{\mathcal{C}} \mathcal{C} \boxtimes_{\mathcal{C}} \mathcal{M} \xrightarrow{\mathrm{id} \boxtimes G \boxtimes \mathrm{id}} \mathcal{M}^{op} \boxtimes_{\mathcal{C}} \mathcal{C} \boxtimes_{\mathcal{C}} \mathcal{M} \to \mathcal{D}\right) \end{aligned}$$

For all triples $\mathcal{C}$,$\mathscr{K}$, $\mathcal{D}$ of fusion categories, $(\mathcal{C},\mathscr{K})$-bimodules $\mathcal{M}$, and $(\mathscr{K},\mathcal{D})$-bimodules $\mathcal{N}$, we have that

$$F_{\mathcal{M}\boxtimes_{\mathscr{K}}\mathcal{N}} = F_{\mathcal{N}} \circ F_{\mathcal{M}}.$$

If $\mathcal{C}$ and $\mathcal{D}$ are spherical fusion categories, then the assignement $\mathcal{M} \mapsto F_{\mathcal{M}}$ induces a bijection.

[WORK: what is the correct statement? Do I have to reduce the class of bimodules I am considering?]

Remark 6.2.19. This theorem is originally due to Etingof-Nikshych-Ostrik [**?**]. It was observed in the theory of gapped boundaries by Kitaev and Kong [**?**]. The proof presented here is original.

Proof. .[WORK: do proof. The first direct is making sure this is a well-defined map and filling in details. That's not very hard.

The big question is showing that this is a *bijection.* That means that we need an inverse to this map. The inverse is suprisingly cute and nice. The forgetful functor $\mathcal{Z}(\mathcal{C}) \to \mathcal{C}$ induces a $\mathcal{Z}(\mathcal{C})$-bimodule structure on $\mathcal{C}$. Given any equivalence $F : \mathcal{Z}(\mathcal{C}) \xrightarrow{\sim} \mathcal{Z}(\mathcal{D})$, we can thus construct the tensor product

$$\mathcal{C} \boxtimes_{\mathcal{Z}(\mathcal{C})\cong\mathcal{Z}(\mathcal{D})} \mathcal{D}.$$

This tensor product is a $(\mathcal{C},\mathcal{D})$ bimodule. The fact that it is an invertible bimodule uses in a key way the fact that the forgetful functors $\mathcal{Z}(\mathcal{C}) \to \mathcal{C}$ and $\mathcal{Z}(\mathcal{D}) \to \mathcal{D}$ are surjective. It's not hard to show that these two constructions are inverses to one another. This gives the proof.] □

As a corollary we find the following theorem, which was first proved by Kitaev and Muger and communicated by Etingof-Nikshych-Ostrik [**?**]. We recall that two fusion categories $\mathcal{C}$, $\mathcal{D}$ are called *Morita equivalent* if their Drinfeld centers are equivalent as braided fusion categories

[WORK: What is the correct statement of this theorem for spherical fusion categories?]

Corollary 6.2.20. *Two fusion categories $\mathcal{C}$, $\mathcal{D}$ are Morita equivalent if and only if there exists an invertible bimodule category between them.*

Proof. This is clear from Theorem [ref]. □

6.2.7 Muger's theorem and Lagrange's theorem for fusion categories

[WORK: There's some results about Frobenius-Perron dimensions which will play a key role in the proof. Can I use quantum dimension instead? Probably not because I'm not assuming spherical.]

[WORK: Out of all this we get Lagrange's theorem for fusion categories, that given a fusion $\mathcal{C}$ with full subcategory $\mathcal{C}$, the ratio $\mathrm{FPdim}(\mathcal{D})/\,\mathrm{FPdim}(\mathcal{C})$ is an algebraic integer. Do I care? Should I include this? Maybe I should have a section with a proof of Muger's theorem plus a proof of Lagrange's theorem for fusion categories.]

6.2.8 Skeletonization of gapped boundaries

[WORK:To be explicitely workable it is nice to reinterpret gapped boundaries in the skeletal language just like how one does with modular categories. In this case the symbols are M3j and M6j symbols, as discussed in Cong-Cheng-Wang. Not sure if I want to do this, though.]

6.3 Symmetry enriched topological order

6.3.1 Physical picture

[WORK: Two additional good references to read for this stuff are [**?**, **?**]]

[WORK:

This section should give an elementary physical picture of what symmetry enriched topological order. The basic idea is that a topological gap might be closable, but maybe closing it has to break some symmetry! This is easy to explain and motivate.

To talk about the next part, people need some idea about how phase transitions correspond to symmetry breaking. Moreover, it would be nice if it was clear how symmetry breaking corresponds to condensing quasiparticles. Burnell has a very nice quote about this which is mysterious to me:

"In a conventional ordering transition, the order parameter results from condensing a bosonic excitation– for example, the ordering of a magnet can be viewed as the Bose condensation of spinons."

I think that getting the example of the magnet phase transition across would be great. If people can understand the magnet, they can understand everything. I don't understand the magnet yet.

]

[WORK: I would like to include the Curie principle - the symmetry of the causes are to be found in the effects! The symmetries $\mathrm{Aut}^{\otimes}(\mathcal{C})$ are nessecarily interesting objects. Why? Curie principle! The curie principle in this case manifests in the possible defects which can appear. While $\mathcal{C}$ and $\mathcal{C}\otimes\overline{\mathcal{C}}$ might *look* like very similar categories, $\mathcal{C}\otimes\overline{\mathcal{C}}$ may have way more symmetries than $\mathcal{C}$ and hence might look like a better candidate for TQC in this guise

The original reference for the Curie principle is [**?**]. The theory of magnetic space groups gives a quite nice example.]

6.3.2 Haldane spin chain

[WORK:

This section should include the easiest example possible of an SPT phase, or at least one that maximizes simplicity and relevance. I'm sure Kitaev has a nice model. People online say that the Haldane phase of the Heisenberg spin chain is easy but I haven't seen it before so I can't be sure.

]

6.3.3 Twist defects in the toric code

[WORK:

Talk about the toric code. Introduce the twist defects, and show how they work. This gives the main example of an SET phase with its defects nice and visible.]

