Topological Quantum Computation and Protected Gates

by

Sumit Sijher

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Applied Mathematics

Waterloo, Ontario, Canada, 2015

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

I am the sole author of all chapters of this thesis, with the exception of Chapter 7. In Chapter 7, the paper *"Protected gates for topological quantum field theories"* is presented in which I am a co-author. The other co-authors of this work are Michael E. Beverland, Oliver Buerschaper, Robert Koenig, Fernando Pastawski, and John Preskill. Although credit must be given to the others, this author would like to note their own contributions to the work. This work was originally initiated without this author, and some results and general development of the theory to classify protected gates was already achieved; namely, the background theory and Chapter 7.3 were essentially complete in addition to initial attempts at characterizing protected gates for abelian models. The particular contributions of this author were more focused on theory building for characterizing protected gates for non-abelian models and developing methods for analyzing the case of the n-punctured sphere. Moreover, personal efforts were invested in carrying out the explicit calculations made in Section 7.6 regarding nonabelian anyon models. In particular, calculations were made for the Ising model on the n-punctured sphere to arrive at Theorem 7.6.2. In addition to general discussion and editing of the paper throughout the process, this author was responsible for constructing many of the figures that appear in the work.

Abstract

This thesis serves to give a mathematical overview of topological quantum computation and to apply the theory to characterize desirable fault-tolerant operations called protected gates. Topological quantum computation is a novel paradigm for quantum computation which seeks to harness certain exotic quantum systems known as topological phases of matter that exhibit unique physical phenomena such as the manifestation of quasiparticle excitations called anyons. The low energy effective field theories of these systems can be expressed by certain topological quantum field theories, which in turn are described in terms of unitary modular tensor categories that capture the essential properties of a topological phase of matter and its corresponding anyon model. An overview of the relevant category theoretic concepts is given, and the axioms of a unitary modular tensor category are made explicit. A topological quantum field theory is then defined and used to describe topological quantum computation. Having developed the necessary theoretical background, the theory is then applied to characterize protected gates. The main result is a no-go theorem which states that, for any model, the set of protected gates is finite, and hence, cannot be used to do universal quantum computation using protected gates alone.

Acknowledgments

I would like to thank my supervisor Robert Koenig for his guidance and the opportunity that he has provided me for my graduate studies. In addition, I would like to thank my thesis committee members Joseph Emerson and Bei Zeng for their patience and support. This thesis would not have come to be as it is if it were not for my collaborators Michael Beverland, Oliver Buerschaper, Fernando Pastawski, and John Preskill. I was fortunate enough to have the opportunity to work with this group on this project, and am humbled and inspired by their brilliance. Most importantly, I must extend a special thank you and acknowledgment to my family—in particular to my Mother and Father, Harvinder and Charan Sijher, whose love and support is the ultimate reason I have come this far. To all these people I will remain eternally grateful.

Table of Contents

Chapter 1

Introduction

Computation, although often thought about purely in the abstract, ought to be regarded as a physical process. If a computer is to exist in the physical world, then it must be a physical system which conforms to the laws of physics. The question of what can and cannot physically computed then ultimately becomes a question of physics. Quantum computation offers a means of bringing the abstract study of computation into the appropriate context of quantum physics. In this regard, a quantum computer is one that uses some quantum system to encode and process information, and can be thought of as a generalization of classical computation for which classical computation is merely a special case.

There are many paradigms of quantum computation that may differ in their abstract formulation as a model of computation and also by the choice of physical system to be harnessed for quantum computation. These different paradigms have their own pros and cons, and there seems to be no ideal method in practice for enacting quantum computation. Topological quantum computation (TQC) is one such paradigm of quantum computation, which gets its name from the topological nature of both the "hardware" and "software" utilized.

Perhaps the most prevalent feature of quantum systems is their inherent fragility and high sensitivity to unwanted noise. Unlike the seemingly robust nature of the classical world, quantum systems are vulnerable to phenomenon which seem to "destroy" their very own quantum nature. Ideally, one would hope that a working quantum computer would be able to operate without fault, but both intrinsic and extrinsic errors may inflict the system. Intrinsic errors may be caused by imperfect or faulty implementations of certain operations. Moreover, extrinsic errors in the form of external noise due to a quantum computer interacting with its environment may occur. Hence, the need for quantum error correction in order to ensure fault-tolerant computation seems inevitable.

Many quantum error correction protocols exist which strive for fault-tolerance through

active algorithmic means. That is, these protocols require the monitoring and processing of information in order to detect and correct possible errors. Furthermore, the resources required to attempt error correction may themselves be prone to error. A main motivating feature for TQC is that the physical system it utilizes is inherently fault-tolerant to some extent. In addition, the way in which certain operations are to be performed on a topological quantum computer is naturally robust to certain errors. In the context of extrinsic errors, it is often assumed that external noise acts locally on some part of the system, and so satisfactory error correction schemes must have a means of dealing with such local noise. If physical systems can be harnessed which are immune to local noise, then they would make ideal candidates for computation. This is precisely the property that is possessed by the quantum systems exploited in TQC.

The physical systems that a topological quantum computer attempts to harness are referred to as *topological phases of matter*. These are many-body condensed matter systems that exhibit some exotic properties. Such systems are assumed to exist on some effectively two-dimensional surface. The Hamiltonian of these systems is comprised of commuting projectors defined to act on some local region of the surface. In the interesting case, the ground space of this Hamiltonian is a degenerate Hilbert space—meaning, it has dimension greater than one. An important property of the ground space is that its dimension typically depends on the topology of the surface on which the system resides. When considering such Hamiltonians defined on sufficiently sophisticated surfaces, the dimension of the corresponding ground space may increase exponentially. Thus, such spaces can serve as an arena for TQC.

An essential feature of interest that also defines a topological phase of matter is the nature of excited states of the Hamiltonian. These excited states can manifest certain quasiparticles called *anyons* that have some peculiar properties. Its worth noting that anyons are not elementary particles in the traditional sense of the term, but rather an emergent property of the entire state of the system. Yet, there is still some notion of an anyon being localized to some region of space and being able to move around on the surface just as standard particles may. Moreover, anyons may come in different types which can in principle be measured and distinguished through some means.

The anyons that may arise from a topological phase of matter also possess some additional properties pertaining to their dynamics. For instance, in a process referred to as *fusion*, two anyons may be combined (or *fused*) together resulting in another type of anyon which depends on the types of the original anyon. For some anyon models, the fusion outcome may not be unique, and multiple anyons of potentially different types may result. In a process opposite to fusion, a single anyon may also *split* to yield two other anyons of various types.

When anyons are present on a surface, a quantum state can be associated to their configu-

ration, and different configurations of anyons may correspond to different states of the system. Interestingly, certain dynamics of anyons may induce a change in the state of the system. Consider a scenario where two anyons exist at two respective locations of the system, and are made to move around each other to interchange their respective positions and then return to their starting positions. There are associated quantum states corresponding to the initial and final configurations of these anyons. Naively, and quite naturally, one may expect the state of the system before and after such an interchange to be equal by virtue of the initial and final anyon configurations being the same. However, in certain situations (depending on the underlying anyon model and the surface upon which the dynamics take place) these two quantum states may be different. In this way, the process of moving the anyons effectively changes the state of the system. One may be familiar of a similar phenomenon for fermions, where when two fermions undergo such an exchange to return to a symmetric configuration the overall state of the system picks up a -1 factor corresponding to a phase factor of π. For certain anyon types, this phase factor may be some nonzero fraction of π. Hence, in this situation it is said that anyons exhibit *fractional exchange statistics*, and this process of interchange is referred to as "braiding" anyons.

In certain instances, when anyons are present on a surface, the state space of the system may also be degenerate and have dimension greater than 1. If this is the case, then when certain braidings of anyons are executed the corresponding transformation to the underlying state space can be represented as a unitary matrix as opposed to a single phase factor. It is in this fashion that quantum information can be processed if the appropriate dynamical process can be controlled and its action known. When braidings of anyons are performed, it turns out that the overall action on the system is independent of the precise paths traversed by the anyons provided the overall braids are equivalent topologically. Therefore, if slight deviations result in the anyon paths during a braid, say, through some intrinsic or extrinsic error, the overall action on the state space remains the same. Herein lies the essence of topological quantum computation.

To fully understand topological quantum computation, a mathematical theory is needed which characterizes all the relevant anyon dynamics. The theory that will serve this purpose is topological quantum field theory (TQFT), but this theory will in turn be described using category theory. The latter offers a formal and mathematically rigorous means to make precise all the relevant notions in an anyon model.

Many physical theories of the world implicitly refer to models of the three-dimensional physical space in which the entities of interest reside and how this space changes in time. That is, they are theories of conventional space-time. On the other hand, the standard mathematical domain of quantum theory takes place in a Hilbert space, which is not a *physical* space in

the sense of ordinary space-time, but a more abstract mathematical space which describes quantum states. In this regard, quantum field theories offer a way to model quantum mechanical phenomenon while also taking into account that the quantum mechanical entities of interest also exist in some space-time model.

As a mathematical formality, the objective of the quantum field theory is to provide a way of associating appropriate Hilbert spaces to space-time, and transformations of this space-time to transformations of the corresponding Hilbert spaces. However, one's own mathematical liberties offer a choice for what transformations of the space-time manifold are considered. For instance, the theory may consider transformations of space-time that preserve the distance and angles between relative points of the space under some suitable metric; in which case the transformations should be taken as *diffeomorphisms* of the space-time. This general setting is the main domain of standard *quantum field theory*. Perhaps the theory is not concerned with operations that preserve distance, but only the relative angles of points in the space; then *conformal* maps should be used instead of diffeomorphisms, and in this case the theory is said to be a *conformal field theory*. Continuing in this forgetful manner, the theory may not even be concerned with transformations of space-time which preserve both distance and angles, but only preserve the fundamental topology of the manifold. In this latter case, the appropriate transformations are *homeomorphisms* of the manifold, and the theory is referred to as a *topological quantum field theory* (TQFTs, for short). Therefore, in some sense, TQFTs may be regarded as the most fundamental theories when compared to more general quantum field theories since they characterize the most essential features of the theory that are independent or remain invariant under such general topological transformations.

For the purpose of topological quantum computation with anyons, TQFTs become relevant because they offer an effective theory which precisely models the anyonic properties and their dynamics. In particular, a $(2+1)$–dimensional TQFT will be of interest in this thesis, since the anyon dynamics are assumed to take place on some oriented two-dimensional surface (where time plays the role of the third dimension). Before proceeding to give a mathematical definition of a TQFT, some effort will be invested in first developing an algebraic theory of anyons. The main mathematical tool for anyon theory will be category theory, which describes in an algebraic fashion all the data necessary to specify an anyon model. Namely, an anyon model will be described mathematically by a *unitary modular tensor category* (UMTC), which contains within it a very rich structure that captures essential anyonic properties of interest.

Roughly speaking, a TQFT takes the data provided by a particular anyon model and assigns certain Hilbert spaces to various surfaces upon which the anyonic dynamics take place. The mathematical entity which describes this assignment will be referred to a *unitary modular tensor category functor* (UMTC functor) and essentially specifies a particular TQFT given an

anyon model. The surface and certain topological transformations of the surface (called *homeomorphisms*), will get mapped by the UMTC functor to appropriate Hilbert spaces and unitary transformations on this Hilbert space, respectively. More generally, transformations between various surfaces are associated to certain linear transformations between the respectively assigned Hilbert spaces. The UMTC functor is essentially a category theoretic concept, and its role can be thought of as providing a structure-preserving representation of the UMTC that describes the anyon dynamics on surfaces to the category of Hilbert spaces, which itself can be thought of as a UTMC.

Having sufficiently developed the relevant background theory to understand topological quantum computation, the rest of this thesis will serve to characterize certain fault-tolerant operations for topological quantum computation referred to as *protected gates*. The mathematical characterization of these protected gates is essentially done using the underlying topological quantum field theory that models the relevant anyon dynamics. The theory developed for this problem and the results that are obtained are based off joint work done in the paper "Protected gates for topological quantum field theories", which is included as one of the final chapters of this thesis. Thus, the ultimate aim of this thesis it to provide the reader with enough background knowledge and motivation to understand the results on protected gates.

A pictorial overview of the various topics discussed in this thesis, and how they relate to each other is provided in Figure 1.1.

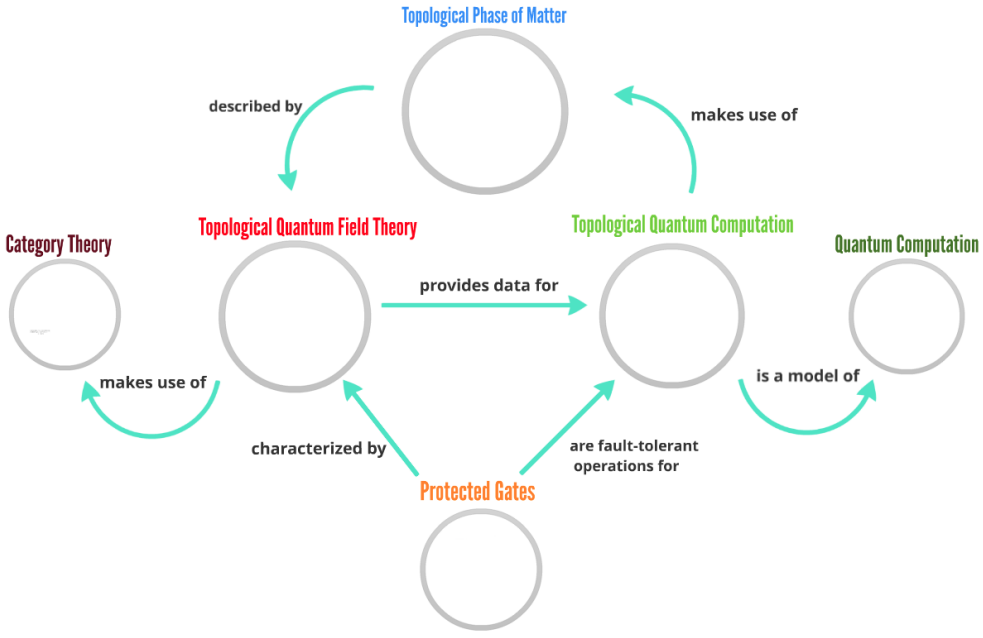


Figure 1.1: A pictorial overview of the topics discussed in this thesis and how they relate to one another.

1.1 Outline

This thesis will initially proceed by introducing a basic example of a topological phase of matter called the *Toric code* in Chapter 2. This section will serve as a primer for topological quantum computation, and introduce some ideas that will be developed more formally throughout the remainder of the thesis. Chapter 3 invests in the relevant background theory to help understand topological quantum computation. For this purpose, Chapter 3.1 defines a category and some other basic notions of category theory. Then Chapter 3.2 proceeds to define a unitary modular tensor category through a series of axioms, while relating the concepts to the various anyon dynamics in the physical picture. Once this is complete, a topological quantum field theory is formally defined in Chapter 3.4. In Chapter 4, a brief investment is made to define some basic concepts from topology. All these theoretical ingredients are then combined to define and understand topological quantum computation in Chapter 5. Having invested in sufficient background theory, the rest of the thesis will then proceed by applying this developed conceptual framework to understand certain fault-tolerant operations for topological quantum computation called protected gates. In Chapter 6, an explicit definition of protected gates is given and the problem of characterizing protected gates is formally stated in Section 6.1. This is followed by an overview in Section 6.2 of the methods developed and the main results in Section 6.3 obtained in the collaborative work presented in the paper *"Protected gates for topological quantum field theories"*. Chapter 7, then supplies this paper verbatim where all proofs, techniques, and results are explicitly described. Following the conclusion in Chapter 8 of this thesis, an Appendix that briefly overviews the stabilizer formalism for purposes of understanding the Toric code is provided.

Chapter 2

The Toric code

2.1 The Toric Code

This section will serve the purpose of exemplifying some essential features of topological quantum computation while also offering both physical and mathematical motivation for the theory to be developed in later sections. The toric code was originally introduced as a paradigmatic example in the pioneering work of A. Y. Kitaev[29], where a more general model for topological quantum computation was also proposed. As the name suggests, the toric code is an example of a quantum error correcting code—in particular, it is a stabilizer code. Moreover, the construction of the toric code involves inherently geometric notions through which unique topological properties become manifest.

Although somewhat pedagogical in character, the description of the toric code given here is presented in the context of the traditional stabilizer framework. The objective is to observe the interplay between the topology and dynamics of anyonic excitations with hopes of demystifying their emergence in the more general theory which is independent of the stabilizer framework. Eventually such low-level, microscopic details pertaining to the Hamiltonian of the system will become irrelevant for the purposes of this thesis, and the main content of this work will proceed in a more high-level fashion using the underlying topological quantum field theory to be developed.

2.1.1 The Hamiltonian

A topological phase of matter is a physical system whose Hamiltonian satisfies certain essential properties. These properties, such as ground space degeneracy with a nonzero spectral gap, and emergent quasiparticles called anyons with fractional exchange statistics, will be characterized

more rigorously throughout what follows. Topology will come into play, because the physical system is assumed to exist on some surface or manifold. For our purposes, the quantum state space of the physical system under consideration will be described by a Hilbert space $\mathcal{H}$ which is the state space of some many-body system. That is,

$$\mathcal{H} = \bigotimes_{j=1}^{N} \mathbb{C}_j^d,$$

where $\mathbb{C}_j^d$ is a d-dimensional complex valued space indexed by j representing some local degree of freedom (i.e. a *qudit* in the quantum information nomenclature).

For the toric code, the physical system will consist of many qubits corresponding to the case $d = 2$. At the physical level these qubits are meant to exist on the surface of the genus-1 torus T. An explicit Hamiltonian $\hat{H}$ for the system will be defined with respect to some discrete triangulation of the torus T. Therefore, there is some notion of geometric locality and what it means for two qubits to be close or interact with one another. Unlike the traditional circuit model, this locality property is essential for the emergence of topological quantum computation. Furthermore, the definition of the Hamiltonian $\hat{H}$ of the physical system $\mathcal{H}$ will depend on the surface topology of T in a fundamental way, and thereby relate the topological phase of matter to the underlying effective topological quantum field theory.

To be more specific, first consider a $k \times k$ square lattice $\mathcal{L}$ consisting of k^2 vertices V and $2k^2$ edges E, which form k^2 square faces F. By identifying the edges along the top of the lattice with the bottom, and the edges along the left side with the right side, the lattice can be thought of as being embedded on the surface of the genus-1 torus (hence the name 'toric' code). Alternatively, the lattice $\mathcal{L}$ can be thought of as having periodic boundary conditions, where a path leaving the lattice from the top side returns to the lattice from the corresponding point on the bottom side of the lattice. Likewise, a path leaving the torus from either the left or right sides would return from the opposite side. Instead of visualizing the lattice on the surface of the torus, this latter picture will be used throughout for convenience.

In the toric code, a qubit is placed on each edge $e \in E$ of the lattice $\mathcal{L}$ so that there are $N := 2k^2$ qubits which comprise the physical system for the $k \times k$ lattice $\mathcal{L}$. Thus, the Hilbert space of the system under consideration is a tensor product of the individual qubit state spaces:

$$\mathcal{H}_N = \bigotimes_{j=1}^{N} \mathbb{C}_{e_j}^2,$$

where the Hilbert space $\mathcal{H}_N$ is parametrized in terms of the number of total qubits N and indexed the qubits by edges $e_j \in E$ of the lattice.

For notational purposes, when some single qubit unitary operator U is applied to only qubit j, write U_j in order to specify the appropriate Hilbert space $\mathbb{C}_j^2$ that U is meant to act on. That is,

$$U_j = I \otimes \cdots \otimes I \otimes U \otimes I \otimes \cdots \otimes I$$

will denote the unitary operator of the whole system $\mathcal{H}_N$ that only applies the single qubit unitary U to the qubit of $\mathbb{C}_j^2$, and acts trivially on all other qubits (here, I denotes the single qubit identity operator on $\mathbb{C}^2$). In this way, the action of the unitary U on the space $\mathbb{C}_j^2 \subset \mathcal{H}_N$ of a single qubit is extended to an operation that acts on the whole space $\mathcal{H}_N$. Therefore, if two single qubit unitaries U and V are to be applied to qubits j_1 and j_2, respectively, it is well defined to simply write this operation as the product $U_{j_1} V_{j_2}$.

Before proceeding with an analysis of the ground space of the system's Hamiltonian, it will be worthwhile to understand some important properties of the operators which comprise the Hamiltonian. There are two basic types of operators that act on the qubits of the lattice which are defined for each vertex and face. These operators will be used to define the Hamiltonian for the toric code, and also yield an algebraic set of operators important for the purpose of error correction — in particular, they will define the stabilizer generators of the toric code. For each vertex $v \in V$ and face $f \in F$ of the lattice $\mathcal{L}$, define the following two operators on $\mathcal{H}_N$:

$$A_v = \prod_{j \in star(v)} \sigma_j^x \quad \text{and} \quad B_f = \prod_{j \in boundary(f)} \sigma_j^z,$$

where σ^x and σ^z are the standard single qubit Pauli operators. Here, $star(v)$ represents the set of 4 edges that meet at vertex v and $boundary(f)$ represents the set of 4 edges that border the face f. In other words, A_v is the operator that applies σ^x to each of the 4 qubits adjacent to vertex v, and B_f is the operator that applies σ^z to each of the 4 qubits that border the particular face f. These operators are illustrated in Figure 2.1 for some particular choice of vertex and face of the lattice.

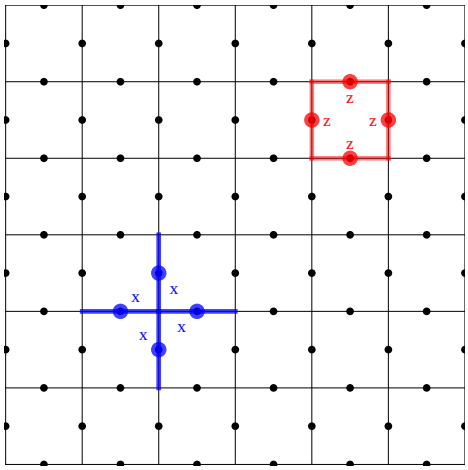


Figure 2.1: The lattice in the toric code has qubits placed on its edges depicted as black dots. The vertex operators A_v applies σ^x operators to the four edges around vertex v, and the face operators B_f applies σ^z operators to the four edges bordering a face f.

The toric code Hamiltonian is then defined as

$$\hat{H} = \sum_{v \in V} \frac{1}{2}(I - A_v) + \sum_{f \in F} \frac{1}{2}(I - B_f), \tag{2.1}$$

where the sums range through all vertices $v \in V$ and faces $f \in F$ of the lattice $\mathcal{L}$. Note that, since both σ^x and σ^z are Hermitian operators, this implies that each A_v and B_f operator is also Hermitian. Consequently, arbitrary sums of these operators will also be Hermitian ensuring that the definition given for $\hat{H}$ is well-defined as a physical Hamiltonian. Moreover, both A_v and B_f have eigenvalues $+1$ and -1. Also, note here that the Hamiltonian has been normalized so that the lowest energy eigenstates of $\hat{H}$ correspond to a state with zero eigenvalue or energy. In what follows, we will be interested in understanding the ground space spanned by zero energy eigenstates of the system, and the spectral gap (or difference in eigenvalues) between the lowest and first excited states.

2.1.2 The stabilizer group

The main claim of this section is that the set of operators

$$S := \langle A_v, B_f \mid v \in V, f \in F \rangle ,$$

generated by all the A_v and B_f operators, forms an abelian subgroup of the N-qubit Pauli group P_N. Then by definition, this commutativity implies that the set S forms a stabilizer group (see Appendix).

That $S \subseteq P_N$ is a subgroup is clear by construction, since each of the A_v and B_f operators are simply tensor products of single qubit Pauli operators acting on the N qubit space $\mathcal{H}_N$. For S to be a stabilizer group it must be the case that each of the A_v and B_f commute with one another. Since A_v and B_p are either products of only σ^x or only σ^z operators, respectively, and because σ^x and σ^z each commute with themselves, it follows that A_v and $A_{v'}$ commute for any vertices v and v', and that B_f and $B_{f'}$ commute for any faces f and f'. However, even though σ^x and σ^z anti-commute with one another, meaning $\sigma^x\sigma^z = -\sigma^z\sigma^x$, it happens to be the case that A_v and B_f do indeed commute for any vertex v and face f. To see this, there are two cases to consider. First, suppose v and f are sufficiently far apart so that there are no qubits in common that are acted on by the operators A_v and B_f. In this case, A_v and B_f trivially commute since the operators σ_j^x and $\sigma_{j'}^z$, with $j \in \mathit{star}(v)$ and $j' \in \mathit{boundary}(f)$, act on different subspaces of $\mathcal{H}_N$.

The only other possibility to consider is when the vertex v happens to be one of the corners of the face f. In this case, there are two distinct qubits in the intersection of $\mathit{star}(v)$ and $\mathit{boundary}(f)$ as shown in Figure 2.2. Each of these two qubits is acted on by σ^x and σ^z, but since $\sigma^x\sigma^z = -\sigma^z\sigma^x$ there are two minus signs that result from the action of A_v and B_f on each of the two qubits which then cancel implying that $A_vB_f = B_fA_v$. Thus, it has been shown that each of the A_v and B_f commute with one another so that the set S generated by their products is indeed a stabilizer group by definition.

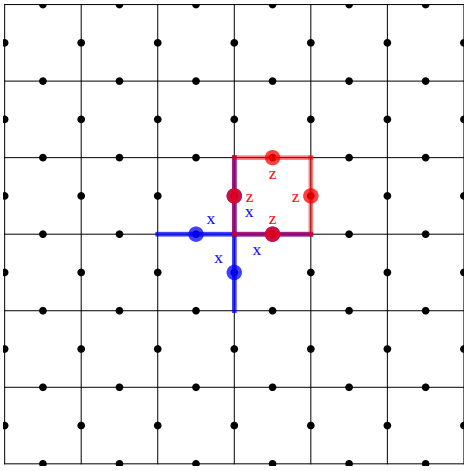


Figure 2.2: Adjacent vertex and face operators commute because they have two edges in common.

It is worthwhile to calculate the number of *independent generators* of S in order to determine further properties of the toric code. A *generating set* of S is a collection of elements of S such that each element of S can be expressed as some product of elements from the generating set.

In addition, it is required that the elements of the generating set be *independent*, meaning that no element of the generating set can be expressed as a product of the other elements of the generating set. Since the elements of S are all expressible by products of the operators A_v and B_f, finding a minimal generating set of S comes down to determining if any of the A_v or B_f operators can be expressed in terms of the others.

In fact, it will now be shown that the following two relationships hold:

$$\prod_{v \in V} A_v = I_{\mathcal{H}_N} \quad \text{and} \quad \prod_{f \in F} B_f = I_{\mathcal{H}_N},$$

where the products range over all vertices $v \in V$ and faces $f \in F$ of the lattice, and $I_{\mathcal{H}_N}$ is the identity operator on the whole space $\mathcal{H}_N$. This is easily seen by noting that for any operator A_v (or B_f) acting on a particular vertex v (or face f) of the lattice, there are four adjacent operators A_{v_i} (or B_{f_i}) where each of the adjacent operators have one edge in common with A_v (or B_f). Therefore, the action of two σ^x (or σ^z) operations on the common edges cancel since $\sigma^x\sigma^x = I = \sigma^z\sigma^z$, which cancels the action of the original A_v (or B_f). Similarly, each of these four vertices v_i adjacent to the original vertex v (or four faces f_i adjacent to the face f) have three other vertices (or faces) adjacent to them not including the original vertex v (or face f). Then the action of the corresponding A_v (or B_f) will cancel the σ^x (or σ^z) operations that act on the shared edges. Continuing in this way, the simultaneous action of every A_v (or B_f) on the lattice will cancel each other resulting in the trivial action $I_{\mathcal{H}_N}$. This pattern is illustrated in Figure 2.3.

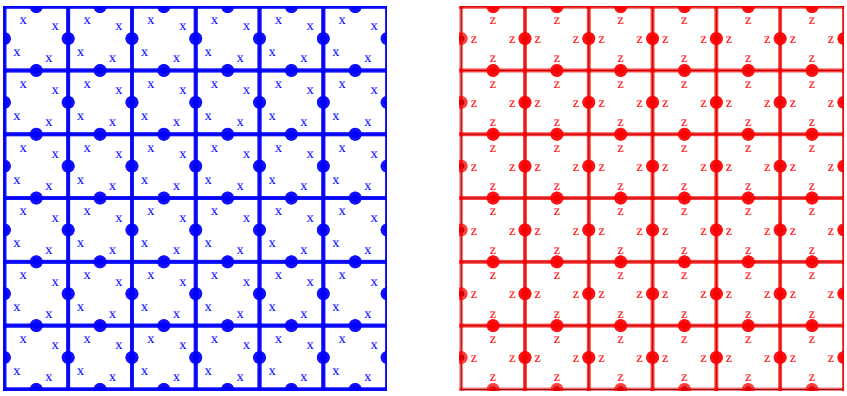


Figure 2.3: The product of all vertex (or face) operators gives the identity $I_{\mathcal{H}_N}$ since each qubit of the lattice is acted on by two σ^x (or two σ^z) operators and $\sigma^{x2} = \sigma^{z2} = I$.

The relationship derived above implies that any single $A_{v'}$ (or $B_{f'}$) can be expressed as the product of all other A_v (or B_f) with $v \neq v'$ (and $f \neq f'$). That is, since $A_v^2 = I_{\mathcal{H}_N}$ and

$B_f^2 = I_{\mathcal{H}_N}$, each A_v and B_f is its own inverse. It then follows that

$$\prod_{v \neq v'} A_v = A_{v'} \quad \text{and} \quad \prod_{f \neq f'} B_f = B_{f'}.$$

Hence, since there are k^2 many A_v operators and also k^2 many B_f operators defined on the $k \times k$ lattice $\mathcal{L}$, there are only $k^2 - 1$ independent operators of each variety. This shows that a minimal generating set for the stabilizer group S consists of $G := 2(k^2 - 1)$ independent elements.

This size of the generating set of S will be relevant when analyzing the *code space* of the toric code to be presented in the next section. The elements of S, and in particular the operators forming the generating set of S, will play a crucial role in the detection of errors or anyonic excitations by serving as *check operators*. Measuring the generators on the qubits of the lattice will (in the ideal case) yield information on whether or not errors have been inflicted on the system, and also serve as means to correct some of the possible errors.

2.1.3 The code space

As described in the previous section, the stabilizer group S generated by the operators A_v and B_f consists of operators that all commute with each other. Therefore, each of the terms in the Hamiltonian $\hat{H}$ also commute with one another. It is a general result in the theory of linear algebra that such a collection of operators can all be simultaneously diagonalized. This implies the existence of a simultaneous eigenspace $\mathcal{H}_g$ corresponding to the groundspace of the Hamiltonian. More precisely, the space $\mathcal{H}_g \subseteq \mathcal{H}_N$ is the vector subspace

$$\mathcal{H}_g := span\{|\psi\rangle \in \mathcal{H}_N : A_v|\psi\rangle = |\psi\rangle, B_f|\psi\rangle = |\psi\rangle \text{ for all } v \in V \text{ and } f \in F\},$$

which is the simultaneous eigenspace spanned by eigenvectors for each A_v and B_f that have eigenvalue $+1$. Recall that such considerations are possible since the A_v and B_f have only eigenvalues $+1$ and -1. In the context of error correcting codes, the subspace $\mathcal{H}_g \subset \mathcal{H}_N$ is called the *code space* of the stabilizer group S. In regards to quantum computation, this space is to be thought of as encoding information that is to remain protected from errors, or processed in some coherent manner. How well suited such a space is, and the computational richness allowed, is determined by the surface topology and Hamiltonian of the model under consideration.

Each of the states $|\psi\rangle \in \mathcal{H}_g$ are states of the entire physical system $\mathcal{H}_N$ consisting of N physical qubits. In the conventional error correcting nomenclature, the states $|\psi\rangle \in \mathcal{H}_g$ are

often called *code words*. If $dim(\mathcal{H}_g)$ is the dimension of $\mathcal{H}_g$, then $N_c := \lfloor log_2(dim(\mathcal{H}_g)) \rfloor$ can be thought of as the maximal number of qubits that are effectively encoded in the code space $\mathcal{H}_g$. For sufficiently nontrivial manifolds, $dim(\mathcal{H}_g) > 1$, and in this case the Hamiltonian $\hat{H}$ is said to have a *groundspace degeneracy*.

There is one remarkable property of the space $\mathcal{H}_g$ which plays a crucial role even for more general models. Unlike the physical state space $\mathcal{H}_N$ which admits a natural tensor product structure in terms of local degrees of freedom, the code space $\mathcal{H}_g$ will in general not permit such a tensor product structure. Instead, the space $\mathcal{H}_g$ is more naturally decomposed in terms of nonlocal degrees of freedom. How this is done will be made more precise in later developments. This property allows such topological models to have a more robust degree of protection from errors, since the information encoded in the state cannot be extracted through local operators, and it is often assumed that noise acts locally. Herein lies one of the motivating features of topological quantum computation.

Of course, now the natural question to ask is how many qubits N_c are encoded by $\mathcal{H}_g$. As consequence of the stabilizer formalism, the number of logical qubits N_c encoded by the space $\mathcal{H}_g$ in general is given by 2^{N-G}, where N is the total number of qubits under consideration and G is the number of independent stabilizer operators that generate S. For the toric code defined on a $k \times k$ lattice $\mathcal{L}$, the number of qubits is $N = 2k^2$ and the number of generators is $G = 2(k^2 - 1)$ as calculated in the previous section. Then the dimension of the code pace $\mathcal{H}_g$ is given by $dim(\mathcal{H}_g) = 2^{N-2(k^2-1)} = 2^2$. Hence $dim(\mathcal{H}_g) = 4$ so that the code space $\mathcal{H}_g$ only encodes $N_c = 2$ logical qubits. Intuitively, this result holds because each independent generator of S can be thought of as halving the dimension of the global space $\mathcal{H}_N$ where $dim(\mathcal{H}_N) = 2^N$. Note that this number N_c does not depend on the characteristic length scale k of the lattice $\mathcal{L}$. This implies that no matter how large the lattice is made in the toric code, the number of encoded qubits always remains the same. This will have interesting consequences when considering the error correcting abilities of the toric code for different lattice sizes.

After describing the properties of anyonic excitations through the manifestation of errors in the toric code, it will be interesting to revisit and analyze the codespace $\mathcal{H}_g$ in order to more explicitly understand the structure of the space in a more topological context. This will also yield an alternate avenue, which is valid for more general models, for calculating the dimension of the groundspace and the form of logical operators acting on the logical qubits.

2.1.4 Errors and anyons

Assume now that the state of the system $\mathcal{H}_N$ is prepared in some ground state $|\psi\rangle \in \mathcal{H}_g$ of the Hamiltonian $\hat{H}$. Then by definition, for any $|\psi\rangle \in \mathcal{H}_g$, measuring the A_v and B_p operators will

all yield eigenvalue $+1$ since $A_v|\psi\rangle = |\psi\rangle$ and $B_f|\psi\rangle = |\psi\rangle$ for all $v \in V$ and $f \in F$. A violation of any of these conditions, meaning some A_v or B_f operator yields an eigenvalue of -1 instead, implies that the state of the system is in some excited state $|\psi'\rangle \notin \mathcal{H}_g$ of the Hamiltonian $\hat{H}$. In the error correcting context, such a violation signals a possible error having occurred on the encoded state $|\psi\rangle \in \mathcal{H}_g$. Thus, errors will be detected by performing *syndrome* measurements using the stabilizer generators A_v and B_f.

The physical nature of various excitations or errors in this model can be understood through the dynamics of certain quasiparticles called anyons that exhibit some peculiar properties. These anyons are not necessarily particles in the traditional sense of an elementary particle, but rather an emergent property of the physical system. Regardless, there is some notion of an anyon being present or localized to a certain region of space. Moreover, the anyons can be mobile and may propagate in space. For a particular model, anyons may come in different physically observable types which can *fuse* or *annihilate* with each other to yield other anyon types or no anyon at all. Alternatively, a single anyon may *split* into multiple anyons of potentially different types. The relative dynamics corresponding to anyons moving around one another (often referred to in the literature as "braiding" anyons) may also enact nontrivial transformations on the underlying state space of the system. In essence, it is through the detection and control of these anyonic excitations of a system by which topological quantum computation is realized.

In this section, an analysis of errors in the toric code will be given to see how some of these anyonic properties manifest themselves. In what follows, the schemes for detecting possible errors occurring on an encoded state $|\psi\rangle \in \mathcal{H}_g$ will initially be described in a case-by-case basis until enough intuition is gathered to describe a more general algebraic structure of the relevant operators acting on the space. In particular, first we will only analyze σ^z errors, and then use this understanding to analogously reason about σ^x errors. It will be the objective of a later section to make these notions more precise and mathematically rigorous so that a more general theory can be applied to arbitrary topological models.

The case of a single σ^z error

Suppose now that some σ_j^z error occurs on qubit j of the lattice (but the location is not known) so that an encoded state $|\psi\rangle \in \mathcal{H}_g$ is transformed into the erred state $|\xi\rangle = \sigma_j^z|\psi\rangle$. In this case, any B_v commutes with σ_j^z as B_v only consists of a product of σ^z operators. Therefore, measuring any of the B_v operators will also return a $+1$ eigenvalue yielding no useful information about the error since

$$B_f|\xi\rangle = B_f\sigma_j^z|\psi\rangle = \sigma^z B_f|\psi\rangle = \sigma^z|\psi\rangle = |\xi\rangle.$$

Any A_v such that v is not one of the two vertices at the end of edge j, will trivially commute with σ_j^z by the mere fact that these operators act on different qubits of the lattice. However, there exists precisely two A_v operators that will anti-commute with σ_j^z: namely, the two A_v that correspond to the two vertices at the ends of edge j. These anti-commute because the A_v operators are in terms of σ^x operators and σ^x and σ^z anti-commute. Hence, when the two A_v operators that act on the qubit on edge j are measured they will give an eigenvalue -1:

$$A_v|\xi\rangle = A_v\sigma_j^z|\psi\rangle = -\sigma^z A_v|\psi\rangle = -\sigma^z|\psi\rangle = -|\xi\rangle.$$

The result of measuring these two A_v operators gives information on exactly which qubit j was inflicted with the σ^z error. Moreover, the error can be corrected by applying σ_j^z to the erred state which returns it back to the original state $|\psi\rangle \in \mathcal{H}_g$.

The pair of vertices at the ends of the edge j corresponding to the location of the σ_j^z error will be thought of as the locations of a pair of anyon excitations. For this, introduce the notation $\textcircled{z}$ to represent a z-type anyon, and place two $\textcircled{z}$ anyons at these two vertex locations as shown in Figure 2.4. In this way, the syndrome measurements given by applying some operator A_v can be thought of as detecting the presence of a $\textcircled{z}$ anyon at that particular vertex.

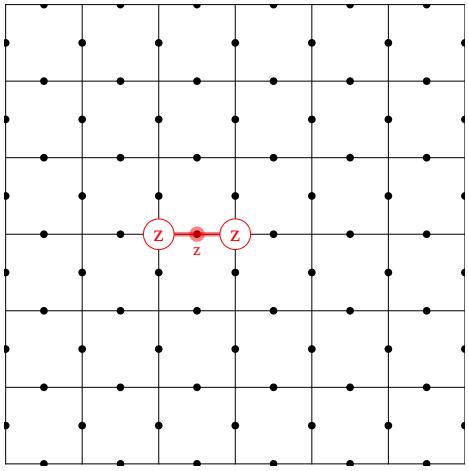


Figure 2.4: A pair of z-anyons are present on the two vertices that uniquely determine the location of a σ^z error acting on a qubit on some edge

The case of a single σ^x error

Instead, suppose now that a single σ_j^x error is inflicted on the qubit located on edge j, but the precise location of j is not known. The detection and correction of such an error proceeds in an analogous manner to the σ_j^z error described in the previous section. This time, the encoded state is transformed into the erred state of the form $|\xi\rangle = \sigma_j^x|\psi\rangle$. Since each of the A_v operators

are comprised of products of σ^x operators as well, they all commute with σ_j^x. Thus measuring each A_v on the lattice gives an eigenvalue $+1$ yielding no information pertaining to the location of the error since

$$A_v|\xi\rangle = A_v\sigma_j^x|\psi\rangle = \sigma^x A_v|\psi\rangle = \sigma^x|\psi\rangle = |\xi\rangle.$$

On the contrary, every B_f operator will commute with the σ_j^x error with the exception of two B_f operators. In this case, the two anti-commuting operators will correspond to the two adjacent faces of the lattice that share the common edge j. Measuring these these two operators leads to the detection of the σ_j^x error due to a -1 eigenvalue:

$$B_f|\xi\rangle = B_f\sigma_j^x|\psi\rangle = -\sigma^x B_f|\psi\rangle = -\sigma^x|\psi\rangle = -|\xi\rangle.$$

Since these two B_f operators correspond to the only adjacent faces next to the error, they uniquely determine the error's location and the error can be corrected by simply applying another σ_j^x operator to bring the erred state $|\xi\rangle$ back to the encoded state $|\psi\rangle \in \mathcal{H}_g$. To signify the presence of this error, a x-type anyon denoted by $\textcircled{x}$ will be introduced. This time, however, two $\textcircled{x}$ anyons will be placed on the two faces adjacent to the location of the σ_j^x error as shown in Figure 2.5. Similar to how the A_v operators are able to detect the presence of a $\textcircled{z}$ anyons representing σ^z errors, the presence of the two $\textcircled{x}$ anyons representing σ^x errors are detected instead by the B_f operators.

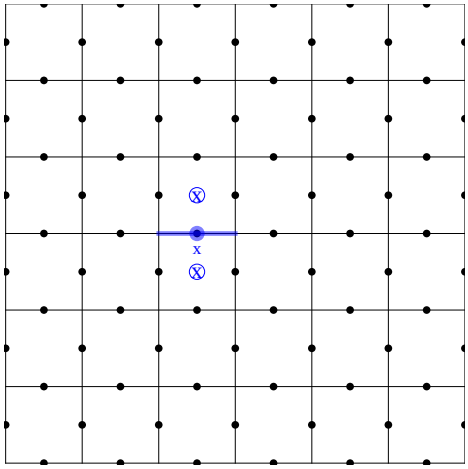


Figure 2.5: A pair of x-anyons are present on the two faces that uniquely determine the location of the σ^x error

Strings of multiple σ^z errors

In the previous section, it was shown how a single σ^z and a single σ^x error can be detected and corrected. This strategy will also work for correcting multiple σ^z and σ^x errors provided

that the errors act on qubits (edges) that are not adjacent (do not share a common vertex). If there happens to be, say, multiple σ^z errors such that the location of the errors forms a chain, or path, as depicted in Figure 2.6, then the error syndrome will be inherently ambiguous and more care must be taken in attempting to correct the errors.

In order to better reason about a chain of adjacent errors, define a *path* $P := \{e_{j_1}, e_{j_2}, \ldots, e_{j_n}\}$ as an ordered sequence of adjacent edges $e_{j_k} \in E$ on the lattice, and introduce the following *string operator*

$$F_z(P) = \prod_{e_j \in P} \sigma_j^z,$$

which applies a σ_j^z along each edge e_j that is a part of the path P. In this way the string $F_z(P)$ represents the case where a sequence of adjacent σ^z errors have inflicted the qubits along the path P on the lattice as shown in Figure 2.6. The case of a σ^z error occurring on a single qubit, as discussed in the previous section, is a special case of a string operator $F_z(P)$ where the path $P = \{e_j\}$ simply consists of a single edge.

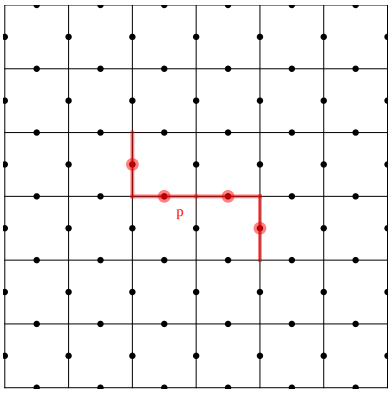


Figure 2.6: An error $F_z(P)$ represents σ^z errors applied to all edges along the path P.

When the string $F_z(P)$ effects an encoded state $|\psi\rangle \in \mathcal{H}_g$ the erred state is of the form $|\xi\rangle = F_z(P)|\psi\rangle$. It will now be shown that detecting the exact locations of all the errors induced by the string $F_z(P)$ using the stabilizer operators A_v and B_f is inherently ambiguous. This is because the stabilizers will only be able to provide information about the two endpoints of the path P, and not uniquely determine the entire path P since there can exist many different paths which happen to share the same endpoints. Naturally, all B_f commute with $F_z(P)$ since B_f consists of σ^z operators, and so will not yield any useful syndrome information. One may be tempted to think that any A_v operator whose vertex v lies on any part of the path P will anti-commute with $F_z(P)$ thereby detecting the presence of all the σ^z errors, but this is not the case. Actually, any A_v whose vertex v lies on the path P with the exception of the two vertices at the endpoints of the path P will also commute with the string $F_z(P)$, because the path P

will always pass through two edges in $star(v)$. For each of these two edges the σ^x from A_v anti-commutes with the error σ^z on that edge producing a -1, but since the other σ^x and σ^z acting on the other common edge also produces a -1 the effect of the two will cancel yielding a trivial syndrome measurement. The only two A_v that manage to detect an error produced by $F_z(P)$ via a -1 syndrome are the two A_v corresponding to the endpoints on edges e_{j_1} and e_{j_n} of the path $P = \{e_{j_1}, e_{j_2}, \ldots, e_{j_n}\}$. These two A_v anti-commute with $F_z(P)$ because A_v and $F_z(P)$ only act on a single common edge in this case. Hence, there are two $\textcircled{z}$ anyons that reside at the endpoints of the path P as shown in Figure 2.7. This exemplifies the important property of the $\textcircled{z}$ anyons that they will always appear as pairs whenever σ^z errors are present.

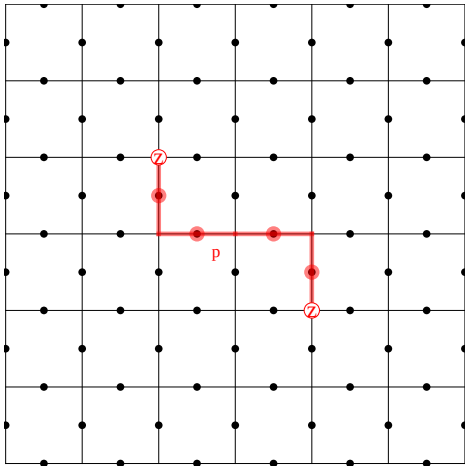


Figure 2.7: Two z-anyons are placed at the endpoints of the error string $F_z(P)$ to signify the vertex locations with nontrivial syndrome measurements

Since the syndrome measurements in the case of a string $F_z(P)$ of σ^z errors only gives information specifying the endpoints of the error string $F_z(P)$, how then are all the errors to be corrected? It would be ideal if the exact path defining the string $F_z(P)$ was known, because then the errors can be corrected by simply applying all the σ^z operators comprising the string. To understand how to overcome this obstacle consider the following.

Since the exact form of the error string $F_z(P)$ is unknown, and only the endpoints of the string can be detected, the best one could do is to guess a path P_g that has the same common endpoints with the actual error path P. Thus, consider some string operator $F_z(P_g)$, where the path P_g has the same endpoints as the actual error path P. Recall that these endpoints are just the locations at which the pair of $\textcircled{z}$ anyons reside. The union of these two paths P and P_g (denoted by the concatenation P_gP) forms a closed loop on the lattice, which we define as a path $L := PP_g = \{e_{j_1}, e_{j_2}, \ldots, e_{j_n}\}$ where the first and last edge are the same: $e_{j_1} = e_{j_n}$. The union of the two paths P and P_g then yields a product of string operators $F_z(L) = F_z(P_g)F_z(P)$.

If the string $F_z(P_g)$ is applied to the erred state $|\xi\rangle = F_z(P)|\psi\rangle$, it is transformed to the state

$$|\xi'\rangle = F_z(P_g)|\xi\rangle = F_z(P_g)F_z(P)|\psi\rangle = F_z(L)|\psi\rangle.$$

Depending on the structure of the loop L it may be the case that $|\xi'\rangle = |\psi\rangle$ implying that the state is returned to its original encoded state. However, it can also be the case that $|\xi'\rangle \neq |\psi\rangle$, but yet $|\xi'\rangle \in \mathcal{H}_g$ is another encoded state in the ground space. In this latter case, the erred state $|\xi\rangle$ is not returned to the original state $|\psi\rangle \in \mathcal{H}_g$. Instead, it is transformed to some other different encoded state $|\xi'\rangle \in \mathcal{H}_g$ and error recovery fails. When this occurs a *logical operation* has been performed on the encoded state—an undesired effect when the objective is to merely preserve the state $|\psi\rangle$. However, it will be shown that such string operators can be used to enact nontrivial operations on the codespace $\mathcal{H}_g$ in a controlled manner. To do this, the topology of loops on the torus must first be understood.

Loops on the torus

The approach described in the previous section, of guessing a string operator $F_z(P_g)$ in hopes of correcting some error caused by the string $F_z(P)$ by forming a loop $L = P_g P$, succeeds depending on the topological nature of the loop L. Since the lattice under considerations is embedded on the surface of a torus, any loop on the lattice comes in essentially two varieties. Whether or not the error is corrected depends on which type of loop is formed in $F_z(L)$.

In general, a loop in a planar region always defines a boundary which partitions the plane into two disjoint parts: an inside and an outside. Such loops can always be contracted to a point on the surface. A loop of this variety will be referred to as a *trivial loop*. On the surface of a torus, or even more generally for higher genus manifolds, this property of a loop being able to contract to a point does not always hold. For instance, closed loops formed around the handle of the torus or around the hole are nonconctractable loops. A noncontractible loop on the torus does not partition the surface of the torus into two disjoint regions, and thus does not have a well defined 'inside' or 'outside'. A loop that cannot be contracted to a single point will be called a *nontrivial* loop. For a torus, there are two such classes of nontrivial loops: ones that loop around the handle of the torus, and ones that loop around the hole. Of course, nontrivial loops may also loop multiple times around the handle or hole the torus in various combinations.

In the lattice picture with periodic boundary conditions representing the surface of a torus, the nontrivial loops may be ones that pass through the periodic boundary on any of the four sides that define the boundary of the lattice. A path on this lattice will form a trivial loop if it never passes through a boundary. Also, if a loop does pass through a boundary, it can still

form a trivial loop provided that it passes back through that same side of a boundary the same number of times before joining itself.

In the next section, it will be shown that the action of the string operator $F_z(L)$ on an encoded state $|\psi\rangle \in \mathcal{H}_g$ is trivial, so that $F_z(L)|\psi\rangle = |\psi\rangle$, if the loop L is trivial. Otherwise, if L is nontrivial, then $F_z(L)|\psi\rangle = |\psi'\rangle$ for some $|\psi'\rangle \in \mathcal{H}_g$ such that $|\psi'\rangle \neq |\psi\rangle$. In this latter case, some logical operation is said to have been enacted on the code space. What operation is performed will depend on the type of nontrivial loop L that defines the string operator.

Correcting σ^z errors

In regards to error recovery, consider some string operator $F_z(L)$ that has been constructed such that L is a trivial loop on the torus. In this case, the loop L forms the boundary of an inner region as shown in Figure 2.8. In this case, $F_z(L)$ can be expressed completely in terms of a certain product of B_f operators as

$$F_z(L) = \prod_{f \in inside(L)} B_f, \tag{2.2}$$

where the (2.2) set $inside(L)$ consists of all the faces inside of the boundary formed by the loop L. This is true because in such a product of B_f operators, any edge inside of the loop is acted on by two adjacent B_f operators so that the action of both of the two σ^z operators on that edge is the identity map. The only participating edges in this product of B_f operators that are acted on nontrivially are precisely those that comprise the loop L. Now, since every B_f is an element of the stabilizer S, the action of $F_z(L)$ on any state $|\psi\rangle \in \mathcal{H}_g$ is trivial. Then if some erred state is of the form $|\xi\rangle = F_z(P)|\psi\rangle$ after the encoded state $|\psi\rangle$ is inflicted with a the string operator $F_z(P)$ acting on some path P, and another guessed string $F_z(P_g)$ is applied so that $F_z(L)$ (where $L = P_g P$) forms a trivial loop, the erred state $|\xi\rangle$ is transformed as

$$F_z(P_g)|\xi\rangle = F_z(P_g)F_z(P)|\psi\rangle = F_z(L)|\psi\rangle = \prod_{f \in inside(L)} B_f|\psi\rangle = |\psi\rangle.$$

This shows that error recovery is successful if the error string is made into a trivial loop.

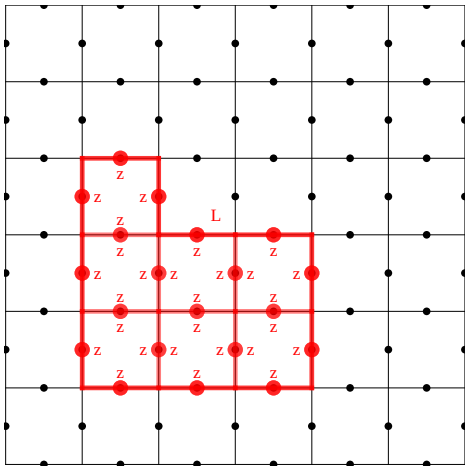


Figure 2.8: A trivial loop L can be expressed as the product of all face operators B_f corresponding to the faces contained inside the boundary formed by the loop.

On the other hand, in the presence of a $F_z(P)$ error string, suppose a string $F_z(P_g)$ was guessed so that the union of the two form a loop string $F_z(L)$ such that $L = P_g P$ is a nontrivial loop. Consequently, The loop L no longer partitions the surface into two disjoint regions. In this scenario, it is impossible to express $F_z(L)$ exclusively in terms of B_f operators as done in the case of a trivial loop. This means that $F_z(L) \notin S$, since it cannot be generated by elements of S. Yet, $F_z(L)$ still commutes with every element of S, because the loop L has no endpoints by definition. More explicitly, for any vertex v on the loop, the loop will always pass through exactly two edges in $star(v)$ making A_v commute with $F_z(L)$. Hence, no element of S is able to detect any of the errors inflicted by $F_z(L)$. Therefore, despite attempting to correct the error on the state $|\psi\rangle \in \mathcal{H}_g$, a logical operation is inadvertently applied to the state transforming it to some other $|\psi'\rangle \in \mathcal{H}_g$ and error recovery fails.

The Dual Lattice

Up until now, the discussion has been mostly focused on σ^z errors and how to correct them. The focus will now shift to correcting strings of σ^x errors. Fortunately, the understanding and intuition developed in the previous sections for the case of σ^z errors naturally extends over to this scenario. This transition will be assisted by considering the *dual lattice* as an abstract aid to reason about σ^x errors.

Relative to the actual square lattice under consideration, the *dual lattice* is the lattice that has vertices at the center of the faces of the main lattice, and has the center of its faces at the locations of the vertices of the main lattice. In the dual lattice, the qubits still reside on the edges and remain in the same location as the main lattice. Naturally, the dual of the dual

lattice is just the main lattice again. The main lattice (in solid lines) and the dual lattice (in dashed lines) are depicted together in Figure 2.9.

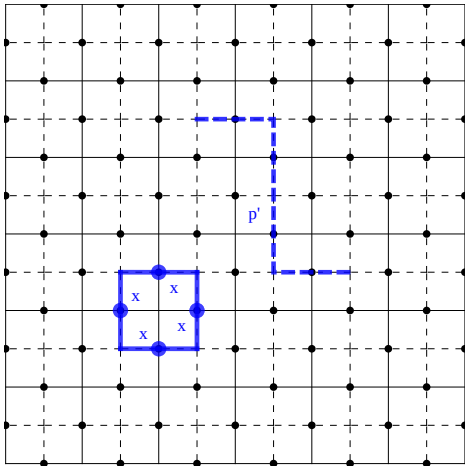


Figure 2.9: The main lattice and the dual lattice are depicted with the dual lattice as dashed lines. A co-path P' of the dual lattice as shown. The vertex operators A_v can be thought of as a face operator on the dual lattice.

The utility in considering the dual lattice comes from being able to reason about σ^x errors analogously to the way σ^z errors were analyzed. Just as paths and loops were considered on the main lattice, paths P' and loops L' will be considered on the dual lattice and will be referred to as *co-paths* or *co-loops*. When displaying figures in the rest of this paper the dual lattice will not be depicted, and co-paths will be drawn as dashed lines as shown in the figure above. One useful consequence of considering the dual lattice is that the vertex operators A_v represented in terms of $star(v)$ on the main lattice can now be perceived as face operators on the dual lattice as shown in Figure 2.9.

Correcting σ^x Errors

Similar to the case of σ^z errors, to represent multiple σ^x errors that are adjacent to each other, define the string operator

$$F_x(P') = \prod_{v \in P'} A_v, \tag{2.3}$$

where the product ranges over vertices v on the co-path P' of the dual lattice. For an open co-path P', a string $F_x(P')$ manifests two $\textcircled{x}$ anyons at its endpoints which lie on the faces of the main lattice. Analogous to the correction of σ^z errors by applying string operators on appropriately chosen paths, the objective of error recovery for σ^x errors will be to appropriately guess co-paths P'_g so that the union $P'_g P'$ forms trivial co-loops on the dual lattice. If $P'_g P'$ is

a nontrivial co-loop, the string operator $F_x(P'_g P')$ applies a logical operation to the encoded state instead.

Any trivial co-loop L' can be expressed in terms of A_v operators as

$$F_x(L') = \prod_{v \in inside(L')} A_v,$$

where now the product ranges over all vertices of the main lattice contained inside of the co-loop L'. Thus, $F_x(L') \in S$ and so acts trivially on any encoded state in $\mathcal{H}_g$. Moreover, any nontrivial co-loop L' lies outside of the stabilizer and so cannot be expressed in terms of the operators in S. However, for a nontrivial co-loop L' the operator $F_x(L')$ commutes with every element of the stabilizer S. Hence, an error of this form cannot be detected by any syndrome measurement. If non-trivial loops of σ^x operators inflict some encoded state to be protected, a logical operation will inevitably be applied and error recovery fails. The reason why this is all the case follows from analogous arguments described in the previous section for σ^z errors.

2.1.5 An error correction protocol

When multiple strings of errors of the same type are present on the lattice, there is an inherent ambiguity of what string operators should be applied in order to correct the errors since the only information that is provided from a syndrome measurement is the locations of the anyons. Any such matching of error strings will result in loops/co-loops (perhaps multiple) on the lattice or dual lattice. Actually, the choice made in this error correction process is somewhat arbitrary. For proper error recovery to take place all that is necessary is for none of the anyons to traverse a nontrivial loop. However, ensuring that error recovery proceeds in this way is still difficult and there is no sure way to guarantee all loops are made trivial. A configuration of errors illustrating this general setting is shown in Figure 2.10. In addition, two other Figures, 2.11 and 2.12, are shown where different guesses are made in an attempt to correct the same configuration of errors. The lighter paths are meant to denote the actual string of errors that were originally present on the lattice. The darker paths represent the paths that were guessed. In both cases, it can be seen that some of the loops formed are trivial loops in which case those particular errors will be corrected, but there are also some nontrivial loops present which result in logical operations being applied to the encoded state.

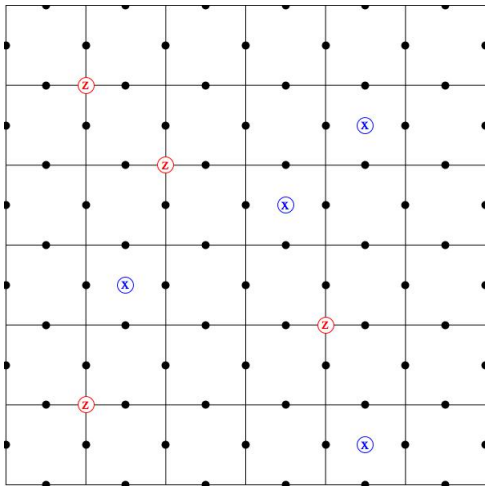


Figure 2.10: In the general case of multiple errors, all that is revealed from the syndrome measurements is the locations of anyon pairs at the endpoints of error strings whose exact shape is unknown.

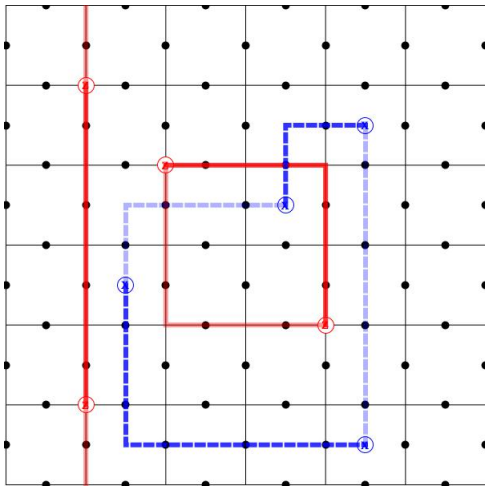


Figure 2.11: A possible correction attempt, where the lighter paths are the actuall error strings, and the darker paths are the guessed paths. All errors in this case are corrected, except for the leftmost string of σ^z errors where a nontrivial loop has been created.

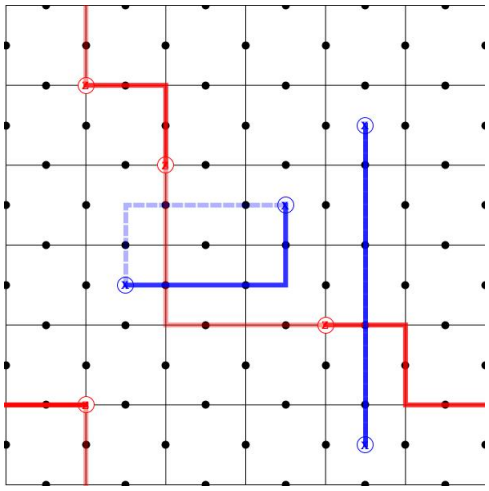


Figure 2.12: Another possible correction attempt, where the lighter paths are the actual error strings, and the darker paths are the guessed paths. All σ^x errors in the case are corrected, but the σ^z error strings have been formed into one nontrivial loop.

The problem of being able to correct multiple errors in the toric code thus reduces to another problem: that of matching error strings accordingly as to only form trivial loops. This is essentially a problem that requires additional post-processing utilizing the information given from the syndrome measurements. The most natural strategy is to guess strings that are of minimal length in fusing the anyon pairs. In the literature, such a strategy is referred to as *minimal weight matching* [14]. One reason why this strategy is justified is because if the probability of a single error occurring on a qubit is small, then it us unlikely that the error strings will be very long. It is more likely that, say, m isolated errors occur at different locations of the lattice resulting in many small-length paths, than it is for all m errors to occur along a single long path of length m. If this is the case, then anyon pairs will tend to stay close to one another. Correcting the errors may then be achieved by connecting anyon pairs that are closest to each other with the appropriate string operator.

For some string $F_z(P)$ or $F_x(P)$ of either σ^z or σ^x errors, define the *length*, or *support*, of the string operator to be the number of edges in the path P defining the string. Then for a $k \times k$ lattice, if some string were to form a nontrivial loop its length must be at least k. This number k is the *code distance* of the toric code. This means that, at least in principle, any error string of length less than k can be detected provided that error recovery proceeds in an appropriate fashion. However, for errors of length greater than k it may not be possible to recover from the error and a logical operation being performed on the encoded state may be inevitable. Let $\lfloor c \rfloor$ denotes the *floor* function defined as the largest integer less than or equal to c. If some error string has length $\lfloor \frac{k-1}{2} \rfloor$, then the error can always be corrected by joining the anyon pair through a minimal length path.

Despite the toric code (as defined on the genus-1 torus) only ever being able to encode 2 logical qubits in the code space regardless of the size k of the lattice $\mathcal{L}$, the benefit of using a larger lattice is apparent. If the probability for an error happening on a single qubit is p, and different errors remain uncorrelated, then it can be seen that the probability of an error string with length k occurring decreases exponentially in k. Thus, the larger the $k \times k$ lattice is made, meaning more physical qubits are used, the more unlikely it becomes for an error string to form a nontrivial loop.

2.1.6 The spectral gap

Now that the nature of possible errors that may occur in the toric code is sufficiently understood, the spectral gap of the toric code Hamiltonian $\hat{H}$ given in (2.1) can be determined. Let $E_0, E_1 \in \mathbb{R}$, be the eigenvalues associated to the ground and first excited states of $\hat{H}$, respectively. Then the spectral gap can be defined as the difference $E_1 - E_0$ between these two eigenvalues. By convention, we have constructed the Hamiltonian $\hat{H}$ of the system so that $E_0 = 0$. Therefore, the quantity of interest is just $E_1 - E_0 = E_1$, which can be determined as the minimal number of vertex and face operators that are violated by an error corresponding to a first excited state of $\hat{H}$.

In the previous section, it was shown that the most primitive errors manifest themselves as pairs of anyonic excitations: either a pair of $\textcircled{z}$ anyons corresponding to a violation of two A_v operators at the endpoints of the error string, or a pair of $\textcircled{x}$ anyons corresponding to a violation of two B_f operators. Thus, denote some first excited state of $\hat{H}$ as $|\psi_1\rangle := F_a(P)|\psi\rangle$, where $|\psi\rangle \in \mathcal{H}_g$, $a \in \{x, z\}$ and P is some open path on the lattice or dual lattice. Then E_1 satisfies $\hat{H}|\psi_1\rangle = E_1|\psi_1\rangle$. Consider the case where $|\psi_1\rangle := F_z(P)|\psi\rangle$ and $v_1, v_2 \in V$ are the endpoints of P. Recall that $A_v F_z(P) = F_z(P)A_v$ for all $v \in V$ such that $v \neq v_1, v_2$. Otherwise, $A_{v_i} F_z(P) = -F_z(P)A_{v_i}$ for $v_i = v_1, v_2$. Moreover, $B_f F_z(P) = F_z(P)B_f$ for all $f \in F$. Therefore, $A_{v_i}|\psi_1\rangle = -|\psi_1\rangle$ for $v_i = v_1, v_2$, and $O|\psi_1\rangle = |\psi_1\rangle$, for all other stabilizer

generators $O \in S$. This implies that

$$\begin{aligned}
\hat{H}|\psi_1\rangle &= \sum_{v\in V}\frac{1}{2}(I-A_v)|\psi_1\rangle + \sum_{f\in F}\frac{1}{2}(I-B_f)|\psi_1\rangle \\
&= \sum_{v=v_1,v_2}\frac{1}{2}(I-A_v)|\psi_1\rangle + \sum_{v\neq v_1,v_2}\frac{1}{2}(I-I)|\psi_1\rangle + \sum_{f\in F}\frac{1}{2}(I-I)|\psi_1\rangle \\
&= \sum_{v=v_1,v_2}\frac{1}{2}(I-A_v)|\psi_1\rangle \\
&= \sum_{v=v_1,v_2}\frac{1}{2}(I+I)|\psi_1\rangle \\
&= 2|\psi_1\rangle,
\end{aligned}$$

which shows that eigenvalue of the a first excited state $|\psi_1\rangle$ is given by $E_1 = 2$. A similar calculation holds for the excited state $|\psi_1'\rangle = F_x(P)|\psi\rangle$ resulting from a string of σ^x errors, which also yields an eigenvalue $E_1 = 2$. Thus, the spectral gap for the toric code Hamiltonian $\hat{H}$ is $E_1 = 2$. In a physical context, this nonzero gap in eigenvalues indicates that some nonzero energy must be imparted into the system in order to transform some ground state to an excited state of the system. This is one reason why the groundspace of $\hat{H}$ may be well suited as a code space for quantum computation.

2.1.7 The anyon model: $\mathbb{Z}_2 \times \mathbb{Z}_2$

An elegant physical interpretation of the nature of errors in the toric code can be given in terms of the anyonic excitations. When the qubits of the lattice encode some state $|\psi\rangle \in \mathcal{H}_g$ which is error free, no anyons are present on the lattice since $|\psi\rangle$ is a $+1$ eigenstate of all stabilzer generators $A_v, B_f \in S$. As a formality, let $\textcircled{1}$ denote the trivial, or *vacuum*, anyon label which is meant to represent the absence of a nontrivial anyon type. In this way, one may imagine the "presence" of the trivial anyon $\textcircled{1}$ at any vertex or face of the lattice; however, such a depiction will not be presented in the figures here and tacitly assumed instead. The groundspace $\mathcal{H}_g$ of the Hamiltonian $\hat{H}$ then corresponds to the scenario where only the trivial anyon type $\textcircled{1}$ is present anywhere on the lattice of the surface, and excited states of $\hat{H}$ correspond to the presence of nontrivial anyon types on the surface.

As mentioned previously, the existence of an open error string $F_z(P)$ results in a pair of $\textcircled{z}$ anyons at the endpoints of the path P. In creating a loop $L = P_g P$ by applying another string $F_z(P_g)$ that starts at one of the end points (where one of the $\textcircled{z}$ anyons is located) and then joining the path to the other endpoint (where the other $\textcircled{z}$ anyon is located), the anyon pair can be thought of as undergoing a dynamical process where a pair of $\textcircled{z}$ anyons is created

from a vacuum state at some location, then one of the anyons moves along the loop L until it returns to *fuse* or *annihilate* with the other to the vacuum. This fusion of a pair of $\textcircled{z}$ anyons to the trivial type $\textcircled{1}$ will be symbolically denoted as $\textcircled{z}\times\textcircled{z}=\textcircled{1}$. Thus, σ^z errors manifest themselves as pairs of $\textcircled{z}$ anyons that reside on the lattice's vertices, and can be made to move around the lattice by applying strings of σ^z operators. The objective of successful error recovery for σ^z errors is not only just to bring these pairs of $\textcircled{z}$ anyons together so they annihilate and disappear to the vaccum $\textcircled{1}$, but to do so in such a way that when they fuse no anyon would have made a non-trivial loop around the torus in order to prevent some logical operation from occurring to the encoded state. Similarly, for anyons of type $\textcircled{x}$ induced by σ^x errors, it is also the case that $\textcircled{x}\times\textcircled{x}=\textcircled{1}$, and an analogous interpretation of their dynamics holds.

In the previous sections, σ^z and σ^x errors were analyzed separately in special cases where only a single string of errors of either type were described. In a more general setting, it is expected that multiple strings of errors of both types can occur on the lattice at any time. Moreover, a particular qubit of the lattice may suffer from both a σ^x and a σ^z error, in which case a $\sigma^y = \sigma^z\sigma^x$ error is produced. In this case, a $\textcircled{y}$ anyon will be introduced and should be thought of as the quasiparticle associated to the pair of $\textcircled{z}$ and $\textcircled{x}$ anyons at that site (a vertex-face pair). Moreover, write $\textcircled{z}\times\textcircled{x}=\textcircled{y}$ to denote the process in which a $\textcircled{z}$ anyon fuses with a $\textcircled{x}$ anyon to form another anyon type $\textcircled{y}$.

Algebraically speaking, the fusion properties of these various anyon types $\mathbb{A} := \{\textcircled{1}, \textcircled{x}, \textcircled{z}, \textcircled{y}\}$ for the toric code can be understood as having some underlying group structure, where the action of fusion $\times : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$ defines the group multiplication on $\mathbb{A}$. In this way, $\textcircled{1}$ is the identity element of the group since $\textcircled{1} \times \textcircled{a} = \textcircled{a}$ for any $\textcircled{a} \in \mathbb{A}$. The inverse, or *conjugate* anyon type, of $\textcircled{a} \in \mathbb{A}$ will be denoted as $\bar{\textcircled{a}}$ and satisfies $\textcircled{a} \times \bar{\textcircled{a}} = \textcircled{1}$. In the case of the toric code, the conjugate anyon type of $\textcircled{a}$ is just itself since $\textcircled{a} \times \textcircled{a} = \textcircled{1}$ for all $\textcircled{a} \in \mathbb{A}$. The only other multiplication relation necessary to completely specify the group structure is the fusion rule $\textcircled{z} \times \textcircled{x} = \textcircled{y}$. Then by assuming that the group multiplication on $\mathbb{A}$ is also commutative, it is readily observed that there is a group isomorphism $\mathbb{A} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, where $\mathbb{Z}_2$ is the cyclic group of order 2.

Later, it will be seen that a general anyon model $\mathbb{A}$ arising from some topological phase of matter corresponding to some Hamiltonian will always carry with it some algebraic structure that represents the fusion properties of the various anyon types. In general, however, this structure will be much richer than that of an ordinary group as in the case of the toric code. To be more precise, the fusion properties of some anyon model will be described by a commutative C^*-algebra, which will be referred to as the *Verlinde algebra*. Additionally, there will be other properties of an anyon model $\mathbb{A}$ which characterize the dynamics of anyons twisting and braiding around one another. The mathematical structure necessary to describe these properties of

anyons is called a *Unitary Modular Tensor Category*, and will be defined in Chapter 3. In regards to topological quantum computation, all of these features play a role in determining the computational power of a particular anyon model.

2.1.8 Logical operations

In general error correcting schemes, a state $|\psi\rangle \in \mathcal{H}_g$ of the code space is prepared and the main objective is to keep the state unchanged. In the presence of errors the state may be mapped outside of the encoded space, and ideally this error can be detected and corrected. This may not always be the case however. Instead, it is possible that the original state get mapped to another state $|\psi'\rangle \in \mathcal{H}_g$ but yet $|\psi\rangle \neq |\psi'\rangle$. In such an occurrence, it was said that the encoded state $|\psi\rangle$ experiences a *logical operation*. The aim of this section is to further characterize the logical operations for the toric code.

For the toric code defined on the physical N-qubit Hilbert space $\mathcal{H}_N$, the N-qubit Pauli group Pauli_N forms an operator basis of an algebra of operators $\mathcal{A} := \{U : \mathcal{H}_N \to \mathcal{H}_N\}$ acting on $\mathcal{H}_N$. Here, we will be interested in the subalgebra $\mathcal{A}_0 \subseteq \mathcal{A}$ that preserves the codespace $\mathcal{H}_g \subseteq \mathcal{H}_N$ defined as $\mathcal{A}_0 := \{U \in \mathcal{A} \mid U|\psi\rangle \in \mathcal{H}_g, \text{ for all } |\psi\rangle \in \mathcal{H}_g\}$. For $U \in \mathcal{A}_0$, write $[U] : \mathcal{H}_g \to \mathcal{H}_g$ to denote the *logical* action of U on the codespace $\mathcal{H}_g$. In particular, this algebra is to be understood in terms of more refined subalgebras defined in terms of string operators associated to various loops of the torus. That is, given an arbitrary loop L defined on the lattice of the torus and anyon type $ⓐ \in \mathbb{A}$, we would like to characterize the logical action $[F_a(L)]$ of string operators on the codespace $\mathcal{H}_g$.

Since the toric code happens to be a particular stabilizer code, the general theory developed for the stabilizer formalism can be used to understand logical operations. Define the centralizer $\mathcal{C}(S)$ of the stabilizer group S as the subgroup of Pauli_N consisting of all elements which commute with those of S. That is,

$$\mathcal{C}(S) := \{u \in \mathsf{Pauli}_N \mid us = su, \text{ for all } s \in S\}.$$

The group $\mathcal{C}(S)$ can be partitioned by considering the equivalence relation $u \sim u'$ if and only if there exists $s \in S$ such that $u' = us$. An equivalence class induced by this relation will be denoted as uS, and is sometimes referred to as a *coset*. By construction, $S \subseteq \mathcal{C}(S) \subseteq \mathsf{Pauli}_N$, and S is a normal subgroup of $\mathcal{C}(S)$ so that the quotient group is well defined as

$$\mathcal{C}(S)/S := \{uS \mid u \in \mathcal{C}(S)\}$$

with corresponding group multiplication $uS \cdot u'S = uu'S$. As operators, each $uS \in \mathcal{C}(S)/S$

defines a logical operation on the codespace $[uS] : \mathcal{H}_g \to \mathcal{H}_g$ in such a way that, if $u \sim u'$, then $[uS] = e^{i\varphi}[u'S]$ so that the two operators yield the same logical action on $\mathcal{H}_g$ up to some unimportant global phase $e^{i\varphi}$. Furthermore, for the identity coset $S \in \mathcal{C}(S)/S$, the logical action is trivial $[S] = I_{\mathcal{H}_g}$.

Returning to string operators for the toric code, recall that as a consequence of Equations (2.2) and (2.3), $F_a(L) \in S$ if L is a topologically trivial loop regardless of the anyon type $ⓐ \in \mathbb{A}$. Therefore, it follows that $[F_a(L)] = [S] = I_{\mathcal{H}_g}$ yields a trivial action on the code space $\mathcal{H}_g$. Actually, it is illuminating to think of the stabilizer generators themselves as string operators $B_f = F_z(L)$ and $A_v = F_x(L')$, where L and L' are the primitive loops or co-loops consisting of the four edges around the face f or vertex v. In this regard, an arbitrary element $s \in S$ can be considered as a product of various string operators $F_z(L)$ and $F_z(L')$ defined on topologically trivial loops L and co-loops L'.

Let L_1 be an arbitrary loop, and consider a trivial loop L_0 such that the intersection of the supports of string operators $F_a(L_0)$ and $F_a(L_1)$ is nonempty. Then since $F_a(L_0) \in S$, it follows that $[F_a(L_1)] = [F_a(L_1)F_a(L_0)]$ so the logical action is equivalent. In this case, the operator $F_a(L_1)F_a(L_0)$ can be interpreted as another string operator $F_a(L_2)$ such that $[F_a(L_2)] = [F_a(L_1)]$, where the loop L_2 is a deformation of the loop L_0 which is of the same topological type. More generally, if L_1 and L_2 are distinct loops belonging to the same topological type, then it will always be the case that $[F_a(L_1)] = [F_a(L_2)]$. Therefore, in order to understand the logical action $[F_a(L)]$ for a string operator defined on an arbitrary loop L, it suffices to characterize the action for only different classes of topologically equivalent loop types.

As argued previously, nontrivial logical operations occurred when a string operator $F_a(L)$ was executed where L is a nontrivial loop and $ⓐ \neq ①$ (since $F_1(L) = I_{\mathcal{H}_g}$ has a trivial action for any loop L). To understand what kind of operations on the encoded state these nontrivial string operators correspond to, recall that there were two types of nontrivial loops on the surface of the lattice: ones that loop around the "handle" of the torus, or ones that loop around the "hole" of the torus. In the lattice picture, one type of loop L_v passes through the 'north-south' boundary, and the other loop L_h through the 'east-west' boundary. Likewise, there were two analogous types of nontrivial co-loops L'_v and L'_h for the dual lattice. However, for our purposes a loop L and its corresponding co-loop L' will be considered as belonging to the same topological type.

For each of these loops, consider the string operators $F_a(L)$ for some nontrivial anyon type $ⓐ \in \mathbb{A}$ and observe the following commutation relations, where for operators A and B we define the commutator as $[A, B] := ABA^{-1}B^{-1}$. For string operators of the same anyon type,

but having support on different loops,

$$[F_z(L_v), F_z(L_h)] = I \qquad \text{and} \qquad [F_x(L'_v), F_x(L'_h)] = I$$

since these string operators are both either products of only σ^z operators or only σ^z operators. Comparing string operators corresponding to different anyon types, but with support on (co)loops of the same topological type,

$$[F_z(L_v), F_x(L'_v)] = I \qquad \text{and} \qquad [F_z(L_h), F_x(L'_h)] = I$$

since in this case the string operators $F_z(L_i)$ and $F_x(L'_i)$ have disjoint support. The only non-commuting string operators are ones that are defined with different anyon types and different loop types

$$[F_z(L_v), F_x(L'_h)] = -I \qquad \text{and} \qquad [F_z(L_h), F_x(L'_v)] = -I,$$

where the $-I$ factor results from the loops L_v and L'_h (and also loops L_h and L'_v) having common support on precisely one edge of the lattice, and from the anticommutation relation $[\sigma^z, \sigma^x] = -I$ between the Pauli operators acting on the qubit associated to that edge.

This analysis of commutation relations shows that logical action of the non trivial string operators on $\mathcal{H}_g$ is isomorphic to the two-qubit Pauli group, $\mathcal{C}(S)/S \cong \mathsf{Pauli}_2$, through the correspondence

$$\bar{X}_1 = [F_x(L'_v)], \qquad \bar{Z}_1 = [F_z(L_h)], \qquad \bar{X}_2 = [F_x(L'_h)], \qquad \bar{Z}_2 = [F_z(L_v)].$$

Here, $\bar{X}_i$ and $\bar{Z}_i$ correspond to logical σ_i^x and σ_i^z operators on qubit i, where $i \in \{1, 2\}$. Consider now the subalgebras of string operators defined as $\mathcal{F}_L := \{F_a(L) \mid ⓐ \in \mathbb{A}\}$ for a nontrivial loop L. Independently, each of the algebras $\mathcal{F}_L$ are isomorphic to the commutative Verlinde algebra given by the fusion rules of the model $\mathbb{A} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Thus, $F_a(L)F_b(L) = F_b(L)F_a(L) = F_{a\times b}(L)$, where $ⓐ \times ⓑ \in \mathbb{A}$ is the result of fusing $ⓐ, ⓑ \in \mathbb{A}$. Note that neither of the subalgebras $\mathcal{F}_{L_v}$ or $\mathcal{F}_{L_h}$ alone contain the full logical Pauli algebra Pauli_2 of the two logically encoded qubits of $\mathcal{H}_g$. Moreover, string operators from both $\mathcal{F}_{L_v}$ and $\mathcal{F}_{L_h}$ are needed to generate the Pauli group for either one of the two logical qubits, which further emphasizes the nonlocal nature of the logical qubit encodings in $\mathcal{H}_g$. Similar properties of string operators and the local algebras $\mathcal{F}_L$ will also hold in the more general setting when considering arbitrary anyon models and higher genus surfaces.

2.1.9 Physical observables and the flux basis of $\mathcal{H}_g$

Any physical theory ought to come equipped with some notion of physical observables which can be measured in principle. In the theory of topological quantum computation, the physical observables correspond to the detection of the total *charge* or *flux* associated to a loop L on the surface under consideration. The flux is given by some anyon type $a \in \mathbb{A}$, or more generally, a superposition of anyon types in $\mathbb{A}$. There are two cases of interest that should be distinguished, depending on whether the loop L is of trivial type as opposed to nontrivial type. Regardless, for an arbitrary loop L there will be associated a projector $P_a(L)$ on the Hilbert space $\mathcal{H}_g$, which defines a subspace of $\mathcal{H}_g$ corresponding to the situation where the state of the system is observed to have flux of type $a \in \mathbb{A}$ on loop L. Moreover, the set of projectors $\{P_a(L)\}_{a\in\mathbb{A}}$ will define a complete set of observables for loop L. Later, it will be seen that these projectors can be represented in a precise way in terms of the string operators $\{F_a(L)\}_{a\in\mathbb{A}}$. For now, some more details about the string operators will be made explicit.

Recall that the stabilizer operators A_v and B_f of the toric code can be thought of as elementary string operators $F_x(L') = A_v$ and $F_z(L) = B_f$ associated to primitive (co)loops on the lattice, which can detect the presence of certain anyon types contained within the loops. In the same way, a string operator defined on an arbitrary trivial loop L, or coloop L', consists of a product of stabilizer generators contained within the region defined by L or L':

$$F_z(L) = \prod_{f\in inside(L)} B_f \qquad \text{and} \qquad F_x(L') = \prod_{v\in inside(L')} A_v.$$

In this case, a string operator $F_a(L)$ can be thought of as detecting the total *charge* or *flux* of anyons present inside the region defined by L. Here, if anyon types $a_1, a_2, \ldots a_m \in \mathbb{A}$ are present inside of some region $inside(L)$, then the total charge is given by the resulting fusion outcome of $a_1 \times a_2 \times \cdots \times a_m \in \mathbb{A}$.

When considering a string operator $F_a(L)$ acting on some nontrivial loop L, there is no well-defined notion of a "region inside L". However, in this setting a flux can still be associated to the loop L, which will be labeled by some anyon type in $\mathbb{A}$ (or more generally, by a superposition of anyon types). For the torus in particular, since there are two complimentary nontrivial loops L_v and L_h which always intersect in at least one location, string operators defined on one loop can be thought of as creating or detecting the flux present on the complementary loop.

Consider one particular nontrivial loop, say L_h, and let $|1\rangle_{L_h} \in \mathcal{H}_g$ label the ground state where loop L_h carries trivial flux. Define

$$|x\rangle_{L_h} := F_x(L_h)|1\rangle_{L_h}, \quad |z\rangle_{L_h} := F_z(L_h)|1\rangle_{L_h}, \quad |y\rangle_{L_h} := F_y(L_h)|1\rangle_{L_h} = F_z(L_h)F_x(L_h)|1\rangle_{L_h}.$$

Then the set $\mathcal{B}_{L_h} := \{|1\rangle_{L_h}, |x\rangle_{L_h}, |z\rangle_{L_h}, |y\rangle_{L_h}\}$ can be taken to be an orthonormal basis of $\mathcal{H}_g$ defined with respect to the string operators $\mathcal{F}_{L_h} := \{F_a(L_h)\}_{a\in\mathbb{A}}$, which will be referred to as the *flux basis* of loop L_h. Alternatively, the other complementary loop L_v of the torus could have been considered together with string operators $\mathcal{F}_{L_v}$ to define a different flux basis given by a state $|1\rangle_{L_v} \in \mathcal{H}_g$ corresponding to loop L_v carrying trivial flux, and three other orthogonal states

$$|x\rangle_{L_v} := F_x(L_v)|1\rangle_{L_v}, \quad |z\rangle_{L_v} := F_z(L_v)|1\rangle_{L_v}, \quad |y\rangle_{L_v} := F_y(L_v)|1\rangle_{L_v} = F_z(L_v)F_x(L_v)|1\rangle_{L_v}.$$

Letting $\mathcal{B}_{L_v} := \{|1\rangle_{L_v}, |x\rangle_{L_v}, |z\rangle_{L_v}, |y\rangle_{L_v}\}$, it should be expected that the two basis $\mathcal{B}_{L_h}$ and $\mathcal{B}_{L_v}$ be related via some unitary matrix U such that $U|a\rangle_{L_h} = |a\rangle_{L_v}$ for all $a \in \mathbb{A}$. Such a change of basis will play a key role in the general theory to be developed. For the torus, this change of basis is often referred to as the S-matrix, and it is defined in terms of characteristic properties of the anyon model $\mathbb{A}$ to be made more precise in the following chapter.

Note here, that the flux bases $\mathcal{B}_{L_h}$ and $\mathcal{B}_{L_v}$ of $\mathcal{H}_g$ are indexed by the anyon types of $\mathbb{A}$ implying that the dimension of $\mathcal{H}_g$ is given by the number of distinct anyon types $|\mathbb{A}|$. For the toric code $|\mathbb{A}| = 4$, and this agrees with the dimension of $\mathcal{H}_g$ as it was calculated in Section 2.1.3 via the stabilizer framework. In that context, even the ground space of interest $\mathcal{H}_g$ was defined with respect to the underlying Hamiltonian $\hat{H}$ defined for the system. The approach partially outlined here in terms of the flux basis offers an alternative avenue for defining a computational code space $\mathcal{H}_T$ for the torus T under consideration such that $\mathcal{H}_T \cong \mathcal{H}_g$. A generalization of this method will be used to define observables and basis states associated to various surfaces in topological quantum field theory.

The effective topological quantum field theory describing an anyonic system $\mathbb{A}$ on some surface Σ provides a way of constructing a Hilbert space $\mathcal{H}_\Sigma$ which functions as the arena for topological quantum computation. The basis states of $\mathcal{H}_\Sigma$ are defined by appropriate labelings of possible flux types to various nontrivial loops on the surface Σ. In this more abstract theory, there will often be no mention of an explicit Hamiltonian of the system defined on Σ. Instead, a starting point will simply be an anyon model $\mathbb{A}$ together with its underlying topological data. It then becomes a question of physics whether or not there exists a Hamiltonian $\hat{H}$ which manifests the anyon model $\mathbb{A}$, with the further property that the ground space $\mathcal{H}_g$ of the Hamiltonian $\hat{H}$ satisfies the isomorphism $\mathcal{H}_g \cong \mathcal{H}_\Sigma$.

Chapter 3

Topological Quantum Field Theory

Many physical theories of the world implicitly refer to models of the three-dimensional physical space in which the entities of interest reside and how this space changes in time. That is, they are theories of conventional space-time. On the other hand, the standard mathematical domain of quantum theory takes place in a Hilbert space, which is not a *physical* space in the sense of ordinary space-time, but a more abstract mathematical space which describes quantum states. In this regard, quantum field theories offer a way to model quantum mechanical phenomenon while also taking into account that the quantum mechanical entities of interest also exist in some space-time model.

As a mathematical formality, the objective of the quantum field theory is to provide a way of associating appropriate Hilbert spaces to space-time, and transformations of this space-time to transformations of the corresponding Hilbert spaces. However, one's own mathematical liberties offer a choice for what transformations of the space-time manifold are considered. For instance, the theory may consider transformations of space-time that preserve the distance and angles between relative points of the space under some suitable metric; in which case the transformations should be taken as *diffeomorphisms* of the space-time. This general setting is the main domain of standard *quantum field theory*. Perhaps the theory is not concerned with operations that preserve distance, but only the relative angles of points in the space; then *conformal* maps should be used instead of diffeomorphisms, and in this case the theory is said to be a *conformal field theory*. Continuing in this forgetful manner, the theory may not even be concerned with transformations of space-time which preserve both distance and angles, but only preserve the fundamental topology of the manifold. In this latter case, the appropriate transformations are *homeomorphisms* of the manifold, and the theory is referred to as a *topological quantum field theory* (TQFTs, for short). Therefore, in some sense, TQFTs may be regarded as the most fundamental theories when compared to more general quantum field theories since they characterize the most essential features of the theory that are independent

or remain invariant under such general topological transformations.

For the purpose of topological quantum computation with anyons, TQFTs become relevant because they offer an effective theory which precisely models the anyonic properties and their dynamics. In particular, a $(2+1)$–dimensional TQFT will be of interest in this thesis, since the anyon dynamics are assumed to take place on some oriented two-dimensional surface (where time plays the role of the third dimension). Before proceeding to give a mathematical definition of a TQFT, some effort will be invested in first developing an algebraic theory of anyons. The main mathematical tool for anyon theory will be category theory, which describes in an algebraic fashion all the data necessary to specify an anyon model. Namely, an anyon model will be described mathematically by a *unitary modular tensor category* (UMTC), which contains within it a very rich structure that captures essential anyonic properties of interest.

Roughly speaking, a TQFT takes the data provided by a particular anyon model and assigns certain Hilbert spaces to various surfaces upon which the anyonic dynamics take place. The mathematical entity which describes this assignment will be referred to a *unitary modular tensor category functor* (UMTC functor) and essentially specifies a particular TQFT given an anyon model. The surface and certain topological transformations of the surface (called *homeomorphisms*), will get mapped by the UMTC functor to appropriate Hilbert spaces and unitary transformations on this Hilbert space, respectively. More generally, transformations between various surfaces are associated to certain linear transformations between the respectively assigned Hilbert spaces. The UMTC functor is essentially a category theoretic concept, and its role can be thought of as providing a structure-preserving representation of the UMTC that describes the anyon dynamics on surfaces to the category of Hilbert spaces, which itself can be thought of as a UTMC.

Many of the category theoretic notions to be developed in this chapter can be found in any standard text on the subject. A quintessential text is by MacLane [33], who happens to be one of the early founders of category theory. These introductory concepts together with more advanced concepts pertaining to modular categories can be found in [13, 29]. A more mathematically sophisticated text regarding modular categories is [2]. Suggested references for topological quantum field theory are [1, 13, 42].

3.1 Category Theory

In this section, some basic definitions and constructions in category theory will be defined which will be necessary for understanding the relevant structures used to describe an anyon model and a topological quantum field theory. Category theory can be regarded as more of a

philosophical perspective of mathematics and how different subfields of mathematics may relate to each other. Typically, in a particular branch of mathematics, the objective is to understand and characterize the various *objects* or mathematical entities of interest such as sets, vector spaces, or abstract manifolds for example. Category theory attempts to understand these objects not as isolated entities by themselves, but rather how an object may relate to other objects in the given category. These relations between objects in a given category are described mathematically by certain maps, called *morphisms*, which preserve the appropriate structure of interest in the category.

For example, in the category of sets the objects are sets and the relevant morphisms are just the usual functions from one set to another defined in the conventional sense. The category of vector spaces will have vector spaces as objects, and linear transformations between vector spaces as the relevant morphisms of the category. The category of manifolds may take manifolds as objects and consider, say, diffeomorphisms between manifolds as the morphisms. Category theory is not so much concerned with the internal structure of a particular object (i.e. the elements of a set), but instead regards the set itself as a single entity and proceeds to characterize the object in a more extrinsic fashion (i.e. how the set relates to itself and other sets through the existence of certain functions). The advantage of such an approach is that relationships in category theory can be defined and understood abstractly without necessarily having to specify a particular category, and thus serves as a more general means to understand the essential features of various categories and branches of mathematics.

3.1.1 Categories and diagrams

Formally, a category is defined as follows.

Definition 3.1.1. *A* **category** $\mathbf{C}$ *is a collection of* **objects** $Ob(\mathbf{C})$*, and for every pair of objects* $A, B \in Ob(\mathbf{C})$ *a set of* **morphisms** $Hom(A, B)$*. For* $f \in Hom(A, B)$*, write* $f : A \to B$*, and call* A *and* B *the* **domain** *and* **codomain** *of* f*, respectively, written* $dom(f) := A$ *and* $cod(f) := B$*. Moreover, objects and morphisms in a category* $\mathbf{C}$ *must satisfy the following:*

- *for all morphisms* $f \in Hom(A, B)$ *and* $g \in Hom(B, C)$*, there exists a* **composition morphism** $h \in Hom(A, C)$ *written as* $h = gf$*.*
- *the composition of morphisms is* **associative***, meaning* $h(gf) = (hg)f$*, whenever the composition is defined.*
- *for every* $A \in Ob(\mathbf{C})$*, there exists an* **identity morphism** $i_A \in Hom(A, A)$*.*

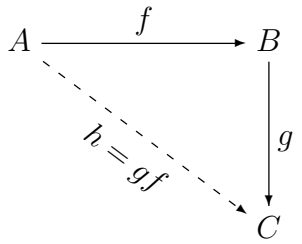
- *for any $f \in Hom(A, B)$, the identity morphisms $i_A \in Hom(A, A)$ and $i_B \in Hom(B, B)$ form right and left* **units** *under composition: $fi_A = i_B f$.*

Relationships in a given category presented through identities involving the compositions of morphisms can be conveniently expressed by use of diagrams which depict various objects and morphisms between them. More explicitly,

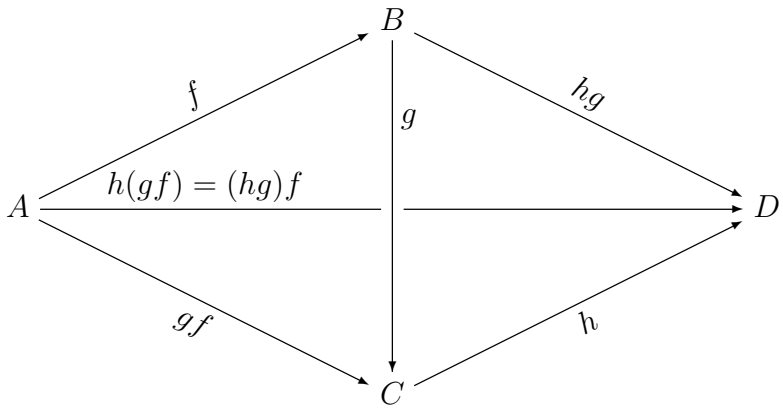
Definition 3.1.2. *A* **diagram** *in a category* $\mathbf{C}$ *is a directed graph whose vertices are labelled by objects in* $\mathbf{C}$ *and edges are labeled by morphisms in* $\mathbf{C}$*. A diagram is said to* **commute***, if all compositions of (at least two) morphisms defined by different directed paths having the same initial and the same final vertex in the diagram are equal.*

The notion of a diagram commuting intuitively captures what can otherwise be equivalently expressed using the more standard algebraic notation for the composition of morphisms. To exemplify this, the properties given in the formal definition of a category can be expressed by the following commutative diagrams:

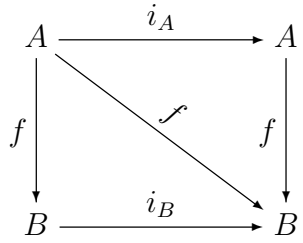
- **composition**: for all morphisms f and g in $\mathbf{C}$ such that $dom(g) = cod(f)$, there exists a morphism $h := gf : dom(f) \to cod(g)$ in $\mathbf{C}$ such that the following diagram commutes



- **associativity**: for all morphisms f, g, and h in $\mathbf{C}$ such that $cod(f) = dom(g)$ and $cod(g) = dom(h)$, the following diagram commutes



- **identity**: for any morphism $f \in Hom(A, B)$ in $\mathbf{C}$, the identity morphisms $i_A \in Hom(A, A)$ and $i_B \in Hom(B, B)$ are such that the following diagram commutes



Some examples of categories are:

- the category of sets, **Set**, where objects are sets $A, B \in Ob(\mathbf{Set})$ and morphisms $f \in Hom(A, B)$ of **Set** are standard functions $f : A \to B$ defined as mappings $f(x) = y$ where for all $x \in A$ there is a unique $y \in B$ such that $f(x) = y$.

- the category of groups, **Grp**, where objects are groups $G, H \in Ob(\mathcal{G})$ and morphisms are group homomorphisms $\rho : G \to H$ which satisfy $\rho(ab) = \rho(a)\rho(b)$ for $a, b \in G$.

- A group $\mathcal{G}$ which has only a single object, call it $G \in Ob(\mathcal{G})$, and morphisms $f_g \in Hom(G, G)$ are indexed by the usual elements $g \in G$ of the group corresponding to the group multiplication: $f_g : G \to G$ where $f_g(a) = g \cdot a$ so that the composition of morphisms is given by $f_h f_g = f_{h \cdot g}$.

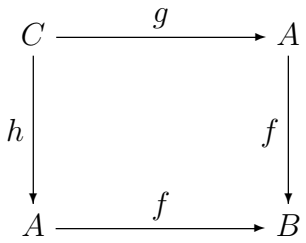
- The category $\mathbf{Vec_k}$ where objects are vector spaces over a field k, and morphisms are linear transformations.

Though perhaps somewhat trivial, it will be left as an exercise for the motivated reader to verify the composition axioms and existence of identity maps for these various categories.

In the category **Set** a morphism $f : A \to B$ may be what is conventionally considered an injection ("1-to-1"), a surjection ("onto"), or perhaps a bijection (both "1-to-1" and "onto"). For an arbitrary category, there is a standard notion for when a morphism satisfies these analogous properties in **Set**, which are usually defined in an intrinsic fashion that makes reference to the elements of the sets under consideration. These concepts can be generalized and stated abstractly in the category theoretic context with the following definitions which only make extrinsic reference to objects in a particular category through its morphisms.

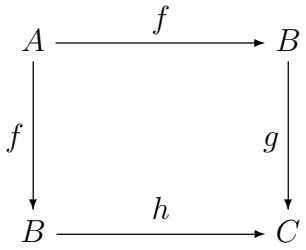
Definition 3.1.3. *A morphism $f : A \to B$ in a category $\mathbf{C}$ is a* **monomorphism** *if for any morphisms $g, h : C \to A$ in $\mathbf{C}$ satisfying $fg = fh$, it is the case that $g = h$. Diagrammatically,*

f is a monomorphism if any diagram in $\mathbf{C}$ *of the form*



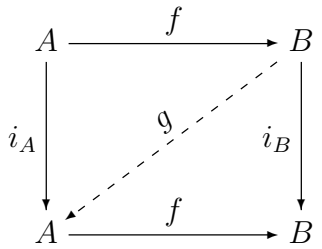
commutes, then it must be that $g = h$.

Definition 3.1.4. *A morphism* $f : A \to B$ *in a category* $\mathbf{C}$ *is an* **epimorphism** *if for any morphisms* $g, h : B \to C$ *in* $\mathbf{C}$ *satisfying* $gf = hf$*, it is the case that* $g = h$*. Diagrammatically,* f *is a epimorphism if any diagram in* $\mathbf{C}$ *of the form*



commutes, then it must be that $g = h$.

Definition 3.1.5. *A morphism* $f : A \to B$ *in a category* $\mathbf{C}$ *is an* **isomorphism** *if there exists a morphism* $g : B \to A$ *in* $\mathbf{C}$ *such that* $gf = i_A$ *and* $fg = i_B$*; or equivalently, if there exists a morphism* g *in* $\mathbf{C}$ *making the following diagram commute:*



In the case that $f \in Hom(A, B)$ *is an isomorphism, let* $f^{-1} := g$ *and call* f^{-1} *the* ***inverse*** *of* f*; moreover, it will be said that "*A *is* ***isomorphic*** *to* B*" and written* $A \cong B$.

By specializing the definitions above for the category **Set**, an equivalence is made between the notions of a morphism $f : A \to B$ in **Set** being a monomorphism/injection, epimorphism/surjection, and isomorphism/bijection. These properties will be used to characterize and define other category theoretic notions necessary to develop an anyon model.

3.1.2 Functors and natural transformations

A particular category $\mathbf{C}$ relates its objects through morphisms which preserve the relevant structure of the category. Abstractly, however, a category is defined merely through axioms for the compositions of these morphisms without concern for the particular kind of morphisms used in the category; and so consequently these composition rules form the essential structure of categories. Given two categories $\mathbf{C}$ and $\mathbf{D}$ there ought to be a way to relate them through an appropriate "morphism" of categories. This is achieved through the notion of a *functor* between categories that assigns objects and morphisms in one category to objects and morphisms in another category. Moreover, such an assignment must be *functorial*, meaning it satisfies certain structure preserving properties of the given categories in order to serve the purpose of appropriately relating the two. This is made explicit in the following definition.

Definition 3.1.6. *A* **functor** F *between categories* $\mathbf{C}$ *and* $\mathbf{D}$*, written* $F : \mathbf{C} \to \mathbf{D}$*, maps objects* $A \in Ob(\mathbf{C})$ *to objects* $F(A) \in Ob(\mathbf{D})$ *and morphisms* $f \in Hom(A, B)$ *in* $\mathbf{C}$ *to morphisms* $F(f) \in Hom(F(A), F(B))$ *in* $\mathbf{D}$ *such that* F *is* **functorial***, meaning*

- F **preserves identities***: for every object* $A \in Ob(\mathbf{C})$*,* $F(i_A) = i_{F(A)}$
- F **preserves composition***: for all morphisms* f *and* g *in* $\mathbf{C}$ *such that the composition* gf *is also defined in* $\mathbf{C}$*, the composition* $F(g)F(f)$ *in* $\mathbf{D}$ *satisfies* $F(gf) = F(g)F(f)$*.*

Note here that a slight abuse of notation will be permitted in specifying the argument for the image $F(\cdot)$ of the functor F, written $F(A)$ and $F(f)$, where it is to be understood by context whether $F(\cdot)$ is an object or morphism in the category $\mathbf{D}$ depending on whether the argument is an object A or morphism f in the category $\mathbf{C}$, respectively.

The existence of a functor $F : \mathbf{C} \to \mathbf{D}$ can be interpreted as modeling the category $\mathbf{C}$ by creating an "image" or "representation" in another category $\mathbf{D}$. In this way, commutativity relations that hold in $\mathbf{C}$ also hold in in $\mathbf{D}$, but such a modeling need not be completely faithful. For instance, a trivial functor may send all objects in $Ob(\mathbf{C})$ to a single object $A \in Ob(\mathbf{D})$, and all morphisms in $\mathbf{C}$ to the identity morphism i_A in $\mathbf{D}$.

As another example of a functor consider a group $\mathcal{G}$ thought of as a category with a single object $G \in Ob(\mathcal{G})$, and the category $\mathbf{Vec_k}$ of vector spaces over a field k. Then a functor $F : \mathcal{G} \to \mathbf{Vec_k}$ defines a group representation as follows. The single object $G \in Ob(\mathcal{G})$ gets mapped to an object $F(G) \in Ob(\mathbf{Vec_k})$, which is a vector space of some dimension n. Moreover, the morphisms $f_g : G \to G$ in $\mathcal{G}$ map to morphisms $F(f_g) : F(G) \to F(G)$ in $\mathbf{Vec_k}$, which are just linear transformations from the vector space $F(G)$ to itself (i.e. elements of the group of linear transformations of dimension n over the field k denoted $\mathcal{L}_n(k)$ upon choosing a basis for

the vector space $F(G)$). Thus, the map $\rho : Hom(G) \to \mathcal{L}_n(k)$ defined as $\rho(f_g) := F(f_g)$ yields a group representation since F is functorial which implies that ρ is a valid group homomorphism.

With the interpretation that functors play the role of "modelling" one category in another, consider now two functors $F, F' : \mathbf{C} \to \mathbf{D}$ which effectively yield two different models of the category $\mathbf{C}$ in $\mathbf{D}$. In certain circumstances two such functors or models may be related or "translated" in an appropriate fashion. This notion is captured formally by a *natural transformation* between the two functors.

Definition 3.1.7. *A* ***natural transformation****, α, between two functors $F, F' : \mathbf{C} \to \mathbf{D}$, written $\alpha : F \implies F'$, is a collection of morphisms $\alpha_A \in Hom(F(A), F'(A))$ in $\mathbf{D}$ indexed by all objects $A \in \mathbf{C}$ satisfying the property that for all morphisms $f \in Hom(A, B)$ in $\mathbf{C}$ the identity $F'(f)\alpha_A = \alpha_B F(f)$ holds in $\mathbf{D}$; or equivalently that the following diagram commutes:*

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(B) \\ \Big\downarrow{\scriptstyle \alpha_A} & & \Big\downarrow{\scriptstyle \alpha_B} \\ F'(A) & \xrightarrow{F'(f)} & F'(B) \end{array}$$

A natural transformation is said to be a ***natural isomorphism*** *if each of the morphisms α_A are isomorphisms in $\mathbf{D}$.*

For an illustrative example of a natural transformation consider again a group $\mathcal{G}$ thought of as a category with a single object $G \in Ob(\mathbf{G})$, and two group representations $F, F' : \mathcal{G} \to \mathbf{Vec_k}$ given as functors. The existence of a natural transformation $\alpha : F \implies F'$ in this case is given by a single isomorphism $\alpha_G : F(G) \to F'(G)$, which is just a linear transformation from the vector spaces $F(G)$ to $F'(G)$ such that $F(f_g)\alpha_G = \alpha_G F'(f_g)$ for all morphisms f_g in $\mathcal{G}$. The acquainted reader may recognize the map α_G as an *intertwining operator* in the usual setting of representation theory, which makes explicit the equivalence of the two representations via a change of basis from one representation to the other.

In what follows, natural transformations will be utilized to capture the desired physical concepts that characterize an anyon model and its possible dynamics.

3.2 Modular Tensor Categories

Many fields of mathematics make use of the familiar notion of a product defined on some set S as a mapping $S \times S \to S$ that takes two elements $a, b \in S$ and returns another element $a \times b \in S$.

For instance, there is the standard product of multiplication of two real numbers, and more abstractly the notion of a tensor product of two vector spaces which yields another vector space. Moreover, in this latter case, the tensor product space comes equipped with additional structure to define a tensor product of vectors and linear transformations of the constituent spaces. In the context of category theory, a similar product can be defined for a category $\mathbf{C}$, which takes two objects $A, B \in Ob(\mathbf{C})$ and returns another object $A \otimes B \in Ob(\mathbf{C})$. Categories in which such a product is defined are called *monoidal categories* or synonymously *tensor categories*. In regards to the theory of anyons, the notion of fusing anyons will be captured by interpreting anyons as objects $A, B \in Ob(\mathbf{C})$ in a monoidal category $\mathbf{C}$. In this way, the process of fusion is described by a monoidal product $\otimes$, and the resulting anyon type after fusion is given by another object $A \otimes B \in Ob(\mathbf{C})$ of the category.