6.3.4 The algebraic theory of SET phases

In this section, we will introduce the algberaic theory of symmetry enriched topological phases.

[WORK:

Why categorical G-actions? Why G-graded categories? It would be great if I could work up to the picture

$$\mathcal{C} < --confinement, defectification -- > \mathcal{C}_G^\times$$

If I could even get in the fact that there are obstructions that would be awesome. Of course, I can't really prove much. The hope is that I can state everything trivially, and not have to make any big claims...]

[WORK: Another good thing to note is that there are generalizations of the notion of symmetry in this context! In particular we have the work of Cui-Zini-Wang [?]. It's not clear that group actions are the only symmetries which could protect defects.]

[WORK:

A really important theorem in this space is EGNO's observation that Aut and Pic are isomorphic. Does this come up on its own already, or do I need to add this in? I'm hazy now on the physical significance of this isomorphism, and on what categorical level it holds.

Zhenghan made a point to me that noninvertible defects break the theorem (they aren't in the picard group), but the philosophy is still there. Namely, the category (appropriately defined) Pic $(\mathcal{B}_G^\times)$ should be isomorphic to some endomorphism group. The philosophy holds (though I am hazy on it), but there is no known theorem. This is something to look into!]

Definition 6.3.1 (Categorical group action)**.** A *categorical group action* of a finite group G on a fusion category $\mathcal{C}$ is the following data:

1. A function $\rho : G \to \mathrm{Aut}^{\otimes}(\mathcal{C})$;
2. A natural isomorphism of functions of fusion categories

$$\eta_{g,h} : \rho(g) \circ \rho(h) \xrightarrow{\sim} \rho(gh)$$

for all $g, h \in G$.

Such that:

1. The square

$$\begin{tikzcd}
\rho(g_0) \circ \rho(g_1) \circ \rho(g_2) \arrow[r, "\eta_{g_0,g_1}"] \arrow[d, "\eta_{g_1,g_2}"'] & \rho(g_0 g_1) \circ \rho(g_2) \arrow[d, "\eta_{g_0 g_1, g_2}"] \\
\rho(g_0) \circ \rho(g_1 g_2) \arrow[r, "\eta_{g_0, g_1 g_2}"] & \rho(g_0 g_1 g_2)
\end{tikzcd}$$

commutes for all $g_0, g_1, g_2 \in G$.

2. There is an equality of functors $\rho(e) = \mathrm{id}_{\mathcal{C}}$, where $e \in G$ is the identity element[3].

[3]The condition is added for simplicity of notation down the line - the axioms already imply that there is an equivalence $\rho(e) \cong \mathrm{id}_{\mathcal{C}}$.

$\square$

We can similarly define a categorical group action on a spherical fusion category and modular category. Namely, the group of automorphisms is replaced by the group of automorphisms which respect the additional structure, and the natural isomorphisms between those functors are required to respect that extra structure as well. In this case we allow ourselves extra adjectives to emphasize the additonal structure. Namely, we refer to a *braided* categorical group action of a group on a braided fusion category. We can thus give the following physical principle:

$$\text{(Symmetry enriched topological phases)} \iff \left(\begin{array}{c}\text{triples } (\mathcal{C}, G, \rho),\\ \text{where } \mathcal{C} \text{ is a modular category, } G \text{ is a finite group}\\ \text{and } \rho \text{ is a braided categorical group action}\end{array}\right).$$

Algebraically, the physical phenominon of *symmetry breaking* is extremly clear. It is the act of taking a symmetry enriched phase $(\mathcal{C}, G, \rho)$ and passing some subgroup $H \leq G$, yield $(\mathcal{C}, H, \rho|_H)$. Passing all the way to the trivial group yields the ordinary topological phase $\mathcal{C}$.

We now move on to discussing symmetry fractionalization.

[WORK: motivate the answer physically.

It's quite important that NOT every symmetry can be fractionalized. This is where the gauging anomaly shows up. Talk about this.]

Definition 6.3.2 (G-graded fusion category)**.** A *G-graded fusion category* over a finite group G is the following data:

1. A fusion category $\mathcal{C}$;
2. A full subcategory $\mathcal{C}_g$ of $\mathcal{C}$ for each $g \in G$.

Such that:

1. The functor

$$\boxplus_{g \in G} \mathcal{C}_g \xrightarrow{\sim} \mathcal{C}$$
$$(A_g)_{g\in G} \mapsto \bigoplus_{g \in G} A_g$$

is an equivalence of categories;

2. The tensor product on $\mathcal{C}$ restricts to a map $\otimes : \mathcal{C}_g \times \mathcal{C}_h \to \mathcal{C}_{gh}$;
3. (Faithfullness[4]) The subcategories $\mathcal{C}_g$ are nonzero for all $g \in G$.

$\square$

Definition 6.3.3 (G-crossed braided fusion category)**.** A *G-crossed braided fusion category* over a finite group G is the following data:

1. A G-graded fusion category $\mathcal{C}_G^\times$ with g-component $\mathcal{C}_g$;

[4]This condition is not included in the definition by many authors.

2. A categorical group action ρ of G on $\mathcal{C}_G^\times$;

3. A natural isomorphism

$$\beta_{g,A,B} : A \otimes B \to \rho(g)(B) \otimes A$$

for all $A \in \mathcal{C}_g$, $B \in \mathcal{C}_G^\times$, $g \in G$.

Such that:
.[WORK: add compatibility. Namely, heptagon.
Also there's another big one:

$$\rho(g)(\mathcal{C}_h) \subseteq \mathcal{C}_{ghg^{-1}}.$$

]

□

Finally, we arrive at the definition of a G-crossed modular category:

Definition 6.3.4 (G-crossed modular category)**.** A *G-crossed modular category* over a finite group G is the following data:

1. A G-crossed braided fusion category $\mathcal{C}_G^\times$;

2. A spherical structure on $\mathcal{C}_G^\times$;

Such that:

1. .[WORK: the spherical structure should be compatible with the G-crossed braided structure].

2. $\mathcal{C}_e$ is a modular category, where $e \in G$ is the identity element. [WORK: say this nicer. Should I introduce better notation for group elements?]