Before defining a monoidal product and the appropriate axioms it should satisfy, the following construction for categories will be needed which serves to generalize the usual Cartesian product of sets:

Definition 3.2.1. *Given two categories* $\mathbf{C}$ *and* $\mathbf{C}'$*, the* ***Cartesian product category****, denoted by* $\mathbf{C} \times \mathbf{C}'$*, is the category where:*

- *objects in* $\mathbf{C} \times \mathbf{C}'$ *are ordered pairs* (A, A')*, where* $A \in Ob(\mathbf{C})$ *and* $A' \in Ob(\mathbf{C}')$*.*
- *morphisms in* $\mathbf{C} \times \mathbf{C}'$ *are ordered pairs* $(f, f') : (A, A') \to (B, B')$*, where* $f : A \to B$ *is a morphism in* $\mathbf{C}$ *and* $f' : A' \to B'$ *is a morphism in* $\mathbf{C}'$*.*
- *composition of morphisms* (f, f') *and* (g, g') *in* $\mathbf{C} \times \mathbf{C}'$ *such that* $cod((f, f')) = dom((g, g'))$ *is defined component-wise as* $(g, g')(f, f') := (gf, g'f')$*.*
- *the identity morphism for each object* $(A, A') \in Ob(\mathbf{C} \times \mathbf{C}')$ *is given as* $i_{(A,A')} := (i_A, i_{A'})$*, where* i_A *and* $i_{A'}$ *are identity morphisms of* $A \in Ob(\mathbf{C})$ *and* $A' \in Ob(\mathbf{C}')$*, respectively.*

3.2.1 Tensor categories

In this section, the formal properties of a tensor/monoidal category will be given. Although somewhat abstract, the notion of a monoidal product can be thought of as generalizing the more familiar notion of a tensor product of vector spaces. Thus, it is worthwhile to consider the properties of this standard tensor product of vector spaces when trying to understand the properties given in the definition of a monoidal product. This analogy will be further clarified after presenting the definition.

Definition 3.2.2. *A* ***tensor/monoidal category****,* $\mathbf{C}$*, is a category with the following:*

- *a* **tensor product functor** $\otimes : \mathbf{C} \times \mathbf{C} \to \mathbf{C}$ *whose action on objects* $(A, A') \in Ob(\mathbf{C} \times \mathbf{C})$ *and morphisms* $(f, f') : (A, A') \to (B, B')$ *in the category* $\mathbf{C} \times \mathbf{C}$ *is denoted as* $A \otimes A' \in Ob(\mathbf{C})$ *and* $f \otimes f' : A \otimes A' \to B \otimes B'$*, respectively.*

- *a* ***unit object*** $I \in Ob(\mathbf{C})$*,*

- *a natural isomorphism* a*, called the* ***associator****, given by isomorphisms in* $\mathbf{C}$ *indexed by triples* $A, B, C \in Ob(\mathbf{C})$*:*

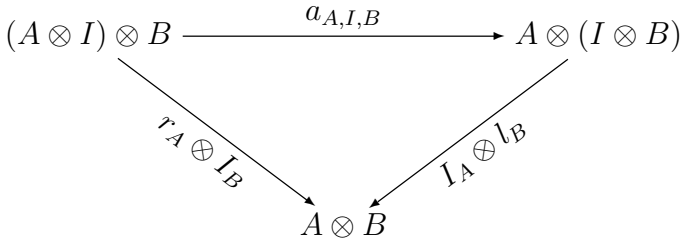
$$a_{A,B,C} : (A \otimes B) \otimes C \to A \otimes (B \otimes C),$$

- *natural isomorphisms,* l *and* r*, called the* ***left*** *and* ***right unitors****, respectively, given by isomorphisms indexed by all objects* $A \in Ob(\mathbf{C})$*:*

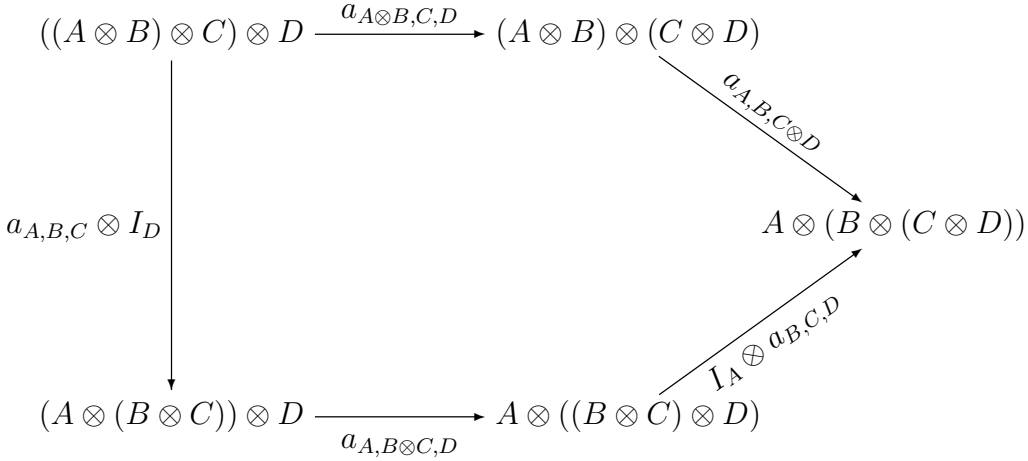
$$l_A : I \otimes A \to A,$$
$$r_A : A \otimes I \to A.$$

subject to the condition that the following diagrams commute

- ***triangle equation****: for all* $A, B \in Ob((\mathbf{C})$*,*



- ***pentagon equation****: for all objects* $A, B, C, D \in Ob((\mathbf{C})$*,*



In regards to objects of a monoidal category, the object $A \otimes B \in Ob(\mathbf{C})$ can be thought of as another object consisting of A *and* B. When an anyon model is interpreted as a monoidal category $\mathbf{C}$, the tensor product of anyon types $A, B \in Ob(\mathbf{C})$ is meant to represent the fusion of anyon A with anyon B. In any category morphisms may be composed, but in a monoidal category morphisms may also be done in "parallel". The parallel process of two morphisms $f : A \to B$ and $f' : A' \to B'$ in $\mathbf{C}$ is given by the tensor product $f \otimes f' : A \otimes A' \to B \otimes B'$, and can be thought of as acting on the joint parallel object of A and A' denoted by $A \otimes A'$. Furthermore, a monoidal category allows more than two objects and morphisms, say $A, B, C \in Ob(\mathbf{C})$ and corresponding morphisms acting on these objects, to be considered in parallel. Again, for an anyon model, this situation represents the scenario when three different anyons A, B and C are fused together. The existence of the associator, a, ensures that the two ways of considering such a triple of objects through the orderings $(A \otimes B) \otimes C$ and $A \otimes (B \otimes C)$ are isomorphic. When considering four objects $A, B, C, D \in Ob(\mathbf{C})$, there are five different ways to order the tensor product as depicted in the diagram for the pentagon equation. The pentagon equation (i.e. commutativity of the diagram) ensures that all these different objects are isomormorphic. One may wonder what other additional coherence relations would be necessary for establishing an appropriate equivalence when considering some larger arbitrary number of objects in parallel with the tensor product functor. Although it will not be stated here, MacLanes Coherence Theorem [33] ensures that the axioms given above for a monoidal category suffice for establishing the relevant isomorphisms between tensor products of an arbitrary number of objects.

The functoriality of the tensor product functor $\otimes : \mathbf{C} \times \mathbf{C} \to \mathbf{C}$ implies that all composable pairs of morphisms (f, f') and (g, g') in $\mathbf{C} \times \mathbf{C}$ satisfy

$$(g \otimes g')(f \otimes f') = gf \otimes g'f'.$$

In particular, functoriality also implies that, for identity morphisms i_A and $i_{A'}$ in $\mathbf{C}$, the tensor product morphism satisfies $i_A \otimes i_{A'} = i_{A \otimes A'}$.

In terms of anyons, the unit object $I \in Ob(\mathbf{C})$ represents the trivial anyon type having the property that when fused with any other anyon type $A \in Ob(\mathbf{C})$ yields A again: $A \otimes I \cong A$. The existence of a unit object $I \in Ob(\mathbf{C})$ together with the left and right unitors can be thought of as being analogous to the role a one-dimensional vector space plays in the standard tensor product for vector spaces (i.e. $\mathbb{C}^n \otimes \mathbb{C} \cong \mathbb{C} \cong \mathbb{C} \otimes \mathbb{C}^n$ where say $\mathbb{C}^n$ is some Hilbert space and $\mathbb{C}$ is the one-dimensional Hilbert space). Moreover, the triangle equation ensures that the two ways of considering the tensor product of the unit object I with two other objects A and B, either as $(A \otimes I) \otimes B$ or as $A \otimes (I \otimes B)$, is isomorphic to simply taking the tensor product $A \otimes B$. In this way, any valid morphisms defined through compositions of associators and left/right unitors is always itself an isomorphism.

3.2.2 Semisimple categories

When considering an anyon model as a certain monoidal category $\mathbf{C}$, the monoidal product $\otimes : \mathbf{C}\times\mathbf{C} \to \mathbf{C}$ introduced in the previous section serves as a mathematical tool to define the fusion of two anyons $A, B \in Ob(\mathbf{C})$ as another object $A \otimes B \in Ob(\mathbf{C})$. Thus, a monoidal category has objects denoted as $A, B \in Ob(\mathbf{C})$, but also as $A \otimes B \in Ob(\mathbf{C})$. However, in an anyon model the object $A \otimes B$ may be isomorphic to another object, say $C \in Ob(\mathbf{C})$, so that $A \otimes B \cong C$. Under appropriate assumptions (as explained further below), an equivalence relation can be made on the objects $Ob(\mathbf{C})$ of the category which partitions $Ob(\mathbf{C})$ into equivalence classes where arbitrary objects $A, B \in Ob(\mathbf{C})$ (or tensor products $A \otimes B$ of objects) are in the same class if $A \cong B$ in the category; that is, A and B are in the same equivalence class if there exists an isomorphism $f : A \to B$ in $\mathbf{C}$. Objects in a particular equivalence class can then be regarded as being the same, and representative objects from each equivalence class can be chosen to represent any of the objects in that class. These representative objects will be referred to as *simple objects* in $\mathbf{C}$ and represent the different primitive types of anyons in a particular anyon model corresponding to $\mathbf{C}$. In what follows, the set of representatives from each equivalence class will be denoted by $[\mathbf{C}]$.

In some anyon models, the fusion outcome of two anyons $A \otimes B$ may not be unique since multiple anyons may result from the fusion. In order to further describe the properties of anyon fusion, the monoidal category $\mathbf{C}$ will also come equipped with another product functor $\oplus : \mathbf{C}\times\mathbf{C} \to \mathbf{C}$ which is necessary to properly describe the resulting object $A \otimes B \in Ob(\mathbf{C})$ after fusion. Recall that the object $A \otimes B$ is to be interpreted as considering anyons A *and* B, but as mentioned for certain anyon models the object resulting from fusion may itself be multiple different objects, say C *or* D, where $C, D \in Ob(\mathbf{C})$. Such a scenario may be represented mathematically as $A \otimes B = C \oplus D$. More generally, the result of fusion will be described though equations of the form

$$A \otimes B = \bigoplus_{C\in[\mathbf{C}]} N_{A,B}^{C} C,$$

where the "sum" ranges over simple objects $C \in |\mathbf{C}| \subseteq Ob(\mathbf{C})$ and $N_{A,B}^{C}$ are nonnegative integers that represent how many copies of object C appear after the result of fusion. If $N_{A,B}^{C} = 0$ then $C \in [\mathbf{C}]$ is not a possible fusion outcome. The interplay between the two "products" $\otimes$ and $\oplus$ defined on a category $\mathbf{C}$, and the characteristic numbers $N_{A,B}^{C}$, will be used to describe the fusion of arbitrary anyon types in $\mathbf{C}$, and will be referred to as the *fusion rules*. A monoidal category $\mathbf{C}$ where the fusion of anyons can always be decomposed in this way will be referred to as a *semisimple* category.

Appealing to an analogy pertaining to vector spaces, a familiar monoidal product in the category $\mathbf{Vec}_{\mathbb{C}}$ is just the usual tensor product of vector spaces. In this context, $\mathbf{Vec}_{\mathbb{C}}$ often

comes equipped with another different product $\oplus : \mathbf{Vec}_{\mathbb{C}} \times \mathbf{Vec}_{\mathbb{C}} \to \mathbf{Vec}_{\mathbb{C}}$ given by the standard direct sum $V \oplus W$ of two vector spaces $V, W \in Ob(\mathbf{Vec}_{\mathbb{C}})$, and in turn allows direct sums of linear transformations to be taken. In $\mathbf{Vec}_{\mathbf{k}}$, it is well known that the sets of morphisms of the category $Hom(V, W)$ themselves can be made into a vector space structure through the usual addition and multiplication of linear transformations. The direct sum of vector spaces offers another way of considering two vector spaces, but yet behaves differently in subtle ways when compared to the tensor product. In $\mathbf{Vec}_{\mathbb{C}}$ for instance, where the one-dimensional space $\mathbb{C}$ serves as the tensor unit ($\mathbb{C} \otimes \mathbb{C}^n \cong \mathbb{C}^n$), the zero-dimensional space $\{0\}$ serves as the unit under the direct sum operation ($\{0\} \oplus \mathbb{C}^n \cong \mathbb{C}^n$) and is refered to as the *zero object* or *null object*. Moreover, this object $\{0\} \in Ob(\mathbf{Vec}_{\mathbb{C}})$ serves to define a *zero morphism* $0_{V,W} : V \to W$ between two vector spaces $V, W \in Ob(\mathbf{C})$, which is defined as $0_{V,W}(v) = 0$ for all $v \in V$.

The existence of zero objects and zero morphisms in a category such as $\mathbf{Vec}_{\mathbf{k}}$ allow certain relationships to hold which may otherwise get taken for granted. In particular, the notion of a *kernel* of a linear transformations $L : V \to W$ in $\mathbf{Vec}_{\mathbf{k}}$ can be defined as $ker(L) := \{v \in V \mid L(v) = 0\}$, and special means to characterize the morphism L using the kernel can be deployed. In $\mathbf{Vec}_{\mathbf{k}}$, one such property is that $L : V \to W$ is an isomorphism if it is both a monomorphism and an epimorphism. Note that this property is a categorification of the otherwise obvious fact that a function is a bijection if it is both an injection and a surjection in **Set**. Another familiar property in $\mathbf{Vec}_{\mathbf{k}}$ is that any injection (monomorphism) $L : V \to W$ is an isomorphism if and only if it has a trivial kernel, meaning $ker(L) = \{0\}$.

Categories which possess this kind of direct sum structure and have notions of a kernel as in $\mathbf{Vec}_{\mathbf{k}}$ are called *abelian categories* in the literature. Although explicit details needed to rigorously define abelian categories will not be given here, it will be sufficient for the purposes of this thesis to work with the following high-level definition motivated by the previous exposition.

Definition 3.2.3. *An* **abelian category** $\mathbf{C}$ *such that:*

- *Every set of morphisms $Hom(A, B)$ in $\mathbf{C}$ forms a k-vector space, and the composition of morphisms in bilinear, meaning*

$$(f + f')g = fg + f'g \quad \textit{and} \quad h(f + f') = hf + hf',$$

  for all morphisms $f, f' \in Hom(A, B)$, $g \in Hom(D, A)$, and $h \in Hom(B, C)$.

- *There exists a* **zero object** $0 \in Ob(\mathbf{C})$ *such that for all $A \in Ob(\mathbf{C})$, $Hom(A, 0) = 0_{A,0}$ and $Hom(0, A) = 0_{0,A}$ where $0_{A,0}$ and $0_{0,A}$ are the* **zero morphisms**.

- *Finite* **direct sums** *exist in $\mathbf{C}$ given by a functor $\oplus : \mathbf{C} \times \mathbf{C} \to \mathbf{C}$.*

- *The* **kernel** *of any morphism f in* $\mathbf{C}$ *exists, and satisfies properties as in* $\mathbf{Vec_k}$.

With these remarks in mind, the concept of a *simple object* in an abelian category can be more formally defined. Note that the notion of a simple object of $\mathbf{C}$ is only relevant for an abelian category, and therefore it will be implicit that the category $\mathbf{C}$ under consideration is an abelian category when speaking of simple objects in $\mathbf{C}$.

Definition 3.2.4. *A non-zero object $A \in Ob(C)$ of an abelian category $\mathbf{C}$ is a* **simple object** *if any monomorphism $f : B \to A$ (for arbitrary objects $B \in Ob(\mathbf{C})$) is either the zero morphism, $f = 0_{B,A}$, or an isomorphism.*

This characterization essentially ensures that a simple object A does not contain any non-trivial "subobjects" that are isomorphic to A. Furthermore, in this way an equivalence relation on $\mathbf{C}$ can be made as described above, where each equivalence class is represented by a simple object such that non-isomorphic simple objects belong to distinct equivalence classes.

Definition 3.2.5. *For a category $\mathbf{C}$, denote by $[\mathbf{C}] \subseteq Ob(\mathbf{C})$ a set of mutually non-isomorphic simple objects.*

The simple objects in $[\mathbf{C}]$ may be regarded as the primitive objects of a category through which any object of $\mathbf{C}$ can be "built up" using the direct sum of objects. When this is the case, the category $\mathbf{C}$ is said to be *semisimple*. More precisely:

Definition 3.2.6. *An abelian category $\mathbf{C}$ is* **semisimple** *if any object $A \in Ob(\mathbf{C})$ can be expressed as*

$$A \cong \bigoplus_{A_i \in [\mathbf{C}]} N_{A_i} A_i,$$

for some nonnegative integers N_i, where the $A_i \in [\mathbf{C}]$ index all nonzero, mutually non-isomorphic simple objects of $\mathbf{C}$.

A monoidal category $\mathbf{C}$ which is semisimple reveals characterizing information about the interplay between the $\otimes$ and $\oplus$ operations. In the context of anyon fusion, it implies that the fusion outcome of any two simple objects is given by a direct sum of simple objects.

Definition 3.2.7. *For simple objects $A, B \in [\mathbf{C}]$, the* **fusion coefficients** *$N_{A,B}^C$ are nonnegative integers which satisfy*

$$A \otimes B \cong \bigoplus_{C \in [\mathbf{C}]} N_{A,B}^C C,$$

Instead of having to consider all arbitrary objects in $Ob(\mathbf{C})$ in a semisimple category, it is sufficient to limit discussion of properties of anyons to just the simple objects $[\mathbf{C}]$ of the category. Most of the remainder of this thesis will proceed in this fashion.

Recall that the definition of an abelian category had a choice of field k which defined the vector spaces that the sets of morphisms formed. From here on, it will be assumed that this field is the complex numbers $k = \mathbb{C}$. This then implies that, for simple objects $A \in [\mathbf{C}]$,

$$Hom(A, A) = \mathbb{C} \tag{3.1}$$

as a vector space (this result holds more generally as long as the field k is algebraically closed). Furthermore, for simple objects $A, B \in [\mathbf{C}]$ such that $A \ncong B$,

$$Hom(A, B) = 0. \tag{3.2}$$

For simple objects $A, B, C \in [\mathbf{C}]$, the fusion coefficients also determine the dimension of the vector space $Hom(A \otimes B, C)$ via

$$dim\ Hom(A \otimes B, C) = N_{A,B}^{C}. \tag{3.3}$$

The structure of a semisimple category with its fusion rules will play an important role in later developments. For topological quantum field theories, it will also serve as a first step in associating a vector space to a surface upon which the anyon dynamics take place. Moreover, it will be used to define an essential algebra of observables for the theory of topological quantum computation. The remaining part of this chapter will define additional categorical structures and appropriate axioms for a UTMC. These structures are meant to algebraically encapsulate the possible dynamics in an anyon model.

3.2.3 Rigid categories

Recall that a monoidal category $\mathbf{C}$ comes equipped with a tensor unit $1 \in [\mathbf{C}]$ representing the trivial anyon type such that $A \otimes 1 \cong A \cong 1 \otimes A$ for every object $A \in [\mathbf{C}]$. One important feature of all anyon models is the notion of a *dual* anyon (also referred to as the *conjugate* or *antiparticle*) for an anyon $A \in [\mathbf{C}]$, denoted as another object A^*, such that $A \otimes A^* \cong 1$. That is, when an anyon of type A fuses with its dual A^*, the result of fusion is the trivial anyon type 1. This process $A \otimes A^* \to 1$ will be referred to as *annihilation*. In a process opposite annihilation, an anyon type may also be *split* into a pair of anyons in a process given by a morphism $1 \to A^* \otimes A$. This process will be referred to as *creation*. Furthermore, such

processes should exist for each anyon type $A \in [\mathbf{C}]$. The following definition is motivated by this phenomenon.

Definition 3.2.8. *A simple object $A \in [\mathbf{C}]$ has a* **dual** *$A^* \in |C|$ if there exists a pair of morphisms*

$$n_A : 1 \to A \otimes A^* \quad \textit{and} \quad u_A : A^* \otimes A \to 1,$$

corresponding to the processes of anyon **creation/fusion** *from/to the vacuum, respectively, such that the following diagrams commute*

$$\begin{array}{ccccc} A & \xrightarrow{l_A^{-1}} & 1 \otimes A & \xrightarrow{n_A \otimes I_A} & (A \otimes A^*) \otimes A \\ \downarrow{\scriptstyle I_A} & & & & \downarrow{\scriptstyle a_{A,A^*,A}} \\ A & \xleftarrow[r_A]{} & A \otimes 1 & \xleftarrow[I_A \otimes u_A]{} & A \otimes (A^* \otimes A) \end{array}$$

and

$$\begin{array}{ccccc} A^* & \xrightarrow{r_{A^*}^{-1}} & A^* \otimes 1 & \xrightarrow{I_{A^*} \otimes n_A} & A^* \otimes (A \otimes A^*) \\ \downarrow{\scriptstyle I_{A^*}} & & & & \downarrow{\scriptstyle a^{-1}_{A^*,A,A^*}} \\ A^* & \xleftarrow[l_{A^*}]{} & 1 \otimes A^* & \xleftarrow[u_A \otimes I_{A^*}]{} & (A^* \otimes A) \otimes A^* \end{array}$$

A **rigid category** *is a monoidal category $\mathbf{C}$, such that every object $A \in [\mathbf{C}]$ has a dual $A^* \in [\mathbf{C}]$ with corresponding pairs of morphisms n_A and u_A as defined above satisfying the commutation relations.*

The category $\mathbf{Vec}_{\mathbb{C}}$ is an example of a rigid monoidal category. The dual of a vector space $V \in Ob(\mathbf{C})$ is given by the usual dual space V^* which consists of linear functions $f : V \to \mathbb{C}$. Letting $\{e_i\}_{i=1}^n$ be basis vectors of V, and $f_j : V \to \mathbb{C}$ be the functional in V^* defined by $f_j(e_j) = \delta_{i,j}$ (the *Kronecker delta function*), the two rigidity morphisms are given as

$$n_V : \mathbb{C} \to V \otimes V^* \ \text{ mapping } \ 1 \mapsto \sum_{i=1}^{n} e_i \otimes f_i,$$

and

$$u_V : V^* \otimes V \to \mathbb{C} \ \text{ mapping } \ f_j \otimes e_j \mapsto f_j(e_i).$$

In a rigid monoidal category $\mathbf{C}$, the notion of a conjugate morphism $f^* : B^* \to A^*$ in $\mathbf{C}$

can also be defined for a morphism $f : A \to B$ in $\mathbf{C}$. Given $f : A \to B$ in $\mathbf{C}$, the conjugate $f^* : B^* \to A^*$ is given by the following composition

$$B^* \xrightarrow{I_{B^*} \otimes n_A} B^* \otimes A \otimes A^* \xrightarrow{I_{B^*} \otimes f \otimes I_{A^*}} B^* \otimes B \otimes A^* \xrightarrow{u_B \otimes I_{A^*}} A*$$

Note that here, the right unitor r_{B^*} and left unitor l_{A^*} have been implicitly omitted at the beginning and end of the composition, respectively.

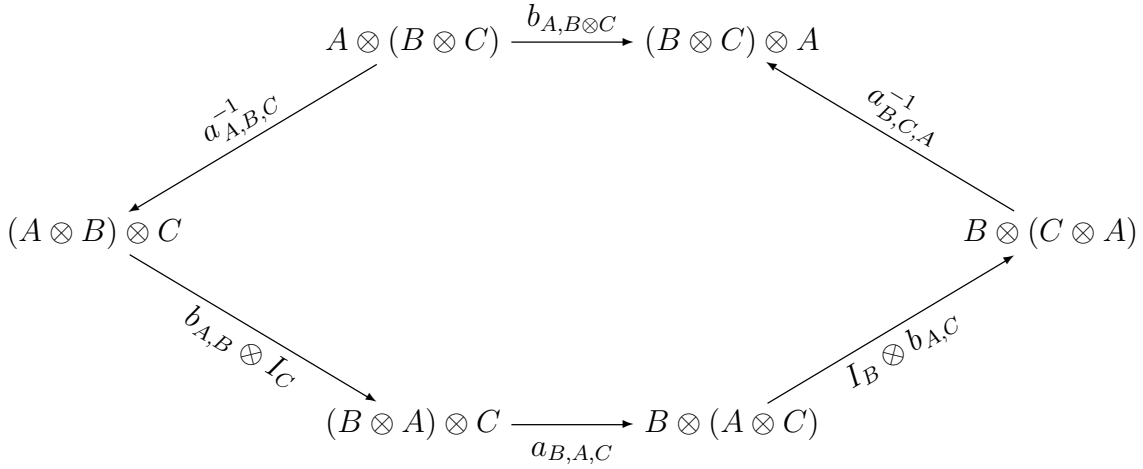
3.2.4 Braided categories

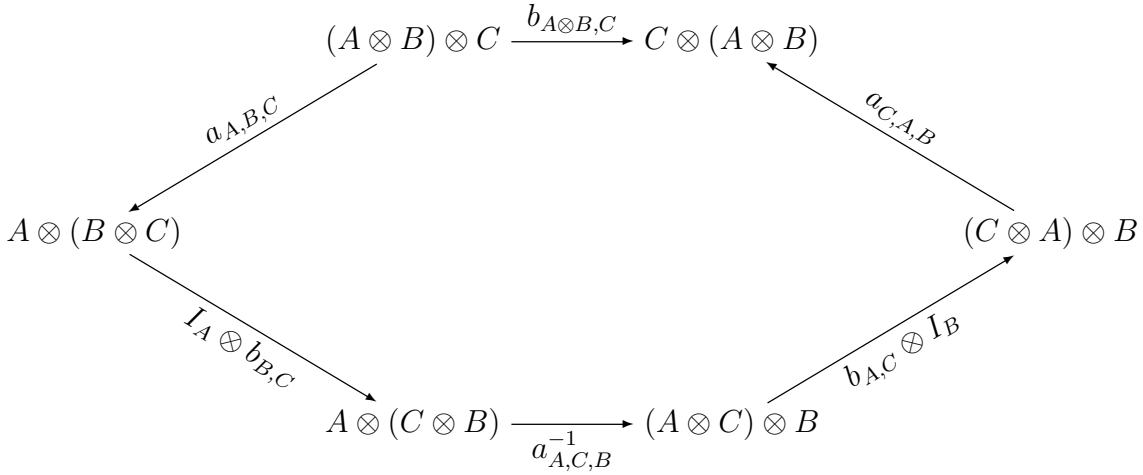
When anyons are present on some two-dimensional surface they may move around on the surface. In certain dynamical processes the starting and ending configuration of two anyons may be interchanged by moving them around one another. In the world-line picture, the paths of these anyons will trace out a *braid* in time. Such a braiding yields either an "over-crossing" or an "under-crossing" of the strings. However, these two interchanges can be seen as inverse processes of one another. Categorically, such a braiding process will be given as a natural isomorphism with component isomorphisms given as morphisms in $Hom(A \otimes B, B \otimes A)$ representing the interchange of anyons $A, B \in [\mathbf{C}]$. Moreover, these braiding morphisms must satisfy certain coherence relations that ensure a compatibility of the underlying monoidal structure of the category. This is made explicit in the following definition and axioms.

Definition 3.2.9. *A* **braided category** *is a monoidal category* $\mathbf{C}$ *equipped with a natural isomorphism* b*, called the* **braiding***, given by a family of isomorphisms in* $\mathbf{C}$ *indexed by pairs* $A, B \in [\mathbf{C}]$

$$b_{A,B} : A \otimes B \to B \otimes A$$

such that the following diagrams commute for all $A, B, C \in [\mathbf{C}]$*. The identities satisfied by these diagrams are called the* **hexagon equations***:*





Omitting the associators, the first of the hexagon equations essentially imply that braiding a simple object $A \in [\mathbf{C}]$ with a tensor product $B \otimes C \in Ob(\mathbf{C})$ of objects is the same as first braiding A with B and then A with C. That is, $b_{A,B\otimes C} = (I_B \otimes b_{A,C})(b_{A,B} \otimes I_C)$. Similarly, the second hexagon equation states that $b_{A\otimes B,C} = (b_{A,C} \otimes I_B)(I_A \otimes b_{B,C})$.

As a consequence of these axioms, braiding with the tensor unit $1 \in [\mathbf{C}]$ is trivial: $b_{A,1} = I_A = b_{1,A}$.

The category $\mathbf{Vec_k}$ can be made into a braided category by simply defining the braiding as the map $b_{V,W} : V \otimes W \to W \otimes V$ for vector spaces $V, W \in Ob(\mathbf{Vec_k})$, which maps the tensor product of vectors $v \in V$ and $w \in W$ as $b_{V,W}(v \otimes w) = w \otimes v$. Later, after defining a TQFT, more interesting braiding maps will be defined on appropriate Hilbert spaces in terms of the underlying braided category that represents an anyon model. These braiding maps will serve to enact nontrivial operations on the Hilbert spaces of interest, which will be the main avenue

for quantum computation.

3.2.5 Ribbon categories

In the definitions and axioms stated thus far, various morphisms were introduced that were defined in terms of a tensor product of simple objects. Here, another important ingredient to fully characterize an anyon model will be given in terms of a morphism $A \to A$, called the *twist*. The twist map corresponds to the process where an anyon "twists" or rotates about itself. This degree of freedom implies that anyons should actually be thought of as an extended object as opposed to a point-like entities. Moreover, such a process must behave coherently with the other constructs and morphisms introduced previously (i.e. the monoidal structure, rigidity, and braiding).

Definition 3.2.10. *A* **ribbon category** *is a rigid, braided tensor category* $\mathbf{C}$ *with a natural isomorphism* δ *consisting of isomorphisms* $\delta_A : A \to A^{**}$ *indexed by objects* $A \in [\mathbf{C}]$ *subject to the following consistency equations.*

$$\begin{aligned} \delta_{A\otimes B} &= \delta_A \otimes \delta_B \\ \delta_{A^*} &= (\delta_A^*)^{-1} \\ \delta_1 &= I_1 \end{aligned}$$

The existence of the natural isomorphism δ which satisfies the defining properties above is independent of the existing structure in a rigid, braided tensor category, and must be posited instead. Regardless, in a rigid, braided tensor category the following morphism $\psi_A : A^{**} \to A$ can always be defined for every object $A \in [\mathbf{C}]$ via the composition

$$\psi_A : A^{**} \xrightarrow{n_A \otimes I_{A^{**}}} A \otimes A^* \otimes A^{**} \xrightarrow{I_A \otimes b^{-1}_{V^*,V^{**}}} A \otimes A^{**} \otimes A^* \xrightarrow{I_A \otimes u_{A^*}} A$$

Note here that the unitors have been omitted at the start and end of the composition for convenience. With these morphisms just introduced, the desired twist map can be defined.

Definition 3.2.11. *In a ribbon category* $\mathbf{C}$*, a natural isomorphism* θ*, called the* **twist***, consists of isomorphisms given by* $\theta_A := \psi_A \delta_A : A \to A$ *indexed by objects* $A \in [\mathbf{C}]$ *satisfying the following*

$$\begin{aligned} \theta_{A\otimes B} &= b_{B,A} b_{A,B} (\theta_A \otimes \theta_B) \\ (\theta_A \otimes I_{A^*}) n_A &= (I_A \otimes \theta_{A^*}) n_A \\ \theta_1 &= I_1 \end{aligned}$$

Instead of depicting dynamical processes of anyons as world-*lines*, a more faithful representation can be achieved by using *ribbons* which can be twisted about their centers (hence the name, "ribbon categories"). For the purposes of this thesis, such a convention will not be adopted and instead it will be made implicit that anyon worldlines can be twisted in the appropriate fashion.

For any simple object $A \in [\mathbf{C}]$, since $Hom(A, A) \cong \mathbb{C}$ due to the assumed semisimple structure of the ribbon category, it follows that $\theta_A \in Hom(A, A)$ can be represented by a scalar quantity $\alpha \in \mathbb{C}$ such that

$$\theta_A = \alpha I_A$$

In what follows, for notational convenience, the twist map will simply be identified with this scalar quantity so that $\theta_A := \alpha \in \mathbb{C}$. The set of these scalars $\{\theta_A\}_{A\in[\mathbf{C}]}$ for simple objects are characteristic numbers associated to the anyon model represented by the ribbon category $\mathbf{C}$, and will be used to define certain operations for the corresponding TQFT.

Returning to the definition of the twist map, the first of these equations states that twisting together the tensor product $A \otimes B$ is the same as performing twists individually on the objects A and B followed by a double braiding. The second establishes a consistency with the rigid structure: after the creation of an anyon pair A and its dual A^*, applying the twist θ_A to A has the same result as applying the twist θ_{A^*} to A^* instead. From these axioms, it can be seen that the twists satisfy

$$\theta_1 = 1 \quad \text{and} \quad \theta_{A^*} = \overline{\theta}_A,$$

for all $A \in [\mathbf{C}]$. Note that here $\theta_1 = 1 \in \mathbb{C}$ is the complex number 1, whereas the index for θ_1 is the tensor unit $1 \in [\mathbf{C}]$ (trivial anyon type).

3.2.6 Traces and quantum dimensions

In the category $\mathbf{Vec_k}$, for linear transformations $L, L' : V \to V$ acting on some vector space $V \in Ob(\mathbf{Vec_k})$, there is a standard notion of the *trace* operation which returns a scalar quantity $tr(L) \in k$. Moreover, this trace operation satisfies worthwhile properties such as

$$tr(L \otimes L') = tr(L)tr(L'), \quad tr(LL') = tr(L'L), \quad tr(L^*) = tr(L).$$

In this setting of finite dimensional vector spaces, the trace also serves as a means to compute the *dimension* of the vector space V as $dim(V) = tr(I_V)$ where $I_V : V \to V$ is the identity operation on V. Consequently, the relations

$$dim(V \otimes W) = dim(V)dim(W), \quad dim(V^*) = dim(V)$$

hold in Vec_k. Motivated by this construction for the category $\mathbf{Vec_k}$, an analogous trace operation can be defined for a morphism $f : A \to A$ in a ribbon category as follows.

Definition 3.2.12. *The* **trace** *of a morphism $f : A \to A$ in a ribbon category $\mathbf{C}$, denoted by $tr(f)$, is the morphism $tr(f) : 1 \to 1$ given by the composition*

$$tr(f) : 1 \xrightarrow{n_A} A \otimes A^* \xrightarrow{f \otimes I_{A^*}} A \otimes A^* \xrightarrow{\delta_A \otimes I_{A^*}} A^{**} \otimes A^* \xrightarrow{u_{A^*}} 1.$$

Due to the semisimple structure assumed for the ribbon category, recall that $Hom(1, 1) \cong \mathbb{C}$. Hence, the trace morphism $tr(f) \in \mathbb{C}$ is a scalar quantity. Likewise, for any simple object $A \in [\mathbf{C}]$ the semisimple structure also implies that $Hom(A, A) \cong \mathbb{C}$, which motivates the following definition.

Definition 3.2.13. *For a simple object $A \in [\mathbf{C}]$, define the* **quantum dimension** *of A as the positive real numbers $d_A := tr(I_A) \in \mathbb{R}$, where $I_A : A \to A$ is the identity morphism of A.*

The **global quantum dimension** *of $\mathbf{C}$ is the positive quantity $\mathcal{D}$ given by $\mathcal{D}^2 := \sum_{A \in [\mathbf{C}]} d_A^2$.*

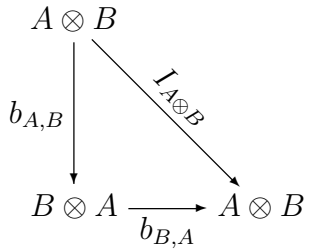
The set of quantum dimensions $\{d_A\}_{A \in [\mathbf{C}]}$ will also serve as characterizing numbers for the anyon model represented by the ribbon category $\mathbf{C}$. With these definitions of the trace and quantum dimension, the analogous properties of the trace that held for $\mathbf{Vec_k}$ can be verified. In particular, from these definitions it is readily observed (as in [29]) that the quantum dimensions satisfy $d_1 = 1$, $d_{A^*} = d_A$, and

$$d_A d_B = \sum_{C \in [\mathbf{C}]} N_{AB}^C d_C.$$

3.2.7 Modular categories

In this section, one of the last definitions will be made in order to define a *modular category* which completely captures the algebraic properties of an anyon model. The notions previously introduced to define a ribbon category are sufficient to understand what a modular category is. Roughly speaking, a modular category is one that satisfies a certain nondegeneracy condition on the braiding in the category. Given two simple objects $A, B \in \mathbf{C}$, consider the morphism $b_{B,A} b_{A,B} : A \otimes B \to A \otimes B$ which describes a double braiding of A with B. Now consider

diagrams of the following form for all simple objects $A, B \in [\mathbf{C}]$.



Essentially, a ribbon category is *modular*, if for all nontrivial simple objects $1 \neq A \in [\mathbf{C}]$, there exists at least one object $B \in \mathbf{C}$ such that the diagram *does not* commute. That is, $b_{B,A}b_{A,B} \neq I_{A\otimes B}$ for some $B \in [\mathbf{C}]$.

Alternatively, this nondegeneracy property that modularity demands can be stated more formally as follows. Since the double braiding $b_{B,A}b_{A,B}$ is a morphism from $A \otimes B$ to itself, the trace $tr(b_{B,A}b_{A,B})$ can be defined. This motivates the following

Definition 3.2.14. *For a ribbon category* $\mathbf{C}$*, the* S**-matrix** *is the square matrix whose rows/columns are indexed by simple objects* $A, B \in [\mathbf{C}]$*, with coefficients given by* $(S)_{A,B} = s_{AB}$ *where*

$$s_{AB} := \frac{1}{\mathcal{D}} tr(b_{B,A}b_{A,B}).$$

The quantity s_{AB} describes a certain invariant associated to anyon types A and B, and characterizes the process where the two anyon world-lines form a *Hopf link*. For a fixed type $A \in [\mathbf{C}]$ (referring to a certain row/column of the S-matrix), consider the vector S_A given by the A^{th} row of the S-matrix $(S_A)_B := s_{AB}$. The modularity condition of interest here is whether or not the vectors S_A for $A \in [\mathbf{C}]$ are linearly independent, which can be mathematically characterized efficiently by means of the determinant of the S-matrix (i.e. a matrix S has linearly independent rows/columns if and only if $\det(S) \neq 0$). In this way, a *modular* category is one in which the various quantities associated to the double-braidings are sufficiently nondegenerate.

Definition 3.2.15. *A ribbon category* $\mathbf{C}$ *is* **modular** *is there are a finite number of simple objects* $A \in [\mathbf{C}]$ *and the S-matrix satisfies* $\det(S) \neq 0$.

Why such categories are referred to as being "modular" in this setting will become more apparent once various topological notions are established in Chapter 4. For the anticipating reader, it will be seen that the S-matrix together with the T-matrix, defined as the diagonal square matrix consisting of the twist scalars θ_A given as $(T)_{A,B} = \theta_A \delta_{A,B}$, yield a projective representation of the *modular group* $SL_2(\mathbb{Z})$. The modular group, to be defined more formally later, is a group that captures the algebraic and topological properties of various homeomorphisms of the genus-1 torus.

3.2.8 Unitary modular tensor categories (UMTC)

The construction of a modular category and all its morphisms given here is motivated by finding a mathematical structure that captures the essence of a physical anyon model and all of its relevant dynamical processes. Continuing in this direction, since the ultimate objective is to define a valid quantum theory of the anyon model, the ribbon category of interest must also come equipped with a notion of morphisms being hermitian and unitary in order to properly describe the observables and time evolution of the theory.

Definition 3.2.16. *A ribbon category* $\mathbf{C}$ *is* **hermitian** *if for every morphism* $f : A \to B$ *in* $\mathbf{C}$ *there is a morphism* $f^\dagger : B \to A$ *such that*

$$f^{\dagger\dagger} = f, \quad (f \otimes g)^\dagger = f^\dagger \otimes g^\dagger, \quad (gf)^\dagger = f^\dagger g^\dagger$$

A ribbon category $\mathbf{C}$ *is* **unitary** *if every morphism* $f : A \to B$ *has an inverse which satisfies* $f^{-1} = f^\dagger$*. A* **unitary modular tensor category** *(written* **UMTC** *for short), is a modular category that is unitary.*

Having defined a UTMC, this now completes the description of the category theoretic concepts needed to describe an anyon model. In what follows it will be assumed that the category of interest that represents an anyon model is a UMTC. Consequently, both S and T matrices as defined in the previous section will be taken to be unitary. Moreover, the S matrix is symmetric so that the following symmetries hold

$$s_{AB} = s_{BA} = s_{A^*B^*} = \bar{s}_{A^*B} = \bar{s}_{BA^*} = \bar{s}_{AB^*} = \bar{s}_{B^*A},$$

where $\bar{z}$ denotes complex conjugation of $z \in \mathbb{C}$.

3.3 The Verlinde algebra

For notational convenience, throughout the remainder of this thesis, objects of a UTMC $\mathbf{C}$ will be denoted by lowercase letters $a, b \in [\mathbf{C}]$ with the exception of the tensor unit $1 \in [\mathbf{C}]$. Recall that the underlying monoidal structure is described by fusion rules of the form

$$a \otimes b = \sum_{c \in [\mathbf{C}]} N_{a,b}^c c.$$

where the fusion coefficients satisfy $N_{a,b}^c = dim Hom(a \otimes b, c)$. Since a braiding $b_{a,b} : a \otimes b \to b \otimes a$ defines an isomorphism it follows that $Hom(a \otimes b, c) \cong Hom(b \otimes a, c)$ implying that $N_{a,b}^c = N_{b,a}^c$.

Hence, fusion is essentially commutative. Also note that $N_{a,1}^c = N_{1,a}^c = \delta_{a,c}$ because of the defining properties of the tensor unit $1 \in [\mathbf{C}]$. With this in mind, a commutative C^*-algebra can be defined that captures the fusion properties of $\mathbf{C}$.

Definition 3.3.1. *The* **Verlinde algebra** *associated to the modular category* $\mathbf{C}$*, denoted by* $\mathsf{Ver}_{\mathbf{C}}$*, is the commutative* C^**-algebra with basis elements* $\{f_a\}_{a\in[\mathbf{C}]}$ *with multiplication satisfying*

$$f_a f_b = \sum_{C\in[\mathbf{C}]} N_{a,b}^c f_c, \tag{3.4}$$

and involution * *given by* $f_a^* = f_{a^*}$*.*

In the literature, the Verlinde algebra for a semisimple monoidal category $\mathbf{C}$ is often referred to as the *Groethendieck ring* of $\mathbf{C}$. Here, the basis element $f_1 \in \mathsf{Ver}_{\mathbf{C}}$ corresponds to the identity element of $\mathsf{Ver}_{\mathbf{C}}$ denoted as $I = f_1$. It is a general theorem of commutative C^*-algebras that states that such an algebra is isomorphic to a direct sum of copies of $\mathbb{C}$. This structure theorem for the Verlinde algebra will be important in deriving the results to follow.

Theorem 3.3.2. *The Verlinde algebra* $\mathsf{Ver}_{\mathbf{C}}$ *has dimension of size* $|[\mathbf{C}]|$*, where* $|[\mathbf{C}]|$ *denotes the number of simple objects in the category* $\mathbf{C}$*, and is isomorphic as an algebra to a direct sum of* $|[\mathbf{C}]|$ *copies of* $\mathbb{C}$ *written*

$$\mathsf{Ver}_{\mathbf{C}} \cong \mathbb{C}^{\oplus|[\mathbf{C}]|}.$$

Before establishing some further properties of $\mathsf{Ver}_{\mathbf{C}}$, consider the $|[\mathbf{C}]| \times |[\mathbf{C}]|$ matrices N_a (indexed by objects $b, c \in [\mathbf{C}]$) defined for each object $a \in [\mathbf{C}]$ as $(N_a)_{b,c} := N_{a,b}^c$. This matrix gives the action of multiplication by some fixed f_a on the basis $\{f_b\}_{b\in[\mathbf{C}]}$. Since fusion is commutative, $N_a N_b = N_b N_a$ for all $a, c \in [\mathbf{C}]$. Therefore, as a standard consequence of linear algebra the matrices $\{N_a\}_{a\in[\mathbf{C}]}$ can all be simultaneously diagonalized via a change of basis. In particular, the S matrix accomplishes this. To make this more precise, also define for each $a \in [\mathbf{C}]$, define the diagonal matrix D_a with entries $(D_a)_{b,c} = \frac{s_{a,b}}{s_{1b}}\delta_{bc}$.

Theorem 3.3.3. *The* S*-matrix diagonalizes the fusion rules. That is, for each* $a \in [\mathbf{C}]$*,*

$$SN_aS^{-1} = D_a.$$

Rearranging this expression in the theorem statement as $N_a = S^{-1}D_aS$, and equating matrix coefficients yields the following remarkable formula for the fusion coefficients $N_{a,b}^c$ which expresses them exclusively in terms of the entries of the S-matrix.

Theorem 3.3.4. *The fusion coefficients* $N_{a,b}^c$ *of a UMTC* $\mathbf{C}$ *satisfy*

$$N_{a,b}^c = \sum_{x\in[\mathbf{C}]} \frac{s_{ax}s_{bx}s_{c^*x}}{s_{1x}}, \tag{3.5}$$

which is known as the **Verlinde formula**.

Returning now to the Verlinde algebra $\mathsf{Ver}_{\mathbf{C}}$, in order to better characterize $\mathsf{Ver}_{\mathbf{C}}$, define the algebra elements $\{p_a\}_{a\in[\mathbf{C}]}$ as

$$p_a := \sum_{b\in[\mathbf{C}]} s_{1a}\bar{s}_{ba} f_b. \tag{3.6}$$

These identities can be inverted to express the basis $\{f_b\}_{b\in[\mathbf{C}]}$ in terms of the $\{p_a\}_{a\in[\mathbf{C}]}$ as

$$f_b = \sum_{b\in[\mathbf{C}]} \frac{s_{ba}}{s_{1b}} p_b. \tag{3.7}$$

The motivation for introducing the elements $\{p_a\}_{a\in[\mathbf{C}]}$ is to be able to decompose $\mathsf{Ver}_{\mathbf{C}}$ in an appropriate fashion as made explicit in the following

Theorem 3.3.5. *The set of algebra elements $\{p_a\}_{a\in[\mathbf{C}]}$ form a unique and complete set of minimal, orthogonal idempotents that span $\mathsf{Ver}_{\mathbf{C}}$, which can be decomposed as*

$$\mathsf{Ver}_{\mathbf{C}} = \bigoplus_{a\in[\mathbf{C}]} \mathbb{C}p_a, \tag{3.8}$$

and satisfy the properties $p_a p_b = \delta_{ab} p_b$, and $\sum_{a\in[\mathbf{C}]} p_a = f_1 =: I$.

That the set $\{p_a\}_{a\in[\mathbf{C}]}$ spans $\mathsf{Ver}_{\mathbf{C}}$ follows from the relation (3.7), and the fact that $\mathsf{Ver}_{\mathbf{C}}$ is constructed to be spanned by the basis $\{f_a\}_{a\in[\mathbf{C}]}$. Here, "minimal" simply means that the number of elements in $\{p_a\}_{a\in[\mathbf{C}]}$ is as small as possible, yet still spans $\mathsf{Ver}_{\mathbf{C}}$. The identity $p_a p_b = \delta_{ab} p_b$ expresses the orthogonality condition, and as a special case when $a = b$ yields idempotency: $p_a p_a = p_a$.

This analysis of the Verlinde algebra will be essential in defining an algebra of observables for topological quantum computation by means a suitable representation of $\mathsf{Ver}_{\mathbf{C}}$ acting on an appropriate Hilbert space defined by the underlying TQFT. Furthermore, the decomposition of $\mathsf{Ver}_{\mathbf{C}}$ given in (3.8) will be exploited to characterize *protected gates* to be studied later.

3.4 TQFTs as monoidal functors

In general, a TQFT is specified by a positive integer $n+1$ where n is the number of spatial dimensions of the space-time manifold of interest. Time functions as an additional temporal dimension to give a $(n+1)$-TQFT. Temporal change of the space under consideration is then described by certain transformations of the n-dimensional space and is given by a space-time

manifold having dimension $n+1$. Here it will be assumed that all manifolds under consideration are *smooth*, *compact* and *orientable* in the case where the latter can be defined. Moreover, the manifolds of interest can either be *open* or *closed* manifolds, meaning with or without boundaries, respectively. For some manifold M, denote by ∂M, the *boundary* of M. If M is a manifold of dimension $n+1$, then the boundary ∂M will generally have some dimension less than m. If M has no boundary, M will be called a *closed manifold* and ∂M will be the *empty manifold*, denoted as $\emptyset$, and it will be written $\partial M = \emptyset$. For the purposes of this thesis, in the case where M has a nonempty boundary, attention will be restricted to only the case where ∂M has dimension $m-1$.

3.4.1 Cobordism categories

The relevant mathematical entity that will be used to define an $(n+1)$-TQFT is a *cobordism category*, denoted $(\mathbf{n+1})\mathbf{Cob}$, which has n dimensional manifolds as objects and certain $n+1$ dimensional manifolds as morphisms. In particular, since this thesis is only concerned with $(2+1)$-TQFTs, the definition presented here will only be given specifically for **3Cob**. Before defining **3Cob** formally, consider the following preliminary definitions. A 2-dimensional orientable manifold, called a *surface*, can be oriented in 2 different ways. For a surface Σ with a given orientation, denote as $\overline{\Sigma}$ the same surface but with the opposite orientation. Given two surfaces Σ and Σ' of dimension n, define an operation $\amalg$ which gives another n dimensional manifold $\Sigma \amalg \Sigma'$ through the disjoint union of the two manifolds. Roughly speaking, the manifold $\Sigma \amalg \Sigma'$ represents Σ and Σ' being placed in the same ambient space together. This operation will serve to equip the category **3Cob** with a monoidal/tensor product on its objects.

Definition 3.4.1. *A* **cobordism** (M, Σ, Σ') *between n-dimensional manifolds Σ and Σ' is a $(n+1)$-manifold M whose boundary is the disjoint union of Σ and Σ', so that $\partial M = \Sigma \amalg \Sigma'$.*

In this definition, a cobordism is specified by a triple (M, Σ, Σ'), where Σ can be regarded as an *incoming* boundary component and Σ' an *outgoing* boundary component of M. Otherwise, regarding some manifold M as a cobordism may be somewhat ambiguous since a particular manifold M with boundary may have boundary components that can be decomposed in various ways. When this is clear by context, a cobordism specified by a triple (M, Σ, Σ') will simply be denoted by just M.

Definition 3.4.2. *The category* **3Cob** *is a monoidal category with*

- *objects $\Sigma, \Sigma' \in Ob(\mathbf{3Cob})$ given as surfaces (2-dimensional manifolds)*
- *morphisms $M : \Sigma \to \Sigma'$ being 3-dimensional cobordisms (M, Σ, Σ') such that $\partial M = \bar{\Sigma} \amalg \Sigma$*

- *composition of morphisms* $M : \Sigma \to \Sigma'$ *and* $M' : \Sigma' \to \Sigma''$ *given by* $M' \circ M : \Sigma \to \Sigma''$ *representing the cobordism* $(M' \circ M, \Sigma, \Sigma'')$ *with boundary* $\partial(M' \circ M) = \overline{\Sigma} \amalg \Sigma''$ *which glues* M *and* M' *along the common boundary* Σ'.

- *an identity morphism* $I_\Sigma : \Sigma \to \Sigma$, *for each object* $\Sigma \in Ob(\mathbf{3Cob})$, *given by the cobordism called the* **cylinder** *of* Σ *defined as* $I_\Sigma := \Sigma \times [0,1]$, *where* $[0,1]$ *is the unit interval, so that* $\partial I_\Sigma = \overline{\Sigma} \amalg \Sigma$

- *tensor products of objects given by the disjoint union* $\Sigma_1 \amalg \Sigma_2 \in Ob(\mathbf{3Cob})$

- *tensor products of morphisms* $M_1 : \Sigma_1 \to \Sigma_1'$ *and* $M_2 : \Sigma_2 \to \Sigma_2'$ *given by* $M_1 \amalg M_2 : \Sigma_1 \amalg \Sigma_2 \to \Sigma_1' \amalg \Sigma_2'$, *where* $M_1 \amalg M_2$ *is the cobordism with* $\partial(M_1 \amalg M_2) = (\overline{\Sigma_1 \amalg \Sigma_2}) \amalg (\Sigma_1' \amalg \Sigma_2')$.

- *a tensor unit given by the empty manifold* $\emptyset$ *so that* $\Sigma \amalg \emptyset = \Sigma = \emptyset \amalg \Sigma$

Though not explicitly stated for **3Cob** as a monoidal category, the left and right unitors, and associators for the category should be clear from context, and will not be too important for further developments. Actually, as it will be seen later, the category **3Cob** can be further equipped with more structure making it a modular category with a rigid, braided, and ribbon structure. This richer structure will become relevant for topological quantum computation, and will be introduced in later developments when the data of a UMTC will come into play for a TQFT.

3.4.2 $(2+1)$-TQFTs

The mathematical domain of quantum theory takes place on abstract vector spaces that are Hilbert spaces, which describe the state space of the quantum system. On the other hand, relativity theory is concerned with certain space-time manifolds on which various dynamics of physical entities takes place. The objective of a topological quantum field theory is to associate appropriate Hilbert spaces to topological manifolds that represent the space-time. Moreover, this correspondence should be such that transformations of the space-time get associated to appropriate linear transformations on the relevant Hilbert spaces. It is the focus of this thesis to study $(2+1)$ dimensional space-times, and so space-time will be modeled by 3-dimensional cobordisms. Thus, a $(2+1)$-TQFT can be thought of as a rule which makes a correspondence between two categories: $\mathbf{3Cob} \to \mathbf{Vec}_{\mathbb{C}}$. More specifically, a TQFT will be defined as a *monoidal functor* which maps objects and morphisms from one category to the other in a way that preserves the monoidal structure of the two categories. This is made explicit in the following definition.