□

We observe from our definitoins that the identity graded component $\mathcal{C}_e$ of any G-crossed modular category is itself a modular category. The assignment $\mathcal{C}_G^\times \mapsto \mathcal{C} = \mathcal{C}_e$ corresponds to the physical transition from a phase where defects exist and can be freely manipulated, and a phase in which no free defects can be made. This is known physically as *confinement*. This gives us the following picture:

$$\begin{tikzcd}
\mathcal{C} \arrow[r, shift left, "\text{fractionalization}"] & \mathcal{C}_G^\times \arrow[l, shift left, "\text{confinement}"] \\
\substack{\text{modular category} \\ \text{with braided} \\ \text{categorical } G\text{-action}} \arrow[u, squiggly] & \substack{G\text{-crossed} \\ \text{modular category}} \arrow[u, squiggly]
\end{tikzcd}$$

as mentioned, it is not always possible to fractionalize symmetries. We will discuss this in more detail in section [ref].

6.3.5 Gauging symmetries

[WORK: This is the section where I talk about gauging. Not sure how much I would have mentioned it before. First off, it would be nice to talk about gauging from a physical perspective. The end game is to state the maps

$$\mathcal{C}_G^\times < - - condensation, gauging - - > \left(\mathcal{C}_G^\times\right)^G$$

properly. General discussion gauge symmetry breaking phase transition would be nice to talk about. If I could state everything clearly mathematically that would be great.]

Proposition 6.3.5. *Let $\mathcal{C}$ be a fusion category with a categorical G action. Define a category $\mathcal{C}^G$ as follows. It's objects are pairs (A, γ), where $A \in \mathcal{C}$ is an object and*

$$\gamma_{g,A} : \rho(g)(A) \xrightarrow{\sim} A$$

is an isomorphism for all $g \in G$, $A \in \mathcal{C}$ such that

[WORK: add diagram]

commutes. The morphisms in $\mathcal{C}^G$ are morphisms in f such that

[WORK: add diagram]

commutes. [WORK: define the rest of the structure]. This endows $\mathcal{C}^G$ with the structure of a fusion category. We call $\mathcal{C}^G$ the equivariantization of G.

[WORK: the space of possible maps γ making $(n \cdot \mathbf{1}, \gamma)$ an element of $\mathcal{C}^G$ is equivalent to the space of n-dimensional representations of G. To make this canonical, however, one needs to choose a choice of trivialization of $\rho(g)(\mathbf{1})$ for all $g \in G$. That is, an isomorphism $\rho(g)(\mathbf{1}) \cong \mathbf{1}$.

I figured it out. I added the axiom that $\rho(e)$ is the identity. We thus have the distinguished map

$$\begin{aligned}
&\rho(g)(\mathbf{1})\\
&\to \rho(g)(\mathbf{1}) \otimes \rho(e)(\mathbf{1})\\
&\to \rho(g)(\mathbf{1}) \otimes \rho(g)\rho(g^1)(\mathbf{1})\\
&\to \rho(g)(\mathbf{1} \otimes \rho(g^{-1})(\mathbf{1}))\\
&\to \rho(g)(\rho(g^{-1})(\mathbf{1}))\\
&\to \rho(e)(\mathbf{1})\\
&\to \mathbf{1}
\end{aligned}$$

which fixes the issue of canonical trivialization. Should I add this as a footnote maybe? Feels overly technical.]

[WORK: figure out how to pass this lemma through once there's extra structure added onto $\mathcal{C}$.]

Proof. .[WORK: do proof] □

In light of the above proposition, we give the following definition:

Definition 6.3.6 (Internal G-symmetry)**.** An *internal G-symmetry* of a fusion category $\mathcal{C}$ is a fully faithful functor $\mathbf{Rep}(G) \to \mathcal{C}$.

[WORK: I'm realizing that I haven't done much with representation categories up to here. Should I talk about them more? Say some generalities about representation theory?]

Proposition [ref] tells us that every fusion category with a categorical G-action induces a fusion category with an internal G-symmetry. [WORK: give motivation for why this is gauging].

We now discuss *condensation*. As discussed above, condensation should serve as an inverse to gauging. Thus, it should take as an input a category with an internal G-symmetry and output a category with a categorical G-action. We define this procedure as follows:

Proposition 6.3.7. *.[WORK: define equivariantization and assert that it behaves well]*

Proof. .[WORK: do proof] □

We now verify that these two constructions are indeed inverses to one another:

Proposition 6.3.8. *. [WORK: define maps*

$$\mathcal{C} \to (\mathcal{C}^G)_G$$

and

$$\mathcal{C} \to (\mathcal{C}_G)^G.$$

State that these are equivalences of categories. Furthermore, assert that these equivalences of categories go through when we add all of our extra structure back on.

*The principle here is that the data of a G-grading is the same as the data of an internal G-symmetry. This is the "main principle" of Bruguieres and Muger [Bru00, **?**]. A good exposition of it is in [**?**].]*

Thus, combining the results of this section with the ones from the previous section we get the following picture:

[WORK: add picture; gauging, condensing, defectifying, confining]

6.3.6 Obstruction theory, anomalies, and zesting

[WORK: this section is devoted to mathematical results which are neccecary from the first two sections. This might have to be broken up for readability]

[WORK: A lot of the stuff in this section is going to be about graded categories. There needs to be a good discussion of equivariantization and deequivariantization. I suppose there also needs to be some discussion of Tannakian subcategories. Lots of stuff to do - this section could be quite mathematically intricate. I will NOT prove the main obstruction theory theorem from ENO. It would be nice to have a proper statement of it though... Maybe the modern theory of zesting is relevant for a good statement?

The theory of zesting seems to be pretty good. There are several papers which have made major progress on it: it was formally introduced in [**?**]. The paper [**?**] explains how zesting gives MTCs with the same modular data - this could be a good exercise for the end of the section. The paper I care about is [**?**], which allows me to go from solution-to-solution in obstruction theory, realizing the torsor action.]

6.3.7 G-crossed modularity

[WORK:

There's nice stuff to be said about the modular representation of a G-crossed MTC. After the original Barkeshli paper, the follow up paper [?] included a lot of the nice results.