Definition 3.4.3. *A $(2+1)$-TQFT is a* **monoidal functor** $\mathcal{T} : \mathbf{3Cob} \to \mathbf{Vec}_{\mathbb{C}}$ *which maps surfaces $\Sigma \in Ob(\mathbf{3Cob})$ to vector spaces $\mathcal{T}(\Sigma) \in Ob(\mathbf{Vec}_{\mathbb{C}})$ and cobordisms $M : \Sigma \to \Sigma'$ in* **3Cob** *to linear transformations $\mathcal{T}(M) : \mathcal{T}(\Sigma) \to \mathcal{T}(\Sigma')$ in $\mathbf{Vec}_{\mathbb{C}}$. If two cobordisms M and M' are homeomorphic as manifolds, written $M \simeq M'$, then $\mathcal{T}(M) = \mathcal{T}(M')$. Here, a functor $\mathcal{T}$ is a monoidal functor if it satisfies the following:*

1. *The identity morphism (cobordism) $I_\Sigma : \Sigma \to \Sigma$ gets assigned to the identity linear transformation $\mathcal{T}(I_\Sigma) = I : \mathcal{T}(\Sigma) \to \mathcal{T}(\Sigma)$.*

2. *If $M = M'' \circ M'$ in* **3Cob**, *then $\mathcal{T}(M) = \mathcal{T}(M'')\mathcal{T}(M')$ in $\mathbf{Vec}_{\mathbb{C}}$.*

3. *An object $\Sigma \in Ob(\mathbf{3Cob})$ given by the disjoint union $\Sigma = \Sigma_1 \amalg \Sigma_2$ gets mapped to the tensor product of vector spaces $\mathcal{T}(\Sigma) = \mathcal{T}(\Sigma_1) \otimes \mathcal{T}(\Sigma_2) \in Ob(\mathbf{Vec}_{\mathbb{C}})$.*

   The disjoint union of two cobordisms $M = M_1 \amalg M_2$ in **3Cob** *gets mapped to the tensor product of linear transformation $\mathcal{T}(M) = \mathcal{T}(M_1) \otimes \mathcal{T}(M_2)$.*

4. *The empty surface $\emptyset \in Ob(\mathbf{3Cob})$ gets assigned to the field $\mathcal{T}(\emptyset) = \mathbb{C} \in Ob(\mathbf{Vec}_{\mathbb{C}})$, and the empty cobordism $\emptyset \to \emptyset$ to the unit $1 \in \mathbb{C}$.*

Here, the condition that $\mathcal{T}(M) = \mathcal{T}(M')$ if $M \simeq M'$, meaning that two cobordisms M and M' are homeomorphic as manifolds (defined formally in Definition 4.1.1), is a naturality condition. This implies that a TQFT only considers homeomorphism classes of cobordisms, which is an essential feature of a TQFTs and will be exploited later. Statements 1 and 2 are just explicit ways of saying that $\mathcal{T}$ is a functor of categories, and statements 3 and 4 are the necessary conditions for the functor being a *monoidal functor* which preserves the tensor product structure.

A closed 3 dimensional manifold M without boundary may be regarded as a cobordism $(M, \emptyset, \emptyset)$ since $\partial M = \emptyset \amalg \emptyset = \emptyset$. Then as a consequence, since $\mathcal{T}(\emptyset) = \mathbb{C}$, the TQFT will associate the closed manifold M (thought of as a cobrdism $M : \mathcal{T}(\emptyset) \to \mathcal{T}(\emptyset)$) to a linear transformation $\mathcal{T}(M) : \mathbb{C} \to \mathbb{C}$, which is uniquely specified by its action on the unit $1 \in \mathbb{C}$ implying that $\mathcal{T}(M)$ is a scalar value in $\mathbb{C}$. Moreover, this quantity is the same for homeomorphic manifolds $M \simeq M'$ since in this case $\mathcal{T}(M) = \mathcal{T}(M')$ by naturality. It is in this sense that a TQFT is said to yield a *topological invariant* of closed 3-dimensional manifolds.

Despite describing the essence of a TQFT by means of a monoidal functor $\mathcal{T} : \mathbf{3Cob} \to \mathbf{Vec}_{\mathbb{C}}$, the precise form of the associated vector spaces $\mathcal{T}(\Sigma) \in Ob(\mathbf{Vec}_{\mathbb{C}})$ for some surfaces $\Sigma \in \mathbf{3Cob}$ has not been made explicit. To achieve such a description, the functor $\mathcal{T}$ requires additional data that will be provided by a UMTC which specifies a particular anyon model. Hence, for each UTMC $\mathbf{C}$, a TQFT can be constructed via a monoidal functor $\mathcal{T}_{\mathbf{C}}$. In Section

5.1, this construction will be described in detail and thereby provide an avenue for topological quantum computation.

Chapter 4

Topology

4.1 Topology of surfaces

Before investing in further details, some standard notions and terminology in the field of topology will be made in order to better understand the developing theory. Essentially, what is needed is a description of the various relevant surfaces (2-dimensional manifolds), and the nature of closed loops that can exist on them. Additionally, topological transformations called *homeomorphisms* of these surfaces and how these transformations change loops on the surface also need to be understood. A procedure for constructing more complicated surfaces from more elementary ones through "gluing", and deconstructing surfaces into simpler ones through "cutting" will serve as a method of understanding general surfaces. This will provide a means to construct the appropriate Hilbert spaces of interest, and the relevant algebra of observables, which will be defined in terms of the surfaces, loops, and a choice of an anyon model represented by a UMTC.

Most definitions presented here are standard notions in the field of topology and algebraic topology; and hence, can be found in most standard texts. A particularly enlightening reference is [25]. Although excessive for the purposes of this thesis, [17] offers an in-depth study on mapping class groups of surfaces.

4.1.1 Classification of surfaces

Topology is the study of spaces without regard to any metric that may be put on the space. Thus, the quantitative distance between two points is not relevant; yet, a topological space still holds some notion of points being "close" to one another and can deal with notions of continuity. The primary means of relating topological spaces is through the concept of a *homeomorphism*.

Definition 4.1.1. *Two topological spaces X and Y are considered topologically equivalent, written $X \simeq Y$, if there exists a map called a* **homeomorphism**, *$\vartheta : X \to Y$ such that ϑ is a bijection, continuous, and has an inverse map ϑ^{-1} that is also continuous.*

An equivalence relation can be put on topological spaces using the relation $X \simeq Y$ whenever there exists a homeomorphism $\vartheta : X \to Y$. However, determining wether two spaces X and Y are or are not homeomorphic can be a highly nontrivial task.

In what follows, the discussion will be limited to topological spaces that are surfaces (i.e. are 2-dimensional manifolds), since this is the physical arena where anyons are manifest. In addition, most surfaces under consideration will be assumed to be *connected*, roughly speaking "one piece", and otherwise considered *disconnected* being comprised of "many pieces". This is made formal in the following definition.

Definition 4.1.2. *A surface Σ is* **path-connected**, *if for any two points $x, y \in \Sigma$ there exists a continuous function called a* **path** *$P : [0, 1] \to \Sigma$ such that $P(0) = x$ and $P(0) = y$. If Σ is not path-connected, then it is assumed to be* **disconnected** *and is given as the disjoint union $\Sigma = \Sigma_1 \amalg \Sigma_2 \amalg \cdots \amalg \Sigma_k$, for some integer $k \geq 2$, where each Σ_i is path-connected and called a* **connected-component** *of Σ.*

With this is mind, it is sufficient to simply understand connected surfaces, since more general disconnected surfaces can be constructed through the disjoint union of these connected surfaces. The following Theorem 4.1.3 offers a characterization of connected surfaces. It states that orientable surfaces can be described by two values (g, b), where g is an integer representing the *genus* of the surface and b is the number of *boundary components* of the surface. Roughly speaking, the genus of a surface is the number of distinct "handles" that the surface has, and a boundary component is a "hole" in the surface whose boundary forms some closed loop. Each orientable surface can be oriented in two ways, and so one may regard two surfaces with the same genus and number of boundary components, but with opposite orientation, as distinct surfaces. Such distinctions between the choice of orientation assigned to a surface should be taken into consideration in appropriate contexts. In what follows, it will simply be assumed that a particular orientation is fixed when considering a surface, since the theory to be developed will be ultimately concerned with *orientation-preserving* homeomorphisms of surfaces.

Theorem 4.1.3. *A path-connected, compact, orientable manifold Σ is homeomorphic to precisely one surface $\Sigma_{(g,b)}$ having genus g and b boundary components so that $\partial\Sigma = B_1 \amalg B_2 \amalg \cdots \amalg B_b$, where each boundary component B_i is homeomorphic to the circle $S^1 \simeq B_i$.*

Note that the property that $\partial\Sigma = B_1 \amalg B_2 \amalg \cdots \amalg B_b$ consists of a disjoint union of circles follows from making the assumption that the boundary $\partial\Sigma$ is a closed 1-dimensional manifold.

Moreover, it will be assumed throughout that the orientations associated to each boundary component $B_i \subset \partial\Sigma$ of an open surface Σ is oriented so that moving along the boundary component B_i in the direction of the orientation is such that the surface Σ appears on the left-hand side.

4.1.2 DAP-decompositions

In algebraic topology, methods are deployed which seek to study topological spaces through more algebraic means. In particular, a space X can be characterized by the properties of various closed loops that may exist on the space. Formally,

Definition 4.1.4. *A* **loop** *on a topological space X is the image of a continuous map $C : [0,1] \to X$ such that $C(0) = C(1)$.*

The map which defines a loop $C : [0,1] \to X$ embeds some parametrization of the circle into the space X. Technically speaking, it is the image $C([0,1]) \subseteq X$ thought of as a subspace of X that corresponds to the actual loop on the space X. Regardless, for notational convenience, when referring to a loop the map C will be conflated with the image $C([0,1])$ throughout this thesis.

Given two loops $C, C' \subseteq X$ on a topological space X, one natural question to ask is whether or not one loop can be continuously deformed into the other. This motivates the following definition

Definition 4.1.5. *Two loops $C, C' : [0,1] \to X$ are said to be* **homotopic***, if there exists a continuous function called a* **homotopy** *$H : [0,1] \times [0,1] \to X$ such that $H(t,0) = C(t)$ and $H(t,1) = C'(t)$. A loop C is said to be* **null-homotopoic** *or a* **trivial loop** *if it is homotopic to a loop $C_0 : [0,1] \to X$ which is a constant function; meaning $C_0(t) = x \in X$ for all $t \in [0,1]$.*

In this definition, a trivial loop is essentially one which can be contracted to a single point in X. For a topological space X, this notion of homotopy can be used to put an equivalence relation on loops where two loops are in the same *homotopy class* if and only if they are homotopic. Furtheremore, the set of equivalence classes of homotopic loops for a surface $\Sigma_{(g,b)}$ is always finite. Every surface has trivial loops, but not all surfaces have non-trivial loops. An example of the latter is the 2-dimensional sphere $S^2 \simeq \Sigma_{(0,0)}$, which is a surface with zero genus and no boundary components. In this case, the sphere S^2 has only one trivial homotopy class of loops on the surface. If there exists a non-contractable/non-trivial loop on a surface, then the surface has either a non-empty boundary, and/or has a nonzero *genus*, implying that there exists at least one other nontrivial homotopy class of loops on the surface.

Given some surface Σ and some loop $C \subset \Sigma$, a new surface Σ_C can be defined which is the resulting surface obtained by *cutting* Σ along the loop C. Depending on the topological nature of the loop C as it exists on the surface this resulting surface can be of two types, either a connected surface or a disconnected surface with two additional boundary components, as made precise in the following definition.

Definition 4.1.6. *Let Σ be a surface and $C \subset \Sigma$ some loop. Define the* **cut surface** *Σ_C to be the surface that results from* **cutting** *Σ along the loop C.*

A loop C is **disconnecting** *if $\Sigma_C = \Sigma_1 \amalg \Sigma_2$ is a disconnected surface where the cut along C yields two additional boundary components $C_1 \subset \partial\Sigma_1$ and $C_2 \subset \partial\Sigma_2$ on the resulting surfaces Σ_1 and Σ_2, respectively.*

A loop C is **non-disconnecting** *or* **connecting** *if the surface Σ_C which results from cutting Σ along C is a connected surface with two additional boundary components $C_1, C_2 \subset \partial\Sigma_C$ such that $\partial\Sigma_C = \partial\Sigma \amalg C_1 \amalg C_2$.*

For two surfaces Σ_1 and Σ_2 such that each surface has at least one boundary component (where by assumption each boundary is homeomorphic to the circle S^1), a new surface can be constructed that *glues* Σ_1 and Σ_2 along some choice of two boundary components from the respective surfaces. This is made formal in the following definition.

Definition 4.1.7. *Let Σ_1 and Σ_2 be two connected surfaces with nonempty boundaries, and let $B_1 \subset \partial\Sigma_1$ and $B_2 \subset \partial\Sigma_2$ be some boundary component of Σ_1 and Σ_2, respectively. Define the* **glued surface** *$\Sigma_1 \cup_{(B_1,B_2)} \Sigma_2$ which identifies the two boundary components B_1 and B_2. If Σ_1 and Σ_2 are surfaces of type (g_1, b_1) and (g_2, b_2), respectively, then $\Sigma_1 \cup_{(B_1,B_2)} \Sigma_2$ is a surface of type $(g_1 + g_2, b_1 + b_2 - 2)$.*

For the cutting process a convention is adopted where the orientations of the additional boundary loops C_1, C_2 that result from cutting, are chosen so that the orientation(s) of the resulting surface(s) is consistent with the original(s).

Three particular elementary surfaces will play a special role in understanding more general surfaces. For this reason, they are given the following names:

Definition 4.1.8. *Call any surface Σ an* **elementary surface** *if it is homeomorphic to either of the following:*

- *a* **disk** *if $\Sigma \simeq \Sigma_{(0,1)}$*
- *an* **annulus** *if $\Sigma \simeq \Sigma_{(0,2)}$*

- *a* **pant** *if* $\Sigma \simeq \Sigma_{(0,3)}$

With this in mind, the characterization of arbitrary surfaces $\Sigma_{(g,b)}$ can be further understood through the cutting of $\Sigma_{(g,b)}$ into a collection of elementary surfaces. Equivalently, any general surface $\Sigma_{(g,b)}$ can be constructing from gluing together some collection of elementary surfaces.

Theorem 4.1.9. *Any surface homeomorphic to* $\Sigma_{(g,b)}$*, can be cut along a set* $\mathcal{C}$ *of nonintersecting curves on the surface, so that the resulting surface(s) are homeomorphic to disks, annuli, or pants.*

A collection of nonintersecting curves $\mathcal{C}$ that achieves a decomposition mentioned in Theorem 4.1.9, is not unique. It can be possible that two collections of curves $\mathcal{C}$ and $\mathcal{C}'$ both yield decompositions into elementary surfaces, but only have some or no curves in common. Moreover, the number of curves in some collection $\mathcal{C}$ can be made arbitrarily large while still achieving such a decomposition. However, in this case, the resulting elementary surfaces may be redundant. Therefore, attention will be restricted to a set of curves $\mathcal{C}$ that contains the minimal number of curves such that cutting along the curves in $\mathcal{C}$ yields the smallest number of constituent pieces that are homeomorphic to disks, annuli, and pants.

Definition 4.1.10. *For a closed surface* Σ*, a collection of nonintersecting curves* $\mathcal{C}$ *is called a* **DAP-decomposition** *if cutting along the set of curves yields a minimum number of surfaces that are homeomorphic to only disks, annulli, and pants. For an open surface* Σ*, the DAP-decomposition* $\mathcal{C}$ *must include curves that are homotopic to each boundary component of* Σ*.*

Local moves

Even with the restricted Definition 4.1.10, a DAP-decomposition need not be unique. However, in certain cases the loops in two different DAP-decompositions may be related through certain *local moves* of the surface under consideration which interchange certain pairs of loops on the surface. To illustrate this, consider the torus $T := \Sigma_{(1,0)}$, which has two nontrivial homotopy classes of loops represented by C and C'. Both singleton sets $\mathcal{C} = \{C\}$ and $\mathcal{C}' = \{C'\}$ suffice to yield valid DAP-decompositions which cut T into a single annulus. Note that these primitive loops C and C' intersect each other once and will be called *conjugate loops*. In this case, there exists a local move called the *S-move* which transforms one loop to the other. In fact, such a transformation can be achieved by a homeomorphism $s : T \to T$ as described in the next section.

For higher genus closed surfaces of the form $\Sigma_{(g,0)}$ there are g "handles" on the surface, and for each handle a pair of conjugate loops C_i and C_i' (where $1 \leq i \leq g$) that belong to distinct

nontrivial homotopy classes. Accordingly, for each pair there is a corresponding *local S-move* that interchanges the two conjugate loops.

Now consider the genus-zero open surface $\Sigma_{(0,4)}$ referred to as the 4-*punctured sphere*. In addition to the four loops homotopic to the four boundary components of $\Sigma_{(0,4)}$, a valid DAP-decomposition $\mathcal{C}$ can be achieved with either of the two loops C and C' which cut the surface into two pants $\Sigma_{(0,3)} \amalg \Sigma_{(0,3)}$. Despite intersecting each other, these two loops belong to distinct nontrivial homotopy classes. The local move which interchanges C and C' on the 4-punctured sphere is called the *F-move*.

Generalizing this scheme, for the $\Sigma_{(0,n)}$ referred to as the *n-punctured sphere*, valid DAP-decompositions can be achieved by choosing $n-2$ loops C_i which cut the surface into $n-2$ many pants. Each such loop has a corresponding conjugate loop C_i' that could alternatively be chosen for the DAP-decomposition. Then analogously, for each pair there is also a corresponding local F-moves which interchanges the conjugate loops C_i and C_i'.

A combination of the methods just described for surfaces of type $\Sigma_{(g,0)}$ and $\Sigma_{(0,b)}$, with $g, b \geq 1$, can be used to construct DAP-decompositions of an arbitrary surface $\Sigma_{(g,b)}$. Moreover, a combination of local S-moves and F-moves can be used to relate various DAP-decompositions. These local moves alone do not suffice to construct any possible DAP-decomposition from a given one. As it will be seen in the next section, homeomorphisms of $\Sigma_{(g,b)}$ can also relate more general DAP-decompositions to one another. Then with these homeomorphisms in addition to the local moves, arbitrary DAP-decompositions of a particular surface can be related.

4.1.3 The Mapping Class Group

When considering a surface Σ it is natural to think of the surface as being *embeded* in the higher 3 dimensional space which contains it, say $\mathbb{R}^3$. More formally:

Definition 4.1.11. *An* **embedding** *of a surface Σ in $\mathbb{R}^3$ is given by an injective and continuous function $f : \Sigma \to \mathbb{R}^3$, such that Σ is homeomorphic to its image $f(\Sigma) \subset \mathbb{R}^3$.*

With this definition in mind, a loop $C \subset \Sigma$ as defined in Definition 4.1.4, can be equivalently defined as an embedding map $f : S^1 \to \Sigma$ which embeds the circle S^1 into a surface Σ. Again, just as it was done with loops, the surface Σ and its embedding $f(\Sigma)$ will be conflated for notational convenience whenever it is implicit that the surface under consideration is embedded since $\Sigma \simeq f(\Sigma)$.

Of course, there can exist many ways to embed a particular object in a space. Consider embeddings $f, f_1, f_2 : \Sigma \to \mathbb{R}^3$ of a surface Σ. Then naturally by definition, the embedded

surfaces are always homeomorphic: $f(\Sigma) \simeq f_1(\Sigma) \simeq f_2(\Sigma)$. Let $\vartheta_1 : f(\Sigma) \to f_1(\Sigma)$ and $\vartheta_2 : f(\Sigma) \to f_2(\Sigma)$ be the corresponding homeomorphisms. Despite this natural equivalence between different embeddings of a surface, a finer notion of equivalence between the different homeomorphisms ϑ_1 and ϑ_2 can be made that is analogous to the notion of homotopy introduced in Definition 4.1.5 for loops. This is the topic of the next discussion.

When there exists a homeomorphism $\vartheta : f_1(\Sigma) \to f_2(\Sigma)$, a continuous map is defined that maps points of $f_1(\Sigma)$ to points of $f_2(\Sigma)$. However, this is essentially a static notion relating the two surfaces— a sort of "before-and-after" map. Instead, one can imagine a more dynamical process in which the points of $f_1(\Sigma)$ continuously change in time rearranging themselves in a form equivalent to the arrangement of points on the embedded surface $f_2(\Sigma)$ such that, at every moment in time, the surface remains embedded and homeomorphic to itself. If such a dynamical process exists, the two homeomorphisms ϑ_1 and ϑ_2 will be related and referred to as being *isotopic*.

Now, restrict attention to *self-homeomorphisms* $\vartheta : \Sigma \to \Sigma$ of some surface Σ to itself that preserve the orientation of Σ, and in the case that Σ has a nonempty boundary, the homeomorphism acts as the identity on the boundary components. All such self-homeomorphosms of a surface Σ can be thought of as an abstract topological space denoted $Homeo(\Sigma)$. A single point in $\vartheta \in Homeo(\Sigma)$ is a homeomorphism $\vartheta : \Sigma \to \Sigma$. In general, the space $Homeo(\Sigma)$ may be disconnected, and a connected component of $Homeo(\Sigma)$, called an *isotopy class*, consists of homeomorphisms ϑ_1 and ϑ_2 which can be connected by a continuous path in the space $Homeo(\Sigma)$ that represents an *isotopy*. In this way, an equivalence relation can be put on $Homeo(\Sigma)$ where two homeomorphisms $\vartheta_1, \vartheta_2 \in Homeo(\Sigma)$ are in the same equivalence class if and only if they are in the same isotopy class. For $\vartheta \in Homeo(\Sigma)$, denote its equivalence class as $[\vartheta]$.

Two homeomorphisms $\vartheta_1, \vartheta_2 \in Homeo(\Sigma)$ can be composed to yield another homeomorphism $\vartheta := \vartheta_2\vartheta_1 : \Sigma \to \Sigma$. Moreover, a composition of isotopy classes of $Homeo(\Sigma)$ can be defined as $[\vartheta] = [\vartheta_2][\vartheta_1]$. Since the identity homeomorphism is always defined for any surface, and all homeomorphisms have inverses, this composition rule can be used to define a group structure on the set of isotopy classes of $Homeo(\Sigma)$.

Definition 4.1.12. *The* **mapping class group** *of a surface Σ, denoted MCG_Σ, is the group of isotopy classes of orientation-preserving self-homeomorphisms $\vartheta : \Sigma \to \Sigma$ which fix the boundary and act as the identity on any boundary components of Σ. The group operation on elements $[\vartheta_1], [\vartheta_2] \in \mathsf{MCG}_\Sigma$ is given by the composition of isotopy classes: $[\vartheta_2][\vartheta_1] = [\vartheta_2\vartheta_1]$.*

As an analogy, when studying linear transformations of vector spaces, the action of a linear transformation can be characterized by its action on vectors of the particular vector space which

serves as the domain of the linear transformation. In the same way, when studying homeomorphisms of a surface Σ, it is useful to characterize the action of a homeomorphism through its action on various loops $C \subset \Sigma$ that can exist on the surface. Thus, a homeomorphism $\vartheta : \Sigma \to \Sigma$ will often be described by how it transforms a loop $C \mapsto \vartheta(C)$ on the surface Σ.

With this in mind, consider a surface Σ and some DAP-decomposition $\mathcal{C} = \{C_i\}_{i=1}^n$ of the surface. Then given some homeomorphism $\vartheta : \Sigma \to \Sigma$, its action on loops $C_i \in \mathcal{C}$ transforms them to loops $\vartheta(C_i) \subset \Sigma$ such that the set of loops $\{\vartheta(C_i)\}_{i=1}^n$ yields another valid DAP-decomposition of Σ. This property will play an essential role in understanding protected gates in the context of topological quantum computation.

Chapter 5

Topological quantum computation

As described in the Section 3.4, a $(2+1)$-topological quantum field theory is essentially given by a functor between categories

$$\mathcal{T} : \mathbf{3Cob} \to \mathbf{Vec}_{\mathbb{C}}.$$

Given a surface $\Sigma \in Ob(\mathbf{3Cob})$, a TQFT associates a Hilbert space $\mathcal{T}(\Sigma) \in Ob(\mathbf{Vec}_{\mathbb{C}})$. However, no details were given to describe the precise form of the Hilbert space $\mathcal{T}(\Sigma)$. This is because there exists a multitude of ways to construct such a functor which satisfies the axioms of a TQFT given in Definition 3.4.3. To accomplish this, first a choice of some UMTC must be made. Then once the data provided by a UTMC $\mathbf{C}$ is given a particular functor $\mathcal{T}_{\mathbf{C}} : \mathbf{3Cob} \to \mathbf{Vec}_{\mathbb{C}}$ can be constructed which provides an explicit way to associate a Hilbert space $\mathcal{T}_{\mathbf{C}}(\Sigma)$ for an arbitrary surfaces Σ. These spaces will function as the computational Hilbert space associated to the arena where anyons are manifest. Section 5.1 will serve to describe these topological Hilbert spaces through an axiomatic approach, and then explicitly give certain basis representations of the spaces for certain surfaces.

Furthermore, the functor $\mathcal{T}_{\mathbf{C}}$ will also give explicit representations of a cobordism $M : \Sigma \to \Sigma'$, as linear transformations $\mathcal{T}_{\mathbf{C}}(M) : \mathcal{T}_{\mathbf{C}}(\Sigma) \to \mathcal{T}_{\mathbf{C}}(\Sigma')$. In this context, the cobordisms M will describe certain transformations of the surface Σ to another Σ', which describe various anyon dynamics that may take place. For most scenarios of interest in this thesis attention will be restricted to cobordisms $M : \Sigma \to \Sigma$ from a surface to itself. In this case, the transformation described by M will correspond to a self-homeomorphism $\vartheta_M : \Sigma \to \Sigma'$. The linear transformations that represent these morphisms will be unitary operators $U : \mathcal{H}_\Sigma \to \mathcal{H}_\Sigma$ and be expressed, for example, by S, T, F and R matrices (as they are commonly referred to in the literature) that describe the action of certain basis changes and anyonic dynamics such as twisting and braiding. Therefore, by considering all self-homemorphisms $\vartheta_M \in \mathsf{MCG}_\Sigma$ of the mapping class

group of Σ, the action of the functor $\mathcal{T}_{\mathbf{C}}$ provides a group representation of Σ

$$\begin{aligned} \mathcal{T}_{\mathbf{C}} : \Sigma &\to \mathcal{U}(\mathcal{H}_\Sigma) \\ \vartheta_M &\mapsto \mathcal{T}_{\mathbf{C}}(\vartheta_M), \end{aligned} \tag{5.1}$$

where $\mathcal{U}(\mathcal{H}_\Sigma)$ is the group of unitary operators acting on $\mathcal{H}_\Sigma$. Note that the single functor $\mathcal{T}_{\mathcal{C}}$ defined by the TQFT gives such a group representation of Σ for each surface Σ. It is through these transformations that quantum computation can be enacted on suitable Hilbert spaces. The nature of the image under the representation $\mathcal{T}_{\mathbf{C}}(\Sigma) \subseteq \mathcal{U}(\mathcal{H}_\Sigma)$ determines the computational power the model can afford (i.e. what "quantum gates" can be performed).

Some useful references to the literature pertaining to topological quantum computation can be found in the Appendix of [29], the lecture notes of [40], and in [13].

5.1 The topological Hilbert space $\mathcal{H}_\Sigma := \mathcal{T}_{\mathbf{C}}(\Sigma)$

Let $\mathbf{C}$ be a UTMC representing some anyon model of interest, and consider the $(2+1)$-TQFT

$$\mathcal{T}_{\mathbf{C}} : \mathbf{3Cob} \to \mathbf{Vec}_{\mathbb{C}},$$

where $\mathcal{T}_{\mathbf{C}}$ is a functor which maps surfaces $\Sigma \in Ob(\mathbf{3Cob})$ to some Hilbert space $\mathcal{T}_{\mathbf{C}}(\Sigma) \in Ob(\mathbf{Vec}_{\mathbb{C}})$. The space $\mathcal{T}_{\mathbf{C}}(\Sigma)$ will be defined with respect to the anyon model $\mathbf{C}$ and surface Σ, but since the category/anyon model $\mathbf{C}$ is fixed such a subscript will be notationally redundant in specifying the Hilbert space $\mathcal{T}_{\mathbf{C}}(\Sigma)$. Therefore, make the following notational definition when it is understood and made implicit what UMTC $\mathbf{C}$ is being used to define the TQFT $\mathcal{T}_{\mathbf{C}}$.

Definition 5.1.1. *Let $\mathcal{H}_\Sigma := \mathcal{T}_{\mathbf{C}}(\Sigma)$ denote the Hilbert space assigned to the surface Σ under the TQFT $\mathcal{T}_{\mathbf{C}}$.*

In particular, the properties of $\mathcal{H}_\Sigma$ which depend on Σ will be inherently topological and provided through DAP-decompositions of Σ. In regards to the dependence of the UTMC $\mathbf{C}$, all that is essentially needed to define the space $\mathcal{H}_\Sigma$ is the nature of the fusion rules of the anyon model represented by $\mathbf{C}$. Recall that the fusion rules of the model are expressed in terms of the anyon types/simple objects $[\mathbf{C}]$ together with their corresponding fusion coefficients $N_{a,b}^c$ as defined in Definition 3.2.7, and the richer categorical structure of $\mathbf{C}$ is not explicitly needed. Therefore, the anyon types/simple objects will be denoted by a *label set* $\mathbb{A}$ and the following notational conventions will be made.

Definition 5.1.2. *Let* $\mathbb{A} := [\mathbf{C}]$ *denote the finite set of labels which represent the anyon types/simple objects of the UTMC* $\mathbf{C}$*. Let* $1 \in \mathbb{A}$ *denote the trivial anyon type, and let* $\bar{a}$ *denote the dual anyon type of* $a \in \mathbb{A}$*.*

Although the fusion rules of a UTMC $\mathbf{C}$ suffice to specify a basis of $\mathcal{H}_\Sigma$, the richer categorical structure of $\mathbf{C}$ arising from the modularity conditions will be necessary to relate different choices of a basis for $\mathcal{H}_\Sigma$. In particular, this additional algebraic and topological data will be used to give representations of various local moves that may be performed on loops as well as representations of the mapping class group as in Equation (5.1). This will be further described in a later section of this chapter.

5.1.1 The flux basis of $\mathcal{H}_\Sigma$

The general ingredients for constructing the Hilbert space $\mathcal{H}_\Sigma$ will be given through axioms which specify elementary Hilbert spaces $\mathcal{H}_\Sigma$ for the elementary surfaces $\Sigma_{(0,b)}$ for $b = 1, 2, 3$ (a disk, annulus, and pant). Then an additional axiom, called *the gluing axiom* will given which serves as a recipe for constructing the Hilbert space associated to a surface Σ that results from gluing together two boundary components B and B' of a surface(s). These axioms will then be sufficient to describe a basis for the Hilbert space $\mathcal{H}_\Sigma$ for an arbitrary surface Σ by means of a DAP-decomposition, which relates Σ to its constituent elementary surfaces that comprise it. Different DAP-decompositions of Σ will yield different basis of $\mathcal{H}_\Sigma$.

A basis for $\mathcal{H}_\Sigma$ is made explicit through certain labelings of the loops $C \in \mathcal{C}$ of some DAP-decomposition $\mathcal{C}$ of Σ. In particular, the loops of $\mathcal{C}$ will be labeled by anyon types $\mathbb{A}$ of a fixed model under consideration; hence, a labeling will be given by a map $\ell : \mathcal{C} \to \mathbb{A}$. Moreover, various loops of $\mathcal{C}$ must be labelled according to some rules which satisfy *fusion consistency* relations. In regards to faithfully modeling the actual physics of the theory, the motivation for defining the Hilbert space $\mathcal{H}_\Sigma$ in this way is that the loops of a valid DAP-decomposion of a surface Σ are precisely those loops on the physical surface represented by $\mathcal{H}_\Sigma$ that can carry a physically observable flux along the loop. The flux associated to a loop is specified by an anyon type in $\mathbb{A}$, and the various types of flux associated to various possible loops on the surface must be related in a physically consistent way as made mathematically formal in Definition 5.1.3 given below for a *fusion consistent labeling*.

Before proceeding, one technicality regarding open surfaces $\Sigma_{(g,b)}$ with $b \geq 1$ must be mentioned. Recall that in Definition 4.1.10 of a DAP-decomposition $\mathcal{C}$, loops $C_i \subset \partial\Sigma_{(g,b)}$ corresponding to the boundary loops must be included in $\mathcal{C}$. When considering open surfaces, an anyon type $a_i \in \mathbb{A}$ will be associated to the boundary loops when considering the surface.

Hence, such surfaces will be denoted as $\Sigma_{(g,b)}^{(a_1,\ldots,a_b)}$ in order to specify that boundary loop C_i is labelled with anyon type $a_i \in \mathbb{A}$. The reason for this is that open surfaces $\Sigma_{(g,b)}^{(a_1,\ldots,a_b)}$ in this study correspond to the physical scenario where fixed anyon types $a_i, \ldots, a_b \in \mathbb{A}$ are present on the surface. The detection of one of these anyons can be made in principle by a measurement corresponding to a closed loop containing a particular anyon. Furthermore, it is assumed that the flux associated to the boundary loops cannot be changed. In this sense, considering the surface $\Sigma_{(g,b)}^{(a_1,\ldots,a_b)}$ is like imposing certain "boundary conditions" which must be preserved.

Definition 5.1.3. *A* **labelling** *is a map $\ell : \mathcal{C} \to \mathbb{A}$ of a DAP-decomposition $\mathcal{C}$ of a surface Σ, and is said to be a* **fusion consistent labeling** *if the following is true:*

- *If for any loop $C \in \mathcal{C}$ that defines the boundary of a disk $\Sigma_{(0,1)}$, then $\ell(C) = 1$.*
- *If for any pair of loops $C_1, C_2 \in \mathcal{C}$ that define the boundary of an annulus $\Sigma_{(0,2)}$, then $\ell(C_1) = \overline{\ell(C_2)}$.*
- *If for any triple of loops $C_1, C_2, C_2 \in \mathcal{C}$ that define the boundary of a pant $\Sigma_{(0,3)}$, the labelling satisfies $N_{\ell(C_1),\ell(C_2)}^{\overline{\ell(C_3)}} \neq 0$.*
- *If $\Sigma = \Sigma_{(g,b)}^{(a_1,\ldots,a_b)}$ is an open surface with labelled boundary components $C_1, \ldots, C_b \in \mathcal{C}$, then the labelling must satisfy $\ell(C_i) = a_i$ for $1 \leq i \leq b$.*

Denote by $\mathsf{L}(\mathcal{C})$ the **set of all fusion consistent labelings** *of a DAP-decomposition $\mathcal{C}$.*

Having defined the set $\mathsf{L}(\mathcal{C})$ of fusion consistent labelings of a DAP-decomposition $\mathcal{C}$ of a surface Σ, the axiom which describes the Hilbert space $\mathcal{H}_\Sigma$ can be stated.

Axiom 1 (Flux Basis). *Let $\mathcal{C}$ be a DAP-decomposition of Σ, then the Hilbert space $\mathcal{H}_\Sigma$ is the formal span of fusion consistent labelings $\ell \in \mathsf{L}(\mathcal{C})$:*

$$\mathcal{H}_\Sigma := \sum_{\ell \in \mathsf{L}(\mathcal{C})} \mathbb{C}|\ell\rangle,$$

where the set $\{|\ell\rangle\}_{\ell \in \mathsf{L}(\mathcal{C})}$ forms an orthonormal basis of $\mathcal{H}_\Sigma$ with an inner-product satisfying $\langle \ell \mid \ell' \rangle = \delta_{\ell,\ell'}$ for $\ell, \ell' \in \mathsf{L}(\mathcal{C})$.

To summarize the Flux Basis Axiom, let $\{P_a(C)\}_{a \in \mathbb{A}}$ be a set of projectors corresponding to some fixed loop $C \subset \Sigma$ carrying a flux of type $a \in \mathbb{A}$. There exists such a family of projectors for every loop $C \in \Sigma$. Given a DAP-decomposition $\mathcal{C}$ of Σ, and a fusion consistent labelling $\ell \in \mathsf{L}(\mathcal{C})$, a basis state $|\ell\rangle \in \mathcal{H}_\Sigma$ corresponds to the simultaneous $+1$ eigenspace of the set of projectors $\{P_{\ell(C)}\}_{C \in \mathcal{C}}$ which correspond to a loop $C \in \mathcal{C}$ carrying a flux of type $\ell(C)$. Thus, the

basis $\{|\ell\rangle\}_{\ell\in\mathsf{L}(\mathcal{C})}$ represents the different compatible ways flux can be associated to the loops on the surface Σ. A general state of $\mathcal{H}_\Sigma$, can then be arbitrary (normalized) linear combinations of these basis states, which provides a notion of the flux to be in a "superposition" of different flux types. Some more physical motivation for the Flux Basis axiom will be provided when applying it to characterize the topological Hilbert spaces associated to the elementary surfaces in Section 5.1.3.

5.1.2 The Gluing Axiom

A DAP-decomposition $\mathcal{C}$ of a surface Σ provides a way of thinking about Σ in terms of its constituent elementary pieces. In this regard, the Gluing Axiom to be stated provides a means of relating the Hilbert space $\mathcal{H}_\Sigma$ to the Hilbert spaces associated to its constituent surfaces. Given a connected surface $\Sigma = \Sigma_{(g,b)}$, cutting along a nontrivial loop $C \subset \Sigma_{(g,b)}$ results in a potentially disconnected surface Σ'_C which has two additional boundary loops $B_1, B_2 \in \partial\Sigma'_C$ that result from cutting along C (which are assumed to be oppositely oriented as to preserve the orientation of the resulting surface). Let $\Sigma'_C(a,\overline{a})$ denote the surface Σ'_C where the two boundary loops have been labeled by $a, \overline{a} \in \mathbb{A}$, respectively. The Gluing Axiom then relates the Hilbert space $\mathcal{H}_\Sigma$ to the spaces $\mathcal{H}_{\Sigma'_C(a,\overline{a})}$ in the case where $C \in \mathcal{C}$ is a loop that is part of a DAP-decomposition of Σ.

Axiom 2 (Gluing). *Let $C \in \mathcal{C}$ be a loop in some DAP-decomposition of a surface Σ, and let $\Sigma'_C(a,\overline{a})$ denote the cut surface that results from cutting Σ along C with the two additional boundary loops labeled by $a, \overline{a} \in \mathbb{A}$, respectively. Then*

$$\mathcal{H}_\Sigma = \bigoplus_{\ell\in\mathsf{L}(\mathcal{C})} \mathcal{H}_{\Sigma'_C(\ell(C),\overline{\ell(C)})}. \tag{5.2}$$

The Gluing Axiom can be interpreted in two equivalent ways. The first, as the name suggests, considers a surface (possibly disconnected) with at least two boundary components labelled with the pair a and $\overline{a}$ of dual anyon types, and defines the Hilbert space $\mathcal{H}_\Sigma$ corresponding to the surface Σ that results when the two labelled boundary components are glued together by taking the direct sum of the Hilbert spaces over fusion-consistent labelings. The second interpretation decomposes the Hilbert space $\mathcal{H}_\Sigma$ into a direct sum of the Hilbert spaces corresponding to the cut surfaces labelled according to fusion-consistent labelings. In this way, the Hilbert spaces associated to arbitrary surfaces can be understood through elementary surfaces since there always exists a DAP-decomposition which relates the arbitrary surface to constituent elementary surfaces

Assuming that Σ is a connected surface, whether or not the cut surface Σ'_C is a (dis)connected surface depends on whether the loop $C \subset \Sigma$ is (dis)connecting (as defined in Definition 4.1.6). If C is a disconnecting curve then $\Sigma'_C = \Sigma_1 \amalg \Sigma_2$ is the disjoint union of two connected surfaces. Let $\Sigma'_C(a, \overline{a}) = \Sigma_1(a) \amalg \Sigma_2(\overline{a})$ be the surface where the two additional boundary components resulting from cutting along C are labelled by $a, \overline{a} \in \mathbb{A}$, respectively. Then by virtue of $\mathcal{T}_{\mathcal{C}}$ being a monoidal functor (Definition 3.4.3, Property 3.) it follows that $\mathcal{H}_{\Sigma'_C(a,\overline{a})} = \mathcal{H}_{\Sigma_1(a)} \otimes \mathcal{H}_{\Sigma_2(\overline{a})}$, and so Equation (5.2) becomes

$$\mathcal{H}_{\Sigma} = \bigoplus_{\ell \in \mathsf{L}(\mathcal{C})} \mathcal{H}_{\Sigma_1(\ell(C))} \otimes \mathcal{H}_{\Sigma_2(\overline{\ell(C)})}. \tag{5.3}$$

In general, by considering surfaces Σ with multiple cuts performed along various loops, the Hilbert space $\mathcal{H}_{\Sigma}$ can be decomposed as a direct sum over a many-fold tensor product of the Hilbert spaces associated to the constituent surfaces resulting from the various cuts. This method will be exemplified in later sections when describing the topological Hilbert space associated to the surface Σ by considering loops belonging to some canonical DAP-decomposition of Σ.

5.1.3 Elementary surfaces

With this Flux Basis Axiom 5.1.1, the Hilbert space $\mathcal{H}_{\Sigma}$ for various elementary surfaces can be understood. These elementary surfaces have the unique property that a DAP-decomposition of $\Sigma_{(0,b)}$ is specified by just the b loops homotopic to the b boundary components of $\Sigma_{(0,b)}$, and no others are necessary. In fact, this essentially motivates the particular explicitness in Definition 5.1.3 of a fusion consistent labeling. In this sense, these surfaces are the primitive constituent pieces that a general surface can be decomposed as in order to apply the Gluing Axiom 5.1.2.

For the disk $\Sigma^{(a)}_{(0,1)}$ with anyon type $a \in \mathbb{A}$ associated to the single boundary curve, $\mathcal{H}_{\Sigma^{(a)}_{(0,1)}} = \mathbb{C}^{\delta_{1,a}}$. That is, $\mathcal{H}_{\Sigma^{(a)}_{(0,1)}} = \{0\}$ is the zero-dimensional space if $a \neq 1$, and otherwise $\mathcal{H}_{\Sigma^{(a)}_{(0,1)}} = \mathbb{C}$ since there is only one fusion consistent labeling of a DAP-decomposition of $\mathcal{H}_{\Sigma^{(a)}_{(0,1)}}$. That this is demanded by Axiom 5.1.1 can be physically justified by a main property that the topological Hilbert space $\mathcal{H}_{\Sigma}$ should satisfy. That is, $\mathcal{H}_{\Sigma}$ is supposed to represent the "vacuum sector" of the theory in which no nontrivial anyons are present on the surface (with the exception of fixed anyon types corresponding to boundary components). Therefore, no anyonic flux should be detected when observing a local region of the surface by making a flux measurement around a homotopically trivial loop around the local region. These trivial loops are precisely those loops that yield a disk when cut out of the surface.

For the annulus $\mathcal{H}_{\Sigma^{(a_1,a_2)}_{(0,2)}}$ with its two boundary components labelled by $a_1, a_2 \in \mathbb{A}$, the

axiom implies that $\mathcal{H}_{\Sigma_{(0,2)}^{(a_1,a_2)}} = \mathbb{C}^{\delta_{a_1,\overline{a_2}}}$. Therefore, $\mathcal{H}_{\Sigma_{(0,2)}^{(a_1,a_2)}}$ is one dimensional if the anyon types a_1 and a_2 associated to the boundary loops are dual to each other, and is otherwise zero-dimensional. The physical motivation for this is that the anyonic flux should be preserved on a surface that corresponds to a cylinder, which is homeomorphic to the annulus. Equivalently, this statement of the axiom can be justified by claiming that the anyonic flux associated to homotopically equivalent loops should be equal. In the case of the annulus (cylinder), the two loops that define the boundary components are always homotopic.

For the pant $\Sigma_{(0,3)}^{(a_1,a_2,a_3)}$ with boundary loops labelled as $\ell(C_i) = a_i \in \mathbb{A}$ for $i = 1, 2, 3$, fusion consistency demands that $\mathcal{H}_{\Sigma_{(0,3)}^{(a_1,a_2,a_3)}} = \mathbb{C}^{N_{a_1,a_2}^{a_3}}$. Therefore, the space has positive dimension if and only if the fusion coefficient satisfies $N_{a_1,a_2}^{a_3} \neq 0$. The physical justification for this is given by the following property of measuring the anyonic charge or flux contained within a region enclosing two anyons (two labeled boundary components). Suppose anyon with type a_1 and a_2 exist on some surface. The type of each of these anyons can be observed through a flux measurement around each anyon. If a flux measurement were to be made around a region containing both anyons, and no others, then the measured flux must be a type that results from the fusion $a_1 \otimes a_2$.

For later notational convenience introduce the following.

Definition 5.1.4. *Let $V_a := \mathcal{H}_{\Sigma_{(0,1)}^{(a)}}$, $V_a^b := \mathcal{H}_{\Sigma_{(0,2)}^{(a,b)}}$ and $V_{a,b}^c := \mathcal{H}_{\Sigma_{(0,3)}^{(a,b,\bar{c})}}$ be the Hilbert spaces associated to the labeled disk, annulus, and pant, respectively.*

As finite dimensional Hilbert spaces of the form $\mathbb{C}^n$, which are classified up to isomorphism by their dimension n, the Hilbert spaces associated to the elementary surfaces can be characterized simply by their dimensions. Thus, in summary, for these elementary surfaces fusion consistency of labelings demands that for the disk $dim(V_a) = \delta_{a,1}$, for the annulus $dim(V_a^b) = \delta_{a,\bar{b}}$, and for the pant $dim(V_{a,b}^c) = N_{a,b}^c$.

5.1.4 The 4-punctured sphere

In general, genus-zero surfaces with nonempty boundary of the form $\Sigma_{(0,n)}$ will be referred to as *n-punctured spheres*, since these surfaces are homeomorphic to the sphere with n disks or "punctures" removed. In this way, the elementary surfaces correspond to the cases $n = 1, 2, 3$ for the disk, annulus, and pant, respectively. Describing the Hilbert spaces for the n-punctured sphere for $n \geq 4$ can be understood in terms of the Hilbert space associated to the 4-punctured sphere, which can in turn be understood in terms of the Hilbert space for the 3-punctured sphere (a pair of pants).

Consider now the 4-punctured sphere $\Sigma := \Sigma_{(0,4)}$, and let $\Sigma(i,j,k,l) := \Sigma_{(0,4)}(i,j,k,l)$ represent the case where the four boundary components are labeled by fixed anyon types $i,j,k,l \in \mathbb{A}$. Physically, this labeled surface corresponds to the scenario where anyons $i,j,k \in \mathbb{A}$ fuse is some order to yield a final anyon type $k \in \mathbb{A}$. The two relevant orders of fusion are $(i \otimes j) \otimes k$ or $i \otimes (j \otimes k)$. That is, in the former case anyons $i,j \in \mathbb{A}$ can fuse first resulting in some intermediary anyon type $a \in \mathbb{A}$ which then fuses with $k \in \mathbb{A}$ to result in final anyon type l; and in the second case anyons $j,k \in \mathbb{A}$ first resulting in some intermediary anyon type $a' \in \mathbb{A}$ followed by fusion with anyon i to result in the final anyon type l. The Hilbert space $\mathcal{H}_{\Sigma(i,j,k,l)}$ will then represent the different possible ways such a fusion process can occur, and the number of possible fusion outcomes will be equal to the dimension of the Hilbert space $\mathcal{H}_{\Sigma(i,j,k,l)}$. It may be the case that there is only one intermediary anyon type in which case $dim(\mathcal{H}_{\Sigma(i,j,k,l)}) = 1$, but the more interesting case occurs when there may exist more than one way this fusion process may occur so that $dim(\mathcal{H}_{\Sigma(i,j,k,l)}) > 1$. In this latter case, by virtue of having a higher dimension, the Hilbert space $\mathcal{H}_{\Sigma(i,j,k,l)}$ may be used to enact nontrivial quantum operations.

Returning to the mathematical axioms that determine the space $\mathcal{H}_{\Sigma(i,j,k,l)}$, as described in Section 4.1.2, there exists two single loop DAP-decompositions $\mathcal{C} = \{C\}$ and $\mathcal{C}' = \{C'\}$ of the surface $\Sigma(i,j,k,l)$. A choice of one of these two particular DAP-decompositions effectively determines one of the two ways to order the fusion of anyons $i,j,k \in \mathbb{A}$ to yield in a final anyon type $k \in \mathbb{A}$. DAP-decomposition $\mathcal{C}$ corresponds to the ordering $(i \otimes j) \otimes k$, and DAP-decomposition $\mathcal{C}'$ corresponds to the order $i \otimes (j \otimes k)$. Each of these DAP-decompositions decompose Σ into a disconnected surface consisting of two pants $\Sigma_{(0,3)} \amalg \Sigma_{(0,3)}$. In regards to labelings of the surfaces in the context of the Gluing Axiom, Equation (5.3) takes on two different forms depending on the choice of DAP-decomposition $\mathcal{C}$ or $\mathcal{C}'$. In the case of choosing DAP-decomposition $\mathcal{C}$, this becomes

$$\mathcal{H}_{\Sigma(i,j,k,l)} = \bigoplus_{\ell \in \mathsf{L}(\mathcal{C})} V_{i,j}^{\ell(C)} \otimes V_{\overline{\ell(C)},k}^{l}, \tag{5.4}$$

and fusion consistency demands that a labeling $\ell \in \mathsf{L}(\mathcal{C})$ must label loop C as $\ell(C) = a$ such that both $N_{i,j}^{a} \neq 0$ and $N_{\bar{a},k}^{l} \neq 0$. Therefore, define the set

$$Q(i,j,k,l) := \{a \in \mathbb{A} \mid N_{i,j}^{a} \neq 0 \ \text{ and} N_{\bar{a},k}^{l} \neq 0\},$$

which represents the possible intermediary fusion outcomes. Then Equation (5.5) can be equivalently expressed as

$$\mathcal{H}_{\Sigma(i,j,k,l)} = \bigoplus_{a \in Q(i,j,k,l)} V_{i,j}^{a} \otimes V_{\bar{a},k}^{l}. \tag{5.5}$$

Alternatively, for the case of DAP-decomposition $\mathcal{C}'$ Equation (5.3) becomes

$$\begin{aligned}\mathcal{H}_{\Sigma(i,j,k,l)} &= \bigoplus_{\ell\in \mathsf{L}(\mathcal{C}')} V^{l}_{i,\overline{\ell(C')}} \otimes V^{\ell(C')}_{j,k} \\ &= \bigoplus_{a'\in Q'(i,j,k,l)} V^{l}_{i,\overline{a'}} \otimes V^{a'}_{j,k}, \end{aligned} \tag{5.6}$$

where in this case

$$Q'(i,j,k,l) := \{a' \in \mathbb{A} \mid N^{l}_{i,\overline{a'}} \neq 0 \ \text{ and} N^{a'}_{j,k} \neq 0\}$$

denotes the possible intermediary fusion outcomes when fusing j and k first.

Note that Equations (5.5) and (5.6) both describe the same Hilbert space $\mathcal{H}_{\Sigma(i,j,k,l)}$ and therefore must have the same dimension which implies that $dim(\mathcal{H}_{\Sigma(i,j,k,l)}) = |Q(i,j,k,l)| = |Q'(i,j,k,l)|$. Let $\mathcal{B}_{\mathcal{C}} := \{|a\rangle_{\mathcal{C}}\}_{a\in Q(i,j,k,l)}$ and $\mathcal{B}_{\mathcal{C}'} := \{|a'\rangle_{\mathcal{C}'}\}_{a'\in Q'(i,j,k,l)}$ be the two respective basis of $\mathcal{H}_{\Sigma(i,j,k,l,)}$. The matrix that represents the change-of basis between $\mathcal{B}_{\mathcal{C}}$ and $\mathcal{B}_{\mathcal{C}'}$ is given by the *F-matrix* that corresponds to the local F-move.

5.1.5 The torus

In this section, an explicit construction for the Hilbert spaces associated to the torus $\Sigma_{(1,0)}$ will be provided. Like the 4-punctured sphere $\Sigma_{(0,4)}$, a single loop can suffice to yield a valid DAP-decomposition. However, for the torus such a DAP-decomposition is even simpler in terms of the resulting elementary surfaces, and therefore also simpler to describe since the fusion consistency requirements are less stringent. The Hilbert spaces for more general higher genus surfaces can then be understood in terms of these.

Let $T := \Sigma_{(1,0)}$ be the genus-1 torus, and recall from Section 4.1.2 that a DAP-decomposition can be achieved with a single loop $\{C\} = \mathcal{C}$, where $C \subset T$ is either of the two nontrivial simple loops. As described previously, cutting along C yields an annulus. Therefore, let $V^{\overline{a}}_{a} := \mathcal{H}_{\Sigma^{(a,\overline{a})}_{(0,2)}}$ be the Hilbert space of the annulus with its two boundaries labelled by the pair $(a,\overline{a})$. Then the Gluing Axiom 5.2 states that

$$\mathcal{H}_T = \bigoplus_{\ell\in \mathsf{L}(\mathcal{C})} V^{\overline{\ell(C)}}_{\ell(C)},$$

where in this case any labeling $\ell : \{C\} \to \mathbb{A}$ assigning $\ell(C) = a \in \mathbb{A}$ arbitrarily is fusion consistent since $a = \overline{\overline{a}}$ for all $a \in \mathbb{A}$ (that is, the dual of the dual of an anyon is the anyon itself). Therefore, the direct sum can be indexed as

$$\mathcal{H}_T = \bigoplus_{a\in\mathbb{A}} V^{\overline{a}}_{a}, \tag{5.7}$$

implying that $dim(\mathcal{H}_\Sigma) = |\mathbb{A}|$ since $dim(V_a^{\overline{a}}) = 1$ for all $a \in \mathbb{A}$ as determined in Section 5.1.3. Thus, a basis for $\mathcal{H}_T$ for a particular anyon model can simply be indexed by the different anyon types $a \in \mathbb{A}$. To exemplify this in the case of the Toric code, where $\mathbb{A} = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $|\mathbb{A}| = 4$, it is seen that $dim(\mathcal{H}_T) = 4$. This finally offers the alternative means for determining the dimension of the code space as promised in Section 2.1.9.

Note again that Equation (5.7) describes the Hilbert space $\mathcal{H}_T$ for any DAP-decomposition of T. Letting $\mathcal{C} := \{C\}$ and $\mathcal{C}' := \{C'\}$ be the two standard DAP-decompositions of T associated to the pair of conjugate simple loops, two different basis can be given:

$$\mathcal{B}_\mathcal{C} := \{|a\rangle_\mathcal{C}\}_{a\in\mathbb{A}} \quad \text{and} \quad \mathcal{B}_{\mathcal{C}'} := \{|a\rangle_{\mathcal{C}'}\}_{a\in\mathbb{A}}. \tag{5.8}$$

The two basis $\mathcal{B}_\mathcal{C}$ and $\mathcal{B}_{\mathcal{C}'}$ can be related through a change-of-basis matrix. This matrix is given by a representation of the local S-move (as discussed in Section 4.1.2) which relates the two loops C and C' that define the DAP decompositions $\mathcal{C}$ and $\mathcal{C}'$. The S-move actually corresponds to a particular homeomorphism $s \in T$ of the mapping class group of the torus T whose action on the loops is related by $s(\mathcal{C}) = \mathcal{C}'$.