There is a G-crossed verlinde formula - [?]. Seeing as it is new it is not very well known, and could easily be overlooked. I'm sure the proof isn't that bad, and it would be really good to have included. It feels important to me.]

[WORK: Here are some tricks I found useful a few months ago when I was doing this

1. Given any $A \in \mathcal{C}_g$, all other elments of $\mathcal{C}_g$ an be obtained by fusion with an element of $\mathcal{C}_e$;
2. Rank($\mathcal{C}_g$)=# fixed points of $\mathcal{C}_e$ under action of g

is this a good section to include them in?]

6.3.8 Skeletonization of SET phases

.[WORK: I want to list data for SET phases soon, so skeletonization is important. Talk about it. Set it up right. Do it.]

6.4 Fermionic topological order

6.4.1 Physical picture

6.4.2 Kitaev spin chain

[WORK: talk about Kitaev spin chain. Emphasize that bulk defects are fermions! These fermions can interact with the boundary Majorana modes.]

6.4.3 The algebraic theory of fermionic topological order

.[WORK: give the algebraic theory. This should be very easy to set up based on the work I've done in the previous sections.

I should talk about 16 fold way too. Prove that if a gauging exists then there are 16 solutions. State the 16 fold way theorem, but don't prove it. The proof is [?] and it is very deep. Talking to Theo, he emphasizes that the proof is highly nontrivial and is not very physically motivated.]

6.4.4 The 16-fold way on the trivial fermionic theory

.[WORK: Talk about Kitaev's 16-fold way on the trivial fermionic theory.

This means showing that the obstruction vanishes, and then constructing all 16 theories, and saying the relevant things about them.]

6.4.5 Modular representations of fermionic topological order

[WORK:

One easy thing to do is the modular representation of fermionic topological order. It just has a small subtlety (you have to pass to a congruence subgroup for spin structure reasons) but then everything works out! This is shown here: [?].

Maybe there's more to say in this section? Talk about Verlinde formula and other hallmarks of modular categories, but just insofar as they have special applications to fermionic topological order.]

6.4.6 Super-groups and Deligne's theorem

[WORK:

A very important theorem in this area is Deligne's theorem for fusion categories: Every symmetric fusion category is equivalent to the category of representations of a finite group or super-group. The original proof is in [Del02], but that's way too general and I'm sure there are better/more modern proofs for my case.

Depending on how important this theorem is, I might have to move this up. In Theo's paper [?] he talks about Deligne's theorem + his obstruction results gives a complete picture for modularization and gauging away centers. This is an interesting perspective which I would like to include.]

History and further reading:
(Boundaries and domain walls)

The first major work on boundaries in conformal field theory was Cardy's semimal 1989 paper [?]. This work was then reinterpreted in terms of category theory by Fuchs and Schweigert in 2001 [?], who introduced the idea of interpreting boundaries in terms of module-categories and Frobenius algebras. This theory was then generalized by Frohlich, Fuchs, Runkel, and Schweigert to include a categorical description of domain walls as well [?].

In parallel, Bravyi and Kitaev (along with similar work by Freedman and Meyer [?]) studied the toric code with boundary and discovred that it had two different boundary types [?]. In 2008 Bombin and Martin-Delgado defined a version of the Kitaev quantum double model with boundary based on any finite group [?, ?]. In Kitaev and Kong's 2012 paper [?], they generalized this to an arbitary doubled topological order using the Levin-Wen model. They brought the well-established theory of boundaries in conformal field theory to topological order. The full theory of boundaries and domain walls in topological order was then established in 2016 by Cong, Cheng, and Wang [?].

The canonical reference for the theory of module categories is Etingof-Gelaki-Nikshych-Ostrik [EGNO16]. This reference collected a lot of the earlier literature references, such as [?, ENO05, ?].

History and further reading:
(Symmetry enriched topological order)

Many of the most famous examples of topological quantum systems are not topologically ordered systems, but symmetry protected topological systems. The first example of symmetry protected topological order was the Haldane phase of the odd-integer spin chain [**?**], which is protected by SO(3) spin rotation symmetry. Another famous example is that of the topological insulator, which is portected by $U(1)$ phase symmetry and time-reversal symmetry [**?**, **?**]. The existence of these important examples begs for a description in the category-theoretic language.

This mathematical language, however, had to wait for a while. There are lots of subtlties involved, and people were still working out the theory for ordinary topological order. The notion of G-crossed modular category was introduced in Turaev's giant work on homotopy quantum field theory [**?**]. Homotopy quantum field theory was not intended as a physically relevant work - it was mostly a mathematical curiosity, which was worked on because it seemed natural. The theory of G-crossed fusion categories was then applied to the process of orbifolding in confomral field theory [**?**], though most of the semial work such as Etingof-Nikshych-Ostrik's application of obstruction theory to G-crossed categories was still being done as a purely mathematical exercise.

It was not until the work of the work of Barkeshli-Bonderson-Cheng-Wang that G-crossed modular categories were introduced as the correct formalism for symmetry enriched topological order [**?**]. This bridging of the mathematial literature and the physical literature led to a huge amount of progress in the area.

History and further reading:
(Fermionic topological order)

There is a very strong link between fermions and $\mathbb{Z}_2$-gradings. This link was made popular by the discovery of *supersymmetry* in string theory, which mean passing to a $\mathbb{Z}_2$-graded geometry [**?**]. The fact that topological order whose fundamental degrees of freedom are fermionic need special attention was brough to light by Gu, Wang, and Wen, in a series of foundational papers [**?**, **?**, **?**]. The formalism of super-modular categories was introduced in 2017 [**?**]. This paper brought together a lot of the surrounding literature into a coherent physical narrative. The central conjecture of this narrative was the 16-fold way, which was established in 2024 by Johnson-Freyd and Reutter [**?**]

Exercises:

6.1. .[WORK: show that there is a canonical bijection between structures of a left $\mathcal{C}$-module on $\mathcal{M}$ and $\mathbb{C}$-linear monoidal functors

$$\mathcal{M} \to \mathrm{End}(\mathcal{C}).$$

This is a categorical version of the fact that modules and representations are in bijection.]

6.2. . [WORK: people love the Tambara-Yamagami theorem, and consider it to be very deep. One of the original motivation of the algebraic theory of SET phases is that it gives a quick proof! It would thus be nice to have the Tambara-Yamagmi result here as an exercise. [**?**].]

6.3. .[WORK: categorical group actions can be reinterpreted in terms of funtors. Namely, a category group action is a monoidal functor from the categorified version of the group. The categorified version of the group is defined so that it has an object for each group element, its only morphisms are the identity, and its monoidal structure is given by the group law.]

6.4. . [WORK: There is the principle of *modularization*. Here, we take the center (which will be some symmetric fusion category) and "gauge it away". The fact that this is possible comes from our setup of symmetry enriched toplogical order and fermionic topological order. I don't quite see how it is physically relevant. It seems best left here as an exercise.]

6.5. .[WORK: I think that a SFC is abelian if and only if its Drinfeld center is. This would be a nice exercise to include.]

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 [**?**]. 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.

3. There are many topological quantum systems whose algebraic theory is beyond description in terms of modular categories. These phases require increasingly intricate algebraic descriptions, past what is described in this book. [WORK: I'm really talking about *fractons* here. They were introduced in [**?**] and have garnered a lot of interest since. What else is there?]

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 [**?**]. 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:

$$\begin{tikzcd} \text{QC1} \arrow[r, bend left, "\text{efficient simulation}"] & \text{QC2} \arrow[l, bend left, "\text{efficient simulation}"] \end{tikzcd}$$

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 [**?**, **?**]:

> 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 [**?**]. 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 [**?**, **?**]. 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 [**?**] 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.

There's lots of different ways of doing this of course, coming from the work of different authors. One fun and informative way of doing this could be to use *Kliuchnikov's exact synthesis* method. This method is due to [**?**]. Important follow up works are [**?**] and [**?**]. This method is nice because it demonstrates the power of number theory and deep mathematical ideas in topological quantum information. This is a textbook about the algebraic theory, after all!

]

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.]

]

[WORK: Here's some content which was cut from the classical computing section -

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:

$$\begin{array}{cccc} (\text{abelian}) & \binom{\text{nilpotent}}{\text{non-abelian}} & \binom{\text{solvable}}{\text{non-nilpotent}} & (\text{non-solvable}) \end{array}$$
$$\begin{array}{c}\text{more}\\\text{abelian}\end{array} \longleftrightarrow \begin{array}{c}\text{less}\\\text{abelian}\end{array}$$

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], [**?**])	Fundamental limitations coming from intensive circuit-depth requirements, and the size of the. smallest example. ([**?**]).
solvable non-nilpotent	$G = S_3$, symmetric group with $\lvert S_3\rvert = 6$	Universal with tricks. (Chapter [ref], [**?**])	Has yet to be done. There are some inherent difficulties involved. ([**?**])
nilpotent non-abelian	$G = D_4$, dihedral group with $\lvert D_4\rvert = 8$	?	Preliminary experiments have been successful. ([**?**]) [5]
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], [**?**, **?**])	Widely used in most applications. ([**?**, **?**] [**?**, **?**])

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 $|D_4| = 8$ is larger than $|S_3| = 6$.

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.

]

7.4 Computation with the toric code

[WORK: A good (older) reference which I've never read is [**?**]]

7.5 Computation with Ising anyons

.[WORK: universal TQC with Ising twsit defects]

.[WORK: There is a general picture of computing using mapping class group representations on high genus surfaces. This is discussed in its most general form in [**?**]]

.[WORK: I would like this section to include a general disucssion of genons. This includes the fact that the obstruction to gauging vanishes and that they actually behave like genons as we would want them to. The relevant papers are [**?**, **?**, **?**]]

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. (original paper is [**?**], and then [**?**] has big improvements)

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: [**?**].

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. Another thing to know about is intrinsically topological superconductors, c.f. [**?**].]

[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 [**?**, **?**]. Soon, Freedman, Kitaev, Wang, and Larsen wrote a review article about topological quantum computing which formally started the field in 2002 [**?**]. In these early years, these authors and others introduced a number of techniques for universal topological quantum computation [**?**, **?**, **?**]. 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 [**?**, **?**, **?**]. 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 [**?**, **?**, **?**].

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 [**?**, **?**]. 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 [**?**]. After this there are several review articles [**?**, **?**].

Exercises:

7.1. .[WORK: make exercises]

A Odds and ends

[WORK: I'm not sure where to do this, but I'd like to make a little comment about non-semisimple modular categories. There are inherent limits to the applications of MTCs to quantum topology, as shown in these papers [**?**, **?**]. This motives going beyond semisimplicity.

A nice paper about this from Zhenghan's perspective is [**?**].

The canonical reference is [**?**]. The summary is that "the only physical thing is the derived category". Makes me look at derived categories differently. Another important paper in this area is [**?**].

]

A.1 Topological quantum field theories

A.1.1 Overview

Topological quantum field theory (TQFT) is an important player in the field of topological quantum information. For the purposes of this manuscript, TQFT is treated meerly as a perspective on topological order. TQFT can be connected more directly and deeply to physics using the machinery of effective field theory, which we will not discuss. The TQFT perspective is summarized as follows:

The TQFT perspective: topological order should be studied in terms of the way topological systems react to being put on different manifolds, and by the way they react to topological manipulations on those manifolds.

We now elaborate on what this means. Start with some topological order, perhaps the toric code or some other Kitaev quantum double model. When we refer to *putting the topological order on a manifold*, we mean the following. First, we draw some lattice the manifold, and add Hilbert spaces on the edges of the lattice. Then, we consider the Hamiltonian on the lattice associated with the relevant topological order. This Hamiltonian has a ground space (the zero-energy subspace), which we refer to as the state-space of the topological order on the manifold.

Thus, associated to every two dimensional topological order, we have an assignment from closed surfaces to Hilbert spaces, which sends a surface to its state-space on that surface. We can call this assignment V, depicted below as follows:

[WORK: add picture. Surface with holes, under V, gets assigned a Hilbert space.]