Chapter 6

Protected gates

The objective of this part will be to motivate and describe certain fault-tolerant operations, called *protected gates*, for topological quantum computation. The following sections will provide high-level details, methods, and statements of some results that characterize protected gates. Further details and proofs can then be found in the proceeding part which contains the paper "Protected gates for topological quantum computation" where the results were originally obtained.

6.1 Protected gates: definition and problem statement

Ideally, quantum computation takes place on some Hilbert space $\mathcal{H}_N = \bigotimes_{i=1}^{N} \mathbb{C}_i^d$ which consists of N *qudits* representing some d-level elementary quantum system described by the Hilbert space $\mathbb{C}^d$ having dimension d. Although more general operations are often considered, a quantum computation may be performed by applying some unitary operation $U : \mathcal{H}_N \to \mathcal{H}_N$ on the system and then measuring the resulting quantum state after such an operation has been performed to yield the outcome of the computation. In practice however, implementing the unitary operation U may not be perfect in the sense that errors may occur during the process. The nature of these errors can be both intrinsic and extrinsic—meaning the methods used to implement the operation may themselves be faulty, and also some external noise may inflict the system corrupting the encoded information. This motivates the study of quantum error correction, which is ultimately concerned with methods for performing fault-tolerant quantum computation and characterizing the computational power of such fault-tolerant operations.

In the context of quantum error correction, a suitable subspace called the *code space* $\mathcal{H}_{code} \subset \mathcal{H}_N$ is chosen which effectively encodes some number $M < N$ of *logical qudits*. The code space $\mathcal{H}_{code}$ is to then serve as the computational space where quantum information can be encoded.

It is important to note that the Hilbert space $\mathcal{H}_{code}$ is not necessarily a physical subsystem of the full quantum system that defines the global Hilbert space $\mathcal{H}_N$, but rather a vector subspace of $\mathcal{H}_N$ which is still defined with respect to all N physical qudits of the system. The relevant property here is that the code space satisfies the isomorphism $\mathcal{H}_{code} \cong \bigotimes_{i=1}^{M} \mathbb{C}_i^d$, which functions as an isometry that allows it to encode the M logical qudits using all N physical qudits of the actual system. In this regard, quantum error correction can be thought of as encoding information through the means of redundancy in such a way that performing operations on $\mathcal{H}_N$ enacts desired unitary operations (called *logical operations*) on the code space $\mathcal{H}_{code} \subset \mathcal{H}_N$. These logical operations then serve as a means to perform fault-tolerant quantum computation.

Definition 6.1.1. *Given a code space $\mathcal{H}_{code} \subset \mathcal{H}_N$, a* **logical operation** *or* **automorphism of the code** *is a unitary $U : \mathcal{H}_N \to \mathcal{H}_N$ that preserves the code space: $U\mathcal{H}_{code} = \mathcal{H}_{code}$. The restriction of U onto the code space is denoted as $[U] : \mathcal{H}_{code} \to \mathcal{H}_{code}$, and its action on $\mathcal{H}_{code}$ is referred to as the* **logical action** *of U.*

The protected gates of interest here will be a type of logical operation acting on a code space defined in the context of topological quantum computation. Recall that topological quantum computation assumes the existence of a physical Hilbert space $\mathcal{H}_{phys}$ of a many-body quantum system which realizes some topological phase of matter. Typically, the system is thought of as existing on some surface Σ, and the computational space of interest which is to serve as the code space is precisely the topological Hilbert space $\mathcal{H}_\Sigma \subset \mathcal{H}_{phys}$ of Chapter 5.1. Protected gates are then defined to be certain types of logical operations on $\mathcal{H}_\Sigma$ that also satisfy an additional fault-tolerant property known as *locality preservation*.

To understand what is meant by a locality preserving operation, recall again the N-body physical Hilbert space associated to some topological phase of matter on a surface Σ given as $\mathcal{H}_{phys} = \bigotimes_{i \in \mathcal{L}_N} \mathbb{C}_i^d$. Here, $\mathcal{L}_N \subset \Sigma$ is a triangulation of the surface Σ that identifies the locations of the N qudits that comprise the physical system of $\mathcal{H}_{phys}$. Operators $X : \mathcal{H}_{phys} \to \mathcal{H}_{phys}$ can then act on all or some of the physical qudits of the triangulation $\mathcal{L}_N$ on the surface. Now define the *support* of an operator X, written $supp(X)$, to be the locations of the qudits on the surface Σ for which the operator X acts non-trivially. Although this notion of support is an inherently discrete one since the physical system only consists of some finite number N of qudits, it will be convenient to think of the support of an operator X as a region (or set of regions) of the surface $supp(X) \subseteq \Sigma$. This can be done by simply considering sufficiently small neighborhoods around the locations of the qudits on the surface. By doing this the relevant concepts can be thought about in a more geometrical or topological nature.

Definition 6.1.2. *An operator $U : \mathcal{H}_{phys} \to \mathcal{H}_{phys}$ is* **locality-preserving** *if for any operator $X : \mathcal{H}_{phys} \to \mathcal{H}_{phys}$ having support $supp(X) \subset \Sigma$, the support of the operator $UXU^\dagger$ satisfies $supp(UXU^\dagger) \subset \mathcal{R} \subset \Sigma$, where $\mathcal{R}$ is a constant-size neighborhood of $sup(X)$.*

Thus, a locality-preserving operator U is one which does not significantly change the locality properties of an operator X. Such a property is desirable due to its fault-tolerant nature: if an error represented by an operator X does inflict the system, then a locality-preserving operator U will not spread or propagate the errors too drastically throughout the rest of the system. Therefore, typical errors can remain correctable even after a locality-preserving operator U has been applied to the system. Hence, if an error X has support within some locally defined region, its support will remain contained within a sufficiently local region. This is especially relevant in the context of topological quantum computation when assuming a local noise model, since the code space $\mathcal{H}_\Sigma$ can correct errors whose supports are contained within a topologically trivial region (one that is homeomorphic to a disk).

Finally, with Definitions 6.1.1 and 6.1.2 at hand, a *protected gate* can be defined:

Definition 6.1.3. *A unitary operator U acting on a topological code $\mathcal{H}_\Sigma$ is called a* **protected gate** *if U is both a logical operation and locality-preserving.*

Recall that the topological Hilbert space $\mathcal{H}_\Sigma$ is defined with respect to an anyon model $\mathbb{A}$ arising from some underlying UTMC $\mathbf{C}$. Fixing a choice of $\mathbb{A}$ and a surface Σ, the main problem of interest is to characterize the group generated by all protected gates acting on $\mathcal{H}_\Sigma$:

$$\mathcal{U}_{\mathbb{A},\Sigma} := \langle [U] \mid U : \mathcal{H}_\Sigma \to \mathcal{H}_\Sigma \text{ is a protected gate} \rangle . \tag{6.1}$$

The group $\mathcal{U}_{\mathbb{A},\Sigma} \subseteq \mathcal{U}(\mathcal{H}_\Sigma)$ then determines the computational power of protected gates for the particular anyon model and surface. Here, $\mathcal{U}(\mathcal{H}_\Sigma)$ denotes the set of all general unitary operations defined on $\mathcal{H}_\Sigma$. The main result of this work done in "Protected gates for topological quantum field theories" is that the group of protected gates $\mathcal{U}_{\mathbb{A},\Sigma}$ is always finite regardless of the choice of anyon model $\mathbb{A}$ and surface Σ. Thus, this result can be understood as a no-go theorem: protected gates alone cannot realize universal quantum computation. This implies that in order to achieve computational universality, alternative means for performing quantum computation must be utilized which involve non-local information processing. Further details regarding the main results of this work will be stated more explicitly in Section **??** after highlighting the methods used to characterize protected gates.

6.2 Characterizing protected gates

One way to understand the action of an operator $U : \mathcal{H} \to \mathcal{H}$ on some Hilbert space $\mathcal{H}$ is to understand its action on a set of basis vectors of $\mathcal{H}$. Alternatively, given an appropriate algebra of operators $\mathcal{A}$ acting on $\mathcal{H}$, the operator U can be equivalently understood by characterizing

its action under the conjugation $\rho_U(X) := UXU^\dagger$ for operators $X \in \mathcal{A}$. This latter approach is essentially the one that is taken to characterize protected gates in this study. In what follows, attention is fixed on some choice of an anyon model $\mathbb{A}$ and surface Σ. The underlying TQFT then determines a topological Hilbert space $\mathcal{H}_\Sigma$ for which a protected gate will act on. Different choices for $\mathbb{A}$ and/or Σ will generally lead to a different Hilbert spaces $\mathcal{H}_\Sigma$ and sets of protected gates. Regardless, most of the methods to be developed in order to characterize protected gates are independent of such choices, and can therefore be applied to any such model.

6.2.1 String operators

The particular algebra of operators of interest in this study are operators that act on the physical Hilbert space $\mathcal{H}_{phys}$ associated to some surface Σ that also preserve the topological Hilbert space $\mathcal{H}_\Sigma$. To be specific, define this algebra to be

$$\mathcal{A}_\Sigma := \{X : \mathcal{H}_{phys} \to \mathcal{H}_{phys} \mid X\mathcal{H}_\Sigma = \mathcal{H}_\Sigma\}. \tag{6.2}$$

Since an operator $X \in \mathcal{A}_\Sigma$ preserves the code space, it makes sense to speak of the logical action $[X] : \mathcal{H}_\Sigma \to \mathcal{H}_\Sigma$ of the operator. Therefore, also define the corresponding algebra

$$[\mathcal{A}_\Sigma] := \{[X] : \mathcal{H}_\Sigma \to \mathcal{H}_\Sigma \mid X \in \mathcal{A}_\Sigma\}. \tag{6.3}$$

Ultimately, it is this algebra $[\mathcal{A}_\Sigma]$ which will be used to characterize a protected gate $[U]$. However the algebra $[\mathcal{A}_\Sigma]$ itself will be understood in terms of certain subalgebras $\mathcal{A}(C) \subset \mathcal{A}_\Sigma$ which consist of operators whose supports are contained within a constant-diameter neighborhood of a closed loop $C \subset \Sigma$ on the surface. As it will be seen, only a finite number of distinct loops $C \subset \Sigma$ will be needed to define various subalgebras $\mathcal{A}(C)$, and these subalgebras considered together will comprise the entire general algebra $\mathcal{A}_\Sigma$.

To define the subalgebras $\mathcal{A}(C)$, recall the Verlinde algebra $\mathsf{Ver}_\mathbb{A}$ of Chapter 3.3 and defined in Definition 3.3.1 in terms of some anyon model $\mathbb{A}$. By construction, $\mathsf{Ver}_\mathbb{A}$ is spanned by elements $\{f_a\}_{a\in\mathbb{A}}$ satisfying Equation (3.4):

$$f_a f_b = \sum_{c\in\mathbb{A}} N_{a,b}^c f_c,$$

Now fix any closed loop $C \subset \Sigma$, and consider the following representation of $\mathsf{Ver}_\mathbb{A}$:

$$\begin{aligned} \mathsf{Ver}_\mathbb{A} &\to \mathcal{A}_\Sigma \\ f_a &\mapsto F_a(C). \end{aligned}$$

Such a representation maps the basis elements $f_a \in \mathsf{Ver}_{\mathbb{A}}$ to operators $F_a(C) : \mathcal{H}_{phys} \to \mathcal{H}_{phys}$ preserving the code space $\mathcal{H}_\Sigma$ and also satisfying

$$F_a(C)F_b(C) = \sum_{c\in\mathbb{A}} N_{a,b}^c F_c(C).$$

An operator $F_a(C)$ will be referred to as a *string operator*. The set of operators $\{F_a(C)\}_{a\in\mathbb{A}}$ all have support contained within some constant diameter neighborhood of the loop $C \subset \Sigma$. Let $\mathcal{A}(C)$ be the algebra generated by the string operators for some fixed loop $C \subset \Sigma$. Such an algebra $\mathcal{A}(C)$ can be defined for each loop $C \subset \Sigma$ of the surface, and each one of these carries a representation of $\mathsf{Ver}_{\mathbb{A}}$ so that the two are isomorphic as algebras: $\mathcal{A}(C) \cong \mathsf{Ver}_{\mathbb{A}}$. Moreover, only a finite collection of loops C are required so that the collection of respective subalgebras $\mathcal{A}(C)$ taken together comprise the complete global algebra $\mathcal{A}_\Sigma$ as made precise in Proposition 7.2.2.

Physically, a string operator $F_a(C)$ corresponds to the process in which an anyon and its dual $a, \overline{a} \in \mathbb{A}$ are created from the vacuum and one of the anyons traverses the loop C on the surface to return and fuse with its pair back into the vacuum. In fact, these string operators correspond to the main observables of the theory, which serve to potentially change the flux associated to loops conjugate to C. As an example, these string operators are precisely the ones introduced for the Toric code in Section 2.1.8 where they served as the logical operators acting on $\mathcal{H}_\Sigma$.

For a fixed loop $C \subset \Sigma$, since the string operators $\{F_a(C)\}_{a\in\mathbb{A}} \subset \mathcal{A}(C)$ form a representation and serve as a basis of an algebra isomorphic to the Verlinde algebra $\mathsf{Ver}_{\mathbb{A}}$, idempotents $\{P_a(C)\}_{a\in\mathbb{A}}$ of the algebra $\mathcal{A}(C)$ can be defined analogously to those given for $\mathsf{Ver}_{\mathbb{A}}$ as in Equation (3.6). In this way, the set $\{P_a(C)\}_{a\in\mathbb{A}}$ are orthogonal projectors onto states of $\mathcal{H}_\Sigma$ that correspond to a loop C carrying flux of type $a \in \mathbb{A}$. Given a DAP-decomposition $\mathcal{C}$ of Σ, the set of projectors $\{P_a(C)\}_{a\in\mathbb{A},C\in\mathcal{C}}$ serve as a complete set to define basis states of $\mathcal{H}_\Sigma$.

6.2.2 Constraints from fusion consistency

In order to characterize a protected gate U acting on $\mathcal{H}_\Sigma$, the conjugation action $\rho_U(P_a(C)) := UP_a(C)U^\dagger$ is studied for loops $C \in \mathcal{C}$ of a DAP-decomposition $\mathcal{C}$. The key insight is that, for a fixed loop C, the conjugation action $\rho_U : [\mathcal{A}(C)] \to [\mathcal{A}(C)]$ is an automorphism of $[\mathcal{A}(C)]$. Since $[\mathcal{A}(C)] \cong \mathsf{Ver}_{\mathbb{A}}$, and $\mathsf{Ver}_{\mathbb{A}}$ is a commutative C^*-algebra, an automorphism of $\mathcal{A}(C)$ must yield an automorphism of Ver_Σ. It is a standard result (given in Section 7.3.1), that such automorphisms are in one-to-one correspondence with the permutations on $|\mathbb{A}|$ elements, and effectively permute the idempotents of $\mathsf{Ver}_{\mathbb{A}}$. Therefore, the conjugation action of a U must be

of the form

$$\begin{aligned}\rho_U : [\mathcal{A}(C)] &\to [\mathcal{A}(C)] \\ [P_a(C)] &\mapsto [P_{\pi^C(a)}(C)],\end{aligned}$$

where $\pi^C : \mathbb{A} \to \mathbb{A}$ is a permutation $\pi^C \in S_{|\mathbb{A}|}$ (the symmetric group of size $|\mathbb{A}|$). This is proved more rigorously in Proposition 7.3.1, and is referred to as a local constraint on U since it pertains to a single, yet arbitrary, loop C.

Consider now some DAP-decomposition $\mathcal{C}$ of Σ, which is used to define a basis $\{|\ell\rangle\}_{\ell \in \mathsf{L}(\mathcal{C})}$ of $\mathcal{H}_\Sigma$ from the set of fusion consistent labellings $\mathsf{L}(\mathcal{C})$. The local constraint on a protected gate U just described associates some permutation π^C of anyon labels to each loop $C \in \mathcal{C}$. Let $\vec{\pi} := (\pi^C)_{C \in \mathcal{C}}$ be a family of such permutations. In Proposition 7.3.2, a global constraints on U pertaining to all loops of $\mathcal{C}$ is derived which states that $\vec{\pi}$ defines a permutation of $\mathsf{L}(\mathcal{C})$ as

$$\begin{aligned}\vec{\pi} : \mathsf{L}(\mathcal{C}) &\to \mathsf{L}(\mathcal{C}) \\ \ell &\mapsto \vec{\pi}(\ell),\end{aligned}$$

where the labeling $\vec{\pi}(\ell) : \mathcal{C} \to \mathbb{A}$ is given as $\vec{\pi}(\ell)(C) := \pi^C(\ell(C))$. This proposition effectively states that a protected gate U permutes the basis states of $\mathcal{H}_\Sigma$ via the permutation $\vec{\pi}$ acting on fusion-consistent labelings. More specifically, it states that the logical action of U on basis states $|\ell\rangle \in \mathcal{H}_\Sigma$ is given as

$$[U]|\ell\rangle = \mathrm{e}^{\mathrm{i}\varphi(\ell)}|\vec{\pi}(\ell)\rangle, \tag{6.4}$$

where $\mathrm{e}^{\mathrm{i}\varphi(\ell)}$ is a phase factor associated to the labeling $\ell \in \mathsf{L}(\mathcal{C})$. In some ordered basis of $\mathcal{H}_\Sigma$, this characterization can be equivalently expressed in matrix form as

$$\mathbf{U} = \mathbf{\Pi}\mathbf{D}, \tag{6.5}$$

where $\mathbf{U}$ is the $|\mathsf{L}(\mathcal{C})| \times |\mathsf{L}(\mathcal{C})|$ matrix representing the permutation $\vec{\pi}$ and $\mathbf{D}$ is a diagonal matrix consisting of the phases whose matrix coefficients are given as $(\mathbf{D})_{\ell,\ell'} = \mathrm{e}^{\mathrm{i}\varphi(\ell)}\delta_{\ell,\ell'}$.

The characterization of a protected gate U expressed by Equation (6.5) merely states that a protected gate U must be of the form $\mathbf{U} = \mathbf{\Pi}\mathbf{D}$. In general, it is not true that any such matrix will yield a valid protected gate. The permutation $\mathbf{\Pi}$ is essentially constrained by fusion consistency requirements arising both locally and globally in regards to some DAP-decomposition of the surface, and would therefore be dependent on the particular anyon model $\mathbb{A}$ under consideration and choice of surface Σ.

6.2.3 Constraints from basis changes

Thus far, there has been no theory developed which puts constraints on the permissible phase factors $e^{i\varphi(\ell)}$ of the diagonal matrix $\mathbf{D}$. To arrive at a necessary constraints on the possible phases $e^{i\varphi(\ell)}$ that may define a valid protected gate $\mathbf{U} = \mathbf{\Pi D}$, basis changes of the Hilbert space $\mathcal{H}_\Sigma$ must be considered. In particular, the relevant bases of interest will be those defined through DAP-decompositions. In this regard, consider two DAP-decompositions $\mathcal{C}$ and $\mathcal{C}'$ and the corresponding bases $\mathcal{B}_\mathcal{C}$ and $\mathcal{B}_{\mathcal{C}'}$ of $\mathcal{H}_\Sigma$ that they define. Now consider some protected gate, U. Note that the form of a protected gate as described in Equation (6.5) must hold for any basis defined by a DAP-decomposition. Thus, let $\mathbf{U} = \mathbf{\Pi D}$ and $\mathbf{U}' = \mathbf{\Pi}'\mathbf{D}'$ be representations of a protected gate U in the basis $\mathcal{B}_\mathcal{C}$ and $\mathcal{B}_{\mathcal{C}'}$, respectively. Suppose $\mathbf{V}$ gives the change-of-basis from $\mathcal{B}_\mathcal{C}$ to $\mathcal{B}_{\mathcal{C}'}$. Then a necessary condition is that

$$\mathbf{VU} = \mathbf{U}'\mathbf{V}, \tag{6.6}$$

which yields constraints on the possible permutations and phases associated to the protected gate U.

Recall that different DAP-decompositions $\mathcal{C}$ and $\mathcal{C}'$ of Σ can be related by mapping class group elements $\vartheta \in \mathsf{MCG}_\Sigma$ and/or by the various local F-moves. The underlying TQFT provides unitary matrix representations of these operations via $\mathcal{T}(\vartheta)$ for $\vartheta \in \mathsf{MCG}_\Sigma$ and the corresponding F matrix of the anyon model $\mathbb{A}$ which act as unitary operations on $\mathcal{H}_\Sigma$. If $\vartheta \in \mathsf{MCG}_\Sigma$ transforms the loops in $\mathcal{C}$ to the loops in $\mathcal{C}'$, then $\mathcal{T}(\vartheta)$ will correspond to a change-of-basis between $\mathcal{B}_\mathcal{C}$ and $\mathcal{B}_{\mathcal{C}'}$ so that Equation (6.6) becomes

$$\mathcal{T}(\vartheta)\mathbf{U} = \mathbf{U}'\mathcal{T}(\vartheta). \tag{6.7}$$

Likewise, in regards to basis changes induced by the F matrix, a neccesary constraint is

$$\mathbf{FU} = \mathbf{U}'\mathbf{F}. \tag{6.8}$$

To better understand these constraints, define the set Δ to be all matrices acting on $\mathcal{H}_\Sigma$ of the form $\mathbf{\Pi D}$ as in Equation (6.5) where $\mathbf{\Pi}$ is a permutation of fusion-consistent labellings and $\mathbf{D}$ is a diagonal matrix of phases. Now consider some $\mathbf{U} \in \Delta$ and any $\vartheta \in \mathsf{MCG}_\Sigma$. Say that $\mathbf{U}$ *intertwines* with ϑ if $\mathcal{T}(\vartheta)\mathbf{U}\mathcal{T}(\vartheta)^\dagger \in \Delta$, and let $\Delta_\vartheta \subset \Delta$ be the set of all matrices in that intertwine with ϑ. Now define the set

$$\Delta_{\mathsf{MCG}_\Sigma} := \bigcap_{\vartheta \in \mathsf{MCG}_\Sigma} \Delta_\vartheta,$$

which is just the set of matrices in Δ that intertwine with all $\vartheta \in \mathsf{MCG}_\Sigma$. Then if $\mathbf{U}$ is a valid protected gate, it must be the case $\mathbf{U} \in \Delta_{\mathsf{MCG}_\Sigma}$. This is one of the main characterizations for protected gates.

6.2.4 Additional constraints

In practice, to calculate permissible protected gates U for $\mathcal{H}_\Sigma$, one would use explicit matrix representations of mapping class group transformation $\mathcal{T}(\vartheta)$ and $\mathbf{F}$-moves to yield algebraic equations from the change-of-basis constraint given in Equation (6.6) to infer the form of $\mathbf{U} \in \Delta_{\mathsf{MCG}_\Sigma}$. However, some additional methods and constraints can be used in certain settings. For instance, Proposition 7.3.3 gives another constraint from a fusion-consistency requirement when applied in the context of the Gluing Axiom 5.2. Recall that the gluing axiom gives an isomorphism

$$\mathcal{H}_\Sigma = \bigoplus_{\ell \in \mathsf{L}(\mathcal{C})} \mathcal{H}_{\Sigma'_{\mathcal{C}}(\ell(C),\overline{\ell(C)})},$$

where $\mathcal{H}_{\Sigma'_{\mathcal{C}}(\ell(C),\overline{\ell(C)})}$ is the subspace of $\mathcal{H}_\Sigma$ corresponding to loop $C \in \mathcal{C}$ carrying flux of type $\ell(C) \in \mathbb{A}$. For a protected gate U corresponding to a family of permutations $\vec{\pi}$ of fusion consistent labellings $\mathsf{L}(\mathcal{C})$, Proposition 7.3.3 claims that the local permutation π^C associated to loop $C \in \mathcal{C}$ must satisfy the isomorphism $\mathcal{H}_{\Sigma'_{\mathcal{C}}(\ell(C),\overline{\ell(C)})} \cong \mathcal{H}_{\Sigma'_{\mathcal{C}}(\pi^C(\ell(C)),\overline{\pi^C(\ell(C))})}$ of the corresponding subspaces. This naturally implies that the dimensions of these two subspaces must be equal, which can also readily serve as an immediate constraint when determining permissible permutation π^C for various loops $C \in \mathcal{C}$.

For characterizing protected gates for $\mathcal{H}_{\Sigma_{(0,n)}}$ where $\Sigma_{(0,n)}$ is the n-punctured sphere, Section 7.5 develops techniques with a reductionist flavor that give general constraints for the n-punctured sphere in terms of constraints established for the special case of the 4-punctured sphere. To be more specific, Proposition 7.5.1 states that for a protected gate U of $\mathcal{H}_{\Sigma_{(0,n)}}$, the corresponding phase factor $\mathrm{e}^{\mathrm{i}\varphi(\ell)}$ depends only on "local" information regarding the labellings $\ell(C)$ when the loops $C \in \mathcal{C}$ are certain loops of a DAP-deomposition $\mathcal{C}$ of $\Sigma_{(0,n)}$. With this at hand, various constraints on a protected gate for $\mathcal{H}_{\Sigma_{(0,n)}}$ can be determined by classifying permissible permutations and phases for protected gates acting on spaces $\mathcal{H}_{\Sigma_{(0,4)}}$ with suitably labeled boundaries.

So far so good! Congratulations and thanks for reading this far into this *epic* tome. Take a moment and treat yourself in a manner of your choosing. Then let us, in its fullest form, proceed on to the main results.

6.3 Main Results

Having developed methods to characterize protected gates on the space $\mathcal{H}_\Sigma$ for an arbitrary anyon model $\mathbb{A}$ and surface Σ, the main objective is to determine the nature of the group of protected gates $\mathcal{U}_{\mathbb{A},\Sigma} \subseteq \mathcal{C}(\mathcal{H}_\Sigma)$ in order to acces the computational power of protected gates for the model. The main result of this work given in Theorem 7.4.5 essentially states that the group of protected gates $\mathcal{U}_{\mathbb{A},\Sigma}$ is finite, and hence cannot be universal for quantum computation. This implies the necessity of alternative means outside of locality-preserving logical operations to achieve universality.

There is one important subtle technicality regarding the group $\mathcal{U}_{\mathbb{A},\Sigma}$ in the statement of Theorem 7.4.5. For a gate set to be computationally universal it must be *dense* in the unitary group $\mathcal{U}(\mathcal{H}_\Sigma)$, which implies that the group generated by the gate set must be infinite. Strictly speaking, as a set there may be infinitely many distinct protected gates in $\mathcal{U}_{\mathbb{A},\Sigma}$. However, in certain situations (as argued in Theorem 7.4.5), two distinct protected gates U and U' may yield a certain equivalent action. Such an equivalence is made formal through an equivalence relation that is placed on protected gates as described in Sections 7.4.3 and 7.4.4. By considering protected gates up to this equivalence relation, the potentially infinite set $\mathcal{U}_{\mathbb{A},\Sigma}$ becomes partitioned into only a finite number of equivalence classes. It is then this finite number of equivalence classes that limits interesting protected gates to be finite as well.

One other general result obtained applies to anyon models $\mathbb{A}$ for which the logical operations $\mathcal{T}(\vartheta)$ on some space $\mathcal{H}_\Sigma$ given by mapping class group elements $\vartheta \in \mathsf{MCG}_\mathbb{A}$ are computationally universal. In this case, Corollary 7.4.2 states that there are no nontrivial protected gates on$\mathcal{H}_\Sigma$ (up to the equivalence relations just described on protected gates). Thus, there seems to be an interesting trade off in the computational capabilities of a given model: the more computational power a model can afford through transformations corresponding to $\mathsf{MCG}_\mathbb{A}$, the less can be done using protected gates. This is further exemplified when analyzing various models.

The rest of the study applies various methods developed to characterize protected gates to a few paradigmatic anyon models. In particular, Section 7.6 gives special attention to the Fibonacci and Ising models, which are *non-abelian* anyon models. This property makes the models worth considering in the setting of the n-punctured sphere. In this scenario, Theorem 7.6.1 states that there are non non-trivial protected gates for the Fibonacci anyon model. This result follows from Corollary 7.4.2 since for certain instances of the Fibonacci model in the setting of the n-punctures sphere, it is known that braiding of anyons in the model achieves computational universality. For the Ising model on the n-punctured sphere, the corresponding mapping class group is not universal, and so the other methods described must be used to characterize protected gates. Theorem 7.6.2, concludes that in suitable settings the set of pro-

tected gates is isomorphic to the Pauli group on some number of encoded logical qubits. This existence of some nontrivial gates in this case, contrasts with the nonexistence of protected gates for the Fibonacci model.

One final general result obtained that characterizes protected gates applies to *abelian* anyon models. The Toric code of Chapter 2 is one such example of an abelian anyon model. Recall that in this case the logical operations resulting from various string operators $F_a(C)$, for nontrivial loops $C \subset \Sigma$ on some closed nonzero-genus surface Σ, correspond to Pauli operators on the encoded logical qubits of $\mathcal{H}_\Sigma$. In this context, it is worth considering the Clifford group, which is traditionally defined as the group of unitary operators U such that $UPU^\dagger$ is contained within the Pauli group for all Pauli operators P. For the Toric code, also recall that string operators $F_a(C)$ associated to multiple loops $C \subset \Sigma$ must be considered in order to generate the full Pauli group. That is, when restricting to a single loop $C \subset \Sigma$, the group generated by string operators $\{F_a(C)\}_{a\in\mathbb{A}}$ is a proper subgroup of the full Pauli group. This motivates defining a restricted Pauli group as given in Definition 7.7.6:

$$\mathsf{Pauli}_\Sigma(C) \coloneqq \left\langle \left\{ \lambda[F_a(C)] \;\middle|\; \lambda \in \langle e^{2\pi i/N}\rangle, a \in \mathbb{A} \right\} \right\rangle ,$$

In this way, $\mathsf{Pauli}_\Sigma(C)$ is just the group generated by string operators associated to some fixed loop $C \subset \Sigma$ (with possible phase factors).

Now consider a set $\mathcal{G}$ of loops on Σ that generate MCG_Σ, and define the group (as in Definition 7.7.7)

$$\mathsf{Clifford}^\star_\Sigma \coloneqq \{\lambda[U] \mid [U]\mathsf{Pauli}_\Sigma(C)[U]^{-1} \subset \mathsf{Pauli}_\Sigma(C) \text{ for all } C \in \mathcal{G},\ \lambda \in \langle e^{2\pi i/N}\rangle\} .$$

This group consists of operators $[U]$ which map each of the restricted Pauli groups $\mathsf{Pauli}_\Sigma(C)$ (for $C \in \mathcal{G}$) to themselves. In the case of the Toric code, $\mathsf{Clifford}^\star_\Sigma$ is a proper subgroup of the standard Clifford group. The main result here is the statement that protected gate U must be contained in $\mathsf{Clifford}^\star_\Sigma$. Although this statement was exemplified with the Toric Code, an arbitrary anyon model $\mathbb{A}$ can be considered and analogous groups $\mathsf{Pauli}_\Sigma(C)$ and $\mathsf{Clifford}^\star_\Sigma$ can be defined in terms of the string operators $F_a(C)$ for the particular anyon model $\mathbb{A}$. The general result regarding protected gates U for a general abelian model holds: $[U] \in \mathsf{Clifford}^\star_\Sigma$. A summary of these results is given in Table 7.1.

Chapter 7

"Protected gates for topological quantum field theories"

Authors:

Michael E. Beverland[1], Oliver Buerschaper[2], Robert Koenig[3], Fernando Pastawski[1], John Preskill[1], Sumit Sijher[4]

Afilliations:

1. Institute for Quantum Information & Matter, California Institute of Technology, Pasadena CA 91125, USA
2. Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany
3. IAS & Zentrum Mathematik, Technische Universität München, 85748 Garching, Germany
4. Institute for Quantum Computing & Department of Applied Mathematics, University of Waterloo, Waterloo, ON N2L 3G1, Canada

Abstract:

We give restrictions on locality-preserving unitary automorphisms U, which are protected gates, for topologically ordered systems in 2D. For generic anyon models, we show that such unitaries only generate a finite group, and hence do not provide universality. For non-abelian models, we find that such automorphisms are very limited: for example, there is no non-trivial protected gate for Fibonacci anyons on the torus or the M-punctured sphere. More generally, systems with computationally universal braiding have no such gates. For Ising anyons on the M-punctured sphere, protected gates are elements of the Pauli group. These results are derived by relating such automorphisms to certain symmetries of the underlying anyon model: protected gates realize automorphisms of the Verlinde algebra. We additionally use the compatibility with basis changes arising from local recoupling and the mapping class group to characterize the logical action.

7.1 Introduction

In order to reliably compute, it is necessary to protect information against noise. For quantum computations, this is particularly challenging because noise in the form of decoherence threatens the very quantum nature of the process. Adding redundancy by encoding information into a quantum error-correcting code is a natural, conceptually appealing approach towards building noise-resilient scalable computers based on imperfect hardware.

Among the known quantum error-correcting codes, the class of so-called topological codes stands out. Examples in 2D include the toric code and quantum double models [28], the surface codes [9], the 2D color codes [5], variants of these codes [4, 19], and the Levin-Wen model [34]. In 3D, known examples are Bombin and Martin-Delgado's 3D color code [7], as well as Haah's [23] and Michnicki's [37] models. These codes are attractive for a number of reasons: their code space is topologically protected, meaning that small local deformations or locally acting noise do not affect encoded information. The degree of this protection (measured in information-theoretic notions in terms of code distance, and manifesting itself in physical properties such as gap stability) scales with the system size: in other words, robustness essentially reduces to the question of scalability. Finally, the code space of a topological code is the degenerate ground space of a geometrically local Hamiltonian: this means that syndrome information can be extracted by local measurements, an important feature for actual realizations. Furthermore, this implies that a topological code is essentially a phase of a many-body system and can be characterized in terms of its particle content, their statistics, and the quantum field theory emerging in the continuum limit. In particular, the quantum field theory provides a description of such systems which captures all universal features, independently of microscopic details.

While quantum error-correcting codes can provide the necessary protection of information against noise, a further requirement for quantum computation is the ability to execute gates in a robust manner. Again, topological codes stand out: they usually provide certain intrinsic mechanisms for executing gates in a robust way. More precisely, there are sequences of local code deformations, under which the information stays encoded in a code with macroscopic distance, but undergoes some unitary transformation. In principle, this provides a robust implementation of computations by sequences of local, and hence, potentially experimentally realizable actions. In the case of $2D$-topological codes described by topological quantum field theories, this corresponds to adiabatic movement (braiding) of quasi-particle excitations (also called anyons).

Unfortunately, as is well known, braiding (by which we mean the movement either around each other or more generally around non-trivial loops) of anyons does not always give rise to a universal gate set. Rather, the set of gates is model-dependent: braiding of $D(\mathbb{Z}_2)$-anyons generates only global phases on the sphere, and elements of the Pauli group on non-zero genus surfaces. Braiding of Ising anyons gives Clifford gates, whereas braiding of Fibonacci anyons generates a dense subgroup of the set of unitaries (and is therefore universal within suitable subspaces of the code space). In other words, braiding alone, without additional tricks such as magic state distillation [10] (which has a large overhead [18]), is not in general sufficient to provide universal fault-tolerant computation; unfortunately, the known systems with universal braiding behavior are of a rather complex nature, requiring e.g., 12-body interactions among spins [34]. Even ignoring the question of universality, the use of braiding has some potentially significant drawbacks: in general (in particular for non-abelian anyons), it requires an amount of time which scales with the system size (or code distance) to execute a single logical gate. (Mathematically, this is reflected by the fact that string-operators cannot be implemented in finite depth.) This implies that error-correction steps will be necessary even during the execution of such a gate, which may pose an additional technological challenge, for example, if the intermediate topologies are different.

Given the limitations of braiding, it is natural to look for other mechanisms for implementing robust gates in topological codes. For stabilizer quantum codes, the notion of transversal gates has traditionally been used almost synonymously with fault-tolerant gates: their key feature is the fact that they do not propagate physical errors. More generally, for topological stabilizer codes, we can consider logical gates implementable by constant-depth quantum circuits as a proxy for robust gates: they can increase the weight of a physical error only by a constant, and are thus sufficiently robust when combined with suitable error-correction gadgets. Note that finite-depth local circuits represent a much broader class than transversal gates.

Gate restrictions on transversal, as well as constant-depth local circuits have been obtained

for stabilizer and more general codes. Eastin and Knill [15] argued that for any code protected against local errors, transversal gates can only generate a finite group and therefore do not provide universality. Bravyi and König [11] consider the group of logical gates that may be implemented by such constant-depth local circuits on geometrically local topological stabilizer codes. They found that such gates are contained in $\mathcal{P}_D$, the D-th level of the Clifford hierarchy, where D is the spatial dimension in which the stabilizer code is geometrically local.

In this work, we characterize the set of gates implementable by a locality-preserving unitary in a system described by a 2D TQFT. By doing so, we both specialize and generalize the results of [11]: we restrict our attention to dimension 2, but go beyond the set of local stabilizer codes in two significant ways.

First, we obtain statements which are independent of the particular realization (e.g., the toric code model) but are instead phrased in terms of the TQFT (i.e., the anyon model describing the system). In this way, we obtain a characterization which holds for a gapped phase of matter, rather than just for a particular code representing that phase. On a conceptual level, this is similar in spirit to the work of [16], where statements on the computational power for measurement-based quantum computation were obtained that hold throughout a certain phase. Here we use the term phase loosely – we say that two systems are in the same phase if they have the same particle content. To avoid having to make any direct reference to an underlying lattice model, we replace the notion of a constant-depth local circuit by the more general notion of a locality-preserving unitary: this is a unitary operation which maps local operators to local ones.

Second, our results and techniques also apply to non-abelian anyon models (whereas stabilizer codes only realize certain abelian models). In particular, we obtain statements that can be applied, e.g., to the Levin-Wen models [34], as well as chiral phases. Our approach relates locality-preserving unitaries to certain symmetries of the underlying anyon model; this imposes constraints on the allowed operations. We consider the Fibonacci and Ising models as paradigmatic examples and find that there are no non-trivial gates in the former, and only Pauli operations in the latter case. Our focus on these anyons models is for concreteness only, but our methods and conclusions apply more generally. Some of our more general conclusions are that

(i) protected gates generically (see Section 7.4.5 discussing the necessity of certain technical assumptions) form only a finite group and

(ii) when the representation of the mapping class group is computationally universal (i.e., forms a dense subgroup), then there are no non-trivial protected gates.

Model	mapping class group contained in	locality-preserving unitaries contained in
$D(\mathbb{Z}_2)$	Pauli group	restricted Clifford group
abelian anyon model	generalized Pauli group	generalized Clifford group
Fibonacci model	universal	global phase (trivial)
general anyon model	universal	global phase (trivial)
Ising model	Clifford group	Pauli group
generic anyon model	model-dependent	finite group

Table 7.1: We study different anyon models (first column). The second column describes the properties of the unitary group generated by the (projective) representation of the mapping class group (see Section 7.2.6) – this corresponds to braiding for punctured spheres. The third column characterizes the set of protected gates. Our results suggest a trade-off between the computational power of the mapping class group representation and that of gates implementable by locality-preserving unitaries.

Our observations are summarized in Table 7.1.

Finally, let us comment on limitations, as well as open problems arising from our work. The first and most obvious one is the dimensionality of the systems under consideration: our methods apply only to $2D$ TQFTs. The mathematics of higher-dimensional TQFTs is less developed, and currently an active research area (see e.g., [32]). While the techniques of [11], which have recently been significantly strengthened by Pastawski and Yoshida [39], also apply to higher-dimensional codes (such as Haah's), they are restricted to the stabilizer formalism (but importantly, [39] also obtain statements for subsystem codes). Obtaining non-abelian analogues of our results in higher dimensions appears to be a challenging research problem. A full characterization of the case $D = 3$ is particularly desirable from a technological viewpoint.

Even in $2D$, there are obvious limitations of our results: the systems we consider are essentially "homogenous" lattices with anyonic excitations in the bulk. We are not considering defect lines, or condensation of anyons at boundaries; for example, our discussion excludes the quantum double models constructed in [3], which have domain walls constructed from condensation at boundaries using the folding trick. Again, we expect that obtaining statements on protected gates for these models requires additional technology in the form of more refined categorical notions, as discussed by Kitaev and Kong [30]. Also, although we identify possible locality preserving logical unitaries, our arguments do not show that these can necessarily be realized, either in general TQFTs or in specific models that realize TQFTs. Lastly, our work is based on the (physically motivated) assumption that a TQFT description is possible and the underlying data is given. For a concrete lattice model of interacting spins, the problem of identifying this description (or associated invariants [27, 35, 24]), as well as constructing the

relevant string-operators (as has been done for quantum double models [28, 6] as well as the Levin-Wen models [34]), is a problem in its own right.

Rough statement of problem

Our results concern families of systems defined on any 2-dimensional orientable manifold (surface) Σ. Typically, such a family is defined in terms of some local physical degrees of freedom (spins) associated with sites of a lattice embedded in Σ. We refer to the joint Hilbert space $\mathcal{H}_{\text{phys},\Sigma}$ of these spins as the 'physical' Hilbert space. The Hamiltonian H_Σ on $\mathcal{H}_{\text{phys},\Sigma}$ is local, i.e., it consists only of interactions between "neighbors" within constant-diameter regions on the lattice. More generally, assuming a suitable metric on Σ is chosen, we may define locality in terms of the distance measure on Σ.

We are interested in the ground space $\mathcal{H}_\Sigma$ of H_Σ. For a topologically ordered system, this ground space is degenerate with dimension growing exponentially with the genus of Σ, and is therefore suitable for storing and manipulating quantum information. We will give a detailed description of this space below (see Section 7.2); it has a preferred basis consisting of labelings associated with some set $\mathbb{A}$. This is a finite set characterizing all distinct types of anyonic quasiparticle excitations of H_Σ in the relevant low energy sector of $\mathcal{H}_{\text{phys},\Sigma}$.

Importantly, the form of $\mathcal{H}_\Sigma$ is independent of the microscopic details (in the definition of H_Σ): it is fully determined by the associated TQFT. In mathematical terms, it can be described in terms of the data of a modular tensor category, which also describes fusion, braiding and twists of the anyons. We will refer to $\mathcal{H}_\Sigma$ as the TQFT Hilbert space.

The significance of $\mathcal{H}_\Sigma$ is that it is protected: local observables can not distinguish between states belonging to $\mathcal{H}_\Sigma$. This implies that $\mathcal{H}_\Sigma$ is an error-correcting code with the property that local regions are correctable: any operator supported in a small region which preserves the code space must act trivially on it (otherwise it could be used to distinguish between ground states).

To compute fault-tolerantly, one would like to operate on information encoded in the code space $\mathcal{H}_\Sigma$ by acting with a unitary $U : \mathcal{H}_{\text{phys},\Sigma} \to \mathcal{H}_{\text{phys},\Sigma}$ on the physical degrees of freedom. There are a number of features that are desirable for such a unitary to be useful – physical realizability being an obvious one. For fault-tolerance, two conditions are particularly natural:

(i) the unitary U should preserve the code space, $U\mathcal{H}_\Sigma = \mathcal{H}_\Sigma$ so that the information stays encoded. We call a unitary U with this property an automorphism of the code and denote its restriction to $\mathcal{H}_\Sigma$ by $[U] : \mathcal{H}_\Sigma \to \mathcal{H}_\Sigma$. The action $[U]$ defines the logical operation or gate that U realizes.

(ii) typical errors should remain correctable under the application of the unitary U. In the context of topological codes, which correct sufficiently local errors, and where a local error model is usually assumed, this condition is satisfied if U does not significantly change the locality properties of an operator: if an operator X has support on a region $\mathcal{R} \subset \Sigma$, then the support of $UXU^\dagger$ is contained within a constant-size neighborhood of $\mathcal{R}$. We call such a unitary a locality-preserving unitary.

We call a unitary U satisfying (i) and (ii) a locality-preserving unitary automorphism of the code (or simply a topologically protected gate). Our goal is to characterize the set of logical operations that have the form $[U]$ for some locality-preserving[1] unitary automorphism U. For example, if $\mathcal{H}_\Sigma$ is a topologically ordered subspace of $\mathcal{H}_{\mathrm{phys},\Sigma}$, the Hilbert space of a spin lattice, then (ii) is satisfied if U is a constant-depth local circuit. Another important example is the constant-time evolution $U = \mathcal{T}\exp[-i\int dt H(t)]$ of a system through a bounded-strength geometrically-local Hamiltonian $H(t)$. Here, Lieb-Robinson bounds [36, 8] provide quantitative statements on how the resulting unitary may be exponentially well approximated by a locality-preserving unitary. This is relevant since it describes the time evolution of a physical system and can also be used to model adiabatic transformations of the Hamiltonian [12].

From a computational point of view, the group

$$\langle \{[U] \mid U \text{ locality-preserving unitary automorphism}\} \rangle$$

generated by such gates is of particular interest: it determines the computational power of gates that are implementable fault-tolerantly with locality preserving automorphisms.

Outline

In Section 7.2, we provide a brief introduction to the relevant concepts of TQFTs. We then derive our main results on the characterization of protected gates in Section 7.3. Further restrictions on the allowed protected gates are provided in Sections 7.4 and 7.5. In Section 7.6, we apply our results to particular models, deriving in particular our characterizations for Ising and Fibonacci anyons. Finally, in Section 7.7 we use additional properties of abelian models to show that their protected gates must be contained within a proper subgroup of the generalized Clifford group, which is similar to the result of [11], but goes further.

[1] As a side remark, we mention that our terminology is chosen with spin lattices in mind. However, the notion of locality-preservation can be relaxed. As will become obvious below, our results apply more generally to the set of *homology-preserving* automorphisms U. The latter can be defined as follows: if the support of an operator X is contained in a region $\mathcal{R} \subset \Sigma$ which deformation retracts to a closed curve C, then the support of $UXU^\dagger$ must be contained in a region $\mathcal{R}' \subset \Sigma$ which deformation retracts to a curve C' in the same homology class as C. For example, for a translation-invariant system, translating by a possibly extensive amount realizes such a homology-preserving (but not locality-preserving) automorphism.

7.2 TQFTs: background

In this section, we provide the necessary background on topological quantum field theories (TQFTs). Our discussion will be rather brief; for a more detailed discussion of topological quantum computation and anyons, we refer to [40]. Following Witten's work [44], TQFTs have been axiomatized by Atiyah [1] based on Segal's work [41] on conformal field theories. Moore and Seiberg [38] derived the relations satisfied by the basic algebraic data of such theories (or more precisely, a modular functor). Here we borrow some of the terminology developed in full generality by Walker [26] (see also [21]). For a thorough treatment of the category-theoretic concepts, we recommend the appendix of [29].

Our focus is on the Hilbert space $\mathcal{H}_\Sigma$ spanned by the vacuum states of a TQFT defined on the surface Σ. Recall that this is generally a subspace $\mathcal{H}_\Sigma \subset \mathcal{H}_{\text{phys},\Sigma}$ of a Hilbert space of physical degrees of freedom. The TQFT is specified by a finite set of anyon labels $\mathbb{A} = \{1, a, b, c \dots\}$, their *fusion rules* (described using a non-negative integer N_{ab}^c for each triple of anyons a, b, c, called fusion multiplicities), along with S, F, R and T matrices (complex valued matrices with columns and rows indexed by anyon labels). If the TQFT arises from taking continuous limits of a local Hamiltonian model such as the toric code, the anyons are simply the elementary excitations of the model, and the fusion rules and matrices can be understood in terms of creating, combining, moving and annihilating anyons in the surface. The anyon set must contain a trivial particle $1 \in \mathbb{A}$ such that when combined with any particle, the latter remains unchanged $N_{a1}^c = N_{1a}^c = \delta_a^c$, and each particle $a \in \mathbb{A}$ must have an antiparticle $\overline{a} \in \mathbb{A}$ such that $N_{a\overline{a}}^1 \neq 0$. We will restrict our attention to models where $N_{ab}^c \in \{0, 1\}$ for all $a, b, c \in \mathbb{A}$ for simplicity (our results generalize with only minor modifications).

7.2.1 String-like operators and relations

We are interested in the algebra $\mathcal{A}_\Sigma$ of operators $X : \mathcal{H}_{\text{phys},\Sigma} \to \mathcal{H}_{\text{phys},\Sigma}$ which preserve the subspace $\mathcal{H}_\Sigma$. We call such an element $X \in \mathcal{A}_\Sigma$ an automorphism and denote by $[X] : \mathcal{H}_\Sigma \to \mathcal{H}_\Sigma$ the restriction to $\mathcal{H}_\Sigma$. We call X a representative (or realization) of $[X]$. Operators of the form $[X]$, where $X \in \mathcal{A}_\Sigma$, define an associative $*$-algebra $[\mathcal{A}_\Sigma]$ with unit and multiplication $[X][Y] = [XY]$. The unit element in $[\mathcal{A}_\Sigma]$ is represented by the identity operator id on the whole space $\mathcal{H}_{\text{phys},\Sigma}$.

Our constraints on protected gates are derived by studying how they transform certain operators acting on $\mathcal{H}_{phys,\Sigma}$ (see Fig. 7.1). To define the latter, fix a simple closed curve $C : [0, 1] \to \Sigma$ on the surface and an "anyon label" $a \in \mathbb{A}$. (The set of labels $\mathbb{A}$ is determined by the underlying model.) Then there is a "string-operator" $F_a(C)$ acting on $\mathcal{H}_{\text{phys},\Sigma}$, supported

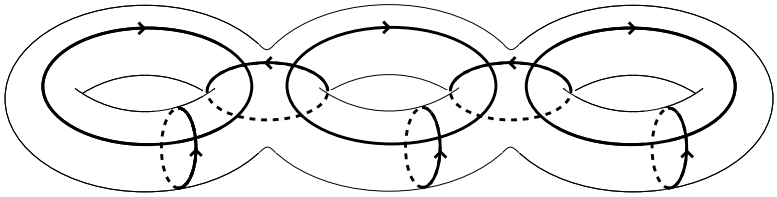


Figure 7.1: Closed 2-manifolds are characterized by their genus g. The figure illustrates the 3-handled torus Σ_g corresponding to $g = 3$. A canonical set of $3g-1$ generators of the mapping class group of the surface Σ_g can be specified in terms of a set $\mathcal{G} = \{C_j\}_{j=1}^{3g-1}$ of loops (each associated with a Dehn twist). Dragging an anyon a around such loop $C : [0,1] \to \Sigma_g$ and fusing to the vacuum implements an undetectable operator $F_a(C)$; homologically non-trivial loops realize logical operations. The full algebra of logical operators is generated by the set of operators $\{F_a(C)\}_{a\in\mathbb{A},C\in\mathcal{G}}$. However, these operators are generally not independent.

in a constant-diameter neighborhood of C. It corresponds to the process of creating a particle-antiparticle-pair $(a, \overline{a})$, moving a along C, and subsequently fusing to the vacuum. The last step in this process involves projection onto the ground space, which is not trivial in general: the operator $F_a(C)$ can involve post-selection, in which case it is a non-unitary element of $\mathcal{A}_\Sigma$.

The operators $\{F_a(C)\}_{a\in\mathbb{A}}$ form a closed subalgebra $\mathcal{A}(C) \subset \mathcal{A}_\Sigma$: they preserve the ground space and satisfy

$$F_a(C)F_b(C) = \sum_n N_{ab}^n F_n(C) \ , \qquad F_a(C)^\dagger = F_{\overline{a}}(C) \qquad \text{and} \qquad F_1(C) = \mathsf{id}_{\mathcal{H}_{\text{phys}}} \tag{7.1}$$

for the fusion multiplicities N_{ab}^n (see Section 7.2.2). In addition, reversing the direction of C, i.e., considering $C^{-1}(t) \equiv C(1-t)$, is equivalent to exchanging the particle with its antiparticle, i.e.,

$$F_a(C^{-1}) = F_{\overline{a}}(C) \ . \tag{7.2}$$

Here $a \mapsto \overline{a}$ is an involution on the set of particle labels $\mathbb{A}$, again defined by the underlying model. Properties (7.1) and (7.2) of the string-operators can be shown in the diagrammatic formalism mentioned below (but this is not needed here; we will use them as axioms).

We denote the restriction of $F_a(C)$ to the code space $\mathcal{H}_\Sigma$ by $[F_a(C)]$. Note that, while $[F_a(C)]$ is unitary in abelian anyon models, this is not the case in general.

Example 7.2.1 ($D(G)$ and Kitaev's toric code)**.** *As an example, consider a model described by the quantum double $D(G)$ of a finite group G, for which Kitaev has constructed a lattice model [28]. In the case where G is abelian, we have $D(G) \cong G \times G$, i.e., the particles and fusion rules are simply given by the product group $\mathbb{A} = G \times G$.*

Specializing to $G = \mathbb{Z}_2$ gives the particles commonly denoted by $1 = (0,0)$ (vacuum), $m = (1,0)$, $e = (0,1)$ and $\epsilon = m \times e = (1,1)$. For the toric code model, the associated ribbon operators are

$$F_1(C) = \mathsf{id} \quad F_e(C) = \bar{X}(C) \quad F_m(C) = \bar{Z}(C) \quad F_\epsilon(C) = \bar{X}(C)\bar{Z}(C) \ ,$$

where $\bar{X}(C) = \otimes_{j \in \partial_+ C} X_j$ and $\bar{Z}(C) = \otimes_{j \in \partial_- C} Z_j$ are appropriate tensor products of Pauli-X and Pauli-Z-operators along C (as specified in [28]).

Specializing to $G = \mathbb{Z}_N$, with $\omega_N = \exp(2\pi i/N)$ and generalized N-dit Pauli operators X and Z (and their inverses), defined by their action

$$X|j\rangle = |j+1 \mod N\rangle \qquad Z|j\rangle = \omega_N^j |j\rangle$$

on computational basis states $\{|j\rangle\}_{j=0,\ldots,N-1}$, we can consider such a model (the $\mathbb{Z}_N$-toric code) with generalized ribbon operators. Here

$$F_{(a,a')}(C) = \bar{X}(C)^a \bar{Z}(C)^{a'},$$

where $\bar{X}(C)$ is a tensor product of Pauli-X and its inverse depending on the orientation of the underlying lattice, and similarly for $\bar{Z}(C)$.