These Hilbert spaces are the basic objects of study in the TQFT perspective. For instance, their dimensions give information about the anyon types and fusion rules of the topological order:

[WORK: add table. V(sphere)=1;

V(torus)= number of anyons types...;

V(two-holdes torus) = $\sum_{a,b,c\in\mathcal{L}}(N_c^{a,b})^2$.]

[WORK: I think that I should add a heuristic derivation of these state-space dimensions. I want to use the example of the two-holed torus, and not having a basis is causing me trouble.]

Of course, without any additional structure there is no information in a vector space beyond its dimension. For this reason, to make the TQFT perspective useful one must consider not only the dimensions of these vector spaces but also the way they react to topological manipulations of manifolds. In the remainder of this appendix, we will dicuss exactly what these extra manipulations are, use them to define an object called a TQFT, and explore the ramifications of this perspective.

A.1.2 Dehn twists in the toric code

In the TQFT perspective, we are interested in studying the way that state-spaces of topological order on different manifolds behave under topological manipulations. We illustrate the sort of topological manipulations we are interested in though a paradigmatic example, a *Dehn twist* on the torus, illustrated below:

[WORK: dehn twist on torus, decomposed into cut, twist, and glue.]

The crucial point is that this topological manipulation on the torus induces a linear transformation on the state-space of any topological order on the torus. The TQFT perspective says that studying the linear transformation on the state-space of the torus induced by the Dehn twist is a good thing to do.

We now describe this induced linear transformation, using the explicit example of the toric code. Consider a square lattice on the torus, with qubits placed at edges, equipped with the toric code Hamiltonian. The Dehn twist on the torus is a continuous map from the torus to itself. Acting on the level of lattices, the Dehn twist sends the old lattice to a new lattice as follows:

[WORK: use four-by-four square lattice, write out Dehn twist action explicitely.]

We make a few observations. Firstly, we observe that the permutation on the level of lattice sites induces a linear map on the level of Hilbert spaces. Just like how there is a linear "swap" map $\mathbb{C}^2 \otimes \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$ which sends $|b_0\rangle \otimes |b_1\rangle$ to $|b_1\rangle \otimes |b_0\rangle$, there are linear maps on any tensor-product Hilbert space induced by permuting the components.

Secondly, we observe that the Hamiltonian is *not* invariant under this linear map. This is an immediate corrolary of the fact that the lattice edges are not invariant under the map, and thus plaquette terms which used to act on square faces now act on slanted parallelograms. However, the new Hamiltonian is still manifestly a toric code Hamiltonian, just associated to a different lattice. Thus, the ground space of the old Hamiltonian and the new Hamiltonian are both canonically isomorphic to $\mathbb{C}[H^1(T^2;\mathbb{Z}_2)]$. Thus, identifying the ground space of both Hamiltonians with $\mathbb{C}[H^1(T^2;\mathbb{Z}_2)]$, we find that the Dehn twist induces a linear map

$$\mathbb{C}[H^1(T^2;\mathbb{Z}_2)] \to \mathbb{C}[H^1(T^2;\mathbb{Z}_2)].$$

This linear map can be described entirely explicitely. [WORK: describe the map.]

A.1.3 Defining TQFT

We saw in the last section that some topological transformations on surfaces induce linear maps on the state-space associated to those surfaces under a topological order. In general, we can associated linear maps on state-space to any self-homeomorphism $f : M \to M$ of a surface M.

The induced linear map on state-space is the the same as before. To define state-spaces, we choose a lattice on M. The function f induces a map from this lattice on M to a new lattice. This new lattice has a new Hamiltonian associated with it, in the same topological order. Since the ground states of a topologically ordered Hamiltonian do not depend on the details of the lattice and only on the topology of the manifold, the state-space of the original lattice can be canonically identified with the state-space of the new lattice. Permuting the tensor factors in the Hilbert space via f, we thus get a linear map from the vector space $V(M)$ to itself.

We observe that any two maps $f : M \to M$ which can be continuously deformed from one to another will indcue the same linear map on $V(M)$. This is for the following reason. Suppose that $f_0, f_1 : M \to M$ can be deformed from one to the other. As f_0 deforms to f_1, the image of the lattice will deform continuously as well. This means that the image of the lattice under f_0 and f_1 will be isomorphic as lattices, and thus the maps induces by f_0 and f_1 will be the same. [WORK: add some detail to this argument, it feels too loose.]

Thus, every element of the *mapping class group* of M induces a map $V(M) \to V(M)$, where the mapping class group is defined as the space of self-homeomorphisms $f : M \to M$ modulo continuous deformations:

$$\mathrm{MCG}(M) = (\text{self-homeomorphisms } f : M \to M\ )/(\text{continuous deformations}).$$

The summary of the above dicussion is that assocaited to every topological order we have representations

$$\rho_M : \mathrm{MCG}(M) \to \mathrm{Aut}(V(M))$$

for every surface M. These representations admit a much more fine-grained study of topological order than just the dimensions of $V(M)$.

Of course, not every collection of mapping class group representations will be induced by some topological order. These is a compatibility condition between the mapping class group representations of different surfaces. This compatibility condition comes from the following observation. Suppose we are given two surfaces Σ_g, $\Sigma_{g'}$ of genus g and g' respectively. There is a topological transformation one can do to go from the disjoint union $\Sigma_g \sqcup \Sigma_{g'}$ to the surface $\Sigma_{g+g'}$ of genus $g + g'$. This goes as follows. First, we take our surfaces Σ_g, $\Sigma_{g'}$. Then, we cut small holes into each of them. Then we connect these holes by gluing in a cylinder. This process is shown below:

[WORK: add process showing fusion of Σ_g, $\Sigma_{g'}$ to $\Sigma_{g+g'}$.]

Like with self-homeomorphisms, this process induces a linear map on vector spaces. [WORK: The details of this linear map are more subtle than before. My way of doing it is to use local purfiability to trace out a little bit extra, and then glue in a cylinder of the reference state in the vaccuum sector. Not sure what the most elementary way of saying/doing this is...]