It is easy to check that operators associated with the same loop commute, i.e.,

$$[F_{(a,a')}(C), F_{(b,b')}(C)] = 0 \ , \tag{7.3}$$

and since $Z^a X^b = \omega_N^{ab} X^b Z^a$, we get the commutation relation

$$F_{(a,a')}(C_1) F_{(b,b')}(C_2) = \omega_N^{ab'-a'b} F_{(b,b')}(C_2) F_{(a,a')}(C_1) \tag{7.4}$$

for any two strings C_1, C_2 intersecting once.

Returning to the general case, the algebra of string operators does not necessarily satisfy relations as simple as (7.3) and (7.4). Nevertheless, some essential features hold under very general assumptions. We express these as postulates; they can be seen as a subset of the isotopy-invariant calculus of labeled ribbon graphs associated with the underlying category (see e.g., [20] for a discussion of the latter) and are assumed to be valid for all anyon models considered in this work.

Postulate 7.2.2 (Completeness of string-operators)**.** *Consider an operator U with support in some region $\mathcal{R}$ which preserves the code space $\mathcal{H}_\Sigma$. Then its action on the code space is*

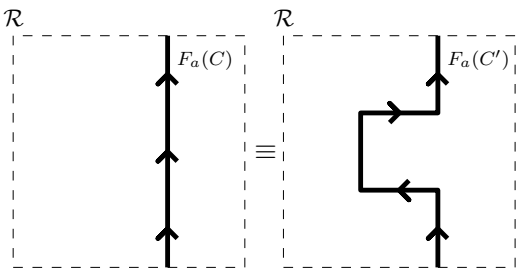
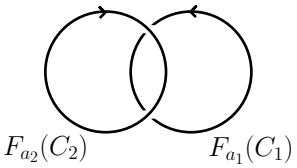


Figure 7.2: The content of Postulate 7.2.3: We can deform a line without changing the logical action of the string-operator.

equivalent to that of a linear combination of products of operators of the form $F_a(C)$, for a closed loop $C : [0, 1] \to \mathcal{R}$ which is supported in $\mathcal{R}$. That is, we have

$$[U] = \sum_j \beta_j \prod_k [F_{a_{j,k}}(C_{j,k})] \ .$$

This postulate essentially means that, as far as the logical action is concerned, we may think of $[U]$ as a linear combination of products of closed-loop string operators. Such products $F_{a_m}(C_m) \cdots F_{a_1}(C_1)$ can conveniently be thought of as 'labeled' loop gases embedded in the three-manifold $\Sigma \times [0, 1]$, where, for some $0 < t_1 < \cdots < t_m < 1$, the operator $F_{a_j}(C_j)$ is applied at 'time' t_j (and hence a labeled loop is embedded in the slice $\Sigma \times \{t_j\}$). Diagrammatically, one represents such a product by the projection onto Σ with crossings representing temporal order, as in

$$F_{a_2}(C_2)F_{a_1}(C_1) \quad = \quad \text{  } \tag{7.5}$$

One may manipulate every term in a linear combination representing U without changing the logical action according to certain local 'moves'; in particular, the order of application of these moves is irrelevant (a fact formalized by MacLane's theorem [33]).

For our purposes, we only require the following 'local' moves, which relate two products U and U' of string-operators given by diagrams such as (7.5). More generally, they may be applied term-by-term to any linear combination if each term contains the same local sub-diagram.

Postulate 7.2.3 (String deformation (see Fig. 7.2))**.** *Suppose operators $U, U' \in \mathcal{A}_\Sigma$ are identical on the complement of some region $\mathcal{R}$. Assume further that inside $\mathcal{R}$, both U and U' contain a single string describing the dragging of the same anyon type along a path C and C', respectively, where C' can be locally deformed into C. Then the logical action of U and U' must be equivalent:*

$[U] = e^{i\theta}[U']$ *for some unimportant phase* $e^{i\theta}$ *(Fig. 7.2.3).*

In particular, this postulate implies that if C and C' are two closed homologically equivalent loops and a is an arbitrary anyon label, then the operators $F_a(C)$ and $F_a(C')$ realized by "dragging" the specified anyon along C and C' respectively have equivalent logical action on the code space, $[F_a(C)] = e^{i\theta}[F_a(C')]$.

The next postulate involves local operators, and essentially states that the space $\mathcal{H}_\Sigma$ is a quantum error-correcting code protecting against local errors. While we may state it in a form only referring to local operators, we will find it more intuitive to combine it with the deformation postulate: this extends correctability from small regions to contractible loops (i.e., loops that are homotopic to a point).

Postulate 7.2.4 (Error correction postulate)**.** *If C is a contractible loop, then for each $a \in \mathbb{A}$, the operator $F_a(C)$ has trivial action on the space $\mathcal{H}_\Sigma$ up to a global constant d_a, that is,*

$$[F_a(C)] = d_a \mathsf{id}_{\mathcal{H}_\Sigma} \ . \tag{7.6}$$

This postulate essentially means that we may remove certain closed loops from diagrams such as (7.5).

An immediate consequence of these postulates is the following statement.

Proposition 7.2.1 (Local completeness of string operators)**.** *Consider an operator $O \in \mathcal{A}_\Sigma$ whose support is contained within a constant-diameter neighborhood of a simple loop C. Then $[O] = [\tilde{X}]$ for some $\tilde{X} \in \mathcal{A}(C)$. In other words, the logical action of O is identical to that of a linear combination of string-operators $F_a(C)$.*

This proposition can be seen as a consequence of the completeness condition for strings (Postulate 7.2.2), the string deformation Postulate 7.2.3 and (7.1). A similar argument leads us to the following conclusion.

Proposition 7.2.2 (Global completeness of few homology classes)**.** *The full logical algebra $[\mathcal{A}_\Sigma]$ is generated by the logical algebras $[\mathcal{A}(C)]$ associated with a finite number of inequivalent non-contractible simple loops C.*

Proof. That the algebra $[\mathcal{A}_\Sigma]$ is finite-dimensional can be seen from the finite dimensionality of the code space $\mathcal{H}_\Sigma$. By Postulate 7.2.2, the algebra $[\mathcal{A}_\Sigma]$ is generated by $\{\mathcal{A}(C)\}_C$. Let us start from a trivial algebra and build up $[\mathcal{A}_\Sigma]$ from a finite number of loops. As long as the algebra is not complete, we may include additional loops C such that $[\mathcal{A}(C)]$ is not included in the partially generated algebra. Such a loop C must be inequivalent to the previously included

loops due to Postulate 7.2.3. After a number of steps no greater than the square of the ground space dimension, we will have constructed the complete algebra. □

Therefore there exists a finite, *minimal* set of loops which is sufficient to span $[\mathcal{A}_\Sigma]$.

7.2.2 The Verlinde algebra

It is convenient to formally introduce some algebraic data defined by the underlying anyon model. We will return to the discussion of string-operators in the next section and relate them to this algebraic language.

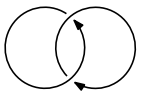
As before, let $\mathbb{A}$ be the set of particle labels (generally a finite set), and let $a \mapsto \overline{a}$ be the involution giving the antiparticle associated with particle a. The *fusion rules* of the model are encoded in integers N_{ab}^c, which are called fusion multiplicites. We will restrict our attention to models where $N_{ab}^c \in \{0, 1\}$ for all $a, b, c \in \mathbb{A}$ for simplicity (our results generalize with only minor modifications).

The *Verlinde algebra* Ver is the commutative associative $*$-algebra spanned by elements $\{\mathbf{f}_a\}_{a\in\mathbb{A}}$ satisfying the relations

$$\mathbf{f}_a\mathbf{f}_b = \sum_c N_{ab}^c \mathbf{f}_c \qquad \text{and} \qquad \mathbf{f}_a^\dagger = \mathbf{f}_{\overline{a}} \,. \tag{7.7}$$

Note that $\mathbf{f}_1 = \mathsf{id}$ is the identity element because the numbers $\{N_{ab}^c\}$ satisfy $N_{a1}^c = N_{1a}^c = \delta_{ac}$.

If braiding is defined, we have $N_{ab}^c = N_{ba}^c$, and Ver is a finite-dimensional commutative C^*-algebra. Therefore $\mathsf{Ver} \cong \mathbb{C}^{\oplus(\dim \mathsf{Ver})}$ is a direct sum of copies of $\mathbb{C}$. The fusion multiplicity N_{ab}^c may also be written in terms of the modular S-matrix, whose matrix elements are, in the diagrammatic calculus, given by the Hopf link and the total quantum dimension $\mathcal{D}$ by

$S_{ab} = \frac{1}{\mathcal{D}}$  .

We consider the case where the S-matrix is unitary: here the isomorphism $\mathsf{Ver} \cong \mathbb{C}^{\oplus(\dim \mathsf{Ver})}$ can be made explicit thanks to the *Verlinde formula* [43]

$$N_{ab}^c = \sum_x \frac{S_{ax} S_{bx} S_{\overline{c}x}}{S_{1x}} \,. \tag{7.8}$$

(Note that $S_{1x} = d_x/\mathcal{D}$ where $\mathcal{D} = \sqrt{\sum_a d_a^2}$.) For this purpose, we define the elements

$$\mathbf{p}_a = S_{1a} \sum_b \overline{S_{ba}} \mathbf{f}_b \qquad \text{for all } a \in \mathbb{A} \,. \tag{7.9}$$

This relation can be inverted by making use of unitarity of the S-matrix

$$\mathbf{f}_b = \sum_a \frac{S_{ba}}{S_{1a}} \mathbf{p}_a \qquad \text{for all } a \in \mathbb{A} \ . \tag{7.10}$$

The main statement we use is the following:

Proposition 7.2.3 (Primitive idempotents)**.** *The elements $\{\mathbf{p}_a\}_{a\in\mathbb{A}}$ are the unique complete set of orthogonal minimal idempotents spanning the Verlinde algebra,*

$$\mathsf{Ver} = \bigoplus_a \mathbb{C}\mathbf{p}_a \ . \tag{7.11}$$

Furthermore, they satisfy

$$\sum_a \mathbf{p}_a = \mathbf{f}_1 = \mathsf{id} \ . \tag{7.12}$$

Proof. That $\{\mathbf{p}_a\}_{a\in\mathbb{A}}$ span the algebra Ver is evident from the fact that $\{\mathbf{f}_a\}_{a\in\mathbb{A}}$ span the algebra, and each $\mathbf{f}_a$ can be written in terms of $\{\mathbf{p}_a\}_{a\in\mathbb{A}}$ via Eq. (7.10). To show they are orthogonal idempotents $\mathbf{p}_a\mathbf{p}_b = \delta_{a,b}\mathbf{p}_a$, first note that

$$\begin{aligned}
\mathbf{p}_a\mathbf{p}_b &= S_{1a}S_{1b} \sum_{g,h} \overline{S_{ga}S_{hb}} \mathbf{f}_g\mathbf{f}_h \\
&= S_{1a}S_{1b} \sum_{g,h,j} \overline{S_{ga}S_{hb}} N_{gh}^j \mathbf{f}_j \\
&= S_{1a}S_{1b} \sum_{g,h,j,x} \overline{S_{ga}S_{hb}} \frac{S_{gx}S_{hx}S_{\bar{j}x}}{S_{1x}} \mathbf{f}_j
\end{aligned}$$

where we used the Verlinde formula (7.8) in the second step. With the unitarity of the S-matrix, we then obtain

$$\begin{aligned}
\mathbf{p}_a\mathbf{p}_b &= S_{1a}S_{1b} \sum_{j,x} \delta_{a,x}\delta_{b,x} \frac{S_{\bar{j}x}}{S_{1x}} \mathbf{f}_j \\
&= \delta_{a,b} S_{1a}^2 \sum_j \frac{S_{\bar{j}a}}{S_{1a}} \mathbf{f}_j \\
&= \delta_{a,b} S_{1a} \sum_j S_{\bar{j}a} \mathbf{f}_j \ .
\end{aligned}$$

It follows that $\mathbf{p}_a\mathbf{p}_b = \delta_{a,b}\mathbf{p}_a$ from the symmetry property $S_{\bar{j}a} = \overline{S_{ja}}$, see e.g., [29, Eq. (224)]. It remains to verify that the set of projectors is unique. Consider $\mathbf{q}_b = \sum_a \alpha_{ba}\mathbf{p}_a$ for some

constants $\alpha_{ba} \in \mathbb{C}$, such that $\mathbf{q}_a \mathbf{q}_b = \delta_{a,b} \mathbf{q}_a$. This implies

$$\begin{aligned} \mathbf{q}_a \mathbf{q}_b &= \sum_{dc} \alpha_{ac} \alpha_{bd} \mathbf{p}_c \mathbf{p}_d \\ &= \sum_{c} \alpha_{ac} \alpha_{bc} \mathbf{p}_c = \delta_{a,b} \sum_{c} \alpha_{ac} \mathbf{p}_c, \end{aligned}$$

which implies $\alpha_{ac}\alpha_{bc} = \delta_{a,b}\alpha_{ac}$ for all $a, c \in \mathbb{A}$ by linear independence of the $\mathbf{p}_a$'s. This implies $\alpha_{ac} = 0, 1$, and can only form a complete basis for the algebra Ver if α_{ac} is a permutation matrix, implying $\{\mathbf{q}_a\}_{a\in\mathbb{A}} \equiv \{\mathbf{p}_a\}_{a\in\mathbb{A}}$.

□

As explained in the next section, the string operators of anyons around a loop C give rise to a representation of the Verlinde algebra. While the projections (introduced in Eq. (7.14) below) associated with the idempotents are not a basis for the logical algebra $[\mathcal{A}_\Sigma]$, they are a basis of a subalgebra $[\mathcal{A}_\Sigma(C)]$ isomorphic to the Verlinde algebra. This algebra must be respected by the locality-preserving unitaries, and this is best understood in terms of the idempotents. This is the origin of the non-trivial constraints we obtain on the realizable logical operators.

7.2.3 Bases of the Hilbert space $\mathcal{H}_\Sigma$

Eq. (7.1) shows that the collection of operators $\{[F_a(C)]\}_{a\in\mathbb{A}}$ form a representation of the Verlinde (fusion) algebra Ver. By linear independence of operators $\{[P_a(C)]\}_{a\in\mathbb{A}}$, we see that the representation is faithful, such that the logical loop algebra is isomorphic to the Verlinde algebra

$$[\mathcal{A}(C)] \cong \mathsf{Ver}. \tag{7.13}$$

This will be central in the following development. Considering the primitive idempotents (7.9), it is natural to consider the corresponding operators in this representation, that is, we set

$$[P_a(C)] = S_{1a} \sum_b \overline{S_{ba}} [F_b(C)] \ . \tag{7.14}$$

Since the set $\{[F_a(C)]\}_{a\in\mathbb{A}}$ forms a representation of the Verlinde algebra, the $\{[P_a(C)]\}_{a\in\mathbb{A}}$ are orthogonal projectors as a consequence of Proposition 7.2.3. The inverse relation to (7.14) is given by

$$[F_b(C)] = \sum_a \frac{S_{ba}}{S_{1a}} [P_a(C)] \ . \tag{7.15}$$

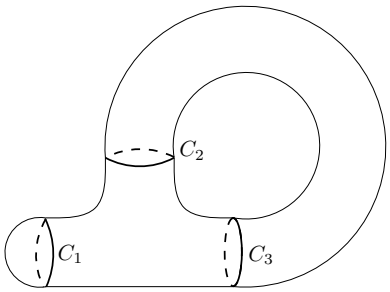


Figure 7.3: A simple DAP decomposition of a torus utilizing a disc enclosed by C_1, an annulus enclosed by $\{C_2, C_3\}$ and a pair of pants enclosed by $\{C_1, C_2, C_3\}$. This decomposition is not minimal in that the same manifold could have been decomposed using a single loop.

While the projectors $[P_a(C)]$ associated with a loop do not span the full logical algebra, they do span the local logical algebra of operators supported along C which must be respected by locality preserving unitaries. Intuitively, $\{P_a(C)\}_{a\in\mathbb{A}}$ are projectors onto the smallest possible sectors of the Hilbert space which can be distinguished by a measurement supported on C. This is the origin of the non-trivial constraints we obtain on the realizable logical operators.

A state in the image of $P_a(C)$ has the interpretation of carrying flux a through the loop C. In particular, since the code space $\mathcal{H}_\Sigma$ corresponds to the vacua of a TQFT, there are no anyons present on Σ, however, there can be flux associated to non-contractible loops. We can use the operators $\{P_a(C)\}_{a,C}$ to define bases of the Hilbert space $\mathcal{H}_\Sigma$.

Let us first define the Hilbert space $\mathcal{H}_\Sigma$ in more detail.

Definition 7.2.5 (DAP-decomposition)**.** *Consider a minimal collection $\mathcal{C} = \{C_j \mid C_j : [0,1] \to \Sigma\}_j$ of pairwise non-intersecting non-contractible loops, which cut the surface Σ into a collection of surfaces homeomorphic to discs, annuli and pants. We call $\mathcal{C}$ a DAP-decomposition.*

A *labeling* $\ell\colon \mathcal{C} \mapsto \mathbb{A}$ is an assignment of an anyon label $\ell(C)$ to every loop $C \in \mathcal{C}$ of a DAP decomposition. We call ℓ fusion-consistent if it satisfies the following conditions:

(i) for every loop $C \in \mathcal{C}$ enclosing a disc on Σ, $\ell(C) = 1$, the vacuum label of the anyon model.

(ii) for every pair of loops $\{C_2, C_3\} \subset \mathcal{C}$ defining an annulus in Σ, $\ell(C_2) = \overline{\ell(C_3)}$ assuming the loops are oriented such that the annulus is found to the left.

(iii) for every triple $\{C_1, C_2, C_3\} \subset \mathcal{C}$ defining a pair of pants in Σ, the labeling ℓ satisfies the fusion rule

$$N_{\ell(C_1),\ell(C_2)}^{\overline{\ell(C_3)}} \neq 0,$$

where the loops are oriented such that the pair of pants is found to the left.

Here we may assume $\ell(C^{-1}) = \overline{\ell(C)}$, where C^{-1} denotes the loop coinciding with C but with opposite orientation.

Now fix any DAP-decomposition $\mathcal{C}$ of Σ and let $\mathsf{L}(\mathcal{C}) \subset \mathbb{A}^{|\mathcal{C}|}$ be the set of fusion-consistent labelings. The Hilbert space $\mathcal{H}_\Sigma$ is the formal span of elements of $\mathsf{L}(\mathcal{C})$

$$\mathcal{H}_\Sigma \coloneqq \sum_{\ell \in \mathsf{L}(\mathcal{C})} \mathbb{C}\ell = \sum_{\ell \in \mathsf{L}(\mathcal{C})} \mathbb{C}\,|\ell\rangle.$$

Any fusion-consistent labeling $\ell \in \mathsf{L}(\mathcal{C})$ defines an element $|\ell\rangle \in \mathcal{H}_\Sigma$ such that the vectors $\{|\ell\rangle\}_{\ell \in \mathsf{L}(\mathcal{C})}$ are an orthonormal basis (which we call $\mathcal{B}_\mathcal{C}$) of $\mathcal{H}_\Sigma$, and this defines the inner product.

It is important to remark that this construction of $\mathcal{H}_\Sigma$ is independent of the DAP-decomposition $\mathcal{C}$ of Σ in the following sense: if $\mathcal{C}$ and $\mathcal{C}'$ are two distinct DAP-decompositions, then there is a unitary basis change between the bases $\mathcal{B}_\mathcal{C}$ and $\mathcal{B}_{\mathcal{C}'}$. In most cases under consideration, this basis change can be obtained as a product of unitaries associated with local "moves" connecting two DAP decompositions $\mathcal{C}$ and $\mathcal{C}'$. One such basis change is associated with a four-punctured sphere (the F-move), and specified by the unitary F-matrix in Fig. 7.4. Another matrix of this kind, the S-matrix (which also arose in our discussion of the Verlinde algebra), connects the two bases $\mathcal{B}_\mathcal{C}$ and $\mathcal{B}_{\mathcal{C}'}$ of $\mathcal{H}_{\text{torus}}$ associated with the first and second non-trivial cycles on the torus (Fig. 7.4). In this case, writing $\mathcal{B}_\mathcal{C} = \{|a\rangle_\mathcal{C}\}_a$ and $\mathcal{B}_{\mathcal{C}'} = \{|a\rangle_{\mathcal{C}'}\}_a$ since each basis element $|\ell\rangle$ is specified by a single label $\ell(C), \ell(C') \in \mathbb{A}$, we have the relation

$$|a\rangle_{\mathcal{C}'} = \sum_b S_{ba} |b\rangle_\mathcal{C} \ . \tag{7.16}$$

Other unitary basis changes arise from the representation of the mapping class group, as discussed in Section 7.2.6. All these basis changes constitute the second ingredient for the non-trivial constraints we obtain on the realizable logical operators.

A basis element $|\ell\rangle \in \mathcal{B}_\mathcal{C}$ associates the anyon label $\ell(C)$ with each curve $C \in \mathcal{C}$. The vector $|\ell\rangle$ spans the simultaneous $+1$-eigenspace of the projections $\{P_{\ell(C)}\}_{C \in \mathcal{C}}$. It is also a simultaneous eigenvector with respect to Dehn-twists along each curve $C \in \mathcal{C}$ with eigenvalue $e^{i\theta_{\ell(C)}}$. The action of Dehn-twists along curves C' not belonging to $\mathcal{C}$ can be obtained by applying the local moves to change into a basis $\mathcal{B}_{\mathcal{C}'}$ associated with a DAP-decomposition $\mathcal{C}'$ containing C'.

7.2.4 Open surfaces: labeled boundaries

So far, we have been discussing the Hilbert space $\mathcal{H}_\Sigma$ associated with closed surfaces; this does not cover the physically important case of pinned localized excitations (which correspond to

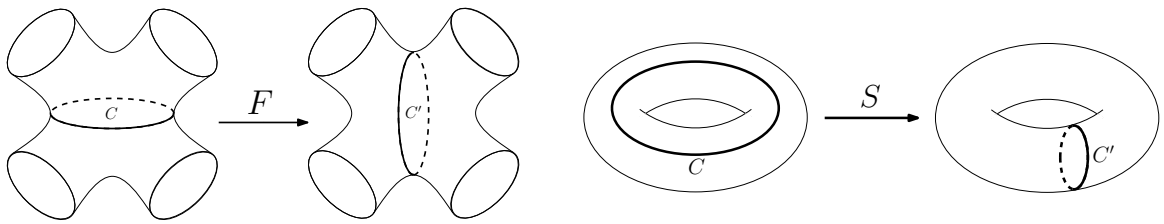


Figure 7.4: Two DAP-decompositions $\mathcal{C} = \{C\}$ and $\mathcal{C}' = \{C'\}$ of either the 4-punctured sphere (left), or the torus (right), are related by an F-move or an S-move, respectively.

punctures/holes in the surface). Here we describe the modifications necessary to deal with surfaces with boundaries. We assume that the boundary $\partial\Sigma = \bigcup_{\alpha=1}^{M} \hat{C}_\alpha$ is the disjoint union of M simple closed curves, and assume that an orientation $\hat{C}_\alpha : [0,1] \to \partial\Sigma$ has been chosen for each boundary component $\hat{C}_\alpha$ such that Σ is found to the left. In addition, we fix a label $a_\alpha \in \mathbb{A}$ for every boundary component $\hat{C}_\alpha$. We call this a labeling of the boundary. Let us write $\Sigma(a_1, \dots, a_M)$ for the resulting object (i.e., the surfaces, its oriented boundary components, and the associated labels). We call $\Sigma(a_1, \dots, a_M)$ a surface with labeled boundary components; slightly abusing notation, we sometimes write $\Sigma = \Sigma(a_1, \dots, a_M)$ when the presence of boundaries is understood/immaterial.

A TQFT associates to every surface $\Sigma(a_1, \dots, a_M)$ with labeled boundary components a Hilbert space $\mathcal{H}_{\Sigma(a_1,\dots,a_M)}$. The construction is analogous to the case of closed surfaces and based on DAP-decompositions. The only modification compared to the case of closed surfaces is that only DAP-decompositions including the curves $\{\hat{C}_\alpha\}_{\alpha=1}^{M}$ are allowed; furthermore, the labeling on these boundary components is fixed by $\{a_\alpha\}_{\alpha=1}^{M}$. That is, "valid" DAP-decompositions are of the form $\mathcal{C} = \{C_1, \dots, C_N, \hat{C}_1, \dots, \hat{C}_M\}$ with curves $\{C_j\}_{j=1}^{N}$ "complementing" the boundary components, and valid labelings are fusion-consistent, i.e., $\ell \in \mathsf{L}(C)$ with the additional condition that they agree with the boundary labels, $\ell(\hat{C}_\alpha) = a_\alpha$ for $\alpha = 1, \dots, M$. To simplify the discussion, we will often omit the boundary components $\{\hat{C}_\alpha\}_\alpha$ and focus on the remaining degrees of freedom associated with the curves $\{C_j\}_j$. It is understood that boundary labelings have to be fusion-consistent with the labeling $\{a_\alpha\}_\alpha$ of the boundary under consideration.

As a final remark, note that boundary components labeled with the trivial particle $1 \in \mathbb{A}$ correspond to contractible loops in a surface without this boundary (i.e., obtained by "gluing in a disc"). This means that they can be omitted: we have the isomorphism

$$\mathcal{H}_{\Sigma(1)} \cong \mathcal{H}_{\Sigma'} \ ,$$

where Σ' is the surface with one boundary component less that of Σ.

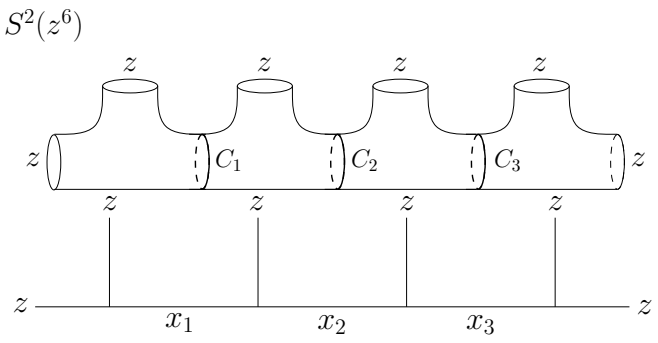


Figure 7.5: The 'standard' DAP-decomposition of the 6-punctured sphere, and the corresponding fusion-tree notation representing the labeling which assigns $\ell(C_i) = x_i$.

Example: the M-anyon Hilbert space

A typical example we are interested in is the labeled surface

$$S^2(z^M) = S^2(\underbrace{z, \ldots, z}_{M \text{ times}}) \ ,$$

where $S^2(\ ,\ ,\ \ldots\ ,\ ,\ )$ is the punctured sphere, and $z \in \mathbb{A}$ is some fixed anyon type (we assume that each boundary component has the same orientation). The Hilbert space $\mathcal{H}_{S^2(z^M)}$ is the space of M anyons of type z. When $M = N + 3$ for some $N \in \mathbb{N}$, we can choose a 'standard' DAP-decomposition $\mathcal{C} = \{C_j\}_{j=1}^N$ as shown in Fig. 7.5. A fusion-consistent labeling ℓ of the standard DAP-decomposition $\mathcal{C}$ corresponds to a sequence $(x_1, \ldots, x_N) = (\ell(C_1), \ldots, \ell(C_N))$ such that

$$N_{zz}^{x_1} = N_{x_N z}^{\overline{z}} = 1 \qquad \text{and} \qquad N_{x_j z}^{x_{j+1}} = 1 \qquad \text{for all } j = 1, \ldots, N-1, \tag{7.17}$$

as illustrated by Fig. 7.5.

7.2.5 The gluing axiom

Consider a closed curve C embedded in Σ. We will assume that C is an element of a DAP-decomposition $\mathcal{C}$; although this is not strictly necessary, it will simplify our discussion. Now consider the surface Σ' obtained by cutting Σ along C. Compared to Σ, this is a surface with two boundary components C_1', C_2' (both isotopic to C) added. We will assume that these have opposite orientation. A familiar example is the case where cutting Σ along C results in

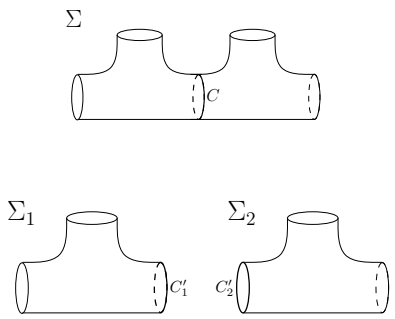


Figure 7.6: Cutting a surface Σ along some closed curve C of a DAP-decomposition yields a disconnected surface $\Sigma' = \Sigma_1 \cup \Sigma_2$ having additional boundary components C'_1 and C'_2.

two disconnected surfaces $\Sigma' = \Sigma_1 \cup \Sigma_2$, as depicted in Fig. 7.6 in the case where Σ is the 4-punctured sphere.

Let a be a particle label. We will denote by $\mathcal{H}_{\Sigma'(a,\overline{a})}$ the Hilbert space associated with the open surface Σ', where boundary C'_1 is labeled by a and boundary C'_2 by $\overline{a}$. The gluing axiom states that the Hilbert space of the surface Σ has the form

$$\mathcal{H}_\Sigma \cong \bigoplus_a \mathcal{H}_{\Sigma'(a,\overline{a})} \tag{7.18}$$

where the direct sum is over all particle labels a that occur in different fusion-consistent labelings of $\mathcal{C}$. In the special case where cutting along C gives two components Σ_1, Σ_2, we have $\mathcal{H}_\Sigma \cong \bigoplus_a \mathcal{H}_{\Sigma_1(a)} \otimes \mathcal{H}_{\Sigma_2(\overline{a})}$.

The isomorphism (7.18) can easily be made explicit. A first observation is that $\mathcal{H}_\Sigma$ decomposes as $\mathcal{H}_\Sigma = \bigoplus_a \mathcal{H}_{a,\Sigma}(C)$, where

$$\mathcal{H}_{a,\Sigma}(C) \coloneqq \mathsf{span}\{|\ell\rangle \mid \ell \in \mathsf{L}(\mathcal{C}), \ell(C) = a\} \tag{7.19}$$

is the space spanned by all labelings which assign the label a to C. It therefore suffices to argue that

$$\mathcal{H}_{a,\Sigma}(C) \cong \mathcal{H}_{\Sigma'(a,\overline{a})} \ . \tag{7.20}$$

To do so, observe that the DAP-decomposition $\mathcal{C}$ of Σ gives rise to a DAP-decomposition $\mathcal{C}' = \mathcal{C}\backslash\{C\}$ of Σ'. Any labeling $\ell \in \mathsf{L}(\mathcal{C})$ with $\ell(C) = a$ restricts to a labeling $\ell' \in \mathsf{L}(\mathcal{C}')$ of the labeled surface $\Sigma'(a, \overline{a})$. Conversely, any labeling $\ell' \in \mathsf{L}(\mathcal{C}')$ of the surface $\Sigma'(a, \overline{a})$ provides a labeling $\ell \in \mathsf{L}(\mathcal{C})$ (by setting $\ell(C) = a$). This defines the isomorphism (7.20) in terms of basis states $\{|\ell\rangle\}_{\ell \in \mathsf{L}(\mathcal{C})}$ and $\{|\ell'\rangle\}_{\ell' \in \mathsf{L}(\mathcal{C}')}$.

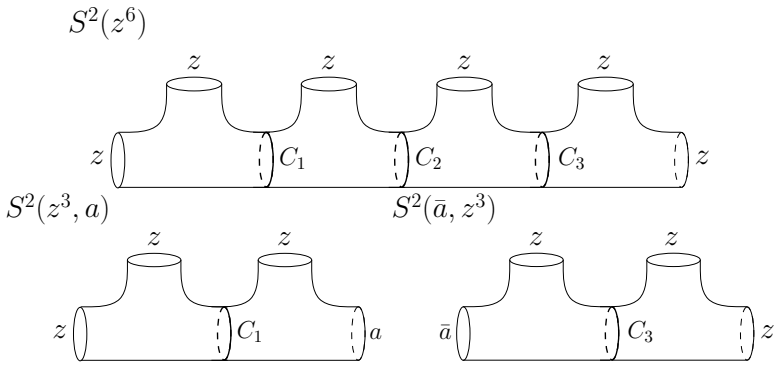


Figure 7.7: The 6-punctured sphere $S^2(z^6)$ shown with three curves $C_1, C_2, C_3 \in \mathcal{C}$ of a DAP-decomposition. Cutting along C_2 with labeling $\ell(C_2) = a$ results in the two surfaces $S^2(z^3, a)$ and $S^2(\overline{a}, z^3)$.

Example: decomposing the M-anyon Hilbert space

Consider the M-punctured sphere $\Sigma = S^2(z^M)$ with the standard DAP decomposition of Fig. 7.5 and boundary labels z (corresponding to M anyons of type z). Cutting $S^2(z^M)$ along C_j gives a surface Σ'_j which is the disjoint union of two punctured spheres, with $j+2$ and $M-j$ punctures, respectively. The resulting surface labelings are $S^2(z^{j+1}, a)$ and $S^2(\overline{a}, z^{M-1-j})$. That is, if $\Sigma = S^2(z^M)$ is the original surface and $\Sigma'_j(a, \overline{a})$ is the resulting one, then

$$\mathcal{H}_{\Sigma'_j(a,\overline{a})} = \mathcal{H}_{S^2(z^{j+1},a)} \otimes \mathcal{H}_{S^2(\overline{a},z^{M-1-j})} \ . \tag{7.21}$$

This is illustrated in Fig. 7.7 for the case $M = 6$ and $j = 2$.

7.2.6 The mapping class group

In the following, we denote by MCG_Σ the *mapping class group* of the surface Σ. Elements of this group are isotopy classes of orientation-preserving diffeomorphisms of Σ preserving labels and commuting with boundary parametrization (see e.g., [21]). Slightly abusing notation, we will often simply write $\vartheta \in \mathsf{MCG}_\Sigma$ for an equivalence class represented by a map $\vartheta : \Sigma \to \Sigma$.

For example, if Σ is the torus, then the mapping class group is generated by two elements, $\mathsf{MCG}_\Sigma = \langle s, t \rangle$ where s and t are the standard generators of the modular group. For the M-punctured sphere $S^2(z^M)$, we will also need the $M-1$ elements $\{\sigma_j\}_{j=1}^{M-1}$, where σ_j braids holes j and $j+1$.

Recall that the Hilbert space $\mathcal{H}_\Sigma$ is equipped with a projective unitary representation

$$\begin{array}{ccc} \mathsf{MCG}_\Sigma & \to & \mathsf{U}(\mathcal{H}_\Sigma) \\ \vartheta & \mapsto & \mathbf{V}(\vartheta) \end{array} \tag{7.22}$$

of the mapping class group MCG_Σ. For example, for the torus, $\mathbf{V}(s) = S$ and $\mathbf{V}(t) = T$ are the usual S- and T-matrices defined by the modular tensor category. For the M-punctured sphere $S^2(z^M)$ with $M = N+3$, we again use the standard DAP-decomposition with associated basis $\{|x\rangle\}_x$. Here the sequences $x = (x_1, \ldots, x_N)$ are subject to the fusion rules (see (7.17)) and the action on such vectors is

$$\begin{aligned} \mathbf{V}(\sigma_1)|x\rangle &= R^{zz}_{x_1}|x\rangle, \\ \mathbf{V}(\sigma_k)|x\rangle &= \sum_{x'} B(x_{k-1}, x_{k+1})_{x' x_k} |x_1, \ldots, x_{k-1}, x', x_{k+1}, \ldots, x_N\rangle \qquad \text{for } k = 2, \ldots, N+1, \\ \mathbf{V}(\sigma_{N+2})|x\rangle &= \overline{R^{zz}_{x_1}}|x\rangle, \end{aligned}$$

where $B(a,b) = F^{-1}RF$ is the braid matrix.

7.3 Constraints on locality-preserving automorphisms

In this section, we derive restrictions on topologically protected gates for general non-abelian models. Our strategy will be to consider what happens to string-operators. We will first consider operators associated with a single loop C, and derive restrictions on the map $F_a(C) \mapsto UF_a(C)U^\dagger$, or, more precisely, its effect on logical operators, $[F_a(C)] \mapsto [UF_a(C)U^\dagger]$. We will argue that this map implements an isomorphism of the Verlinde algebra and exploit this fact to derive a constraint which is 'local' to a specific loop. We will subsequently consider more 'global' constraints arising from fusion rules, as well as basis changes.

We would like to characterize locality-preserving unitary automorphisms $U \in \mathcal{A}_\Sigma$ in terms of their logical action $[U]$. A first goal is to characterize the map

$$\begin{array}{rccc} \rho_U : & [\mathcal{A}_\Sigma] & \to & [\mathcal{A}_\Sigma] \\ & [X] & \mapsto & [UXU^{-1}] \,, \end{array} \tag{7.23}$$

which determines the evolution of logical observables in the Heisenberg picture. (Clearly, this does not depend on the representative, i.e., if $[X] = [X']$, then $\rho_U([X]) = \rho_U([X'])$.) In fact, the map (7.23) fully determines U up to a global phase since $[\mathcal{A}_\Sigma]$ contains an operator basis for linear maps on $\mathcal{H}_\Sigma$. However, it will often be more informative to characterize the action of $[U]$ on basis elements of $\mathcal{H}_\Sigma$. This will require additional effort.

The main observation is that the map (7.23) defines an automorphism of $[\mathcal{A}_\Sigma]$, since

$$\rho_U([X])\rho_U([X']) = \rho_U([X][X']) \qquad \text{for all } X, X' \in \mathcal{A}_\Sigma \qquad \text{and} \qquad \rho_U^{-1} = \rho_{U^{-1}} \ . \tag{7.24}$$

Combined with the locality of U, (7.24) severly constrains ρ_U. Using this fact, we obtain a number of very general constraints, which will be worked out in more detail in the following.

7.3.1 A local constraint from a simple closed loop

Specifying the action of ρ_U on all of $[\mathcal{A}_\Sigma]$ completely determines $[U]$ up to a global phase. However, this is not entirely straightforward; instead, we fix some simple closed curve C and characterize the restriction to the subalgebra $\mathcal{A}(C) \subset \mathcal{A}_\Sigma$, i.e., the map

$$\begin{aligned} \rho_U(C): \ [\mathcal{A}(C)] &\to [\mathcal{A}(C)] \\ [X] &\mapsto [UXU^{-1}] \ , \end{aligned} \tag{7.25}$$

Observe that this map is well-defined since UXU^{-1} is supported in a neighborhood of C (by the locality-preservation of U), and hence $[UXU^{-1}] = [X']$ for some operator $X' \in \mathcal{A}(C)$ (here we have used Proposition 7.2.1). It is also easy to see that it defines an automorphism of the subalgebra $[\mathcal{A}(C)]$.

As we argued above, the algebra $\mathcal{A}(C)$ is isomorphic to Ver. This carries over to $[\mathcal{A}(C)] \cong \mathsf{Ver} \cong \mathbb{C}^{\oplus|\mathbb{A}|}$. As Ver has idempotents $\mathbf{p}_{a\in\mathbb{A}}$, the logical algebra for loop C has idempotents $\{[P_a(C)]\}_{a\in\mathbb{A}}$. We use the following fact:

Lemma 7.3.1. *The set of automorphisms of the algebra* Ver *is in one-to-one correspondence with the permutations* $S_{|\mathbb{A}|}$. *For* $\pi \in S_{|\mathbb{A}|}$, *the associated automorphism* $\rho_\pi : \mathsf{Ver} \to \mathsf{Ver}$ *is defined by its action on the central idempotents* $\mathbf{p}_a$

$$\rho_\pi(\mathbf{p}_a) = \mathbf{p}_{\pi(a)} \qquad \textit{for } a \in \mathbb{A} \tag{7.26}$$

Proof. It is clear that (7.26) defines an automorphism for every $\pi \in S_{|\mathbb{A}|}$. Also, from Eq. (7.24) we see that $\mathbf{p}_a\mathbf{p}_b = \delta_{ab}\mathbf{p}_b$ implies $\rho(\mathbf{p}_a)\rho(\mathbf{p}_b) = \delta_{ab}\rho(\mathbf{p}_b)$, such that $\rho(\mathbf{p}_a) \in \mathsf{Ver}$ are a complete set of projectors (Proposition 7.2.3). As there is a unique set of complete projectors for Ver, we conclude that $\rho(\mathbf{p}_a) = \mathbf{p}_{\pi(a)}$ for some permutation $\pi \in S_{|\mathbb{A}|}$. □

Applying this to $[\mathcal{A}(C)]$ shows that a locality-preserving unitary automorphism realizes, up to*important* phases, a a permutation of labelings. Let us emphasize that it is the projectors (idempotents) $[P_a(C)]$ which are being permuted, and not the string operators $[F_a(C)]$.

Proposition 7.3.1 (Local constraint)**.** *Let U be a locality-preserving automorphism of the code, and let $\rho_U([X]) = [UXU^{-1}]$.*

(i) For each simple closed loop C on Σ, there is a permutation $\pi^C \colon \mathbb{A} \to \mathbb{A}$ of the particle labels such that

$$\begin{array}{rccll} \rho_U : & [\mathcal{A}(C)] & \to & [\mathcal{A}(C)] & \\ & [P_a(C)] & \mapsto & [P_{\pi^C(a)}(C)] & \text{for all } a \in \mathbb{A} \ , \end{array} \tag{7.27}$$

(and linearly extended to all of $[\mathcal{A}(C)]$).

(ii) For some anyon model $\mathbb{A}$ with an associated S matrix, let $D_{a,b} = \delta_{a,b} \cdot d_a$ be the diagonal matrix with the quantum dimensions on the diagonal. Let $\pi^C \colon \mathbb{A} \to \mathbb{A}$ be a permutation associated with a loop C as in (i), and let Π be the matrix defined by $\Pi_{x,y} \coloneqq \delta_{x,\pi^C(y)}$. Define the matrix

$$\Lambda \coloneqq S\Pi^{-1}D\Pi D^{-1}\Pi^{-1}S^{-1} \ . \tag{7.28}$$

Then

$$\rho_U([F_b(C)]) = \sum_{b'} \Lambda_{b,b'}[F_{b'}(C)] \ . \tag{7.29}$$

Proof. We have already argued that (i) holds. For the proof of (ii), we use the relationship between $\{P_a(C)\}_a$ and $\{F_a(C)\}_a$ (cf. (7.14) and (7.15)) to get (suppressing the dependence on the loop C)

$$\rho_U([F_b]) = \sum_a \frac{S_{b,a}}{S_{1,a}}[P_{\pi^C(a)}] = \sum_{b'} \left(\sum_a \frac{S_{b,a}}{S_{1,a}} S_{1,\pi^C(a)} \overline{S_{b',\pi^C(a)}} \right) [F_{b'}] \ .$$

The claim (7.29) follows from this using $(\Pi^{-1}S^{-1})_{a,b'} = (S^{-1})_{\pi^C(a),b'} = \overline{S_{b',\pi^C(a)}}$ by the unitarity of S, as well as the fact that $S_{1,a} = d_a/\mathcal{D}$ and hence $\frac{S_{b,a}}{S_{1,a}} S_{1,\pi^C(a)} = (S\Pi^{-1}D\Pi D^{-1})_{b,a}$. □

7.3.2 Global constraints from DAP-decompositions, fusion rules and the gluing axiom

For higher-genus surfaces, we can obtain information by applying Proposition 7.3.1 to all loops of a DAP-decomposition; these must then satisfy the following consistency condition.

Proposition 7.3.2 (Global constraint from fusion rules)**.** *Let U be a locality-preserving automorphism of the code. Let $\mathcal{C}$ be a DAP-decomposition of Σ, and consider the family of*

permutations $\vec{\pi} = \{\pi^C\}_{C\in\mathcal{C}}$ *defined by Proposition 7.3.1. Then this defines a permutation* $\vec{\pi}\colon \mathsf{L}(\mathcal{C}) \to \mathsf{L}(\mathcal{C})$ *of the set of fusion-consistent labelings via*

$$\vec{\pi}(\ell)(C) \coloneqq \pi^C[\ell(C)] \tag{7.30}$$

for all $C \in \mathcal{C}$*. We have*

$$U|\ell\rangle = \mathrm{e}^{\mathrm{i}\varphi(\ell)}|\vec{\pi}(\ell)\rangle \qquad \text{for all } \ell \in L(\mathcal{C}) \tag{7.31}$$

with some phase $\mathrm{e}^{\mathrm{i}\varphi(\ell)}$ *depending on* ℓ*.*

Proof. Let us fix some basis element $|\ell\rangle \in \mathcal{B}_\mathcal{C}$. The vector $|\ell\rangle$ is a $+1$-eigenvector of $P_{\ell(C)}(C)$ for each $C \in \mathcal{C}$; hence according to (7.27), the vector $U|\ell\rangle$ is a $+1$-eigenvector of $P_{\pi^C[\ell(C)]}(C) = P_{\vec{\pi}(\ell)(C)}(C)$ for every $C \in \mathcal{C}$. This implies that it is proportional to $|\vec{\pi}(\ell)\rangle$, hence we obtain (7.31). Fusion-consistency of $\vec{\pi}(\ell)$ follows because $U|\ell\rangle$ must be an element of $\mathcal{H}_\Sigma$. □

Proposition (7.3.2) expresses the requirement that a locality-preserving automorphism U maps the set of fusion-consistent labelings into itself.

In fact, we can say more: it must be an isomorphism between the subspaces of $\mathcal{H}_\Sigma$ arising from the gluing axiom (i.e., Eq. (7.18)). This allows us to constrain the set of allowed permutations $\vec{\pi} = \{\pi^C\}_{C\in\mathcal{C}}$ arising from locality-preserving automorphisms even further:

Proposition 7.3.3 (Global constraint from gluing)**.** *Let* C *be an element of a DAP-decomposition of* Σ*. Recall that*

$$\mathcal{H}_\Sigma = \bigoplus_a \mathcal{H}_{a,\Sigma}(C)\ , \tag{7.32}$$

where the subspaces in the direct sum are defined by labelings associating a *to* C*. Let* U *be a locality-preserving automorphism of the code and let* $\pi^C\colon \mathbb{A} \to \mathbb{A}$ *be the permutation associated with* C *by Proposition 7.3.1. Then for every* $a \in \mathbb{A}$ *occuring in Eq. (7.32), the restriction of* U *to* $\mathcal{H}_{a,\Sigma}(C)$ *defines an isomorphism*

$$\mathcal{H}_{a,\Sigma}(C) \cong \mathcal{H}_{\pi^C(a),\Sigma}(C)\ . \tag{7.33}$$

In particular, if Σ' *is the surface obtained by cutting* Σ *along* C*, then*

$$\mathcal{H}_{\Sigma'(a,\overline{a})} \cong \mathcal{H}_{\Sigma'(\pi^C(a),\overline{\pi^C(a)})} \tag{7.34}$$

for every $a \in \mathbb{A}$ *occuring in the sum (7.32).*

The reason we refer to Proposition (7.3.3) as a global constraint (even though it superficially only concerns a single curve C) is that the surface Σ' and hence the spaces (7.34) depend on the global form of the surface Σ outside the support of C.

Proof. Proposition (7.3.2) implies that $U\mathcal{H}_{a,\Sigma}(C) \subset \mathcal{H}_{\pi^C(a),\Sigma}(C)$ for any a in expression (7.32). Since U acts unitarily on the whole space $\mathcal{H}_\Sigma$, this is compatible with (7.32) only if $U\mathcal{H}_{a,\Sigma}(C) = \mathcal{H}_{\pi^C(a),\Sigma}(C)$ for any such a. This proves (7.33). Statement (7.34) then immediately follows from (7.20). □

A simple but useful implication of Proposition 7.3.3 is that

$$\dim\left(\mathcal{H}_{\Sigma'(a,\bar{a})}\right) = \dim\left(\mathcal{H}_{\Sigma'(\pi^C(a),\overline{\pi^C(a)})}\right) \tag{7.35}$$

is a necessary condition that π^C has to satisfy.

7.3.3 Global constraints from basis changes

Eq. (7.27) essentially tells us that a locality-preserving protected gate U can only permute particle labels; it indicates that such a gate U is related to certain symmetries of the anyon model. But (7.27) does not tell us what phases basis states may acquire. We show how to obtain constraints on these phases by considering basis changes. This also further constrains the allowed permutations on the labels of the idempotents.

Consider two DAP-decompositions $\mathcal{C}$ and $\mathcal{C}'$. Expressed in the first basis $\mathcal{B}_\mathcal{C}$, we have

$$U|\ell\rangle = \mathrm{e}^{\mathrm{i}\varphi(\ell)}|\vec{\pi}(\ell)\rangle \tag{7.36}$$

for some unknown phase $\varphi(\ell)$ depending only on the labeling $\ell \in \mathsf{L}(\mathcal{C})$. This means that with respect to the basis elements of $\mathcal{B}_\mathcal{C}$, the operator U is described by a matrix $\mathbf{U} = \mathbf{\Pi D}(\{\varphi(\ell)\}_\ell)$, where $\mathbf{\Pi}$ is a permutation matrix (acting on the fusion-consistent labelings $\mathsf{L}(\mathcal{C})$), and $\mathbf{D}$ is a diagonal matrix with entries $\{\mathrm{e}^{\mathrm{i}\varphi(\ell)}\}_\ell$ on the diagonal.

Analogously, we can consider the operator U expressed as a matrix $\mathbf{U}'$ in terms of the basis elements of $\mathcal{B}_{\mathcal{C}'}$. We conclude that $\mathbf{U}' = \mathbf{\Pi}'\mathbf{D}(\{\varphi'(\ell)\}_\ell)$, for $\ell \in \mathsf{L}(\mathcal{C}')$, with a (potentially different) permutation matrix $\mathbf{\Pi}'$, and (potentially different) phases $\{\varphi'(\ell)\}_\ell$.

Let $\mathbf{V}$ be the unitary change-of-basis matrix for going from $\mathcal{B}_\mathcal{C}$ to $\mathcal{B}_{\mathcal{C}'}$. Then we must have

$$\mathbf{VU} = \mathbf{U}'\mathbf{V}. \tag{7.37}$$

We show below that this equation strongly constrains the phases as well as the permutations in (7.31). More specifically, we will examine constraints arising when using basis changes $\mathbf{V}$ defined by F-moves in Section 7.5. In Section 7.4, we consider basis changes $\mathbf{V}$ defined by elements of the mapping class group.

7.4 Global constraints from the mapping class group

The following is based on the simple observation that we must have consistency conditions of the form (7.37) for more general basis changes (in particular, basis changes not made up of F-moves only). We are particularly interested in the case where the basis change is the result of applying a mapping class group element.

7.4.1 Basis changes defined by the mapping class group

A key property of the representation (7.22) of the mapping class group MCG_Σ is that it maps idempotents according to

$$V(\vartheta)P_a(C)V(\vartheta)^\dagger = P_a\big(\vartheta(C)\big)\ . \tag{7.38}$$

Let us fix a 'standard' DAP-decomposition $\mathcal{C}$, and let $\mathcal{B}_\mathcal{C} = \{|\ell\rangle_\mathcal{C}\}_\ell$ be the corresponding standard basis.

Let ϑ be an arbitrary element of MCG_Σ. Consider the basis

$$\mathcal{B}_{\vartheta(\mathcal{C})} \coloneqq \{V(\vartheta)|\ell\rangle\}_\ell.$$

Because of (7.38), this basis is a simultaneous eigenbasis of the complete set of commuting observables associated with the DAP decomposition $\vartheta(\mathcal{C}) \coloneqq \{\vartheta(C_j)\}_{j=1}^M$. The change of basis from $\mathcal{B}_\mathcal{C}$ to $\mathcal{B}_{\vartheta(\mathcal{C})}$ is given by the image $V(\vartheta)$ of the mapping class group element ϑ.

In particular, if $\mathbf{V}(\vartheta)$ is the matrix representing $V(\vartheta)$ in the standard basis, then (7.37) implies

$$\mathbf{V}(\vartheta)\mathbf{\Pi}\mathbf{D} = \mathbf{\Pi}(\vartheta)\mathbf{D}(\vartheta)\mathbf{V}(\vartheta) \tag{7.39}$$

for some permutation matrix $\mathbf{\Pi}(\vartheta)$ and a diagonal matrix $\mathbf{D}(\vartheta)$ consisting of phases.

Some terminology will be useful: Let Δ be the set of matrices of the form $\mathbf{\Pi}\mathbf{D}$, where $\mathbf{\Pi}$ is a permutation of fusion-consistent labelings, and $\mathbf{D}$ is a diagonal matrix with phases (these

are sometimes called *unitary monomial matrices*). For $\mathbf{U} \in \Delta$ and $\vartheta \in \mathsf{MCG}_\Sigma$, we say that $\mathbf{U}$ intertwines with ϑ if

$$\mathbf{V}(\vartheta)\mathbf{U}\mathbf{V}(\vartheta)^\dagger \in \Delta \ .$$

Let $\Delta_\vartheta \subset \Delta$ be the set of matrices that intertwine with ϑ, and let

$$\Delta_{\mathsf{MCG}_\Sigma} = \bigcap_{\vartheta \in \mathsf{MCG}_\Sigma} \Delta_\vartheta$$

be the matrices that are intertwiners of the whole mapping class group representation. We have shown the following:

Theorem 7.4.1. *Let* $\mathbf{U}$ *be the matrix representing a protected gate* U *in the standard basis. Then* $\mathbf{U} \in \Delta_{\mathsf{MCG}_\Sigma}$.

As an example, consider the torus: since $T = \mathbf{V}(t)$ is diagonal, it is easy to see that for any $\mathbf{\Pi D} \in \Delta$, we have $T\mathbf{\Pi D}T^{-1} = \mathbf{\Pi D'}$ for some $\mathbf{D'}$. This implies that $\Delta_t = \Delta$ is generally not interesting, i.e., $\mathbf{U} \in \Delta_t$ does not impose an additional constraint. In contrast, mapping class group elements such as s and st generally give different non-trivial constraints.

7.4.2 Density of the mapping class group representation and absence of protected gates

The following statement directly links computational universality of the mapping class group representation to the non-existence of protected gates.

Corollary 7.4.2. *Suppose the representation of* MCG_Σ *is dense in the projective unitary group* $\mathsf{PU}(\mathcal{H}_\Sigma)$. *Then there is no non-trivial protected gate.*

Proof. Let U be an arbitrary protected gate and let $\mathbf{U} \in \Delta$ be the matrix representing it in the standard basis. Assume for the sake of contradiction that U is non-trivial. Then $\mathbf{U}$ is a unitary with at least two different eigenvalues λ_1, $\lambda_2 \in \mathrm{U}(1)$. In particular, there is a diagonalizing unitary $\mathbf{V}_1$ such that $\mathbf{V}_1\mathbf{U}\mathbf{V}_1^\dagger = \mathsf{diag}(\lambda_1, \lambda_2) \oplus \tilde{\mathbf{U}}$ for some matrix $\tilde{\mathbf{U}}$. Setting $\mathbf{V}_2 = H \oplus I$, where H is the Hadamard matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

and $\mathbf{V} = \mathbf{V}_2\mathbf{V}_1$, we obtain that

$$\mathbf{V}\mathbf{U}\mathbf{V}^\dagger \notin \Delta \tag{7.40}$$

because this matrix contains both diagonal and off-diagonal elements. Note that if $\lambda_2 = -\lambda_1$ one may use the matrix

$$\frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix}$$

instead of H.

Observe also that (7.40) stays valid if we replace $\mathbf{V}$ by a sufficiently close approximation (up to an irrelevant global phase) $\tilde{\mathbf{V}} \approx \mathbf{V}$. In particular, by the assumed density, we may approximate $\mathbf{V}$ by a product $\tilde{\mathbf{V}} = \mathbf{V}(\vartheta_1)\cdots\mathbf{V}(\vartheta_m)$ of images of $\vartheta_1, \ldots, \vartheta_m \in \mathsf{MCG}_\Sigma$. But then we have

$$\mathbf{U} \notin \Delta_{\vartheta_1\cdots\vartheta_m} \ ,$$

which contradicts Theorem 7.4.1. □

Note that in general, the mapping class group is only dense on a subspace $\mathcal{H}_0 \subset \mathcal{H}_\Sigma$. This is the case for example when the overall system allows for configurations where anyons can be present or absent (e.g., a boundary may or may not carry a topological charge). In such a situation, $\mathcal{H}_\Sigma$ decomposes into superselection sectors which are defined by the gluing axiom (i.e., having fixed labels associated with certain closed loops associated). Corollary 7.4.2 can be adapted to this situation, e.g., as explained in Appendix 7.8 (Lemma 7.8.1).

7.4.3 Characterizing diagonal protected gates

Fix a DAP-decomposition $\mathcal{C}$ and let $\vartheta \in \mathsf{MCG}_\Sigma$. Let us call two (fusion-consistent) labelings ℓ_1, ℓ_2 *connected by* ϑ (denoted $\ell_1 \Leftrightarrow_\vartheta \ell_2$) if there is a labeling ℓ such that

$$0 \neq \langle \ell | V(\vartheta) | \ell_m \rangle \qquad \text{for } m = 1, 2 \ .$$

(Here $|\ell\rangle$ is the associated basis element of $\mathcal{B}_\mathcal{C}$.) More generally, let us say ℓ_1, ℓ_2 are connected (written $\ell_1 \Leftrightarrow \ell_2$) if there exists an element $\vartheta \in \mathsf{MCG}_\Sigma$ such that $\ell_1 \Leftrightarrow_\vartheta \ell_2$. Clearly, this notion is symmetric in ℓ_1, ℓ_2, and furthermore, it is reflexive, i.e., $\ell_1 \Leftrightarrow \ell_1$ since $\ell_1 \Leftrightarrow_{\mathsf{id}} \ell_1$. We can therefore define an equivalence relation on the set of labelings: we write $\ell_1 \sim \ell_2$ if there are labelings $k_1, \ldots, k_m$ such that $\ell_1 \Leftrightarrow k_1 \Leftrightarrow \cdots \Leftrightarrow k_m \Leftrightarrow \ell_2$. We point out (for later use) that we can always find a finite collection $\{\vartheta_k\}_{k=1}^M \subset \mathsf{MCG}_\Sigma$ that generates the relation $\sim$ in the

sense that $\ell_1 \sim \ell_2$ if and only if $\ell_1 \Leftrightarrow_{\vartheta_k} \ell_2$ for some k (after all, we only have a finite set of labelings ℓ).

Observe that if the representation of MCG_Σ has a non-trivial invariant subspace, then there is more than one equivalence class. We discuss an example of this below (see Section 7.4.5). However, in important special cases such as the Fibonacci or Ising models, there is only one equivalence class for the relation $\sim$, i.e., any pair of labelings are connected (see Lemma 7.6.3 and Lemma 7.6.4 below).

Lemma 7.4.3. *Consider a protected gate U acting diagonally in the basis $\mathcal{B}_\mathcal{C}$ as $U|\ell\rangle = \mathrm{e}^{\mathrm{i}\varphi(\ell)}|\ell\rangle$.*

(i) Suppose that U also acts diagonally in the basis $\mathcal{B}_{\vartheta(\mathcal{C})}$. Then $\varphi(\ell_1) = \varphi(\ell_2)$ for any pair $\ell_1 \Leftrightarrow_\vartheta \ell_2$ connected by ϑ.

(ii) Suppose that $\{\vartheta_k\}_{k=1}^M \subset \mathsf{MCG}_\Sigma$ generates the relation $\sim$, and U acts diagonally in each basis $\mathcal{B}_{\vartheta_k(\mathcal{C})}$. Then φ assigns the same value to every element of the same equivalence class under $\sim$.

We will refer to a protected gate U with property (ii) as a $\sim$-trivial gate. One implication of Lemma 7.4.3 is that any protected gate which is close to the identity acts as a $\sim$-trivial gate (see the proof of Theorem 7.4.5). In Section 7.4.4, we will show how to use this statement to prove that the set of protected gates is finite up to irrelevant phases.

Proof. Consider two labelings ℓ_1, ℓ_2 satisfying $\ell_1 \Leftrightarrow_\vartheta \ell_2$. Then, writing $\mathbf{V} = \mathbf{V}(\vartheta)$, we know that

$$\mathbf{V}_{\ell,\ell_1} \neq 0 \qquad \text{and} \qquad \mathbf{V}_{\ell,\ell_2} \neq 0 \tag{7.41}$$

for some labeling ℓ, where $\mathbf{V}_{\ell,k} = \langle \ell | V(\vartheta) | k \rangle$. Since U acts diagonally in both bases $\mathcal{B}_\mathcal{C}$ and $\mathcal{B}_{\vartheta(\mathcal{C})}$ by assumption, (7.39) becomes simply

$$\mathbf{V}\mathbf{D}\mathbf{V}^\dagger = \mathbf{D}(\vartheta) \tag{7.42}$$

when written in the standard basis. Here the diagonal matrices are given by $\mathbf{D} = \mathrm{diag}(\{\varphi(\ell)\}_\ell)$ and $\mathbf{D}(\vartheta) = \mathrm{diag}(\{\varphi'(\ell)\}_\ell)$. Taking the diagonal entry at position (ℓ, ℓ) in the matrix equation (7.42), we get the identity

$$\sum_k \mathrm{e}^{\mathrm{i}(\varphi(k) - \varphi'(\ell))} |\mathbf{V}_{\ell,k}|^2 = 1. \tag{7.43}$$

By unitarity of the mapping class group representation, we also have

$$\sum_k |\mathbf{V}_{\ell,k}|^2 = 1. \tag{7.44}$$

By taking the real part of (7.43), it is straightforward to see that compatibility with (7.44) imposes that $\cos\big(\varphi(k) - \varphi'(\ell)\big) = 1$ whenever $|\mathbf{V}_{\ell,k}| \neq 0$ or

$$\varphi(k) \equiv \varphi'(\ell) \mod 2\pi \qquad \text{for all } k \text{ with } |\mathbf{V}_{\ell,k}| \neq 0.$$

With (7.41), we conclude that $\varphi(\ell_1) = \varphi'(\ell) = \varphi(\ell_2)$, which proves claim (i).

The claim (ii) immediately follows from (i). □

We will show how to apply this result to the Fibonacci model in Section 7.6.1. Note that Lemma 7.4.3 does not generally rule out the existence of non-trivial diagonal protected gates in the standard basis (an example is a Pauli-Z in the Ising model, see Section 7.6.2): it is important that the protected gate is diagonal in *several* different bases $\{\mathcal{B}_{\vartheta_k(\mathcal{C})}\}_k$.

A simple consequence of Lemma 7.4.3 is that any protected gate has a finite order up to certain phases:

Lemma 7.4.4. *There is a finite n_0 (depending only on the dimension of $\mathcal{H}_\Sigma$) such that for every protected gate U, there is an $n \leq n_0$ such that U^n is a $\sim$-trivial phase gate.*

Proof. Consider an arbitrary DAP-decomposition $\mathcal{C}$ and suppose U acts as (7.31) in the basis $\mathcal{B}_\mathcal{C}$. Since the permutation $\vec{\pi}$ acts on the finite set $\mathsf{L}(\mathcal{C})$ of fusion-consistent labelings, it has finite order $n_\mathcal{C}$. This means that $U^{n_\mathcal{C}}$ acts diagonally in the basis $\mathcal{B}_\mathcal{C}$.

Assume $\{\vartheta_k\}_{k=1}^M \subset \mathsf{MCG}_\Sigma$ generate the relation $\sim$. Setting $n = \mathsf{lcm}(n_{\vartheta_1(\mathcal{C})}, \ldots, n_{\vartheta_M(\mathcal{C})})$, we can apply Lemma 7.4.3 to U^n to reach the conclusion that U^n is $\sim$-trivial. Furthermore, since the number n depends only on the permutation $\vec{\pi}$, and there are only finitely many such permutations, there is a finite n_0 with the claimed property. □

7.4.4 Finiteness of the set of protected gates

In the following, we will ignore phase differences that are "global" to subspaces of vectors defined by the equivalence classes of $\sim$. That is, we will call two protected gates U_1 and U_2 equivalent (written $U_1 \sim U_2$) if

$$\begin{aligned} \mathbf{U}_1 &= \mathbf{\Pi}\mathbf{D}_1 \\ \mathbf{U}_2 &= \mathbf{\Pi}\mathbf{D}_2 \end{aligned} \qquad \text{and} \qquad (\mathbf{D}_2)_{\ell,\ell} = \mathrm{e}^{\mathrm{i}\varphi([\ell])}(\mathbf{D}_1)_{\ell,\ell} \ ,$$

i.e., they encode the same permutation of fusion-consistent labels, and their phases only differ by a phase $\varphi([\ell])$ depending on the equivalence class $[\ell]$ that ℓ belongs to. This is equivalent to

the statement that $\mathbf{U}_1^{-1}\mathbf{U}_2 = \mathbf{D}_1^{-1}\mathbf{D}_2$ acts as a phase dependent only on the equivalence class, i.e., $U_1^{-1}U_2$ is a $\sim$-trivial phase gate.

We obtain an Eastin and Knill [15] type statement, which is one of our main conclusions.

Theorem 7.4.5 (Finite group of protected gates)**.** *The number of equivalence classes of protected gates is finite.*

In particular, this means that locality-preserving automorphisms on their own do not provide quantum computational universality.

Proof. Assume that there are infinitely many equivalence classes of protected gates. Then we can choose a sequence $\{U_n\}_{n\in\mathbb{N}}$ of protected gates indexed by integers and belonging to different equivalence classes each. Since the number of permutations of fusion-consistent labels is finite, there exists at least one permutation matrix $\mathbf{\Pi}$ such that there is an infinite subsequence of protected gates U_n with $\mathbf{U}_n = \mathbf{\Pi}\mathbf{D}_n$, i.e., they act with the same permutation. Applying the Bolzano-Weierstrass theorem to this subsequence, we conclude that there is a convergent subsequence of protected gates $\{U_{n_j}\}_{j\in\mathbb{N}}$ such that $\mathbf{U}_{n_j} = \mathbf{\Pi}\mathbf{D}_{n_j}$ for all j. Let $U = \lim_{j\to\infty} U_{n_j}$ be the corresponding limit, and let us define $\tilde{U}_j \coloneqq U^{-1}U_{n_j}$. Clearly, each $\tilde{U}_j$ is a protected gate and

$$\tilde{\mathbf{U}}_j = \mathbf{D}^{-1}\mathbf{D}_{n_j} \tag{7.45}$$

acts non-trivially on subspaces defined by equivalence classes, i.e., $\tilde{U}_j$ is a $\sim$-non-trivial phase gate. This is because of the assumption that the original sequence $\{U_n\}_{n\in\mathbb{N}}$ has elements belonging to different equivalence classes. Furthermore, we have that

$$\lim_{j\to\infty} \tilde{\mathbf{U}}_j = \mathbf{I}\ , \tag{7.46}$$

where $\mathbf{I}$ is the identity matrix.

For a mapping class group element $\vartheta \in \mathsf{MCG}_\Sigma$, the matrix expressing the action of $\tilde{U}_j$ in the basis $\mathcal{B}_{\vartheta(\mathcal{C})}$ is given by $\mathbf{V}(\vartheta)\tilde{\mathbf{U}}_j\mathbf{V}(\vartheta)^\dagger$. Because $\tilde{U}_j$ is a protected gate, we get

$$\mathbf{V}(\vartheta)\tilde{\mathbf{U}}_j\mathbf{V}(\vartheta)^\dagger = \tilde{\mathbf{\Pi}}_j\tilde{\mathbf{D}}_j \tag{7.47}$$

for some permutation matrix $\tilde{\mathbf{\Pi}}_j$ and a diagonal matrix $\tilde{\mathbf{D}}_j$ of phases. Combining (7.46), (7.47), using the unitarity of $\mathbf{V}(\vartheta)$ and continuity, we conclude that there exists some $N_0 = N_0(\vartheta)$ such that $\tilde{\mathbf{\Pi}}_j = \mathbf{I}$ for all $j \geq N_0$, i.e., $\mathbf{V}(\vartheta)\tilde{\mathbf{U}}_j\mathbf{V}(\vartheta)^\dagger$ is diagonal for sufficiently large j. Equivalently, for all $j \geq N_0$, $\tilde{U}_j$ acts diagonally in the basis $\mathcal{B}_{\vartheta(\mathcal{C})}$, as well as in the basis $\mathcal{B}_\mathcal{C}$ (by (7.45)).

The latter conclusion can be extended uniformly to a finite collection $\{\vartheta_k\}_{k=1}^M \subset \mathsf{MCG}_\Sigma$ of mapping class group elements: there is a constant $N = N(\vartheta_1, \ldots, \vartheta_M)$ such that for all $j \geq N$, the protected gate $\tilde{U}_j$ acts as a diagonal matrix in all bases $\mathcal{B}_\mathcal{C}$, $\mathcal{B}_{\vartheta_1(\mathcal{C})}$, ..., $\mathcal{B}_{\vartheta_M(\mathcal{C})}$. Taking a finite collection $\{\vartheta_k\}_{k=1}^M \subset \mathsf{MCG}_\Sigma$ that generates the relation $\sim$ and applying Lemma 7.4.3, we reach the conclusion that $\tilde{U}_j$ is a $\sim$-trivial phase gate for all $j \geq N$. This contradicts the fact that each $\tilde{U}_j$ is a $\sim$-non-trivial phase gate, as argued above. □

7.4.5 Necessity of restricting to equivalence classes

Here we briefly argue that without imposing $\sim$-equivalence on protected gates, one can end up with infinitely many protected gates (that are, however, not very interesting).

Concretely, consider a model such as the toric code, with local commuting projector Hamiltonian $H_{top} = -\sum_j \Pi_j$ acting on spins which we collectively denote by A. Let $\mathcal{H}_\Sigma$ be its ground space. We introduce a local spin-degree of freedom B_j associated with each term in the Hamiltonian, and let $B = \bigotimes_j B_j$ the space of these auxiliary degrees of freedom. Define an Ising-like Hamiltonian $H_I = -\sum_{\langle j,j' \rangle} Z_j Z_{j'}$ coupling all nearest neighbors in B (according to some notion). Finally, consider the following Hamiltonian:

$$H = J \cdot H_I - \sum_j \Pi_j \otimes |0\rangle\langle 0|_{B_j} - \sum_j \Pi_j \otimes |1\rangle\langle 1|_{B_j} \ .$$

This Hamiltonian is local, and for large J, has a ground space of the form $(\mathcal{H}_\Sigma \otimes |00\cdots 0\rangle) \oplus (\mathcal{H}_\Sigma \otimes |11\cdots 1\rangle)$. In other words, the ground space (and similarly the low-energy subspace) splits as $\mathcal{H}_\Sigma^{(0)} \oplus \mathcal{H}_\Sigma^{(1)}$ into two isomorphic copies of the space $\mathcal{H}_\Sigma$.

Now take two arbitrary protected gates $U^{(0)}, U^{(1)}$ for H_{top} (these may be global phases, i.e., trivial), implementing logical operations $\overline{U}^{(0)}$, $\overline{U}^{(1)}$. Let us assume that they are implemented by circuits acting locally, i.e., they can be written (arbitrarily – the details do not matter) in the form

$$U^{(m)} = U_{j_1}^{(m)} U_{j_2}^{(m)} \cdots U_{j_{M_m}}^{(m)}$$

with each unitary U_j local near the support of Π_j. Then we can define the unitary

$$U = \prod_{k=1}^{M_0} \left(U_{j_k}^{(0)} \otimes |0\rangle\langle 0|_{B_{j_k}} + \mathsf{id} \otimes |1\rangle\langle 1|_{B_{j_k}} \right) \prod_{k=1}^{M_1} \left(\mathsf{id} \otimes |0\rangle\langle 0|_{B_{j_k}} + U_{j_k}^{(1)} \otimes |1\rangle\langle 1|_{B_{j_k}} \right)$$

on $A \otimes B$. It is easy to check that U is a protected gate and its logical action is

$$\overline{U} = \overline{U}^{(0)} \oplus \overline{U}^{(1)} \ .$$

In particular, such a unitary can introduce an arbitrary relative phase between the "super-selection" sectors $\mathcal{H}_\Sigma^{(0)}$, $\mathcal{H}_\Sigma^{(1)}$: we can choose $U^{(0)} = I$ and $U^{(1)} = e^{i\varphi} I$. The construction here corresponds to the direct sum of two TQFTs; the mapping class group representation is reducible and basis elements belonging to different sectors are inequivalent. Imposing the relation $\sim$ on the set of protected gates renders all such relative-phase gates equivalent.

7.5 Global constraints from F-moves on the n-punctured sphere

We first consider the four-punctured sphere, where there are two inequivalent DAP-decompositions related by an F-move (i.e., the basis change $\mathbf{V}$ is the F-matrix). More generally (e.g., for the 5-punctured sphere), we need to consider several different F-moves and obtain a constraint of the form (7.37) for every pair of bases related by such moves. We describe such global constraints in Section 7.5.3. The results obtained by considering F-moves are summarized in Section 7.5.4: there we outline a general procedure for characterizing protected gates.

7.5.1 Determining phases for the four-punctured sphere: fixed boundary labels

For a four-punctured sphere Σ, we can fix the labels on the punctures to $i, j, k, l \in \mathbb{A}$. The corresponding space $\mathcal{H}_{\Sigma(i,j,k,l)}$ associated to this open surface with labeled boundary components is the fusion space V_{kl}^{ij}. (In the non-abelian case, this space can have dimension larger than 1.) We have two bases $\mathcal{B}_\mathcal{C}$, $\mathcal{B}_{\mathcal{C}'}$ of this fusion space, corresponding to two different DAP-decompositions differing by one loop (Fig. 7.4). We can enumerate basis elements by the label assigned to this loop. Let $\{|a\rangle_\mathcal{C}\}_a$ and $\{|a\rangle_{\mathcal{C}'}\}_a$ be the elements of the bases $\mathcal{B}_\mathcal{C}$ and $\mathcal{B}_{\mathcal{C}'}$, respectively. Note that a ranges over all elements consistent with the fusion rules.

For the models considered in this article, these are $N_{ij}^a = N_{kl}^a = 1$. Let $Q = Q(i, j, k, l)$ be the set of such elements. The basis change is given by the F-matrix

$$|m\rangle_{\mathcal{C}'} = \sum_n F_{kln}^{ijm} |n\rangle_\mathcal{C}.$$

Considering a locality-preserving automorphism which preserves the boundary labels (this is reasonable if we think of them as certain boundary conditions of the system), we can apply the procedure explained above to find the action

$$U|a\rangle_{\mathcal{C}} = \mathrm{e}^{\mathrm{i}\varphi(a)}|\pi^C(a)\rangle_{\mathcal{C}}$$

on basis states. Here $\pi^C\colon Q \to Q$ permutes fusion-consistent labels. To apply the reasoning above, we have to use the $|Q \times Q|$-basis change matrix $\mathbf{V}$ defined by $\mathbf{V}_{m,n} = F^{ijm}_{kln}$.

Solving the consistency relation (7.37) (for the permutations π^C, $\pi^{C'}$ and phases $\{\varphi(a)\}_a, \{\varphi'(a)\}_a$) shows that for any permutation π^C that is part of a solution, the function φ takes the form

$$\varphi(a) = \eta + f(a)\ , \tag{7.48}$$

where η is a global phase and f belongs to a certain set of functions which we denote

$$\mathsf{Iso}\left(\begin{array}{ccccc} & i & & l & \\ j & | & \cdot & | & k \\ \multicolumn{5}{c}{\underline{\qquad\qquad\qquad\qquad}} \end{array} \to \begin{array}{ccccc} & i & & l & \\ j & | & \pi^C(\cdot) & | & k \\ \multicolumn{5}{c}{\underline{\qquad\qquad\qquad\qquad}} \end{array}\right)\ . \tag{7.49}$$

(The reason for this notation will become clearer when we discuss isomorphisms in the next section; here we are concerned with relative phases arising from automorphisms.) In summary, we have

$$U|a\rangle_{\mathcal{C}} = e^{i\eta}e^{if(a)}|\pi^C(a)\rangle_{\mathcal{C}} \qquad \text{where } f \in \mathsf{Iso}\left(\begin{array}{ccccc} & i & & l & \\ j & | & \cdot & | & k \\ \multicolumn{5}{c}{\underline{\qquad\qquad\qquad\qquad}} \end{array} \to \begin{array}{ccccc} & i & & l & \\ j & | & \pi^C(\cdot) & | & k \\ \multicolumn{5}{c}{\underline{\qquad\qquad\qquad\qquad}} \end{array}\right)\ . \tag{7.50}$$

Here the set (7.49) can be computed by solving the consistency relation

$$\mathbf{V\Pi D}(\{\varphi(a)\}_a) = \mathbf{\Pi' D}(\{\varphi'(a)\}_a)\mathbf{V} \tag{7.51}$$

with $\mathbf{V}_{m,n} = F^{ijm}_{kln}$. This scenario is a special case of the commutative diagram displayed in Fig. 7.8.

7.5.2 Determining phases for the four-punctured sphere in general

Consider the four-punctured sphere Σ with fixed labels $i, j, k, l \in \mathbb{A}$ on the punctures. Let $\tilde{\imath}, \tilde{\jmath}, \tilde{k}, \tilde{l}$ be another set of labels such that the spaces $\mathcal{H}_{\Sigma(i,j,k,l)}$ and $\mathcal{H}_{\Sigma(\tilde{\imath},\tilde{\jmath},\tilde{k},\tilde{l})}$ are isomorphic. In this situation, we can try to characterize locality-preserving isomorphisms between two systems defined on $\Sigma(i, j, k, l)$ and $\Sigma(\tilde{\imath}, \tilde{\jmath}, \tilde{k}, \tilde{l})$, respectively. This situation is slightly more general than what we considered before (automorphisms of the same system), but it is easy to see that all

arguments applied so far extend to this situation. Note that we could have phrased our whole discussion in terms of isomorphisms between different spaces. However, we chose not to do so to minimize the amount of notation required; instead, we only consider this situation in this section. This generalization for the 4-punctured sphere is all we need to treat automorphisms on higher-genus surfaces.

For $\mathcal{H}_{\Sigma(i,j,k,l)}$, we have two bases $\mathcal{B}_\mathcal{C}$, $\mathcal{B}_{\mathcal{C}'}$, corresponding to two different DAP-decompositions differing by one loop. Similarly, for $\mathcal{H}_{\Sigma(\tilde{\imath},\tilde{\jmath},\tilde{k},\tilde{l})}$, we have two bases $\tilde{\mathcal{B}}_\mathcal{C}$, $\tilde{\mathcal{B}}_{\mathcal{C}'}$, corresponding to two different DAP-decompositions differing by one loop. We can enumerate the basis elements by the label assigned to this loop. Let $\{|a\rangle_\mathcal{C}\}_a$ and $\{|a\rangle_{\mathcal{C}'}\}_a$ be the elements of the basis $\mathcal{B}_\mathcal{C}$ and $\mathcal{B}_{\mathcal{C}'}$, respectively. Here a ranges over the set $Q = Q(i,j,k,l) \subset \mathbb{A}$ of all elements consistent with the fusion rules, i.e., we must have $N_{ij}^a = N_{kl}^a = 1$. Similarly, let $\{|\tilde{a}\rangle_\mathcal{C}\}_{\tilde{a}}$ and $\{|\tilde{a}\rangle_{\mathcal{C}'}\}_{\tilde{a}}$ be the elements of the basis $\tilde{\mathcal{B}}_\mathcal{C}$ and $\tilde{\mathcal{B}}_{\mathcal{C}'}$, respectively, where now $\tilde{a} \in \tilde{Q} = Q(\tilde{\imath},\tilde{\jmath},\tilde{k},\tilde{l})$.

In this situation, we have two basis changes,

$$|m\rangle_{\mathcal{C}'} = \sum_n \mathbf{V}_{m,n}|n\rangle_\mathcal{C} \text{ where } \mathbf{V}_{m,n} = F_{kln}^{ijm} \qquad \text{and} \qquad |\tilde{m}\rangle_{\mathcal{C}'} = \sum_{\tilde{n}} \tilde{\mathbf{V}}_{\tilde{m},\tilde{n}}|\tilde{n}\rangle_\mathcal{C} \text{ where } \tilde{\mathbf{V}}_{\tilde{m},\tilde{n}} = F_{\tilde{k}\tilde{l}\tilde{n}}^{\tilde{\imath}\tilde{\jmath}\tilde{m}}.$$

Now consider a locality-preserving isomorphism U which takes the boundary labels (i,j,k,l) to $(\tilde{\imath},\tilde{\jmath},\tilde{k},\tilde{l})$. We can then apply the framework above to find the action

$$U|a\rangle_\mathcal{C} = \mathrm{e}^{\mathrm{i}\varphi(a)}|\pi^C(a)\rangle_\mathcal{C} \qquad \text{or} \qquad U|a\rangle_{\mathcal{C}'} = \mathrm{e}^{\mathrm{i}\varphi'(a)}|\pi^{C'}(a)\rangle_{\mathcal{C}'}$$

on basis states. Here $\pi^C, \pi^{C'} \colon Q \to \tilde{Q}$ take fusion-consistent labels on $\Sigma(i,j,k,l)$ to fusion-consistent labels on $\Sigma(\tilde{\imath},\tilde{\jmath},\tilde{k},\tilde{l})$. Because the spaces are isomorphic, we must have $|Q| = |\tilde{Q}|$, hence $\pi^C, \pi^{C'}$ can be represented by permutation matrices $\mathbf{\Pi}, \mathbf{\Pi}'$ in the basis pairs $(\mathcal{B}_\mathcal{C}, \tilde{\mathcal{B}}_\mathcal{C})$ or $(\mathcal{B}_{\mathcal{C}'}, \tilde{\mathcal{B}}_{\mathcal{C}'})$, respectively. Proceeding similarly with $\mathbf{U}$, we get the consistency equation $\tilde{\mathbf{V}}\mathbf{U} = \mathbf{U}'\mathbf{V}$ or

$$\tilde{\mathbf{V}}\mathbf{\Pi}\mathbf{D}(\{\varphi(a)\}_a) = \mathbf{\Pi}'\mathbf{D}(\{\varphi'(a)\}_a)\mathbf{V}, \tag{7.52}$$

which is expressed in the form of a commutative diagram as in Fig. 7.8. Equation (7.52) only differs from equation (7.37) in allowing boundary labels to change and the basis transformation matrix $\tilde{\mathbf{V}}$ must change accordingly.

For a given set of boundary labels (i,j,k,l), $(\tilde{\imath},\tilde{\jmath},\tilde{k},\tilde{l})$, and a fixed choice of π^C (which fixes $\mathbf{\Pi}$), any solution $(\mathbf{\Pi}', \{\varphi(a)\}_a, \{\varphi'(a)\}_a)$ of (7.52) has phases $\{\varphi(a)\}_a$ of the "universal" form

$$\varphi(a) = \eta + f(a) \qquad \text{for all } a \in Q(i,j,k,l)\ , \tag{7.53}$$

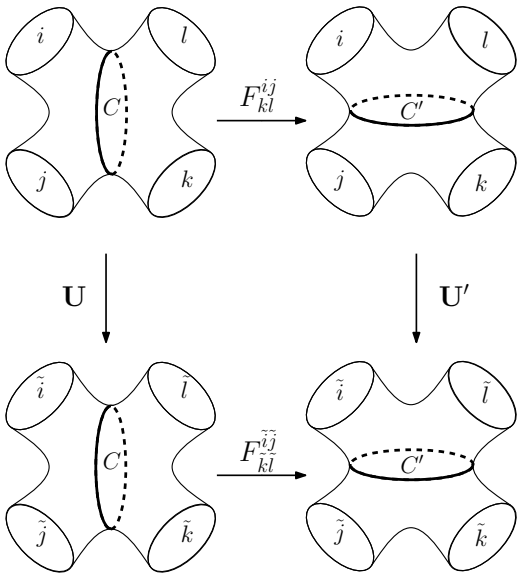


Figure 7.8: An isomorphism $\mathcal{H}_{\Sigma(i,j,k,l)} \to \mathcal{H}_{\Sigma(\tilde{\imath},\tilde{\jmath},\tilde{k},\tilde{l})}$ of two 4-punctured spheres can be given as either $\mathbf{U}$, which relates the bases $\mathcal{B}_C$ of $\mathcal{H}_{\Sigma(i,j,k,l)}$ to $\tilde{\mathcal{B}}_C$ of $\mathcal{H}_{\Sigma(\tilde{\imath},\tilde{\jmath},\tilde{k},\tilde{l})}$, or as $\mathbf{U}'$ relating different bases $\mathcal{B}_{C'}$ of $\mathcal{H}_{\Sigma(i,j,k,l)}$ to $\tilde{\mathcal{B}}_{C'}$ of $\mathcal{H}_{\Sigma(\tilde{\imath},\tilde{\jmath},\tilde{k},\tilde{l})}$. The bases of $\mathcal{H}_{\Sigma(i,j,k,l)}$ and $\mathcal{H}_{\Sigma(\tilde{\imath},\tilde{\jmath},\tilde{k},\tilde{l})}$ are related through the F-moves F^{ij}_{kl} and $F^{\tilde{\imath}\tilde{\jmath}}_{\tilde{k}\tilde{l}}$, respectively. The consistency equation (7.52) can be expressed as a commutative diagram. In the case where $\Sigma(i,j,k,l) = \Sigma(\tilde{\imath},\tilde{\jmath},\tilde{k},\tilde{l})$ have identical boundary labels such an isomorphism becomes an automorphism, and this reduces to the consistency equation (7.51).

where $\eta \in [0, 2\pi)$ is an arbitrary global phase independent of a, and f belongs to a set $\mathsf{Iso}\Big(\underline{j \;\; i \;\; \cdot \;\; l \;\; k} \to \underline{\tilde{j} \;\; \tilde{i} \;\; \pi^C(\cdot) \;\; \tilde{l} \;\; \tilde{k}}\Big)$ of functions that can be computed from (7.52) as discussed below.

In summary, we have shown that U acts as

$$U|a\rangle_{\mathcal{C}} = e^{i\eta} e^{if(a)} |\pi^C(a)\rangle_{\mathcal{C}} \qquad \text{with} \qquad f \in \mathsf{Iso}\Big(\underline{j \;\; i \;\; \cdot \;\; l \;\; k} \to \underline{\tilde{j} \;\; \tilde{i} \;\; \pi^C(\cdot) \;\; \tilde{l} \;\; \tilde{k}}\Big)\,, \tag{7.54}$$

and where the latter set can be determined by solving the consistency relation (7.52).

7.5.3 Localization of phases for higher-genus surfaces

We now argue that the phases appearing in Eq. (7.31) of Proposition 7.3.2 also factorize into certain essentially local terms, similar to how the overall permutation $\vec{\pi}$ of fusion-consistent labelings decomposes into a collection $\vec{\pi} = \{\pi^C\}_{C\in\mathcal{C}}$ of permutations of labels. More precisely, we will argue that conclusion (7.54) can be extended to more general surfaces.

Consider a fixed DAP-decomposition $\mathcal{C}$ of Σ. We call a curve $C \in \mathcal{C}$ *internal* if the intersection of Σ with a ball containing C has the form of a 4-punctured sphere with boundary components C_1, C_2, C_3, C_4 consisting of curves 'neighboring' C in the DAP decomposition. We call $N(C) = \{C_1, C_2, C_3, C_4\}$ the neighbors (or neighborhood) of C as illustrated in Fig. 7.9. Key to the following observations is that a basis vector $|\ell\rangle$ whose restriction to these neighbors is given by $\ell \restriction N(C) = \big(\ell(C_1), \ldots, \ell(C_4)\big)$ gets mapped under U to a vector proportional to $|\vec{\pi}(\ell)\rangle$, which assigns the labels $\vec{\pi}(\ell) \restriction N(C) = \big(\pi^{C_1}[\ell(C_1)], \ldots, \pi^{C_4}[\ell(C_4)]\big)$ to the same curves. This means that the restriction of U to this subspace satisfies similar consistency conditions as the isomorphisms between Hilbert spaces associated with the 4-punctured spheres $\Sigma(\ell \restriction N(C))$ and $\Sigma\big(\vec{\pi}(\ell) \restriction N(C)\big)$ studied in Section 7.5.1. In particular, for a fixed labeling ℓ the dependence of the phase $\varphi(\ell)$ on the label $\ell(C)$ is given by a function from the set $\mathsf{Iso}\Big(\underline{j \;\; i \;\; \cdot \;\; l \;\; k} \to \underline{\tilde{j} \;\; \tilde{i} \;\; \pi^C(\cdot) \;\; \tilde{l} \;\; \tilde{k}}\Big)$, where $(i, j, k, l) = \ell \restriction N(C)$ and $(\tilde{\imath}, \tilde{\jmath}, \tilde{k}, \tilde{l}) = \vec{\pi}(\ell) \restriction N(C)$. In the following, we simply write $\mathsf{Iso}\Big(\ell \restriction N(C) \overset{\pi^C}{\to} \vec{\pi}(\ell) \restriction N(C)\Big)$ for this set.

Proposition 7.5.1 (Localization of internal phases)**.** *Let U be a locality-preserving automorphism. Let $\mathcal{C}$ be a DAP-decomposition of Σ, and let $\vec{\pi} = \{\pi^C\}_{C\in\mathcal{C}}$ be the family of permutations defined by Proposition 7.3.1. Let $\varphi(\ell)$ for $\ell \in \mathsf{L}(\mathcal{C})$ be defined by (7.31). If $C \in \mathcal{C}$ is internal,*

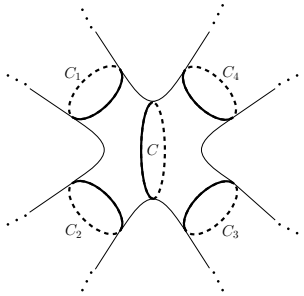


Figure 7.9: For some DAP-decomposition $\mathcal{C}$ of a surface Σ, a curve $C \in \mathcal{C}$ is considered internal if its neighbors $N(C) = \{C_1, C_2, C_3, C_4\}$ define the boundaries of a 4-punctured sphere.

then

$$\varphi(\ell) = \eta(\ell\restriction \mathcal{C}\backslash\{C\}) + f_{\vec{\pi}\restriction N(C)}(\ell \restriction N(C), \ell(C))$$

for some functions η and f. Furthermore, we have

$$f_{\vec{\pi}\restriction N(C)}(\ell \restriction N(C), \cdot) \in \mathsf{Iso}\left(\ell \restriction N(C) \overset{\pi^C}{\to} \vec{\pi}(\ell) \restriction N(C)\right) \ .$$

In particular, the dependence of $\varphi(\ell)$ on $\ell(C)$ is "local" and "controlled" by the labeling $\ell \restriction N(C)$ of the neighbors.

In other words, if we fix a family of permutations $\vec{\pi}$, and the labels on the neighbors $N(C)$, then the dependence on the label $\ell(C)$ of the internal edge is essentially fixed.

Proof. We will focus our attention on the subspace $\mathcal{H}_{(i,j,k,l,\star)} \subseteq \mathcal{H}_\Sigma$ spanned by labelings ℓ with $(\ell(C_1), \ell(C_2), \ell(C_3), \ell(C_4)) = (i, j, k, l)$ and $\ell \restriction \mathcal{C}\backslash\{C, C_1, C_2, C_3, C_4\} = \star$ fixed (arbitrarily). For the purpose of this proof, it will be convenient to represent basis vectors $|\ell\rangle$ associated with such a labeling $\ell \in \mathsf{L}(C)$ as a vector

$$|\ell\rangle = |\ell(C), \ell(C_1), \ell(C_2), \ell(C_3), \ell(C_4), \star\rangle = |a, i, j, k, l, \star\rangle \ .$$

Defining $\tilde{\imath} = \pi^{C_1}(i)$, $\tilde{\jmath} = \pi^{C_2}(j)$, $\tilde{k} = \pi^{C_3}(k)$, $\tilde{l} = \pi^{C_4}(l)$, we can rewrite (7.31) in the form

$$U|a, i, j, k, l, \star\rangle = \mathrm{e}^{\mathrm{i}\varphi(a,i,j,k,l,\star)}|\pi^C(a), \tilde{\imath}, \tilde{\jmath}, \tilde{k}, \tilde{l}, \tilde{\star}\rangle \ ,$$

where $\tilde{\star} = \vec{\pi}_\restriction(\star)$ for some map $\vec{\pi}_\restriction$ taking labelings of the set $\mathcal{C}\backslash\{C, C_1, C_2, C_3, C_4\}$ consistent with (i, j, k, l) to those consistent with $(\tilde{\imath}, \tilde{\jmath}, \tilde{k}, \tilde{l})$. We conclude that the restriction of U to $\mathcal{H}_{(i,j,k,l,\star)}$ implements an isomorphism $\mathcal{H}_{(i,j,k,l,\star)} \cong \mathcal{H}_{(\tilde{\imath},\tilde{\jmath},\tilde{k},\tilde{l},\tilde{\star})}$. Since these spaces are isomorphic to $\mathcal{H}_{\Sigma(i,j,k,l)}$ and $\mathcal{H}_{\Sigma(\tilde{\imath},\tilde{\jmath},\tilde{k},\tilde{l})}$, respectively, we can apply the result of Section 7.5.2. Indeed, the

consistency relation imposed by the F-move is entirely local, not affecting labels associated with curves not belonging to $\{C, C_1, C_2, C_3, C_4\}$. We conclude from (7.54) that

$$\varphi(a,i,j,k,l,\star) = \eta(i,j,k,l,\star) + f(a), \text{ where } f \in \mathsf{Iso}\left(\underset{j}{\overset{i}{|}} \quad \cdot \quad \underset{k}{\overset{l}{|}} \to \underset{\tilde{j}}{\overset{\tilde{i}}{|}} \ \pi^C(\cdot) \ \underset{\tilde{k}}{\overset{\tilde{l}}{|}} \right).$$

Since $(a,i,j,k,l,\star)$ were arbitrary, this proves the claim. □

For example, for $S^2(z^{N+3})$ (as described above), we can apply Proposition 7.5.1 to the j-th internal edge C_j to obtain

$$\varphi(x) = \eta_j(x_1, \ldots, \widehat{x}_j, \ldots, x_N) + f_j(x_{j-1}, x_j, x_{j+1}), \tag{7.55}$$

where

$$f_j(x_{j-1}, \cdot, x_{j+1}) \in \mathsf{Iso}\left(\underset{x_{j-1}}{\overset{z}{|}} \quad \cdot \quad \underset{x_{j+1}}{\overset{z}{|}} \to \underset{\tilde{x}_{j-1}}{\overset{z}{|}} \ \pi^{C_j}(\cdot) \ \underset{\tilde{x}_{j+1}}{\overset{z}{|}} \right),$$

and

$$\tilde{x}_{j-1} = \pi^{C_{j-1}}(x_{j-1}), \qquad \tilde{x}_{j+1} = \pi^{C_{j+1}}(x_{j+1}).$$

Here, we use $\hat{x}_j$ to indicate that this argument is omitted.

7.5.4 Characterizing protected gates on the M-punctured sphere using F-moves

The results in this section give the following procedure for characterizing protected gates associated with $\mathcal{H}_{S^2(z^M)}$, the Hilbert space of $M = N+3$ anyons of type z. We know from Proposition 7.3.2 that the action $U|\ell\rangle = \mathrm{e}^{\mathrm{i}\varphi(\ell)}|\vec{\pi}(\ell)\rangle$ on fusion-consistent labelings is parametrized by certain families $\vec{\pi} = \{\pi^C\}_{C\in\mathcal{C}}$ of permutations, as well as a function φ describing the phase-dependence. To characterize the latter, we

(i) determine the set of allowed 'local' permutations π^C and associated phases f for any occuring internal curve C. This amounts to solving the consistency equation (7.52) for the four-punctured sphere, with appropriate boundary labels. For the standard pants decomposition of the $N+3$-punctured sphere, this means finding all pairs

$$(\pi^{C_j}, f_j) \qquad \text{where } f_j \in \mathsf{Iso}\left(\underset{x_{j-1}}{\overset{z}{|}} \quad \cdot \quad \underset{x_{j+1}}{\overset{z}{|}} \to \underset{\tilde{x}_{j-1}}{\overset{z}{|}} \ \pi^{C_j}(\cdot) \ \underset{\tilde{x}_{j+1}}{\overset{z}{|}} \right).$$

These correspond to isomorphisms between the Hilbert spaces associated with the labeled surfaces $S^2(z, x_{j-1}, x_{j+1}, z)$ and $S^2(z, \tilde{x}_{j-1}, \tilde{x}_{j+1}, z)$, where $x_{j-1}, \tilde{x}_{j-1} \in Q(j-1), x_{j+1}, \tilde{x}_{j+1} \in Q(j+1)$.

(ii) we constrain the family $\vec{\pi} = \{\pi^C\}_{C\in\mathcal{C}}$ of allowed permutations by using the global constraints arising from fusion rules and gluing (Proposition 7.3.3). In the case of $N+3$ Fibonacci anyons on the sphere with standard pants decomposition $\mathcal{C}$, dimensional arguments show that all $\pi^{C_j} = \mathsf{id}$ are equal to the identity permutation. For Ising anyons, the fusion rules imply that every permutation with even index is equal to the identity permutation, $\pi^{C_{2j}} = \mathsf{id}$ (in fact, there is only a single allowed label).

(iii) we determine the phases $\varphi(\ell)$ by using the localization property of Proposition 7.5.1 for internal curves C. For $N+3$ anyons of type z on the sphere, this results in the consistency conditions

$$\varphi(x) = \eta_j(x_1, \dots, \widehat{x}_j, \dots, x_N) + f_j(x_{j-1}, x_j, x_{j+1}) \qquad \text{where}$$
$$f_j(x_{j-1}, \cdot, x_{j+1}) \in \mathsf{Iso}\left(\overset{z}{\underline{x_{j-1}|}} \quad \cdot \quad \overset{z}{\underline{|x_{j+1}}} \to \overset{z}{\underline{\tilde{x}_{j-1}|}} \ \pi^{C_j}(\cdot) \ \overset{z}{\underline{|\tilde{x}_{j+1}}} \right) \qquad \text{for } j = 1, \dots, N \ . \tag{7.56}$$

In Section 7.6.2, we apply this procedure to Ising anyons; in this case, the system of equations (7.56) can be solved explicitly.

7.6 The Fibonacci and Ising models

In what follows, we apply the results of the previous sections to the Fibonacci and Ising models. These can be considered as representative examples of non-abelian anyon models. We illustrate the use of the developed constraints in different scenarios:

In Section 7.6.1, we show that there is no non-trivial gate for the Fibonacci model on the torus. This derivation uses the characterization of protected gates in terms of matrices intertwining with the mapping class group representation obtained in Section 7.4.1. Note that we cannot apply Corollary 7.4.2 because the representation of the mapping class group on the torus is finite for the Fibonacci model.

In Section 7.6.1, we then consider a system with M Fibonacci anyons (where $M \geq 4$ so that the space $\mathcal{H}_{S^2(\tau^M)}$ has non-zero dimension). We establish the following statement:

Theorem 7.6.1 (Fibonacci anyon model)**.** *For $M \geq 4$, any locality-preserving automorphism U on the M-punctured sphere $S^2(\tau^M)$ is trivial (i.e., proportional to the identity).*

This proof is a direct consequence of Corollary 7.4.2 and the known density of braiding [**?**, **?**]. We additionally provide an independent proof not relying on this result.

Finally, we consider systems with M Ising anyons; the associated Hilbert space $\mathcal{H}_{S^2(\sigma^M)}$ has non-zero dimension if and only if $M \geq 4$ is even. In this case, there is a natural isomorphism $\mathcal{H}_{S^2(\sigma^M)} \cong (\mathbb{C}^2)^{\otimes M/2-1}$ (described below, see Eq. (7.62)). Defining the $(M/2-1)$-qubit Pauli group on the latter space in the usual way, we get the following statement:

Theorem 7.6.2 (Ising anyon model)**.** *Any locality-preserving automorphism U of $S^2(\sigma^M)$, where $M \geq 4$ is even, belongs to the $(M/2-1)$-qubit Pauli group.*

Our derivation of this result relies on the use of F-moves, as discussed in Section 7.5.

7.6.1 The Fibonacci model

For the Fibonacci model, we have $\mathbb{A} = \{1, \tau\}$ and the only non-trivial fusion rule is $\tau \times \tau = 1 + \tau$ with $d_\tau = \phi = (1+\sqrt{5})/2$.

On the torus

We first consider the torus Σ and show that every protected gate is trivial. We do so by computing some of the sets Δ_ϑ, $\vartheta \in \mathsf{MCG}_\Sigma$ defined in Section 7.4.1. Recall (see Section 7.2.6) that the mapping class group of the torus is generated by two elements s, t.

The matrix $\mathbf{V}(s) = S$ representing s is the usual S-matrix (expressed with respect to the ordering $(1, \tau)$)

$$S = \frac{1}{\sqrt{\phi+2}} \begin{pmatrix} 1 & \phi \\ \phi & -1 \end{pmatrix}.$$

In particular, the consistency condition (7.39) becomes

$$S\mathbf{\Pi}\mathbf{D}S^{-1} \in \Delta,$$

where $\mathbf{D} = \mathrm{diag}(\lambda_1, \lambda_\tau)$ and $\lambda_a \in \mathrm{U}(1)$. We consider the two cases:

1. For $\mathbf{\Pi} = I$, we get (using $\phi^2 = \phi + 1$)

$$S\mathbf{\Pi}\mathbf{D}S^{-1} = \frac{1}{\phi+2} \begin{pmatrix} \lambda_1 + \lambda_\tau(\phi+1) & (\lambda_1 - \lambda_\tau)\phi \\ (\lambda_1 - \lambda_\tau)\phi & \lambda_1(\phi+1) + \lambda_\tau \end{pmatrix}.$$

   For this to be a unitary monomial matrix, all entries must have modulus 0 or 1. Since $\phi/(\phi+2) < 1/2$, the off-diagonal elements always have modulus less than 1, and hence

must be zero. That is, we must have $\lambda_1 = \lambda_\tau =: \lambda$, and it follows that the right hand side is in Δ. This implies that $\mathbf{\Pi D} = \lambda I$.

2. For $\mathbf{\Pi} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we get

$$S\mathbf{\Pi D}S^{-1} = \frac{1}{\phi+2}\begin{pmatrix} (\lambda_1+\lambda_\tau)\phi & \lambda_1(\phi+1)-\lambda_\tau \\ \lambda_\tau(\phi+1)-\lambda_1 & -(\lambda_1+\lambda_\tau)\phi \end{pmatrix}.$$

To have the absolute value of the first entry equal to 0 (see above), we must have $\lambda_\tau = -\lambda_1$ and we get

$$S\mathbf{\Pi D}S^{-1} = \lambda_1\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

which is a unitary monomial matrix. That is, we have $\mathbf{\Pi D} = \lambda\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Summarizing, we conclude that

$$\Delta_s = \left\{ \lambda I, \lambda\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \mid \lambda \in \mathrm{U}(1) \right\}. \tag{7.57}$$

The element $t \in \mathsf{MCG}_\Sigma$ defined by twisting along one of the homologically non-trivial cycles is represented by the matrix $\mathbf{V}(t) = T = \mathrm{diag}(1, e^{4\pi i/5})$. We consider the consistency condition (7.39) for the composition $st \in \mathsf{MCG}_\Sigma$:

$$(ST)\mathbf{\Pi D}(ST)^{-1} \in \Delta,$$

where $\mathbf{D} = \mathrm{diag}(\lambda_1, \lambda_\tau)$ and $\lambda_a \in \mathrm{U}(1)$. Again, we consider the following two cases:

1. For $\mathbf{\Pi} = I$, we get

$$(ST)\mathbf{\Pi D}(ST)^{-1} = \frac{1}{\phi+2}\begin{pmatrix} \lambda_1+\lambda_\tau(\phi+1) & (\lambda_1-\lambda_\tau)\phi \\ (\lambda_1-\lambda_\tau)\phi & \lambda_1(\phi+1)+\lambda_\tau \end{pmatrix}.$$

This is identical to the first case above, thus $\mathbf{\Pi D} = \lambda I$.

2. For $\mathbf{\Pi} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we get

$$(ST)\mathbf{\Pi D}(ST)^{-1} = \frac{\zeta}{\phi+2}\begin{pmatrix} (\zeta^3\lambda_1-\lambda_\tau)\phi & \zeta^3\lambda_1(\phi+1)+\lambda_\tau \\ -\zeta^3\lambda_1-\lambda_\tau(\phi+1) & -(\zeta^3\lambda_1-\lambda_\tau)\phi \end{pmatrix},$$

where $\zeta = \mathrm{e}^{\mathrm{i}\pi/5}$. Since $\phi/(\phi+2) < 1/2$, the diagonal elements must vanish, that is, we have $\lambda_\tau = \zeta^3\lambda_1$. This indeed then gives an element of Δ, and $\mathbf{\Pi D} = \lambda \begin{pmatrix} 0 & \mathrm{e}^{3\pi\mathrm{i}/5} \\ 1 & 0 \end{pmatrix}$.

In summary, we have shown that

$$\Delta_{st} = \left\{ \lambda I, \lambda \begin{pmatrix} 0 & \mathrm{e}^{3\pi\mathrm{i}/5} \\ 1 & 0 \end{pmatrix} \mid \lambda \in \mathrm{U}(1) \right\}. \tag{7.58}$$

Combining (7.57) and (7.58), we conclude that

$$\Delta_s \cap \Delta_{st} = \{\lambda I \mid \lambda \in \mathrm{U}(1)\},$$

and this means that $\Delta_{\mathsf{MCG}_\Sigma} \subset \Delta_s \cap \Delta_{st} = \{\lambda I \mid \lambda \in \mathrm{U}(1)\}$. According to Theorem 7.4.1, this implies that there is no non-trivial protected gate on the torus.

Note that this conclusion is consistent with the form of a Dehn twist, given by the logical unitary $U = \mathrm{diag}(1, e^{4\pi i/5})$ (with the 'topological' phases or twists on the diagonal): Dehn twists do *not* preserve locality! For example, for a Dehn twist along C_1, an operator supported on C_2 may end up with support in the neighborhood of the union $C_1 \cup C_2$ under conjugation by the unitary realizing the Dehn twist.

On the M-punctured sphere

We now provide a proof of Theorem 7.6.1. As already mentioned, braiding of $M \geq 4$ Fibonacci anyons is known to be universal [**?**], [**?**], hence we could invoke Corollary 7.4.2. Instead, we give a different proof by exploiting the equivalence relation introduced in Section 7.4.3 and analyzing the dimension of the associated spaces (i.e., using the constraints arising from the gluing axiom, see Section 7.3.2).

Consider the M-punctured sphere $\Sigma = S^2(\tau^M)$ corresponding to M Fibonacci anyons. We will use as our 'standard' basis the one arising from the standard DAP decomposition $\mathcal{C}$ of the M-punctured sphere introduced in Section 7.2.5 (see Fig. 7.5). We then have the following statement:

Lemma 7.6.3. *There is only one equivalence class under the relation $\sim$. Furthermore, the set of braids $\{\sigma_j\}_{j=1}^{M-1}$ generates the relation $\sim$.*

Proof. Let x and x' be two fusion-consistent labelings that are related by interchanging $\tau = x_j$ and $1 = x'_j$ (or vice versa) in the j-th entry (but are otherwise the same). Fusion-consistency

implies that $x_{j-1} = x'_{j-1} = x_{j+1} = x'_{j+1} = \tau$. In particular, the relevant braid matrix describing the action of $V(\sigma_j)$ is $B(\tau,\tau)$ which has non-zero entries everywhere. We conclude that

$$\langle x'|V(\sigma_j)|x\rangle \neq 0 \qquad \text{and} \qquad \langle x'|V(\sigma_j)|x'\rangle \neq 0 \ .$$

This implies that $x \Leftrightarrow_{\sigma_j} x'$. Since any fusion-consistent labeling can be obtained from the sequence $\tau^N = (\tau,\ldots,\tau)$ by such interchanges, we conclude that any two fusion-consistent labelings are equivalent. That is, there is only one equivalence class under $\sim$. □

We will now argue that the conditions of Lemma 7.4.3 (ii) apply in this situation: that is, any protected gate U acts diagonally in any of the bases $\mathcal{B}_{\sigma_j(\mathcal{C})}$ obtained from the standard DAP-decomposition by applying a braid group generator σ_j. In fact, we will argue more generally that U acts diagonally in any basis defined by a DAP-decomposition.