In quantum mechanics, the Hilbert space associated with two combined systems is the tensor product of their Hilbert spaces. Thus, the state-space Hilbert space associated with $\Sigma_g \sqcup \Sigma_{g'}$ is $V(\Sigma_g) \otimes V(\Sigma_{g'})$. Thus, the cutting-and-gluing process gives a linear map we call $Z_{g,g'}$:

$$Z_{g,g'} : V(\Sigma_g) \otimes V(\Sigma_{g'}) \to V(\Sigma_{g+g'}).$$

[WORK:

I want to say a little bit about $Z_{g,g'}^\dagger$. It is described geometrically by projecting onto the space of states with trivial charge around the annulus connecting Σ_g and $\Sigma_{g'}$ in the connect sum, tracing out the cylinder, then filling in the holes. The key point to observe is that $Z_{g,g'}$ is an isometric embedding. That is,

$$Z_{g,g'}^\dagger \circ Z_{g,g'} = \mathrm{id}_{V_g \otimes V_{g'}}\,.$$

]

[WORK: This map should be

$$\begin{aligned}\mathbb{C}[\mathcal{L}] \otimes \mathbb{C}[\mathcal{L}] &\to \sum_{a,b,c\in\mathcal{L}} B(V_c^{a,b}) \\ |a\rangle \otimes |b\rangle &\mapsto \sum_{c\in\mathcal{L}} \sqrt{\frac{d_c}{d_a d_b}}\,|\mathrm{id}_{V_c^{a,b}}\rangle\end{aligned}$$

but I don't have the setup for this to be a substantive statement yet.]

Every element of $\mathrm{MCG}(\Sigma_g) \times \mathrm{MCG}(\Sigma_{g'})$ induces an element of $\mathrm{MCG}(\Sigma_{g+g'})$ as follows. Think of $\Sigma_{g+g'}$ as Σ_g connecting with a cylinder to $\Sigma_{g'}$. Then, a pair $(f, f') \in \mathrm{MCG}(\Sigma_g) \times \mathrm{MCG}(\Sigma_{g'})$ acts on $\Sigma_{g+g'}$ by first removing the cyliner, then acting by f on Σ_g and by f' on $\Sigma_{g'}$, and then by reattacing the cylinder at the new locations of the holes. Finally, so that the image of this map is the same as the original manifold, the cylinder is slid across the manifolds back to its original location. The final step of this process is ambiguous because the cylinder could be slid multiple ways, but all of these ways are equivalent up to deformations and thus we get a well-defined element of $\mathrm{MCG}(\Sigma_{g+g'})$.

We can now put all of the maps we have defined together into a commutative diagram which gives the compatibility between the different mapping class group representations. Our maps between $V_g \otimes V_{g'}$ and $V_{g+g'}$ come together to give a map

$$\begin{aligned}\mathrm{Aut}(V_g \otimes V_{g'}) &\to \mathrm{Aut}(V_{g+g'}), \\ h &\mapsto Z_{g,g'} \circ h \circ Z_{g,g'}^\dagger\end{aligned}$$

which is a group homomorphism because $Z_{g,g'}^\dagger \circ Z_{g,g'} = \mathrm{id}_{V_g \otimes V_{g'}}$. All these maps fit into the below diagram, which is immediately seen to be commutative after expanding the definitions:

$$\begin{tikzcd}
\mathrm{MCG}(\Sigma_{g+g'}) \arrow[r, "\rho_{g+g'}"] & \mathrm{Aut}(V_{g+g'}) \\
\mathrm{MCG}(\Sigma_g) \times \mathrm{MCG}(\Sigma_{g'}) \arrow[u, hook] \arrow[r, "\rho_g \otimes \rho_{g'}"] & \mathrm{Aut}(V_g \otimes V_{g'}) \arrow[u, hook, "Z_{g,g'}^\dagger \circ (-) \circ Z_{g,g'}"']
\end{tikzcd}$$

Of course, the above analysis has no been rigorous. It can't be, since we do not have a rigorous definition of topological order! However, what we can do now is *define* a TQFT in terms of this data we have constructed. Namely, we have the following:

Definition A.1.1 (TQFT)**.** A *topological quatum field theory* (TQFT) is the following data:

1. A collection of Hilbert spaces V_g for every integer $g \geq 0$;

2. A unitary representation

$$\mathrm{MCG}(\Sigma_g) \to \mathrm{Aut}(V_g)$$

for every $g \geq 0$;

3. Linear maps

$$Z_{g,g'} : V_g \otimes V_g \to V_{g+g'}$$

for all $g, g' \geq 0$

Such that:

1. $V_0 = \mathbb{C}$;

2. For all $g, g' \geq 0$,

$$Z_{g,g'}^{\dagger} \circ Z_{g,g'} = \mathrm{id}_{V_g \otimes V_{g'}}\ .$$

3. For all $g, g' \geq 0$, the diagram

$$\begin{tikzcd} \mathrm{MCG}(\Sigma_{g+g'}) \arrow[r, "\rho_{g+g'}"] & \mathrm{Aut}(V_{g+g'}) \\ \mathrm{MCG}(\Sigma_g) \times \mathrm{MCG}(\Sigma_{g'}) \arrow[u, hook] \arrow[r, "\rho_g \otimes \rho_{g'}"] & \mathrm{Aut}(V_g \otimes V_{g'}) \arrow[u, hook, "Z_{g,g'}^{\dagger} \circ (-) \circ Z_{g,g'}"'] \end{tikzcd}$$

commutes.

4. .[WORK: I bet I need more axioms. What are they?]

A.2 Quasitriangular weak Hopf algebras

[WORK:

Weak Hopf algebras were introduced in **??**. A good early source about them is [**?**].

Weak Hopf algebras are relevant to the algebraic theory of topological quantum information because the representation category of a weak Hopf algebra is a fusion category. Adding more structure to the weak Hopf algebra gets you all the way up to modular categories. This is Tannaka duality in action. The reference for tannaka duality for modular categories is [**?**].

They are also intimately linked to the theory of module categories. This was first established in [**?**], and then was shown much more explicitely in [**?**].]

A.3 Quantum groups

A.4 Subfactors

A.5 Vertex operator algebras

[WORK:

The connection between vertex operator algebras and topological order comes through conformal field theory. VOAs are at their heart tools for conformal field theory. Of course, since algebraically conformal field theory and topological field theories are so similar, this means that well beahved VOAs describe topological order.

This was first proved in the landmark paper of Huang [**?**]. Of course, there are versions for G-crossed and fermionic theories - [**?**, **?**].

One very nice thing to be aware of is the work of Nikita Sopenko. He is able to prepare topologically ordered states using vertex operator algebras, thus realizing the implicit program in the topological order interpretation of Huang's work [**?**].

A big thing in all of this is the Kazhdan-Lusztig correspondence, which I do not understand very well. A great reference seems to be [**?**].

]

B Anyon data

B.1 Low-rank modular categories

.[WORK: list of all low-rank MTCs.
The relevant papers are [**?**, **?**].]

B.2 Abelian modular categories

.[WORK: classification of abelian MTCs, give data for a lot of examples]

B.3 Group-theoretical modular categories

.[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 [**?**]. Maybe $SU(2)$ quantum group MTCs for various roots of unity would be nice too.]

.[WORK: I would also like to add some fermionic modular categories and symmetry enriched modular categories. Where should I put those?]

[WORK:
List of things to add:

- A big "physics-math dictionary" which allows the translation of everything;
- A table of notation;

]

References

[BK$^+$01] Bojko Bakalov, Alexander A Kirillov, et al. *Lectures on tensor categories and modular functors*, volume 21. American Mathematical Society Providence, RI, 2001.

[Bon21] Parsa Bonderson. Measuring topological order. *Physical Review Research*, 3(3):033110, 2021.

[BR22] Matthew Buican and Rajath Radhakrishnan. Galois orbits of tqfts: symmetries and unitarity. *Journal of High Energy Physics*, 2022(1):1–73, 2022.

[Bru00] Alain Bruguieres. Catégories prémodulaires, modularisations et invariants des variétés de dimension 3. *Mathematische Annalen*, 316(2):215–236, 2000.

[CG93] Antoine Coste and Terry Gannon. Remarks on galois symmetry in rational conformal field theories. Technical report, P00019855, 1993.

[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.

[Del02] Pierre Deligne. Catégories tensorielles. *Mosc. Math. J*, 2(2):227–248, 2002.

[DHW13] Orit Davidovich, Tobias Hagge, and Zhenghan Wang. On arithmetic modular categories. *arXiv preprint arXiv:1305.2229*, 2013.

[EGNO16] Pavel Etingof, Shlomo Gelaki, Dmitri Nikshych, and Victor Ostrik. *Tensor categories*, volume 205. American Mathematical Soc., 2016.

[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.

[FM11] Benson Farb and Dan Margalit. *A primer on mapping class groups (pms-49)*, volume 41. Princeton university press, 2011.

[Gal14] César Galindo. On braided and ribbon unitary fusion categories. *Canadian Mathematical Bulletin*, 57(3):506–510, 2014.

[GdLHJ12] Frederick M Goodman, Pierre de La Harpe, and Vaughan FR Jones. *Coxeter graphs and towers of algebras*, volume 14. Springer Science & Business Media, 2012.

[GN08] Shlomo Gelaki and Dmitri Nikshych. Nilpotent fusion categories. *Advances in Mathematics*, 217(3):1053–1071, 2008.

[GS19] Terry Gannon and Andrew Schopieray. Algebraic number fields generated by frobenius-perron dimensions in fusion rings. *arXiv preprint arXiv:1912.12260*, 2019.

[Hua08] Yi-Zhi Huang. Vertex operator algebras and the verlinde conjecture. *Communications in Contemporary Mathematics*, 10(01):103–154, 2008.

[JMNR21] Corey Jones, Scott Morrison, Dmitri Nikshych, and Eric C Rowell. Rank-finiteness for g-crossed braided fusion categories. *Transformation Groups*, 26(3):915–927, 2021.

[Kit06] Alexei Kitaev. Anyons in an exactly solved model and beyond. *Annals of Physics*, 321(1):2–111, 2006.

[KJ96] Alexander Kirillov Jr. On an inner product in modular tensor categories. *Journal of the American Mathematical Society*, 9(4):1135–1169, 1996.

[KL09] Louis H Kauffman and Samuel J Lomonaco. Topological quantum information theory. In *Proceedings of Symposia in Applied Mathematics*, volume 68, 2009.

[KPEB18] Markus S Kesselring, Fernando Pastawski, Jens Eisert, and Benjamin J Brown. The boundaries and twist defects of the color code and their applications to topological quantum computation. *Quantum*, 2:101, 2018.

[KZ22] Liang Kong and Zhi-Hao Zhang. An invitation to topological orders and category theory. *arXiv preprint arXiv:2205.05565*, 2022.

[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.

[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.

[MS12] Scott Morrison and Noah Snyder. Non-cyclotomic fusion categories. *Transactions of the American Mathematical Society*, 364(9):4713–4733, 2012.

[Müg02] Michael Müger. On the structure of modular categories. *arXiv preprint math/0201017*, 2002.

[PSYZ23] Julia Plavnik, Andrew Schopieray, Zhiqiang Yu, and Qing Zhang. Modular tensor categories, subcategories, and galois orbits. *Transformation Groups*, pages 1–26, 2023.

[Reu23] David Reutter. Uniqueness of unitary structure for unitarizable fusion categories. *Communications in Mathematical Physics*, 397(1):37–52, 2023.

[RT91] Nicolai Reshetikhin and Vladimir G Turaev. Invariants of 3-manifolds via link polynomials and quantum groups. *Inventiones mathematicae*, 103(1):547–597, 1991.

[Sim23] Steven H Simon. *Topological quantum.* Oxford University Press, 2023.

[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.

[Vaf88] Cumrun Vafa. Toward classification of conformal theories. *Physics Letters B*, 206(3):421–426, 1988.

[Ver88] Erik Verlinde. Fusion rules and modular transformations in 2d conformal field theory. *Nuclear Physics B*, 300:360–376, 1988.

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

[Yet92] David N Yetter. Framed tangles and a theorem of deligne on braided deformations of tannakian categories. *Contemp. Math*, 134:325–350, 1992.