To do so, consider first the standard DAP-decomposition and the spaces $\mathcal{H}_{\Sigma'_j(a,a)}$ for $j \in \{1,\ldots,M-3\}$ and $a \in \{1,\tau\}$ (cf. (7.21)), where Σ'_j is obtained from Σ by cutting along the curve C_j which leaves a $j+2$-punctured and a $(M-j)$-punctured sphere, respectively. Note that τ is its own antiparticle ($\overline{\tau} = \tau$), and hence it suffices to consider $\Sigma'_j(\tau,\tau)$ and $\Sigma'_j(1,1)$. Our goal is to identify pairs $(a,\tilde{a})$ such that $\mathcal{H}_{\Sigma'_j(a,a)} \cong \mathcal{H}_{\Sigma'_j(\tilde{a},\tilde{a})}$ are isomorphic, this being a necessary condition for a permutation satisfying $\pi^{C_j}(a) = \tilde{a}$ (see Proposition (7.3.3) and Eq. (7.35)). To compute $\dim \mathcal{H}_{\Sigma'_j(a,a)}$ for $a \in \{1,\tau\}$, we make use of the general fact that $\dim \mathcal{H}_{S^2(\tau^M)} = \Phi_{M-1}$ where Φ_M denotes the M-th Fibonacci number, starting with $\Phi_0 = 0$ and $\Phi_1 = 1$ and satisfying the recurrence relation $\Phi_{M+1} = \Phi_M + \Phi_{M-1}$. From (7.21), we obtain $\dim \mathcal{H}_{\Sigma'_j(1,1)} = \Phi_j \Phi_{M-j-2}$ and $\dim \mathcal{H}_{\Sigma'_j(\tau,\tau)} = \Phi_{j+1}\Phi_{M-j-1}$, excluding the case $j = 1 = M-3$ which satisfies $\dim \mathcal{H}_{\Sigma'_1(1,1)} = \Phi_1\Phi_{M-3} = \dim \mathcal{H}_{\Sigma'_{M-3}(1,1)}$ and $\dim \mathcal{H}_{\Sigma'_1(\tau,\tau)} = \Phi_2\Phi_{M-2} = \dim \mathcal{H}_{\Sigma'_{M-3}(\tau,\tau)}$, it follows from the monotonicity and positivity of Φ that

$$\dim \mathcal{H}_{\Sigma'_j(1,1)} < \dim \mathcal{H}_{\Sigma'_j(\tau,\tau)} \qquad \text{for } M > 4, \text{ and all } j \in \{1,...,M-3\}. \tag{7.59}$$

Hence, according to the consistency condition (7.35), for $M > 4$, we only get an isomorphism $\mathcal{H}_{\Sigma'(a,\overline{a})} \cong \mathcal{H}_{\Sigma'(\pi^C(a),\overline{\pi^C(a)})}$ with $\pi^C = \mathsf{id}$ being trivial for any internal loop C in a standard DAP decomposition. This shows that a protected gate acts diagonally in the standard basis.

Observe that this argument only involved the dimensions of the fusion spaces obtained by cutting along a curve C_j in the pants decomposition. Since it is generally true that cutting along a curve will decompose the M-punctured sphere into an $j+2$-punctured and a $(M-j)$-punctured sphere, respectively (for some j), the argument extends to arbitrary DAP-decompositions. In particular, U is diagonal with respect to each of the bases $\mathcal{B}_{\sigma_j(\mathcal{C})}$, as claimed.

We have shown that the conditions of Lemma 7.4.3 apply. With Lemma 7.6.3, Theorem 7.6.1

is immediate.

7.6.2 The Ising model

The Ising anyon model has label set $\mathbb{A} = \{1, \psi, \sigma\}$ and non-trivial fusion rules

$$\psi \times \psi = 1, \quad \psi \times \sigma = \sigma, \quad \sigma \times \sigma = 1 + \psi.$$

On the 4-punctured sphere

Consider the possible spaces $\mathcal{H}_{S^2(\sigma,j,k,\sigma)}$ for $\{j,k\} \in \mathbb{A}$, and observe that fusion consistency implies

$$\dim \mathcal{H}_{S^2(\sigma,j,k,\sigma)} = \begin{cases} 0 & \text{if } \ j \neq k = \sigma \text{ or } k \neq j = \sigma \\ 1 & \text{if } \ j,k \in \{1,\psi\}, \\ 2 & \text{if } \ j = k = \sigma. \end{cases}$$

Therefore, the only nontrivial case to consider is $\mathcal{H}_{S^2(\sigma,\sigma,\sigma,\sigma)} = \mathcal{H}_{S^2(\sigma^4)}$ with an ordered basis $\{|1\rangle, |\psi\rangle\}$. A locality-preserving automorphism of $\mathcal{H}_{S^2(\sigma^4)}$ will act as

$$U|a\rangle = e^{i\eta} e^{if(a)} |\pi^C(a)\rangle \qquad \text{where } f \in \mathsf{Iso}\left(\underline{\sigma \quad \overset{\sigma}{|} \quad \cdot \quad \overset{\sigma}{|} \quad \sigma} \ \to \ \underline{\sigma \quad \overset{\sigma}{|} \quad \pi^C(\cdot) \quad \overset{\sigma}{|} \quad \sigma} \right)$$

A valid permutation π^C of $\{1,\psi\}$ that defines the action of U, and the set of phases can be determined as follows. Let $\mathcal{B}_{\mathcal{C}} = \{|1\rangle_{\mathcal{C}}, |\psi\rangle_{\mathcal{C}}\}$ and $\mathcal{B}_{\mathcal{C}'} = \{|1\rangle_{\mathcal{C}'}, |\psi\rangle_{\mathcal{C}'}\}$ be corresponding ordered bases of $\mathcal{H}_{S^2(\sigma^4)}$ for the two DAP-decomposition $\mathcal{C}$ and $\mathcal{C}'$, respectively. The F-matrix relating these two bases is given in the ordered basis $\mathcal{B}_{\mathcal{C}}$ as

$$F = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Now consider some locality-preserving automorphism U expressed in the bases $\mathcal{B}_{\mathcal{C}}$ and $\mathcal{B}_{\mathcal{C}'}$ as $\mathbf{U} = \mathbf{\Pi D}$ and $\mathbf{U}' = \mathbf{\Pi}'\mathbf{D}'$ respectively, for some 2×2 permutation matrices $\mathbf{\Pi}, \mathbf{\Pi}'$ and diagonal matrices $\mathbf{D} = \mathrm{diag}(\lambda_1, \lambda_\psi)$ and $\mathbf{D}' = \mathrm{diag}(\lambda'_1, \lambda'_\psi)$ with phases $\lambda_a, \lambda'_a \in \mathrm{U}(1)$. Then the consistency relation takes the form $\mathbf{U}' = F\mathbf{U}F^{-1}$. Next, we find all consistent solutions for a given permutation $\mathbf{\Pi}$.

1. For $\mathbf{\Pi} = I$, we get

$$F\mathbf{\Pi D}F^{-1} = \frac{1}{2} \begin{pmatrix} \lambda_1 + \lambda_\psi & \lambda_1 - \lambda_\psi \\ \lambda_1 - \lambda_\psi & \lambda_1 + \lambda_\psi \end{pmatrix} = \mathbf{\Pi}'\mathbf{D}'. \tag{7.60}$$

Suppose that $\mathbf{\Pi}' = I$. Then the consistency relation (7.60) becomes

$$\frac{1}{2}\begin{pmatrix} \lambda_1 + \lambda_\psi & \lambda_1 - \lambda_\psi \\ \lambda_1 - \lambda_\psi & \lambda_1 + \lambda_\psi \end{pmatrix} = \begin{pmatrix} \lambda_1' & 0 \\ 0 & \lambda_\psi' \end{pmatrix},$$

which implies $\lambda_1 = \lambda_\psi = \lambda_1' = \lambda_\psi' =: \mathrm{e}^{\mathrm{i}\eta}$. Therefore U expressed in the basis $\mathcal{B}_\mathcal{C}$ is trivial up to a global phase:

$$\mathbf{U} = \mathrm{e}^{\mathrm{i}\eta} I.$$

Suppose instead that $\mathbf{\Pi}' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. The consistency relation (7.60) then becomes

$$\frac{1}{2}\begin{pmatrix} \lambda_1 + \lambda_\psi & \lambda_1 - \lambda_\psi \\ \lambda_1 - \lambda_\psi & \lambda_1 + \lambda_\psi \end{pmatrix} = \begin{pmatrix} 0 & \lambda_\psi' \\ \lambda_1' & 0 \end{pmatrix},$$

which implies $\lambda_1 = -\lambda_\psi$ and $\lambda_1' = \lambda_\psi' = \lambda_1$. Setting $\mathrm{e}^{\mathrm{i}\eta} \coloneqq \lambda_1$, implies that U expressed in the basis $\mathcal{B}_\mathcal{C}$ is given by

$$\mathbf{U} = \mathrm{e}^{\mathrm{i}\eta}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

These two solutions of the consistency relation, for the case $\mathbf{\Pi} = I$, now determine the only two functions of the set

$$\mathsf{Iso}\left(\underline{\sigma \quad \overset{\sigma}{|} \quad \cdot \quad \overset{\sigma}{|} \quad \sigma} \;\to\; \underline{\sigma \quad \overset{\sigma}{|} \quad \mathsf{id}(\cdot) \quad \overset{\sigma}{|} \quad \sigma}\right) = \{(f(1), f(\psi))\} = \{(0,0),(0,\pi)\}.$$

2. For $\mathbf{\Pi} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, corresponding to the transposition $(\psi, 1)$, we get

$$F\mathbf{\Pi}\mathbf{D}F^{-1} = \frac{1}{2}\begin{pmatrix} \lambda_1 + \lambda_\psi & \lambda_1 - \lambda_\psi \\ -\lambda_1 + \lambda_\psi & -\lambda_1 - \lambda_\psi \end{pmatrix} = \mathbf{\Pi}'\mathbf{D}'. \tag{7.61}$$

By taking $\mathbf{\Pi}' = I$, this becomes

$$\frac{1}{2}\begin{pmatrix} \lambda_1 + \lambda_\psi & \lambda_1 - \lambda_\psi \\ -\lambda_1 + \lambda_\psi & -\lambda_1 - \lambda_\psi \end{pmatrix} = \begin{pmatrix} \lambda_1' & 0 \\ 0 & \lambda_\psi' \end{pmatrix},$$

which implies $\lambda_1 = \lambda_\psi = \lambda_1' = -\lambda_\psi'$. Letting $\mathrm{e}^{\mathrm{i}\eta} \coloneqq \lambda_1$ allows U to be expressed in the basis $\mathcal{B}_\mathcal{C}$ by

$$\mathbf{U} = \mathrm{e}^{\mathrm{i}\eta}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Instead, suppose now that $\mathbf{\Pi}' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then the consistency relation (7.61) is of the form

$$\frac{1}{2}\begin{pmatrix} \lambda_1 + \lambda_\psi & \lambda_1 - \lambda_\psi \\ -\lambda_1 + \lambda_\psi & -\lambda_1 - \lambda_\psi \end{pmatrix} = \begin{pmatrix} 0 & \lambda'_\psi \\ \lambda'_1 & 0 \end{pmatrix},$$

implying that $\lambda_1 = -\lambda_\psi = -\lambda'_1 = \lambda'_\psi$. Let $\mathrm{e}^{\mathrm{i}\eta} \coloneqq \lambda_1$, then this shows that U expressed in the basis $\mathcal{B}_\mathcal{C}$ is given by

$$\mathbf{U} = \mathrm{e}^{\mathrm{i}\eta}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Furthermore, these two solutions completely determine the relevant set of functions (which happens to be the same as the previous case for $\mathbf{\Pi} = I$):

$$\mathsf{Iso}\left(\begin{array}{ccccc} \sigma & \overset{\sigma}{|} & \cdot & \overset{\sigma}{|} & \sigma \end{array} \to \begin{array}{ccccc} \sigma & \overset{\sigma}{|} & (\psi,1)(\cdot) & \overset{\sigma}{|} & \sigma \end{array}\right) = \{(f(1), f(\psi))\} = \{(0,0),(0,\pi)\}.$$

By denoting the single qubit (logical) Pauli group as

$$\mathcal{P} \coloneqq \left\{ \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \lambda \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \lambda \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \lambda \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \mid \lambda \in \mathrm{U}(1) \right\},$$

these results can be summarized as follows: If U is a locality-preserving automorphism of the fusion space $\mathcal{H}_{S^2(\sigma^4)}$ of the 4-punctured sphere, then U expressed in the basis $\mathcal{B}_\mathcal{C}$ is in $\mathcal{P}$.

On the M-punctured sphere

Let $M \geq 4$ and consider the $M = N + 3$-punctured sphere $S^2(\sigma^M)$ and corresponding space $\mathcal{H}_{S^2(\sigma^M)}$. For the 'standard' DAP-decomposition $\mathcal{C}$ of $S^2(\sigma^M)$, a consistent labeling $\mathsf{L}(\mathcal{C})$ corresponds to a sequence $\big(\ell(C_1), \ldots, \ell(C_N)\big) =: (x_1, \ldots, x_N) =: x$. It is readily observed that $\dim \mathcal{H}_{S^2(\sigma^M)} = 0$ if M is odd, as there are no consistent labelings in this case.

Therefore, in what follows we will restrict our discussion to the $M = N + 3$-punctured sphere where N is any odd positive integer. In this case, any consistent labeling $\ell \in \mathsf{L}(\mathcal{C})$ yields a sequence $(x_1, \ldots, x_N)$ where $x_i \in \{1, \psi\}$ for odd i and $x_i = \sigma$ is fixed for even i. Actually any such labeling of this form is consistent, giving an isomorphism defined in terms of orthonormal basis elements by

$$\begin{array}{rcl} W : \mathcal{H}_{S^2(\sigma^{N+3})} & \to & (\mathbb{C}^2)^{(N+1)/2} \\ |x\rangle & \mapsto & |x_1\rangle \otimes |x_3\rangle \otimes \cdots \otimes |x_N\rangle \ . \end{array} \tag{7.62}$$

Lemma 7.6.4. *Consider the 'standard' basis of the M-punctured sphere $S^2(\sigma^M)$, where $M \geq 4$ is even. Then there is only one equivalence class under the relation $\sim$. Furthermore, the set of braids $\{\sigma_j\}_{j=1}^{M-1}$ generates the relation $\sim$.*

Proof. If two fusion-consistent labelings x, x' differ only in location $2j+1$, they can be connected by σ_{2j+1}: the relevant braid matrix is

$$B(\sigma,\sigma) = \frac{\mathrm{e}^{-3\pi\mathrm{i}/8}}{\sqrt{2}} \begin{pmatrix} \mathrm{i} & 1 \\ 1 & \mathrm{i} \end{pmatrix}.$$

We have $x \Leftrightarrow_{\sigma_{2j+1}} x'$, and it follows that there is only one equivalence class under $\sim$. □

Now consider a locality-preserving automorphism U of $\mathcal{H}_{S^2(\sigma^{N+3})}$ and its associated family $\vec{\pi} = \{\pi^{C_j}\}$ of permutations. Because only sequences x with $x_{2j} = \sigma$ for all j are fusion-consistent, and $\vec{\pi}$ is a permutation on $\mathsf{L}(\mathcal{C})$, we conclude that $\pi^{C_{2j}}(\sigma) = \sigma$ for all j. In other words, we can essentially ignore labels carrying even indices. For odd indices, only labels $x_{2j+1} \in \{1, \psi\}$ are allowed, which means that $\pi^{C_{2j+1}} \in \{\mathsf{id}, (\psi, 1)\}$ either leaves the label invariant or interchanges ψ and 1. In conclusion, $\vec{\pi} = \{\pi^{C_j}\}_{j=1}^{N}$ are of the form $\pi^{C_j} \in \{\mathsf{id}, (\psi, 1)\}$ for odd j, and $\pi^{C_j} = \mathsf{id}$ for even j.

For odd $j = 2k+1$, we obtain the constraint

$$\varphi(x) = \eta_{2k+1}(x_1, \ldots, \widehat{x_{2k+1}}, \ldots, x_N) + f_{2k+1}(x_{2k+1}) \qquad \text{for } k = 0, \ldots, (N-1)/2$$

where $f_{2k+1} \in \mathsf{Iso}\Big(\underline{\sigma \overset{\sigma}{|} \cdot \overset{\sigma}{|} \sigma} \to \underline{\sigma \overset{\sigma}{|} \pi^{C_{2k+1}}(\cdot) \overset{\sigma}{|} \sigma} \Big)$ given that for even labels $\pi^{C_{2m}}(x_{2m}) = x_{2m} = \sigma$. Let us write

$$\varphi(x) = \eta(x) + \sum_{m=0}^{(N+1)/2} f_{2m+1}(x_{2m+1}) \tag{7.63}$$

and show that $\eta(x) = \eta$ is actually independent of the labeling x. Indeed, we can write

$$\begin{aligned} \eta(x) &= \big(\varphi(x) - f_{2k+1}(x_{2k+1})\big) - \sum_{m,m\neq k}^{(N+1)/2} f_{2m+1}(x_{2m+1}) \\ &= \eta_{2k+1}(x_1, \ldots, \widehat{x_{2k+1}}, \ldots, x_N) - \sum_{m,m\neq k}^{(N+1)/2} f_{2m+1}(x_{2m+1}) \end{aligned}$$

Since this holds for all k, we conclude that $\eta(x) = \eta(\widehat{x_1}, x_2, \widehat{x_3}, x_4, \ldots)$ is a function of the even entries only. But the latter are all fixed as $x_{2m} = \sigma$, hence $\eta(x) = \eta$ is simply a global phase.

We can now combine these results into a general statement concerning locality-preserving automorphisms of the M-punctured sphere $S^2(\sigma^M)$. Again, since $\dim \mathcal{H}_{S^2(\sigma^M)} = 0$ for odd M and $\dim \mathcal{H}_{S^2(\sigma^2)} = 1$, we are only concerned with the cases where $M = N + 3 \geq 4$ is even. Let $\{|x\rangle\}_{x \in \mathsf{L}(\mathcal{C})}$ be a basis of $\mathcal{H}_{S^2(\sigma^M)}$. Then such an automorphism must act on $\mathcal{H}_{S^2(\sigma^M)}$ as

$$U|x\rangle = \mathrm{e}^{\mathrm{i}\varphi(x)}|\vec{\pi}(x)\rangle, \qquad \text{where} \qquad \varphi(x) = \eta + \sum_{m=0}^{(N+1)/2} f_{2m+1}(x_{2m+1})$$

and

$$f_{2k+1} \in \mathsf{Iso}\left(\underline{\sigma \quad \overset{\sigma}{|} \quad . \quad \overset{\sigma}{|} \quad \sigma} \;\to\; \underline{\sigma \quad \overset{\sigma}{|} \quad \pi^{C_{2k+1}}(\cdot) \quad \overset{\sigma}{|} \quad \sigma} \right) = \{\big(f(1), f(\psi)\big)\} = \{(0,0),(0,\pi)\}.$$

More explicitly, we have

$$U|x\rangle = e^{i\eta} \left(\prod_{m=1}^{(N+1)/2} e^{if_{2m+1}(x_{2m+1})} \right) |\pi^{C_1}(x_1), x_2, \pi^{C_3}(x_3), x_4, \ldots, \pi^{C_N}(x_N)\rangle.$$

In particular, under the isomorphism (7.62), we get

$$WUW^{-1} = e^{i\eta} \bigotimes_{m=1}^{(N+1)/2} U_m \qquad \text{where} \qquad U_m|a\rangle = e^{if_{2m-1}(a)}|\pi^{C_{2m-1}}(a)\rangle \ .$$

From Section 7.6.2, we know that U_m is a single-qubit Pauli for each m up to a global phase. This concludes the proof of Theorem 7.6.2.

7.7 Abelian anyon models

Our goal in this section is to characterize topologically protected gates in general abelian anyon models. For simplicity, we will restrict our attention to closed 2-manifolds Σ (see Fig. 7.1). We have seen in Lemma 7.3.1 that in an arbitrary anyon model, protected gates permute the idempotents along closed loops. In this section we show that for the case of abelian anyon models, the protected gates can only permute the labels of string operators along closed loops (up to phases), which refines Lemma 7.3.1 for abelian models. To formalize this notion, we introduce the generalized Pauli and Clifford groups in Section 7.7.1. The main result of this Section, can then be stated as follows:

Theorem 7.7.1. *For an abelian anyon model, any locality-preserving unitary automorphism U acting on $\mathcal{H}_\Sigma$ has logical action $[U] \in \mathsf{Clifford}^\star_\Sigma$.*

For abelian anyon models, the set $\mathbb{A}$ of particles is an abelian group and the fusion rules (i.e., the Verlinde algebra (7.7)) are given by the group product, $N_{ab}^c = 1$ if and only if $c = ab$ and $N_{ab}^c = 0$ otherwise. In other words, any two particles a and b fuse to a unique particle $c = ab$, and the identity element $1 \in \mathbb{A}$ is the only particle satisfying $1a = a$ for all $a \in \mathbb{A}$. Another requirement is that the S matrix is composed entirely of phases (divided by the quantum dimension $\mathcal{D}$), and $S_{1a} = S_{a1} = 1/\mathcal{D}$ for all $a \in \mathbb{A}$. Furthermore, the involution $a \mapsto \overline{a}$ defining the antiparticle associated to $a \in \mathbb{A}$ is simple the inverse $\overline{a} = a^{-1}$ with respect to the group multiplication. Note that, by the fundamental theorem of finitely generated abelian groups, the group $\mathbb{A}$ is isomorphic to $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_r}$ for some prime powers N_j. The number $N = \mathsf{lcm}(N_1, \ldots, N_r)$ will play an important role in the following, determining e.g., the order of a protected gate.

It is well known that for abelian anyons a and b, and two inequivalent loops C and C' whose minimal intersection number is 1 in the manifold Σ the relation

$$[F_{\overline{b}}(C')][F_{\overline{a}}(C)][F_b(C')][F_a(C)] = \mathcal{D}S_{ab}[\mathsf{id}] \tag{7.64}$$

holds. As we will see, this provides an additional constraint on the logical action of a protected gate U. The following consistency condition must hold

Lemma 7.7.2. *Consider the action of a locality preserving unitary automorphism of the code on the string operators of a pair of conjugate loops C and C', such that*

$$\rho_U([F_b(C)]) = \sum_d \Lambda_{b,d}[F_d(C)], \qquad \rho_U([F_b(C')]) = \sum_d \Lambda'_{b,d}[F_d(C')]. \tag{7.65}$$

Then the matrices Λ and Λ' must satisfy the following consistency condition

$$\Lambda_{a,c}\ \Lambda'_{b,d}\,(S_{cd} - S_{ab}) = 0 \quad \forall a, b, c, d \in \mathbb{A}. \tag{7.66}$$

Proof. Since in an abelian anyon model every string operator $[F_a(C)]$ is unitary the relation (7.64) is equivalent to the commutation relation

$$[F_b(C')][F_a(C)] = \mathcal{D}S_{ab}[F_a(C)][F_b(C')].$$

Conjugating this by U and rearranging terms yields

$$0 = \sum_{c,d} \Lambda_{a,c}\ \Lambda'_{b,d}\,(\mathcal{D}S_{cd} - \mathcal{D}S_{ab})\,[F_c(C)][F_d(C')]. \tag{7.67}$$

The claim follows from linear independence of the logical operators $[F_c(C)][F_d(C')]$. □

Invoking our previous result of Lemma 7.3.1, the following lemma is implied:

Lemma 7.7.3. *The anyon labels of* string *operators along the loop are permuted by* U

$$\Lambda_{b,d} = e^{i\phi_b}\delta_{d,\tilde{\pi}(b)}, \tag{7.68}$$

for some phase ϕ_b*, and where* $\tilde{\pi}$ *is a permutation of anyon labels.*

Proof. Recall from (7.29) that

$$\Lambda_{b,d} = \sum_a \frac{S_{b,a}}{S_{1,a}} S_{1,\pi^C(a)}\overline{S_{d,\pi^C(a)}} = \sum_a S_{b,a}\overline{S_{d,\pi^C(a)}}, \tag{7.69}$$

where π^C is the permutation of the central idempotents associated with loop C, where the second equality holds for abelian anyons. An analogous equation holds for loop C'. Now sum over all $a \in \mathbb{A}$ in (7.66). To evaluate the sum, we require $\sum_a \Lambda_{a,c}$ and $\sum_a \Lambda_{a,c}S_{ab}$. Firstly,

$$\sum_a \Lambda_{a,c} = \sum_{a,g} S_{a,g}\overline{S_{c,\pi^C(g)}} = \mathcal{D}\sum_g \delta_{g,1}\overline{S_{c,\pi^C(g)}} = \mathcal{D}\overline{S_{c,\pi^C(1)}},$$

where we used unitarity of the S-matrix, $\delta_{1z} = \sum_x \overline{S_{x1}}S_{xz} = \sum_x S_{xz}/\mathcal{D}$. Secondly,

$$\sum_a \Lambda_{a,c}S_{ab} = \sum_{a,g} S_{a,g}\overline{S_{c,\pi^C(g)}}S_{ab} = \sum_{a,g} S_{a,g}\overline{S_{c,\pi^C(g)}S_{a\bar{b}}} = \sum_g \delta_{g,\bar{b}}\overline{S_{c,\pi^C(g)}} = \overline{S_{c,\pi^C(\bar{b})}}.$$

Therefore (7.66) implies

$$\left(\mathcal{D}S_{cd}\overline{S_{c,\pi^C(1)}} - \overline{S_{c,\pi^C(\bar{b})}}\right)\Lambda'_{b,d} = 0 \qquad \forall b, c, d \in \mathbb{A}. \tag{7.70}$$

For any $B \in \mathbb{A}$, there must exist at least one anyon $D \in \mathbb{A}$ such that $\Lambda'_{B,D} \neq 0$. Then

$$\mathcal{D}S_{cD}\overline{S_{c,\pi^C(1)}} - \overline{S_{c,\pi^C(\overline{B})}} = 0 \qquad \forall c \in \mathbb{A}. \tag{7.71}$$

For each $D' \neq D$, there must be some $C \in \mathbb{A}$ such that $S_{CD} \neq S_{CD'}$. Therefore substituting into (7.70) the values $b = B, c = C$ and $d = D'$, the term in brackets must be non-zero, implying $\Lambda'_{B,D'} = 0$ for all $D' \neq D$. Unitarity of U yields the claim for loop C'. □

7.7.1 The generalized Pauli and Clifford groups

Consider the case where $\mathbb{A} = \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_r}$ and set $N = \mathsf{lcm}(N_1, \ldots, N_r)$. We define the following group associated with the surface Σ.

Definition 7.7.4 (Pauli group)**.** *Consider a genus-g surface Σ and let $\mathcal{G} = \{C_j\}_{j=1}^{3g-1}$ be the loops associated with generators of the mapping class group as in Fig. 7.1. The* Pauli group Pauli_Σ associated with Σ *is*

$$\mathsf{Pauli}_\Sigma \coloneqq \left\langle \left\{ \lambda[F_a(C)] \;\middle|\; \lambda \in \langle e^{2\pi i/N} \rangle, a \in \mathbb{A}, C \in \mathcal{G} \right\} \right\rangle ,$$

i.e., the set of logical operators generated by taking products of string-operators associated with $\mathcal{G}$, where $\langle e^{2\pi i/N} \rangle$ is the subgroup of U(1) *consisting of N-th roots of unity.*

According to Eq. (7.64), we can always reorder and write each element $P \in \mathsf{Pauli}_\Sigma$ in the standard form

$$P = \lambda[F_{a_1}(C_1)] \cdots [F_{a_{3g-1}}(C_{3g-1})] \qquad \text{for some } \lambda \in \langle e^{2\pi i/N} \rangle,\ a_j \in \mathbb{A} .$$

This shows that the group Pauli_Σ is finite. Furthermore, since $a^N = 1$ for every $a \in \mathbb{A}$, we conclude that $P^N = \lambda[\mathsf{id}]$ is proportional to the identity up to a phase $\lambda \in \langle e^{2\pi i/N} \rangle$. That is, every element of the Pauli group Pauli_Σ has order dividing N.

Given this definition, we can proceed to give the definition of the Clifford group.

Definition 7.7.5 (Clifford group)**.** *The* Clifford group associated with Σ *is the group of logical unitaries*

$$\mathsf{Clifford}_\Sigma \coloneqq \{\lambda[U] \mid [U]\mathsf{Pauli}_\Sigma[U]^{-1} \subset \mathsf{Pauli}_\Sigma, \lambda \in \langle e^{2\pi i/N} \rangle\} .$$

In this definition, $[U]$ is any logical unitary on the code space.

We can define a 'homology-preserving subgroup' of $\mathsf{Clifford}_\Sigma$. To do so, we first introduce the following subgroup of Pauli_Σ associated with a loop on Σ.

Definition 7.7.6 (Restricted Pauli group)**.** *Let $C \in \mathcal{G}$ be a single closed loop. We set*

$$\mathsf{Pauli}_\Sigma(C) \coloneqq \left\langle \left\{ \lambda[F_a(C)] \;\middle|\; \lambda \in \langle e^{2\pi i/N} \rangle, a \in \mathbb{A} \right\} \right\rangle ,$$

i.e., the subgroup generated by string-operators associated with the loop C.

It is straightforward to check that for any $C \in \mathcal{G}$, the subgroup $\mathsf{Pauli}_{\Sigma_g}(C) \subset \mathsf{Pauli}_{\Sigma_g}$ is normal; furthermore, any $P \in \mathsf{Pauli}_{\Sigma_g}(C)$ has the simple form of a product $P = \lambda[F_{a_1}(C)] \cdots [F_{a_r}(C)]$.

Given this definition, we can define a subgroup of Clifford group elements as follows:

Definition 7.7.7 (Homology-preserving Clifford group)**.** *The* homology-preserving Clifford group associated with Σ *is the subgroup*

$$\mathsf{Clifford}^{\star}_{\Sigma} := \{\lambda[U] \mid [U]\mathsf{Pauli}_{\Sigma}(C)[U]^{-1} \subset \mathsf{Pauli}_{\Sigma}(C) \text{ for all } C \in \mathcal{G},\ \lambda \in \langle e^{2\pi i/N}\rangle\}\ .$$

Note that this is a proper subgroup, i.e., $\mathsf{Clifford}^{\star}_{\Sigma} \subsetneq \mathsf{Clifford}_{\Sigma}$, as can be seen from the following example.

Example 7.7.8. *Consider for example Kitaev's $D(\mathbb{Z}_2)$-code on a torus Σ_2 (cf. Example 7.2.1). In this case, there are two inequivalent homologically non-trivial cycles C_1 and C_2. In the language of stabilizer codes, the logical operators $(\bar{X}_1, \bar{Z}_1) = (F_e(C_1), F_m(C_2))$ and $(\bar{X}_2, \bar{Z}_2) = (F_e(C_2), F_m(C_1))$ are often referred to as the logical Pauli operators associated with the first and second logical qubit, respectively. Consider the logical Hadamard $\bar{H}_1$ on the first qubit, which acts as*

$$\bar{H}_1\bar{X}_1\bar{H}_1^{\dagger} = \bar{Z}_1 \qquad \text{and} \qquad \bar{H}_1\bar{Z}_1\bar{H}_1^{\dagger} = \bar{X}_1$$

but leaves $\bar{X}_2$ and $\bar{Z}_2$ invariant. Then $\bar{H}_1$ belongs to the Clifford group, $\bar{H}_1 \in \mathsf{Clifford}_{\Sigma}$. However, $\bar{H}_1 \notin \mathsf{Clifford}^{\star}_{\Sigma}$ because $\bar{X}_1$ and $\bar{Z}_1$ belong to different homology classes (specified by C_1 and C_2, respectively).

In the following, we make use of the existence of loops conjugate to a given loop C. Note that this is not necessarily given, but works in the special case where C is one of the $3g-1$ curves $\{C_j\}_{j=1}^{3g-1}$ associated with the generators of the mapping class group of the genus-g surface Σ_g (cf. Fig. 1). We are now ready to prove Theorem 7.7.1, i.e., that a protected gate U has logical action $[U] \in \mathsf{Clifford}^{\star}_{\Sigma}$.

Proof. By Lemma 7.7.3, we have that $\sum_c \Lambda_{a,c}\mathbf{F}_c = \lambda\mathbf{F}_b$ for some $\lambda \in \mathrm{U}(1)$ and $b \in \mathbb{A}$. It remains to show that λ is an N-th root of unity. We have

$$\lambda^N[\mathsf{id}] = \lambda^N[F_b(C)^N] = [\lambda F_b(C)]^N = [U][F_a(C)]^N[U^{\dagger}] = [\mathsf{id}]$$

because the string operators $F_a(C)$ have order dividing N, thus we must have $\lambda^N = 1$. Because a and C were arbitrary, this concludes the proof that $[U] \in \mathsf{Clifford}^{\star}_{\Sigma}$. □

7.8 Appendix: Density on a subspace and protected gates

Lemma 7.8.1. *Let $\mathcal{H}_0$ be an invariant subspace under the mapping class group representation, and suppose the action of MCG_Σ is dense in the projective unitary group $\mathsf{PU}(\mathcal{H}_0)$. Let $\mathcal{H}_1$ be the orthogonal complement of $\mathcal{H}_0$ in $\mathcal{H}_\Sigma$. Assume that the decomposition $\mathcal{H}_0 \oplus \mathcal{H}_1$ stems from the gluing axiom in the sense that $\mathcal{H}_j = \bigoplus_{\vec{a}\in\Lambda_j} \mathcal{H}_{\Sigma'(\vec{a})}$ for $j = 0, 1$, where Λ_0, Λ_1 are disjoint set of labelings of the boundary components of the surface Σ' obtained by cutting Σ along a family $\vec{C}$ of pairwise non-intersecting curves. If $\dim \mathcal{H}_1 < \dim \mathcal{H}_0$ (or a similar assumption), then any protected gate U leaves $\mathcal{H}_0$ invariant and acts as a global phase on it.*

Proof. Extending $\vec{C}$ to a DAP-decomposition $\mathcal{C}$, the unitary U expressed in the (suitably ordered) basis $\mathcal{B}_\mathcal{C}$ takes the form

$$\mathbf{U} = \begin{pmatrix} \mathbf{U}_{00} & \mathbf{U}_{01} \\ \mathbf{U}_{10} & \mathbf{U}_{11} \end{pmatrix} ,$$

where $\mathbf{U}_{jk}$ describes the operator $P_{\mathcal{H}_j} U P_{\mathcal{H}_k}$ obtained by projecting the domain and image of U to $\mathcal{H}_k$ and $\mathcal{H}_j$, respectively.

Consider the Schur decomposition $\mathbf{U}_{00} = \mathbf{W}_{00}\Gamma\mathbf{W}_{00}^\dagger$ of $\mathbf{U}_{00}$, i.e., $\mathbf{W}_{00}$ is a unitary matrix and Γ is upper triangular. There are different cases to consider:

(i) If Γ is diagonal with a single eigenvalue λ, then

$$\mathbf{U} = \begin{pmatrix} \lambda I & \mathbf{U}_{01} \\ \mathbf{U}_{10} & \mathbf{U}_{11} \end{pmatrix} .$$

Assume for the sake of contradiction that $\lambda = 0$. Writing $d_j = \dim \mathcal{H}_j$, the $d_1 \times d_0$-matrix $\mathbf{U}_{10}$, must have exactly d_0 non-zero values, each in a different row because $\mathbf{U} \in \Delta$. This is only possible if $d_1 > d_0$, contradicting our assumption.

We conclude that $\lambda \neq 0$. But then the condition $\mathbf{U} \in \Delta$ requires that $\lambda \in \mathrm{U}(1)$ and $\mathbf{U}_{01} = \mathbf{U}_{10} = 0$ (since we cannot have more than one non-zero entry in each column or row).

(ii) Γ has a non-zero off-diagonal element $\Gamma_{j,k}$, $j < k$. We will show that this is not consistent with the fact that U is a protected gate (i.e., leads to a contradiction). By reordering basis elements of $\mathcal{B}_\mathcal{C}$, we can assume without loss of generality that $\Gamma_{1,2} \neq 0$. By using, e.g., Solovay-Kitaev on $\mathcal{H}_0$, we find a product $\tilde{\mathbf{V}} = \mathbf{V}(\vartheta_1) \cdots \mathbf{V}(\vartheta_m)$ of images of mapping

class group elements approximating $\mathbf{V} = \mathbf{W}_{00}^\dagger \oplus \mathbf{W}_{11}$, where $\mathbf{W}_{11}$ is an arbitrary unitary on $\mathcal{H}_1$.

Consider the matrix $\mathbf{VUV}^\dagger$. We have $(\mathbf{VUV}^\dagger)_{j,k} = \Gamma_{j,k}$ for $j,k = 1,\ldots,\dim \mathcal{H}_0$. In particular, $(\mathbf{VUV}^\dagger)_{1,2} \neq 0$ and $(\mathbf{VUV}^\dagger)_{2,1} = 0$.

We claim that we must have $(\mathbf{VUV}^\dagger)_{1,1} = (\mathbf{VUV}^\dagger)_{2,2} = 0$. To show this, assume for the sake of contradiction that one of these diagonal entries is non-zero. Then $\mathbf{VUV}^\dagger \notin \Delta$ since it has two non-zero entries in the same row or column. But this implies $\tilde{\mathbf{V}}\mathbf{U}\tilde{\mathbf{V}}^\dagger \notin \Delta$ since $\tilde{\mathbf{V}}\mathbf{U}\tilde{\mathbf{V}}^\dagger \approx \mathbf{VUV}^\dagger$, a contradiction to the fact that $\mathbf{U} \in \Delta_{\vartheta_1 \cdots \vartheta_m}$.

Now let $X_{j,k} = (\mathbf{VUV}^\dagger)_{j,k}$ for $j,k \in \{1,2\}$ be the principal minor 2×2 submatrix. We have established that its only non-zero entry is $X_{1,2}$. Using the Hadamard matrix H, we then have $(HXH^\dagger)_{1,1} = X_{1,2}/2 \neq 0$ and $(HXH^\dagger)_{1,2} = -X_{1,2}/2 \neq 0$. Let $\mathbf{H} = H \oplus I_{(\dim \mathcal{H}_0 - 2)}$. By Solovay-Kitaev, we can find a product $\tilde{\mathbf{V}}' = \mathbf{V}(\vartheta_1') \cdots \mathbf{V}(\vartheta_\ell')$ of images of mapping class group elements approximating $\mathbf{V}' = \mathbf{H} \oplus \mathbf{W}_{11}'$, where $\mathbf{W}_{11}'$ is an arbitrary unitary on $\mathcal{H}_1$. Then we have

$$\begin{aligned}(\mathbf{V}'\mathbf{VUV}^\dagger(\mathbf{V}')^\dagger)_{1,1} &= X_{1,2}/2 \neq 0 \\ (\mathbf{V}'\mathbf{VUV}^\dagger(\mathbf{V}')^\dagger)_{1,2} &= -X_{1,2}/2 \neq 0\ ,\end{aligned}$$

which shows that $\mathbf{V}'\mathbf{VUV}^\dagger(\mathbf{V}')^\dagger \notin \Delta$. By continuity, this shows that $\tilde{\mathbf{V}}'\tilde{\mathbf{V}}\mathbf{U}\tilde{\mathbf{V}}^\dagger(\tilde{\mathbf{V}}')^\dagger \notin \Delta$, contradicting the fact that $\mathbf{U} \in \Delta_{\vartheta_1' \cdots \vartheta_\ell' \vartheta_1 \cdots \vartheta_m}$.

(iii) Γ is diagonal with distinct eigenvalues: in this case we can apply the same kind of argument as in the proof of Corollary 7.4.2.

□

Acknowledgements

RK and SS gratefully acknowledge support by NSERC, and MB, FP, and JP gratefully acknowledge support by NSF grants PHY-0803371 and PHY-1125565, NSA/ARO grant W911NF-09-1-0442, and AFOSR/DARPA grant FA8750-12-2-0308. RK is supported by the Technische Universität München – Institute for Advanced Study, funded by the German Excellence Initiative and the European Union Seventh Framework Programme under grant agreement no. 291763. OB gratefully acknowledges support by the ERC (TAQ). The Institute for Quantum Information and Matter (IQIM) is an NSF Physics Frontiers Center with support by the Gordon and Betty Moore Foundation. RK and SS thank the IQIM for their hospitality. We thank Jeongwan Haah, Olivier Landon-Cardinal and Beni Yoshida for helpful discussions.

Chapter 8

Conclusion

In summary, the main objective of this thesis was two-fold: first, to provide sufficient theoretical background to understand topological quantum computation; and second, to apply this theory to characterize certain fault-tolerant operations for topological quantum computation called protected gates. The former required investing in category theory for the purposes of axiomatically defining a unitary modular tensor category, which served as a mathematically formal and rigorous way to model the physical properties of anyons. Having developed the sufficient categorical language, a topological quantum field theory was defined which was then used to understand topological quantum computation. The entirety of this thesis focused on the particular setting of two dimensional space where all anyon dynamics were assumed to take place. To model this, a $(2+1)$- dimensional topological quantum field theory was utilized. More generally, $(n+1)$-dimensional topological quantum field theories may be considered, and be particularly relevant for physical purposes in the case of $n = 1$ and $n = 3$. Such theories could be used to model more general anyonic excitations of a physical system, where anyons not only manifest as point like entitties but may be "string-like" or "surface'-like". Another avenue of generalization beyond this setting is to consider more general surfaces with boundaries and corners. In this case, a richer set of anyon dynamics on these surfaces can result where certain anyon types may "condense" or become "confined" on various boundary components. Such theories would require deeper mathematical machinery, and although progress in this regard has been made in the field (see [9, 3, 31, 32]) it seems that considerable progress is still yet to be made.

The second objective of this thesis was to motivate and understand the results obtained in "Protected gates for topological quantum field theories". Here, protected gates were defined to be certain logical operations that act on relevant Hilbert spaces which are also locality-preserving operations. These assumptions were made to conform to certain fault-tolerant considerations in an attempt to understand permissible operations one may be able to perform in

a robust way. The main result here was that, for any given anyon model and choice of surface, the set of protected gates is finite (under a suitable notion of equivalent protected gates). Thus, computational universality cannot be achieved using protected gates alone as one may ideally desire. Therefore, alternative means which go beyond locality-preserving operations must be utilized in order to potentially achieve computational universality. Furthermore, it may be of interest to more explicitly characterize the form of protected gates for various models to understand precisely what group of operations are permissible. Again, this study was restricted to the two-dimensional setting, and asking analogous questions in the context of dimensions other than two remains an open problem.

It is important to note that these results characterizing protected gates were derived using just the underlying topological quantum field theory at play. That is, no reference was made to an explicit Hamiltonian which may realize a certain topological phase of matter of interest. By ignoring such low-level, microscopic details of the system a sufficiently general theory to characterize protected gates for arbitrary models was developed. At this expense, however, no precise method on how to actually implement a particular protected gate can be given. In order to so, it seems necessary to refer to specific Hamiltonian realizations of a topological phase of matter (as done in [28, 6, 34]). Hence, these results merely provide restrictions on protected gates that are permissible *mathematically*, and not necessarily implementable *physically*. Moreover, given a mathematical description of some Hamiltonian which realizes a topological phase of matter, it ultimately becomes a question of physics whether or not such a system can be found or manifested in nature.

APPENDIX

The Stabilizer Formalism

Consider the single qubit unitary matrices commonly referred to as the Pauli matrices defined as:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma^y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

It is worth noting that the operator Y is commonly defined instead as the operator $\tilde{\sigma}^y = i\sigma^y$, but the definition of σ^y introduced here will be convenient for our purposes. These operators satisfy the following properties:

$$\begin{aligned} \sigma^{x2} = \sigma^{z2} = -\sigma^{y2} = I \\ \sigma^x\sigma^y = -\sigma^y\sigma^x = \sigma^z, \\ \sigma^y\sigma^x = -\sigma^z\sigma^y = \sigma^x, \\ \sigma^z\sigma^x = -\sigma^x\sigma^z = \sigma^y. \end{aligned}$$

These properties give the set $P = \{\pm I, \pm\sigma^x, \pm\sigma^y, \pm\sigma^y\}$ a group structure under the usual matrix multiplication. Define $P_n := \{U_1 \otimes \cdots \otimes U_n \mid U_j \in P, 0 \leq j \leq n\}$, as the set of n-fold tensor products of Pauli operators from P. The set P_n also forms a group structure under the natural multiplication and is called the *Pauli group* with order $|P_n| = 2^{2n+1}$.

An important property about the Pauli operators is that they span the space of unitary operators acting on a single qubit. That is, any single qubit unitary U can be expressed as

$$U = c_I I + c_x\sigma^x + c_y\sigma^y + c_z\sigma^z,$$

where the vector (c_I, c_x, c_y, c_z) consists of complex numbers and is of unit norm. Similarly, any unitary operator acting on a n-qubit Hilbert space can be expressed in terms of elements of the Pauli group P_n. Moreover, the Pauli Group P_n also satisfies the following properties:

1. Every $M \in P_n$ in unitary: $M^\dagger = M^{-1}$.

2. Every $M \in P_n$ satisfies $M^2 = \pm I^{\otimes n}$.

3. If $M^2 = I^{\otimes n}$, then $M = M^\dagger$; if $M^2 = -I$, then $M = -M^\dagger$.

4. For any $M, N \in P_n$, either $MN = NM$ (they commute) or $MN = -NM$ (they anti-commute).

Consider some abelian subgroup $S \subset P_n$, consisting of elements that all commute with one another. Then all elements of S can be simultaneously diagonalized. The subspace $\mathcal{H}_S \subset \mathcal{H}^{2^n}$ defined as

$$\mathcal{H}_S := \{|\psi\rangle \in \mathcal{H}^{2^n} \mid M|\psi\rangle = |\psi\rangle \text{ for all } M \in S\}$$

consists of the simultaneous eigenspace with eigenvalue $+1$ of elements of S. The space $\mathcal{H}_S$ is called the *stabilizer code* associated with S, and S is called the *stabilizer* of the code.

A *generating set* of S is a collection of elements of S such that each element of S can be expressed as some product of elements from the generating set. In addition, it is required that the elements of the generating set be *independent*, meaning that no element of the generating set can be expressed as a product of the other elements of the generating set. It can be shown (as in [22]) that if S has $n-k$ generators, then the codes space $\mathcal{H}_S$ has dimension 2^k implying that it can effectively encode k qubits. In what follows, the elements of a generating set of a stabilizer S will be indexed as $\{M_1, \ldots, M_{n-k}\}$.

The utility of the stabilizer formalism for quantum error correction comes from the fact that the elements of S serve as operators for detecting possible errors that may occur to an encoded state of $|\psi\rangle \in \mathcal{H}_S$. In general, an error can be represented in terms elements $E_a \in P_n$. Then since every E_a either commutes or anti-commutes with some generator $M_j \in S$, the following two cases may occur.

If E_a anti-commutes with some M_j, then for $|\psi\rangle \in \mathcal{H}_S$,

$$M_j E_a |\psi\rangle = -E_a M_j |\psi\rangle = -E_a |\psi\rangle,$$

which implies that the error can be detected if the the erred state $E_a|\psi\rangle$ is acted on by M_j.

If E_a commutes with some M_j, then for $|\psi\rangle \in \mathcal{H}_S$,

$$M_j E_a |\psi\rangle = E_a M_j |\psi\rangle = E_a |\psi\rangle,$$

and the error may go undetected when the erred state $E_a|\psi\rangle$ is acted on by M_j.

A more thorough error syndrome can be provided by measuring each of the $n-k$ stabilizer generators. That is for a particular error E_a, consider the set of values $\{s_{a,j}\}$, where each $s_{a,j} \in \{0,1\}$ satisfies

$$M_j E_a = (-1)^{s_{a,j}} E_a M_j.$$

If it is the case that for every $a \neq b$, with $s_{a,j} \neq s_{b,j}$ for all j, then the code is considered to be *non degenerate* and there will be no ambiguity in what error occurred allowing for the error to be corrected by measuring the $n-k$ generators of S.

Another condition which must be satisfied by the stabilizer S in order to ensure complete error recovery due to arbitrary errors is that, for each possible error E_a, E_b and any $|\psi\rangle \in \mathcal{H}_S$,

$$\langle\psi|E_a^\dagger E_b|\psi\rangle = C_{ab},$$

such that the constants C_{ab} are independent of $|\psi\rangle$. This condition can be equivalently shown to hold if one of the following holds for each possible pair of errors E_a and E_b:

(1) $E_a^\dagger E_b \in S$,
(2) There exists an $M \in S$ that anti-commutes with $E_a^\dagger E_b$.

In this way, error recovery may fail if both conditions are violated. That is, if there exists some $E_a^\dagger E_b$ that commutes with every element of S, but yet $E_a^\dagger E_b \notin S$. In this circumstance, the operator $E_a^\dagger E_b$ that preserves the code space $\mathcal{H}_S$ but still modifies it in a non trivial way, implying that encoded information may still be transformed. In addition, both E_a and E_b will have the same syndrome leaving an inherent ambiguity on how either error should be corrected, and any mistake in diagnosis can apply a nontrivial transformation to the encoded space.

References

[1] M. Atiyah. Topological quantum field theories. *Inst. Hautes Études Sci. Publ. Math.*, 68:175–186, 1989.

[2] B. Bakalov and A. Kirillov. *Lectures on tensor categories and modular functors*. University Lecture Series. American Mathematical Society, 2001.

[3] S. Beigi, P. W. Shor, and D. Whalen. The quantum double model with boundary: Condensations and symmetries. *Communications in Mathematical Physics*, 306(3):663–694, 2011.

[4] H. Bombin. Topological order with a twist: Ising anyons from an abelian model. *Phys. Rev. Lett.*, 105:030403, 2010.

[5] H. Bombin and M. A. Martin-Delgado. Topological quantum distillation. *Phys. Rev. Lett.*, 97, 2006.

[6] H. Bombin and M. A. Martin-Delgado. Family of non-abelian Kitaev models on a lattice: Topological condensation and confinement. *Phys. Rev. B*, 78:115421, Sep 2008.

[7] H. Bombin and M.A. Martin-Delgado. Topological computation without braiding. *Phys.Rev.Lett.*, 98:160502, 2007.

[8] S. Bravyi, M. Hastings, and F. Verstraete. Lieb-Robinson Bounds and the Generation of Correlations and Topological Quantum Order. *Physical Review Letters*, 97(5):050401, July 2006.

[9] S. Bravyi and A. Y. Kitaev. Quantum codes on a lattice with boundary. 1998. arXiv:quant-ph/9811052.

[10] S. Bravyi and A. Y. Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A*, 71:022316, Feb 2005.

[11] S. Bravyi and R. König. Classification of topologically protected gates for local stabilizer codes. *Phys. Rev. Lett.*, 110:170503, Apr 2013.

[12] Xie Chen, Zheng-Cheng Gu, and Xiao-Gang Wen. Local unitary transformation, long-range quantum entanglement, wave function renormalization, and topological order. *Physical Review B*, 82(15):155138, October 2010.

[13] B. Coecke et. al. *New Structures for Physics*. Lecture Notes for physics. Springer, 2011.

[14] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill. Topological quantum memory. *J. Math. Phys.*, 43(9):4452, 2002.

[15] B. Eastin and E. Knill. Restrictions on transversal encoded quantum gate sets. *Phys. Rev. Lett.*, 102:110502, Mar 2009.

[16] D. V. Else, I. Schwarz, S. D. Bartlett, and A. C. Doherty. Symmetry-protected phases for measurement-based quantum computation. *Phys. Rev. Lett.*, 108:240505, Jun 2012.

[17] B. Farb and D. Margalit. *A Primer on Mapping Class Groups*. Princeton University Press, 2011.

[18] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland. Surface codes: Towards practical large-scale quantum computation. *Phys. Rev. A*, 86:032324, Sep 2012.

[19] A. G. Fowler, A. M. Stephens, and P. Groszkowski. High threshold universal quantum computation on the surface code. *Phys. Rev. A*, 80:052312, 2009.

[20] M. Freedman, C. Nayak, K. Walker, and Z. Wang. *On Picture (2+1)-TQFTs*, chapter 2, pages 19–106. August 2008.

[21] M. H. Freedman, A. Y. Kitaev, and Z. Wang. Simulation of topological field theories by quantum computers. *Commun. Math. Phys.*, 227:587–603, 2002.

[22] D. Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997.

[23] J. Haah. Local stabilizer codes in three dimensions without string logical operators. *Phys. Rev. A*, 83:042330, 2011.

[24] J. Haah. An invariant of topologically ordered states under local unitary transformations, July 2014. arXiv:1407.2926.

[25] A. Hatcher. *Algebraic Topology*. Cambridge University Press, 2001.

[26] Walker. K. On Witten's 3-manifold invariants, 1991. Lecture notes, http://canyon23.net/math/1991TQFTNotes.pdf.

[27] A. Kitaev and J. Preskill. Topological entanglement entropy. *Phys. Rev. Lett.*, 96:110404, Mar 2006.

[28] A. Y. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2, 2003.

[29] A. Y. Kitaev. Anyons in an exactly solved model and beyond. *Ann. Phys.*, 321(1):2, 2006.

[30] A. Y. Kitaev and L. Kong. Models for gapped boundaries and domain walls. *Communications in Mathematical Physics*, 313(2):351–373, 2012.

[31] A. Y. Kitaev and L. Kong. Models for Gapped Boundaries and Domain Walls. *Communications in Mathematical Physics*, 313(2):351–373, June 2012.

[32] L. Kong and X.-G. Wen. Braided fusion categories, gravitational anomalies, and the mathematical framework for topological orders in any dimensions, May 2014. arXiv:1405.5858.

[33] S. M. Lane. *Categories for the Working Mathematician*. Graduate Texts in Mathematics. Springer New York, 1998.

[34] M. A. Levin and X.-G. Wen. String-net condensation: A physical mechanism for topological phases. *Phys. Rev. B*, 71:045110, Jan 2005.

[35] M. A. Levin and X.-G. Wen. Detecting topological order in a ground state wave function. *Phys. Rev. Lett.*, 96:110405, Mar 2006.

[36] Elliott H. Lieb and Derek W. Robinson. The finite group velocity of quantum spin systems. *Communications in Mathematical Physics*, 28(3):251–257, 1972.

[37] K. Michnicki. 3-d quantum stabilizer codes with a power law energy barrier. 2012. arXiv:1208.3496.

[38] G. Moore and N. Seiberg. Polynomial equations for rational conformal field theories. *Physics Letters B*, 212(4):451–460, October 1998.

[39] F. Pastawski and B. Yoshida. Fault-tolerant logical gates in quantum error-correcting codes, August 2014. arXiv:1408.1720.

[40] J. Preskill. Lecture notes on quantum computation, 2004. available at http://www.theory.caltech.edu/people/preskill/ph229/ lecture.

[41] G. Segal. *The definition of conformal field theory*, volume 308. London Math. Soc. Lecture Note Ser., Cambridge University Press, 2004. preprint.

[42] V. G. Turaev. *Quantum invariants of knots and 3-manifolds*. Studies in Mathematics. De Gruyter, 2010.

[43] E. Verlinde. Fusion rules and modular transformations in 2d conformal field theory. *Nucl. Phys. B*, 300:360–376, 1988.

[44] E. Witten. Quantum field theory and the Jones polynomial. *Comm. Math. Phys.*, 121(3):351–399, 1989.